Anexa nr.1
la Ordinul ministrului finanţelor

nr. 115 din 15.09.2021

DOCUMENTAŢIA STANDARD
pentru realizarea achiziţiilor publice de bunuri şi servicii

INSTRUCŢIUNI PENTRU AUTORITĂŢI CONTRACTANTE ŞI OFERTANŢI

Secţiunea 1

Dispoziţii generale

1. Prezenta Documentaţie reprezintă o instrucţiune pentru autorităţile contractante şi ofertanţi, utilizată la iniţierea şi desfăşurarea procedurilor de achiziţii publice de bunuri şi servicii. La procedurile de achiziţii de bunuri şi servicii iniţiate şi desfăşurate prin cererea ofertelor de preţuri şi achiziţiile de valoare mică, autorităţile contractante pot simplifica formularele în dependenţă de complexitatea achiziţiei.

2. Prezenta Documentaţie conţine anexe destinate iniţierii, publicării, atribuirii şi modificării procedurilor de achiziţii publice, precum şi destinate să faciliteze elaborarea şi prezentarea ofertei, şi a documentelor care să permită grupului de lucru examinarea şi evaluarea tuturor ofertelor depuse, după cum urmează:

1) Anunţ de intenţie (anexa nr.1);
2) Anunţ de participare, inclusiv pentru procedurile de preselecţie/procedurile negociate (anexa nr. 2);
3) Invitaţie de participare la etapele de preselecţie/la procedurile negociate (anexa nr. 3);
4) Proces-verbal cu privire la rezultatele preselecţiei candidaţilor (anexa nr. 4);
5) Anunţ de atribuire (anexa nr. 5);
6) Anunţ privind modificarea contractului de achiziţii publice/acordului-cadru (anexa nr. 6);
7) Cerere de participare (anexa nr. 7);
8) Declaraţie privind valabilitatea ofertei (anexa nr. 8);
9) Scrisoare de garanţie bancară (anexa nr. 9);
10) Garanţia de bună execuţie (anexa nr. 10.);
11) Informaţii privind asocierea (anexa nr. 11);
12) Declaraţie privind lista principalelor livrări/prestări efectuate în ultimii 3 ani de activitate (anexa nr. 12);
13) Declaraţie privind dotările specifice, utilajul şi echipamentul necesar pentru îndeplinirea corespunzătoare a contractului (anexa nr. 13);
14) Declaraţie privind personalul de specialitate propus pentru implementarea contractului (anexa nr. 14);
15) Lista subcontractanţilor şi partea/părţile din contract care sunt îndeplinite de aceştia (anexa nr. 15);
16) Angajament terţ susţinător financiar (anexa nr. 16);
17) Declaraţie terţ susţinător financiar (anexa nr. 17);
18) Angajament privind susţinerea tehnică şi profesională a ofertantului/grupului de operatori economici (anexa nr. 18);
19) Declaraţie terţ susţinător tehnic (anexa nr. 19);
20) Declaraţie terţ susţinător profesional (anexa nr. 20);
21) Caiet de sarcini (anexa nr. 21);
22) Specificaţii tehnice (anexa nr. 22);

23) Specificaţii de preț (anexa nr. 23);
24) Contract – model (anexa nr. 24);
25) Acord adițional (anexa nr. 25);
26) Acord-cadru (anexa nr. 26).

3. Detaliile privind cantitățile de bunuri și servicii, specificațiile tehnice, standardele și resursele sunt prezentate în caietul de sarcini (anexa nr. 21).

4. Autoritatea contractantă urmează să se asigure că la momentul inițierii procedurii de achiziție publică, mijloacele financiare sunt alocate sau există o garanție a alocării lor și destinate exclusiv achiziției în cauză.

5. Atribuirea contractului de achiziție publică de bunuri și servicii se realizează în conformitate cu prevederile Legii nr. 131/2015 privind achizițiile publice.

6. În cazul în care autoritatea contractantă inițiază un acord-cadru, ca modalitate specială de atribuire a contractelor de achiziții publice de bunuri și de servicii, procedura se desfășoară conform Regulamentului cu privire la acordul-cadru ca modalitate specială de atribuire a contractelor de achiziții publice, aprobat prin Hotărârea Guvernului nr. 694/2020.

7. În cazul în care autoritatea contractantă inițiază procedura de negociere, procedura se desfășoară conform Regulamentului cu privire la achizițiile publice folosind procedura de negociere, aprobat prin Hotărârea Guvernului nr. 599/2020.

8. În cazul în care autoritatea contractantă inițiază proceduri cu preselecție se utilizează anexele ce țin de procedurile date: anexa nr. 1, anexa nr. 3, anexa nr. 4, anexa nr. 5, anexa nr. 6 și anexa nr. 25.

9. Ofertantul suportă toate costurile asociate elaborării și prezentării ofertei sale, precum și documentelor care o însoțesc.

10. Cererea de participare (anexa nr. 7), Oferta, Documentul Unic de Achiziții European (în continuare - DUAE), documentația de atribuire, caietul de sarcini şi toată corespondenţa dintre ofertant şi autoritatea contractantă se întocmește în limba română, sau după caz, toate documentele enumerate pot fi întocmite în una din limbile de circulaţie internaţională. Documentele justificative şi literatura de specialitate tipărită, care fac parte din ofertă, pot fi întocmite și în altă limbă, specificată în documentaţia de atribuire, cu condiţia ca acestea să fie însoţite de o traducere exactă a fragmentelor relevante în limba română.

11. În cazul în care autoritatea contractantă a depistat că ofertantul a fost implicat în practicile descrise la pct. 22 și pct. 23 în cadrul procedurii de atribuire pentru contractul de achiziție publică aceasta:

1) exclude ofertantul din procedura respectivă de achiziție și înaintează solicitarea către Agenția Achiziții Publice privind includerea lui în Lista de interdicție, conform prevederilor Hotărârii Guvernului nr. 1420/2016 pentru aprobarea Regulamentul privind evidenţa Listei operatorilor economici calificaţi; sau

2) întreprinde orice alte măsuri prevăzute în art. 42 al Legii nr. 131/2015 privind achiziţiile publice.

12. Sunt interzise următoarele acţiuni în cadrul procedurii de achiziție:

1) promisiunea sau oferirea unei persoane cu funcție de răspundere, personal sau prin mijlocitor, de bunuri sau servicii, sau privilegii, sau avantaje sub orice formă, pentru a influența acțiunile unei alte părți;

2) orice acțiune sau omisiune, inclusiv interpretare eronată, care, conștient sau din neglijență, induce în eroare sau tinde să inducă în eroare o parte pentru obţinerea unui beneficiu financiar sau de altă natură ori pentru a evita o obligaţie;

3) înţelegerea interzisă de lege, între două sau mai multe părţi, realizată în scopul coordonării comportamentului lor la procedurile de achiziţii publice;

4) prejudicierea, direct sau indirect, a oricărei părţi sau a proprietăţii acestei părţi, pentru a influenţa în mod necorespunzător acţiunile acesteia;

5) distrugerea intenţionată, falsificarea, contrafacerea sau ascunderea materialelor de evidenţă ale investigării, sau prezentarea unor informaţii false organelor de urmărire penală, pentru a împiedica esenţial urmărirea penală condusă de către organele de resort în vederea identificării unor practici frauduloase, precum şi ameninţarea, hărţuirea sau intimidarea oricărei părţi pentru a o împiedica să divulge informaţia cu privire la chestiuni relevante urmăririi penale.

Secţiunea a 2-a

Calificarea candidaților/ofertanților

13. Orice operator economic, rezident sau nerezident, persoana fizică sau juridică de drept public sau privat ori asociație de astfel de persoane are dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii.

14. Persoana fizică sau juridică care a participat la întocmirea documentației de atribuire are dreptul, în calitate de operator economic, de a fi ofertant, ofertant asociat sau subcontractant, dar numai în cazul în care implicarea sa în elaborarea documentației de atribuire nu este de natură să distorsioneze concurența. Persoana fizică sau juridică care participă direct în procesul de verificare şi evaluare a ofertelor nu are dreptul de a fi ofertant, ofertant asociat sau subcontractant, sub sancțiunea excluderii din procedura de atribuire.

15. Mai multe persoane juridice au dreptul să se asocieze în scopul depunerii unei oferte comune, de asemenea, fiecare asociat urmează să prezinte DUAE-ul separat. Asocierea trebuie prezentată în formă scrisă la solicitarea autorității contractante, odată ce a fost declarat în DUAE.

16. Filialele agenților economici, cu personalitate juridică şi înregistrate în conformitate cu prevederile pct. 29, au dreptul de a participa la procedura de atribuire a contractului de achiziție publică de bunuri și servicii în nume propriu și, în acest scop, trebuie să prezinte documente care dovedesc eligibilitatea, înregistrarea, capacitatea tehnică și capacitatea economico-financiară.

17. Sucursalele au dreptul de a participa la procedura de atribuire a contractului de achiziţie publică de bunuri și servicii şi de a încheia contractul respectiv numai în numele persoanei juridice, prin împuternicire. În acest caz documentele prezentate, care dovedesc eligibilitatea, înregistrarea, capacitatea tehnică şi capacitatea economico-financiară, trebuie să fie cele ale persoanei juridice.

18. Pentru confirmarea datelor de calificare în cadrul procedurii de achiziții publice, operatorul economic completează și prezintă DUAE, conform formularului standard al Documentului unic de achiziții European, aprobat prin Ordinul ministrului finanțelor nr. 72/2020, în conformitate cu cerințele stabilite de autoritatea contractantă. Prezentarea oricărui alt formular DUAE, este temei de descalificare de la procedura de achiziție publică.

19. În dependență de specificul achiziției și procedura aleasă, autoritatea contractantă are obligația de a stabili pentru fiecare procedură în parte criteriile de calificare cât și documentele suport necesare pentru a fi prezentate de către operatorii economici.

20. Autoritatea contractantă aplică criterii și cerințe de calificare numai referitoare la:

1) eligibilitatea ofertantului sau candidatului;

2) capacitatea de exercitare a activității profesionale;

3) capacitatea economică şi financiară;

4) capacitatea tehnică;

5) standarde de asigurare a calității;

6) standarde de protecție a mediului.

21. Pentru constatarea datelor de calificare în cadrul procedurilor de achiziții publice, operatorul economic prezintă la momentul evaluării documentele solicitate de către autoritatea contractantă în cadrul procedurilor de achiziții publice. Documentele se prezintă în format electronic, utilizînd Sistemul informaţional automatizat "Registrul de stat al achiziţiilor publice" (în continuare - SIA RSAP), cu excepția cazurilor prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

22. Se exclude de la procedura de atribuire a contractului de achiziții publice orice ofertant sau candidat despre care se confirmă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane.

23. Se exclude de la procedura pentru atribuire a contractului de achiziţie publică, şi respectiv, nu este eligibil, orice ofertant care se află în oricare dintre situaţiile prevăzute la art. 19 alin. (2) şi alin. (3) și art. 16 alin. (6) al Legii nr. 131/2015 privind achizițiile publice.

24. Orice ofertant/candidat care se află în una din situațiile menționate la pct. 22 și pct. 23 furnizează dovezi care să arate că măsurile luate de el sunt suficiente pentru a demonstra fiabilitatea și credibilitatea sa, în pofida existenței unui motiv de excludere. Dacă autoritatea contractantă consideră astfel de dovezi suficiente, ofertantul/candidatul în cauză nu este exclus de la procedura de achiziție publică, cu excepția cazului în care operatorul economic a fost exclus prin hotărâre definitivă a unei instanțe de judecată de la participarea la procedurile de achiziții publice.

25. Autoritatea contractantă extrage informaţia necesară pentru constatarea existenţei sau inexistenţei circumstanţelor menţionate la pct. 22 și pct. 23 în bazele de date disponibile ale autorităţilor publice sau ale părţilor terţe. Dacă acest lucru nu este posibil, autoritatea contractantă are obligaţia de a accepta ca fiind suficient şi relevant pentru demonstrarea faptului că ofertantul/candidatul nu se încadrează în una dintre situaţiile prevăzute la pct. 22 și pct. 23 orice document considerat edificator, din acest punct de vedere, în ţara de origine sau în ţara în care ofertantul este stabilit, cum ar fi certificate, caziere judiciare sau alte documente echivalente emise de autorităţi competente din ţara respectivă.

26. În ceea ce privesc referințele de la pct. 23, în conformitate cu legislaţia internă a statului în care sunt stabiliţi ofertanţii, aceste solicitări se referă la persoanele fizice şi persoanele juridice, inclusiv, după caz, la directori de companii sau la orice persoană cu putere de reprezentare, de decizie ori de control în ceea ce priveşte ofertantul/candidatul.

27. În cazul în care în ţara de origine sau în ţara în care este stabilit ofertantul/candidatul nu se emit documente de natura celor prevăzute la pct. 22 sau respectivele documente nu vizează toate situaţiile referitoare de la pct. 23, autoritatea contractantă are obligaţia de a accepta o declaraţie pe propria răspundere sau, dacă în ţara respectivă nu există prevederi legale referitoare la declaraţia pe propria răspundere, o declaraţie autentică dată în faţa unui notar, a unei autorităţi administrative sau judiciare sau a unei asociaţii profesionale care are competenţe în acest sens.

28. Autoritatea contractantă evaluează măsurile întreprinse de către operatorii economici ținînd seama de gravitatea și circumstanțele particulare ale infracțiunii sau ale abaterii. În cazul în care consideră că măsurile întreprinse sunt insuficiente, autoritatea contractantă informează ofertantul/candidatul despre motivele excluderii.

29. Autoritatea contractantă solicită oricărui ofertant să prezinte dovada din care să rezulte o formă de înregistrare în cazul persoanei juridice, capacitatea legală de a executa documentația de atribuire și de a livra/presta bunurile/serviciile, în conformitate cu prevederile legale din țara în care este stabilit.

30. Ofertantul urmează să dispună de un nivel minim de capacitate economică și/sau financiară și să prezinte informații/documente privind capacitatea economică și/sau financiară pentru a se califica conform cerinţelor de îndeplinire a contractului, cum ar fi:

1) realizarea unei cifre medii anuale de afaceri în ultimii 3 ani egală sau mai mare decât suma stabilită în pct. 16 din anexa nr. 2, care nu trebuie să depășească de două ori valoarea estimată a contractului, cu excepția cazurilor bine justificate, precum cele legate de riscurile speciale aferente naturii bunurilor sau serviciilor;

2) declaraţii bancare corespunzătoare sau, după caz, dovezi privind asigurarea riscului profesional;

3) situația financiară pentru perioada de gestiune anterioară, avizat şi înregistrat de organele competente, și orice alte documente legale edificatoare prin care ofertantul își poate dovedi capacitatea economico-financiară.

31. Atunci când un contract este împărțit pe loturi, indicele cifrei de afaceri se aplică pentru fiecare lot individual. Cu toate acestea, autoritatea contractantă urmează să stabilească cifra de afaceri anuală minimă impusă operatorilor economici cu referire la grupuri de loturi, dacă ofertantului câștigător îi sunt atribuite mai multe loturi care trebuie executate în același timp.

32. La solicitarea autorității contactante, ofertantul urmează să prezinte documentele care demonstrează capacitatea tehnică și/sau profesională pentru executarea viitorului contract numai în măsura în care aceste informaţii sînt relevante pentru îndeplinirea contractului și nu sînt disponibile în bazele de date ale autorităților publice sau ale părților terțe:

1) o listă a principalelor livrări de bunuri/servicii similare efectuate în ultimii 3 ani, conform Anexei nr. 12. Respectivele certificări indică beneficiarii, indiferent dacă aceştia sunt autorităţi contractante sau clienţi privaţi, valorile și perioadele de livrare/prestare.

2) declaraţia referitoare la echipamentele tehnice şi la măsurile aplicate în vederea asigurării calităţii, precum şi, dacă este cazul, la resursele de studiu şi cercetare;

3) informaţii referitoare la personalul/organismul tehnic de specialitate de care dispune sau al cărui angajament de participare a fost obţinut de către ofertant/candidat, în special pentru asigurarea controlului calităţii;

4) certificate sau alte documente emise de organisme abilitate în acest sens, care să ateste conformitatea bunurilor, identificată clar prin referire la specificaţii sau standarde relevante;

5) mostre (în măsura în care necesitatea prezentării este justificată), descrieri şi/sau fotografii a căror autenticitate trebuie să poată fi demonstrată în cazul în care autoritatea contractantă solicită acest lucru;

6) informaţii referitoare la studiile, pregătirea profesională şi calificarea personalului de conducere, precum şi ale persoanelor responsabile pentru îndeplinirea contractului conform Anexei nr. 14;

7) declaraţia referitoare la efectivele medii anuale ale personalului angajat şi ale cadrelor de conducere în ultimii 3 ani;

8) dacă este cazul, informaţii privind măsurile de protecţie a mediului pe care operatorul economic le poate aplica în timpul îndeplinirii contractului de bunuri/servicii, în corespundere cu pct. 36;

9) informaţii referitoare la utilajele, instalaţiile, echipamentele tehnice de care dispune operatorul economic pentru îndeplinirea corespunzătoare al contractului de bunuri/servicii conform Anexei nr. 13;

10) informaţii privind partea din contract pe care operatorul economic are, eventual, intenţia să o subcontracteze, conform Anexei nr. 15. De asemenea, urmează a fi atașat/atașate la Anexa nr. 15, copia/copiile contractului/contractelor încheiat/încheiate cu subatreprenorii.

33. Ofertantul urmează să dispună de un nivel minim de experienţă pentru a se califica conform cerinţelor de îndeplinire a contractului prin demonstrarea experienţei specifice fiind minimum de 3 ani în livrarea/prestarea bunurilor/serviciilor similare, confirmată prin anexarea copiilor contractelor, facturilor și actelor de primire-predare.

34. Operatorul economic urmează să prezinte, în cazul solicitării din partea autorității contactante, documente și certificate emise de organisme independente, prin care se atestă faptul că respectă anumite standarde de asigurare a calităţii (ISO 9001), acestea trebuie să se raporteze la sistemele de asigurare a calităţii, bazate pe seriile de standarde europene relevante, certificate de organisme conforme cu seriile de standarde europene privind certificarea, sau la standarde internaționale pertinente, emise de organisme acreditate.

35. În conformitate cu principiul recunoaşterii reciproce, autoritatea contractantă are obligaţia de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deţine un certificat de calitate astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligaţia de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al calităţii.

36. Operatorul economic prezintă documente, certificate, emise de organisme independente, prin care se atestă faptul că respectă anumite standarde de protecţie a mediului, aceasta trebuie să se raporteze:

1) la Sistemul Comunitar de Management de Mediu şi Audit (EMAS), sau;

2) la standarde de gestiune ecologică bazate pe seriile de standarde europene sau internaţionale în domeniu, certificate de organisme conforme cu legislaţia comunitară ori cu standardele europene sau internaţionale privind certificarea.

37. În conformitate cu principiul recunoaşterii reciproce, autoritatea contractantă are obligaţia de a accepta certificatele echivalente emise de organismele stabilite în statele membre ale Uniunii Europene. În cazul în care operatorul economic nu deţine un certificat de mediu astfel cum este solicitat de autoritatea contractantă, aceasta din urmă are obligaţia de a accepta orice alte certificări prezentate de operatorul economic respectiv, în măsura în care acestea confirmă asigurarea unui nivel corespunzător al protecţiei mediului.

38. Autoritățile contractante pot utiliza o serie de criterii generale privind durabilitatea pentru livrarea bunurilor și prestarea serviciilor:

1) Etichetele cu criterii multiple: eticheta europeană (floarea), eticheta scandinavă (lebăda nordică) şi etichetele naţionale (precum îngerul albastru german);

2) Achiziționarea alimentelor organice și cu un aport nutrițional echilibrat pentru școli/gradinițe;

3) Posibilitățile de reciclare/reutilizare a produsului după scoaterea din uz a acestuia;

4) Folosirea de recipiente sau ambalaje reutilizabile pentru transportarea produselor;

5) Furnizarea de hârtie ecologică și reciclată (fără clor și fibră);

6) Restricțiile de utilizare a anumitor substanțe periculoase în compoziția produsului;

7) Sisteme eficiente de tratare a deșeurilor în aer și în apă în fabricarea produselor;

8) Utilizarea sistemelor și schemelor de management de mediu (de exemplu EMAS, ISO 14001);

9) Reducere ale emisiilor de CO2 și a altor gaze prin scăderea frecvenței livrării și opțiuni noi de ambalare;

10) Reciclarea sau reutilizarea ambalajelor care însoțesc produsele;

11) Introducerea specificațiilor pentru vehicole cu cel mai mic nivel posibil de emisii de CO2 pentru categoria și dimensiunile respective, standarde EURO privind emisiile de particule și de Nox;

12) Încurajarea utilizării vehiculelor cu combustibili alternativi și a variantelor electrice sau hibride;

13) Achiziționarea vehiculelor cu sisteme de aer condiționat cu agenți de răcire cu nivel scăzut de GWP (potențial de încălzire globală);

14) Achiziționarea echipamentelor/utilajelor din clasa de eficiență energetică cea mai ridicată;

15) Achiziționarea corpurilor de iluminat cu un conținut scăzut de mercur;

16) Reducerea poluării aerului în orașe (prin achiziția de autobuze și automobile cu nivel scăzut al emisiilor de pulberi în suspensie și oxizi de azot);

17) Achiziționarea de alimente organice și nemijlocit susținerea agriculturii durabile;

18) Economisirea resurselor naturale (prin achiziția de produse obținute din materiale reciclate, reducerea consumului de hârtie prin achiziționarea, promovarea utilizării dispozitivelor multifuncționale);

19) Achziționarea de materiale de construcție și aprovizionare durabilă;

20) Încurajarea utilizării de materiale reciclate în construcție;

21) Aprovizionarea cu produse certificate ca fiind durabile (Patru etichete ecologice ale UE pentru componente);

22) Achiziționarea și utilizarea de materiale de construcție cu impact redus asupra mediului;

23) Serviciile pentru depozitarea deșeurilor reciclabile și sistemul de gestionare a deșeurilor;

24) Gestionarea deșeurilor din demolări;

25) Achiziționarea serviciilor de curăţenie ecologică folosind produse care întrunesc cerințele etichetelor ecologice;

26) Achiziționarea serviciilor de catering cu alimente ecologice (bio), indicînd procentul de alimente ecologice;

27) Utilizarea unui sistem de management de mediu (EMS) pentru servicii de catering;

28) Utilizarea de metode non-chimice, care respectă mediul;

29) Achiziționarea de energie electrică ecologică;

30) Impunerea unor durate de viață prelungite ale produselor și a unei garanții pentru piesele de schimb;

31) și altele.

39. În cazul unei asocieri, cerințele solicitate pentru îndeplinirea criteriilor de calificare și de selecție referitoare la situația economică și financiară sau a capacităților tehnice și profesionale pot fi îndeplinite prin cumul proporțional sarcinilor ce le revin fiecărui asociat.

40. În ceea ce privește criteriile privind cifra de afaceri, în cazul unei asocieri, cifra de afaceri medie anuală luată în considerare este valoarea generală, rezultată prin însumarea cifrelor de afaceri medii anuale corespunzătoare fiecărui membru al asocierii.

41. În ceea ce priveşte experienţa, pentru a se califica conform cerinţelor stabilite, asociațiile trebuie să demonstreze o experiență proporțională sarcinilor ce revin fiecărui asociat.

42. Capacitatea economică şi financiară, cât și capacitatea tehnică şi/sau profesională a ofertantului/candidatului poate fi susţinută, pentru îndeplinirea unui contract, şi de o altă persoană, indiferent de natura relaţiilor juridice existente între ofertant/candidat şi persoana respectivă.

43. În cazul în care ofertantul/candidatul îşi demonstrează capacitatea economică şi financiară cât și capacitatea tehnică şi/sau profesională invocînd şi susţinerea acordată, în conformitate cu prevederile pct. 42 de către o altă persoană, acesta are obligaţia de a dovedi susţinerea de care beneficiază prin prezentarea în formă scrisă a unui angajament ferm al persoanei respective, încheiat în formă autentică (conform anexelor nr. 16 și nr. 18) şi declaraţiile terţului susţinător

financiar şi terţului susţinător tehnic și profesional (anexele nr. 17, nr. 19 şi nr. 20), prin care această persoană confirmă faptul că pune la dispoziţia ofertantului/candidatului resursele financiare cât și resurse tehnice și profesionale invocate. Prezentarea angajamentului se face la solicitarea autorității contractante odată ce a fost declarat în DUAE. Persoana care asigură susţinerea financiară cât și tehnică și profesională trebuie să îndeplinească criteriile de selecție relevante și nu trebuie să se afle în niciuna dintre situaţiile prevăzute la pct. 22 și pct. 23 care determină excluderea din procedura de atribuire.

Secţiunea a 3-a

Pregătirea/Elaborarea ofertelor

44. Autoritatea contractantă în caietul de sarcini descrie condițiile/cerințele de furnizare:

a) ***a energiei electrice,*** în conformitate cu Legea nr. 174/2017 cu privire la energetică și actele normative de reglementare adoptate de către Consiliul de administrație al Agenției Naţionale pentru Reglementare în Energetică (în continuare – ANRE), de exemplu: Regulamentul privind furnizarea energiei electrice, aprobat prin Hotărârea ANRE nr. 23/2017, Regulamentul privind racordarea la rețele electrice și prestarea serviciilor de transport și de distribuție a energiei electrice, aprobat prin Hotărârea ANRE nr. 168/2019, Metodologia de calculare, aprobare și aplicare a tarifelor reglementate pentru serviciile auxiliare prestate de operatorii de sistem din sectorul electroenergetic, aprobată prin Hotărârea ANRE nr. 269/2018, Instrucțiunea privind calcularea pierderilor de energie electrică activă și reactivă în elementele de rețea aflate la balanța consumatorului, aprobată prin Hotărârea ANRE nr. 246/2007, Instrucţiunea privind calcularea consumului tehnologic de energie electrică în reţelele de distribuţie, în funcţie de valoarea factorului de putere în instalaţiile de utilizare, aprobată prin Hotărârea ANRE nr. 89/2003 etc.

b) a gazelor naturale în conformitate cu Legea nr. 108/2016 cu privire la gazele naturale și Legea nr. 174/2017 cu privire la energetică și actele normative de reglementare ale ANRE, de exemplu: Regulamentul privind furnizarea gazelor naturale, aprobat prin Hotărârea ANRE nr. 113/2019.

c) a energiei termice în conformitate cu Legea nr. 92/2014 cu privire la energia termică și promovarea cogenerării și Legea nr. 174/2017 cu privire la energetică, și actele normative de reglementare ale ANRE, de exemplu: Regulamentul privind furnizarea energiei termice, aprobat prin Hotărârea ANRE nr. 169/2019.

d) a alimentării cu apă şi canalizare în conformitate cu Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare și actele normative secundare, de exemplu: Regulamentul-cadru de organizare și funcționare a serviciului public de alimentare cu apă și de canalizare, aprobat prin Hotărârea ANRE nr. 355/2019 sau Regulamentele de organizare și funcționare a serviciului public de alimentare cu apă și de canalizare aprobate de autoritățile publice locale de nivelul întâi, în cazul în care au fost elaborate și aprobate.

e) ***a produselor petroliere pentru alimentarea automobilelor*** conform listei complete privind rețeaua de distribuție la nivelul țării din care să rezulte ca ofertantul deține stații de alimentare în localitățile indicate în documetația de atribuire. Carburantul se livrează la stația de alimentare în baza cardurilor emise de către Furnizor. Ofertantul oferă autorității contractante posibilitatea de a achiziționa carburant (fără plată în numerar) prin intermediul cardurilor valorice la stațiile de alimentare ale furnizorului la nivelul fiecăreia dintre localitățile menționate în documetația de atribuire. În cazul în care locul destinației finale îl constituie mai multe localități/regiuni, atribuirea contractelor de achiziție se realizează pe loturi pentru fiecare localitate/regiune în parte. Livrarea cardurilor se face pe baza unei cereri de emitere de card din partea autorității contractante. Termenul solicitat pentru livrarea cardurilor la sediul autorităţii contractante este de 5 zile lucrătoare de la data intrării în vigoare a contractului şi, respectiv, de la data transmiterii cererii de emitere de carduri suplimentare.

45. Autoritatea contractantă în caietul de sarcini precizează detalii privind modul de transportare, prestare, utilizare a produselor/serviciilor:

a) produselor petroliere pentru alimentarea automobilelor

Furnizorul acordă permanent achizitorului posibilitatea accesării on-line a informaţiilor privind situaţia detaliată a tuturor achiziţiilor de carburant efectuate de către fiecare autovehicul al său. Posibilitatea achizitorului de a obţine la orice staţie de distribuţie pe bază de card, informaţii privind valoarea rămasă pentru fiecare card în parte. Furnizorul gestionează lista cardurilor pierdute sau furate şi are obligaţia să blocheze/deblocheze utilizarea acestora în cel mult 24 ore de la solicitarea achizitorului. Furnizorul are obligația de a garanta că produsele furnizate respectă standardele minime de poluare aprobate conform legislației naționale și pot fi alimentate de la stațiile existente în localitățile indicate în documetația de atribuire. Carburanţii livraţi trebuie să corespundă calitativ normelor în vigoare. Se prezintă în partea II, Condițiile Speciale a Contractului, cât și în anexa nr.1 la Contract „Specificaţii Tehnice", condiţiile tehnice de calitate şi metodele de determinare a produselor, având la bază standarde şi omologări naţionale sau internaţionale. Furnizorul asigură personalizarea cardurilor pe fiecare autovehicul (pe număr de înmatriculare), configurarea cardului pe tipul carburantului. Furnizorul asigură asistență permanentă 24 h, 7 zile din săptămână, pentru ca, în cazul apariției anumitor deficiențe în funcționarea cardurilor pentru carburant, Furnizorul să fie în măsură să soluționeze problemele apărute în cel mai scurt timp posibil. Furnizorul specifică dacă toate cardurile sunt acceptate la toate stațiile PECO situate în localitățile menționate în documentația de atribuire. Furnizorul pune la dispoziţia achizitorului instrucţiuni de folosire a cardului. Autoritatea contractantă își rezervă dreptul de a mări sau micșora numărul de carduri și de a suplimenta sau diminua cantitatea de carburanți în baza prevederilor normative.

b) ***de furnizare a energiei electrice***

Evidența consumului de energie electrică se efectuează prin intermediul echipamentului de măsurare al Beneficiarului care este responsabil de integritatea acestuia. În cazul în care echipamentul de măsurare este instalat în limitele proprietății operatorului de sistem, responsabil de integritatea echipamentului de măsurare și a sigiliilor aplicate este operatorul de sistem. Operatorul de sistem asigură, la solicitare, accesul Beneficiarului la echipamentul de măsurare. În acest caz, Beneficiarul este în drept să aplice sigiliul său echipamentului de măsurare. Lucrările de instalare, exploatare, deservire, reparare, verificare metrologică periodică și de înlocuire a echipamentului de măsurare al Beneficiarului se efectuează în conformitate cu Legea nr. 174/2017 cu privire la energetică și Legea nr. 107/2016 cu privire la energia electrică, iar cheltuielile se suportă de către Beneficiar. Controlul echipamentului de măsurare și al sigiliilor aplicate acestuia se efectuează de către operatorul de sistem, după necesitate, și numai în prezența reprezentantului Beneficiarului. Citirea indicilor echipamentului de măsurare în scopul facturării energiei electrice consumate de Beneficiar, se efectuează de operatorul de sistem lunar. Personalul operatorului de sistem și utilizatorul de sistem sunt în drept să stabilească, de comun acord, timpul efectuării activităților pentru citirea indicilor echipamentului de măsurare. Cantitatea energiei electrice furnizate Beneficiarului se determină în baza indicilor echipamentului de măsurare, citite la fiecare loc de consum, sau, în cazurile prevăzute în Regulamentul pentru furnizarea energiei electrice, se calculează prin estimare. În cazul deteriorării echipamentului de măsurare sau dacă se constată încălcarea de către Beneficiar a prevederilor Legii cu privire la energia electrică, care a dus la consum de energie electrică prin evitarea echipamentului de măsurare, prin denaturarea indicațiilor echipamentului de măsurare sau alte modalități de consum neînregistrat de echipamentul de măsurare, contravaloarea energiei electrice consumate se calculează în conformitate cu prevederile Regulamentului pentru furnizarea energiei electrice. Contravaloarea pierderilor de energie electrică în transformatoarele de forță și în liniile electrice ce aparțin Beneficiarului, se calculează în baza Instrucțiunii privind calcularea pierderilor de energie electrică activă și reactivă în elementele de rețea aflate la balanța consumatorului, aprobată prin Hotărârea ANRE nr. 246/2007.

46. Autoritatea contractantă în caietul de sarcini precizează modalitatea de calculare a costului/prețului bunului/serviciului, prin trimitere la actele normative din domeniu.

a) a produselor petroliere pentru alimentarea automobilelor

Prețul unui litru de carburant ofertat va fi cel afișat la stațiile de alimentare ale ofertantului cu aplicarea discount-ului ofertat.
Furnizorul asigură autorității contractante posibilitatea de a stabili limite individuale valorice pentru fiecare card, inclusiv de a le modifica în sensul majorării sau micșorării acestora. Prețul unitar ofertat constituie prețul mediu calculat de către ofertant utilizînd prețurile afișate la panourile informative în toate stațiile din localitate/regiune indicate în documentația de atribuire, în decurs de 15 zile până la data publicării anunțului de participare în Buletinul achizițiilor publice, la care se aplică un discount.

Calcularea prețului unitar se efectuează conform formulei:

$$\text{Pu} = \frac{(\text{M1} + \text{M2} + \cdots + \text{M15})}{15} - D\%$$

Unde,

Pu – reprezintă prețul unitar ofertat;

M_1–reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru prima zi;

M_2– reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru a doua zi;

M_{15}– reprezintă media prețurilor afișate la **toate stațiile din localitatea/regiunea specificată în pct. 1** pentru a cincisprezecea zi;

D% –reprezintă discount-ul aplicat.

Discount-ul este specificat expres în ofertă și ulterior în anexa nr. 2 la contract, rămânînd neschimbat pe întreaga perioadă de valabilitate al acestuia. Propunerea financiară este însoțită obligatoriu de documentele confirmative cu privire la prețurile prezentate (bon fiscal). Furnizorul facturează contravaloarea produselor la sfârșitul fiecărei luni, pentru consumul efectuat, conform unei centralizări cu cantitatea alimentată pe fiecare autovehicul în parte. Factura aferentă consumului înregistrat pe fiecare card în parte este însoțită de un raport de consum care conține informații detaliate cu privire la tranzacțiile efectuate pe fiecare card și mașină, locație, dată, ora alimentării, tipul carburantului și, după caz, subtotalul cardului și totalul general de carburant după fiecare tranzacție.

În cazul procurării produselor petroliere pentru alimentarea automobilelor, în conformitate cu art. 26 al Legii nr.131/2015 privind achizițiile publice, se aplică criteriul cel mai bun raport calitate-preț, din care factorul de evaluare prețul, constituie minimum 60%, iar restul factorilor sunt la decizia autorității contractante (ex: discount-ul, amplasarea stațiilor PECO, etc.).

În restul cazurilor ce ține de achiziționarea de carburanţi lichizi şi/sau gazoşi în vrac, uleiuri, etc. se utilizează principiul general de procurare a bunurilor.

b) ***a energiei electrice***

Consumul tehnologic de energie electrică, cauzat de factorul de putere din instalaţiile electrice ale Beneficiarului se facturează numai în cazul în care factorul de putere Cos φ, calculat în punctul de delimitare, este mai mic de _____(0,92 pentru instalația de utilizare racordată la tensiunea 0,4 kV și 0,87 la tensiunea 10(6) kV). Cantitatea consumului tehnologic de energie electrică, cauzat de factorul de putere din instalaţiile electrice ale Beneficiarului se calculează în baza Instrucţiunii privind calcularea consumului tehnologic de energie electrică în reţelele de distribuţie, în funcţie de valoarea factorului de putere în instalaţiile de utilizare, aprobată prin Hotărârea Consiliului de administraţie al Agenţiei nr.89 din 13/2003. În cazul în care furnizorul

calculează prețul reieșind din tariful ANRE minus – discount-ul, modul de calculare a prețului se indică în condițiile speciale a contractului și de asemenea se indică și cazurile de modificare a lui. Micșorarea și/sau majorarea prețului și valorii contractului se efectuează prin acord adițional la contract.

47. Operatorul economic interesat de a participa la procedura de achiziție publică este obligat să depună până la expirarea termenului-limită stabilit de către autoritatea contractantă, în acest sens, o cerere de participare, în cazul aplicării prevederilor art. 33 alin. (7) și alin. (11) al Legii nr. 131/2015. În celelalte cazuri, aceasta se depune odată cu oferta.

48. Oferta cuprinde următoarele formulare:

1) Propunerea tehnică - ofertantul elaborează propunerea tehnică, astfel încât aceasta să respecte în totalitate cerinţele de calificare, precum şi cerinţele prevăzute în caietul de sarcini. Propunerea tehnică conține -Specificaţii tehnice (anexa nr. 22);

2) Propunerea financiară- ofertantul elaborează propunerea financiară, astfel încât aceasta să furnizeze toate informaţiile solicitate cu privire la preţuri, tarife, precum şi la alte condiţii financiare şi comerciale legate de obiectul contractului de achiziţie publică de bunuri și servicii. Propunerea financiară conține - Specificații de preț (anexa nr.23);

3) DUAE;

4) Garanția pentru ofertă, după caz (anexa nr.9).

49. Toate documentele menţionate la pct. 48 se completează fără nici o modificare sau abatere de la formulare, spaţiile goale fiind completate cu informaţia solicitată. Completarea defectuoasă a formularelor atrage respingerea ofertei.

50. Operatorii economici pregătesc ofertele conform cerințelor stabilite în anunțul de participare, publicat de către autoritatea contractantă în Buletinul achizițiilor publice, și depun ofertele în mod electronic, folosind fluxurile interactive de lucru puse la dispoziție de platformele electronice, cu excepția cazurilor prevăzute la art. 33 alin. (7) şi alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

51. Ofertantul depune garanția pentru ofertă conform prevederilor Legii nr. 131/2015 privind achizițiile publice.

52. În cazul unei asocieri, garanția pentru ofertă se depune de liderul asociației.

53. Ofertantul are obligația, prin depunerea declarației privind valabilitatea ofertei (anexa nr. 8), de a menține oferta valabilă pe toată perioada de valabilitate prevăzută în documentația de atribuire. Termenul valabilităţii ofertei începe să decurgă din momentul termenului limită de depunere a ofertelor. Orice ofertă valabilă pentru o perioadă mai mică decât cea prevăzută în anexa nr. 2 se respinge de către grupul de lucru ca fiind necorespunzătoare.

54. În cazul extinderii perioadei de valabilitate a ofertei, perioada de valabilitate a garanției pentru ofertă se prelungește în mod corespunzător.

55. Ofertantul are obligația de a comunica autorității contractante dacă este sau nu este de acord cu prelungirea perioadei de valabilitate a ofertei. Ofertantul care nu este de acord cu prelungirea perioadei de valabilitate a ofertei se consideră că și-a retras oferta, fără ca acest fapt să atragă pierderea garanției pentru ofertă.

56. Ofertele care conţin o perioadă de garanţie mai mică decât perioada de valabilitate a ofertelor prevăzută în anexa nr. 2 se resping de către grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice.

57. Autoritatea contractantă stabileşte perioada maximă de livrare/prestare a bunurilor/serviciilor în anexa nr. 2.

58. Preţurile pentru bunurile/serviciile solicitate se indică în lei moldoveneşti, cu două cifre după virgulă, cu excepţia cazurilor în care anexa nr. 2 prevede altfel.

Secţiunea a 4-a

Depunerea și deschiderea ofertelor

59. Oferta scrisă şi semnată în format electronic, de către administratorul companiei indicat în Extrasul Registrului de Stat al persoanelor juridice sau de către persoana împuternicită atât și în cazul delegării sau împuternicirii persoanei, la ofertă se anexează actul/documentul de împuternicire și se prezintă conform cerinţelor expuse în anexa nr. 2 în conformitate cu instrumentele existente în SIA RSAP, cu excepția cazurilor prevăzute la art. 33 alin. (7) şi alin. (11) din Legea nr. 131/2015 privind achizițiile publice.

60. Ofertantul trebuie să ia toate măsurile, astfel încât oferta să fie recepționată și înregistrată în SIA RSAP până la data limită pentru depunerea ofertelor, ținând cont de timpul necesar pentru încărcarea ofertei în sistem. În cazul prezentării ofertelor pe suport de hârtie, autoritatea contractantă eliberează operatorului economic, în mod obligatoriu, o recipisă în care indică data și ora recepționării ofertei.

61. Documentele justificative în sprijinul informațiilor declarate în DUAE, care conțin date cu caracter personal, se prezintă separat, pe suport de hârtie sau în formă scanată, cu aplicarea semnăturii electronice, utilizînd mijloace electronice de comunicare sau alte mijloace la etapa evaluării ofertelor, la solicitarea autorității contractante.

62. SIA RSAP nu acceptă ofertele transmise după expirarea termenului limită de depunere a ofertelor.

63. În cazurile prevăzute la art. 33 alin. (7) și alin. (11) din Legea nr. 131/2015 privind achizițiile publice, ofertele depuse după termenul limită de deschidere a ofertelor se înregistrează de către autoritatea contractantă și se restituite ofertantului, fără a fi deschise.

64. În cazul asocierii conform pct. 15, fiecare dintre aceştia îşi asumă obligaţia pentru oferta comună şi răspunde pentru orice consecinţe ale viitorului contract de achiziţie publică. Informaţia privind asocierea se prezintă completînd anexa nr. 11.

65. Ofertantul nu are dreptul de a depune decât o singură ofertă de bază. Ofertanţii asociaţi nu au dreptul de a depune alte oferte, în mod individual, pe lângă oferta comună. Ofertele alternative se depun numai dacă autoritatea contractantă a precizat explicit în anunţul de participare că permite sau solicită depunerea de oferte alternative.

66. Persoanele juridice nominalizate ca subcontractanţi în cadrul uneia sau mai multor oferte nu au dreptul de a depune oferta în nume propriu sau în asociere.

67. Ofertantul are dreptul să modifice sau să retragă oferta înainte de expirarea termenului de depunere a ofertelor, fără a pierde dreptul de retragere a garanţiei pentru ofertă.

Secţiunea a 5-a

Evaluarea și compararea ofertelor

68. În cazul în care ofertele conțin secrete tehnice, comerciale sau țin de protecția proprietății intelectuale, autoritatea contractantă asigură păstrarea confidenţialităţii asupra conţinutului ofertei, precum şi asupra oricărei informaţii privind ofertantul și totodată, asigura dreptul operatorului economic de a nu face publice aceste date prin aplicarea art. 33 alin. (7) și alin. (11)

al Legii nr. 131/2015 privind achizițiile publice, însă aplicarea acestui articol se referă numai la partea ce conțin datele enumeratate mai sus.

69. Examinarea documentelor de către autoritatea contractantă se efectuează în baza informațiilor prezentate de către operatorii economici în DUAE, și conform cerințelor stipulate în anunțul de participare prin care menționează că:

1) este eligibil să participe la procedurile de achiziții publice și nu există motive de excludere din cadrul procedurilor de achiziții publice pentru atribuirea contractului de achiziție publică;

2) îndeplinește criteriile referitoare la situația economică și financiară și/sau capacitatea tehnică și profesională stabilite de autoritatea contractantă în anunțul de participare sau în documentația de atribuire.

3) se obligă să asigure și să respecte standardele de asigurare a calităţii și standardele de protecție a mediului.

70. DUAE a operatorilor economici se verifică după caz, direct de către autoritatea contractantă prin procedurile automate desfășurate în SIA RSAP, prin accesarea unei baze de date a autorităților publice sau a terților din Republica Moldova, iar atunci când este necesar și în alte state.

71. În cazul în care la evaluare se stabilesc discrepanțe între informațiile prezentate de către operatorul economic în DUAE și cerințele stabilite de către autoritatea contractantă, operatorul economic se descalifică, ceea ce duce la respingerea ofertei, fiind stabilită ca inacceptabilă și neconformă, și se examinează documentele următorului ofertant/candidat.

72. Operatorul economic a cărui informație prezentată în DUAE corespunde cerințelor/condițiilor specificate de către autoritatea contractantă în anunț/invitația de participare are obligația să prezinte la cerere și fără întârziere documentele justificative.

73. Ofertantul clasat pe primul loc după aplicarea criteriului de atribuire prezintă documentele justificative prin care să demonstreze că îndeplineşte în totalitate cerinţele corespunzătoare criteriilor de calificare și de selecție, în conformitate cu informaţiile cuprinse în DUAE, cu excepţia procedurilor desfăşurate în mai multe etape, când documentele justificative sunt solicitate înainte de transmiterea invitaţiilor pentru etapa a doua către candidaţii selectaţi.

74. Ofertele se examinează de către grupul de lucru creat de autoritatea contractantă sau, după caz, specialistul certificat în domeniul achizițiilor publice.

75. Grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice are obligaţia de a stabili care sunt clarificările necesare pentru evaluarea fiecărei oferte, precum şi perioada acordată pentru transmiterea clarificărilor.

76. În cazul unei oferte care are un preț anormal de scăzut în raport cu prețul estimat al achiziției, autoritatea contractantă are obligația de a efectua controlul calculării elementelor prețului și de a verifica și anumite elemente ale propunerii financiare stabilite ca fiind cu preț anormal de scăzut cât și respectarea de către ofertant a cerințelor tehnice indicate în caietul de sarcini, și de a solicita în scris, și înainte de a lua o decizie de respingere a acelei oferte, detalii și precizări pe care le consideră relevante cu privire la ofertă, precum, și de a verifica răspunsurile care justifică prețul respectiv.

77. Grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice respinge oferta în oricare dintre următoarele cazuri:

1) ofertantul nu îndeplinește cerințele de calificare și de selecție;

2) oferta nu respectă cerinţele prevăzute în documentaţia de atribuire pentru elaborarea şi prezentarea ofertelor;

3) ofertantul nu transmite în perioada stabilită clarificările solicitate;

4) oferta financiară nu are un preț fixat;

5) ofertantul modifică, prin clarificările pe care le prezintă, conţinutul propunerii tehnice şi/sau al propunerii financiare, cu excepţia situaţiei în care modificarea este determinată de corectarea erorilor aritmetice sau abaterilor neînsemnate;

6) oferta este anormal de scăzută potrivit art. 70 al Legii nr. 131/2015 privind achizițiile publice;

7) atunci când explicațiile prezentate de ofertant, la solicitarea autorității contractante, nu sunt concludente şi/sau nu sunt susținute de documentele justificative cerute de către grupul de lucru sau, după caz, specialistul certificat în domeniul achizițiilor publice;

8) s-a constatat comiterea unor acte de corupţie, acte conexe actelor de corupţie sau fapte coruptibile confirmate prin hotărâre definitivă a instanţei de judecată.

78. Dacă oferta, inclusiv formularele care o însoțesc, nu corespunde cerințelor prestabilite în invitația/anunțul de participare, inclusiv în documentația de atribuire sau aceasta nu este completată, semnată electronic și după caz, semnată și ștampilată în modul corespunzător, ea se respinge de către autoritatea contractantă, și nu poate fi rectificată cu scopul de a corespunde cerințelor, prin corectarea sau extragerea devierilor sau rezervelor necorespunzătoare, excepție constituind doar corectarea greșelilor aritmetice sau abaterilor neînsemnate.

79. Autoritatea contractantă poate, la discreţia sa, să ceară oricăruia dintre ofertanţi o clarificare a ofertei acestora, pentru a facilita examinarea, evaluarea și compararea ofertelor. Nu se solicită, nici nu se permit schimbări în preţurile sau în conţinutul ofertei, cu excepţia corectării erorilor aritmetice descoperite de către autoritatea contractantă în timpul evaluării ofertelor.

80. Erorile aritmetice se corectează după cum urmează: dacă există o discrepanţă între preţul pentru o unitate de măsură şi preţul total (care este obţinut prin multiplicarea preţului cu cantitatea totală), se ia în considerare preţul pe unitate, iar preţul total este corectat în mod corespunzător.

81. Grupul de lucru, după caz, specialistul certificat în domeniul achizițiilor publice are dreptul de a corecta erorile aritmetice numai cu acceptul ofertantului. Dacă ofertantul nu acceptă corectarea acestor erori, oferta sa se consideră necorespunzătoare şi, în consecinţă, se respinge de către grupul de lucru.

82. Operatorul economic este obligat să răspundă la solicitarea de clarificare a autorității contractante în cel mult 3 zile lucrătoare sau, în cazul în care procedura folosită este cererea ofertelor de preţuri, cel mult o zi lucrătoare de la data expedierii acesteia, iar în cazul în care ofertantul nu suplimentează, nu prezintă clarificări sau nu completează informațiile sau documentele solicitate de autoritatea contractantă în termenele stabilite de aceasta, oferta se respinge şi se selectează următoarea după clasament dintre ofertele rămase în vigoare.

83. Oferta care corespunde tuturor termenilor, condiţiilor şi specificaţiilor din documentele de atribuire, fără abateri esenţiale sau cu abateri neînsemnate, erori sau omiteri ce pot fi înlăturate fără a afecta esenţa ei, se consideră conformă.

84. Autoritatea contractantă descalifică ofertantul care depune documente ce conţin informaţii false, cu scopul calificării, sau derutează ori face reprezentări neadevărate pentru a demonstra corespunderea sa cerinţelor de calificare. În cazul în care acest lucru este dovedit, autoritatea contractantă declară ofertantul respectiv ca fiind neeligibil pentru participarea ulterioară în contractele de achiziţii publice, în urma includerii lui în Lista de interdicţie a operatorilor economici.

85. Autoritatea contractantă solicită ofertanţilor să demonstreze împuternicirea de a încheia contractele de achiziţii publice şi componenţa fondatorilor, asociațiilor, acționarilor, administratorilor și a beneficiarilor efectivi.

86. Ofertantul/ofertantul asociat desemnat câștigător este obligat de a completa și prezenta declarația cu privire la beneficiarii efectivi în conformitate cu Ordinul ministrului finanțelor nr.

145/2020 cu privire la aprobarea Declarației privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani.

Secţiunea a 6-a

Atribuirea contractului

87. Autoritatea contractantă anulează procedura de atribuire a contractului de achiziţie publică conform art. 71 din Legea nr. 131/2015 privind achizițiile publice.

88. Decizia de anulare nu creează vreo obligație a autorității contractante față de ofertanţi, cu excepţia returnării garanţiei pentru ofertă. Decizia de anulare a procedurii de atribuire se expediază Agenției Achiziții Publice nu mai târziu de data informării despre rezultatele procedurii de atribuire prevăzută la art. 31 alin. (1) al Legii nr. 131/2015 privind achizițiile publice.

89. În cazul în care se anulează aplicarea procedurii pentru atribuirea contractului de achiziţie publică, autoritatea contractantă are obligaţia de a comunica în scris tuturor participanţilor la procedura de achiziţie publică, în cel mult 3 zile de la data anulării procedurii, atât încetarea obligaţiilor pe care aceştia şi le-au creat prin depunerea de oferte, cât şi motivul anulării.

90. Darea de seamă privind anularea procedurii de achiziţie publică este întocmită de către autoritatea contractantă şi este publicată în Buletinul achizițiilor publice nu mai târziu de data emiterii deciziei de anulare a procedurii de achiziţie publică.

91. La momentul încheierii contractului, dar nu mai târziu de data expirării garanţiei pentru ofertă, după caz, ofertantul câştigător prezintă garanţia de bună execuţie, în conformitate cu cerințele stipulate în art. 68 al Legii nr. 131/2015 privind achizițiile publice.

92. Garanția de bună execuție a contractului, dacă părțile agreează, se constituie din:

1) reţineri succesive din plata cuvenită pentru facturile fiscale înaintate, cu efectuarea transferului sumei respective pe un cont special deschis de către operatorul economic, pus la dispoziția autorității contractante, la o bancă licențiată, agreată de ambele părți;
2) reţineri succesive directe din plata cuvenită pentru facturile fiscale înaintate;
3) transfer pe contul autorității contractante;
4) formă de garanţie bancară de la o instituţie licenţiată, (anexa nr.10).

93. Refuzul ofertantului câştigător de a depune garanţia de bună execuţie sau de a semna contractul constituie motiv pentru anularea atribuirii contractului şi reţinerii garanţiei pentru ofertă. În acest caz, autoritatea contractantă poate atribui contractul următorului ofertant cu oferta cea mai bine clasată, a cărui ofertă este conformă cerinţelor şi care este apreciată de către autoritatea contractantă a fi calificată în executarea contractului. Totodată, autoritatea contractantă este în drept să respingă toate celelalte oferte.

94. La expirarea perioadei de aşteptare sau, după caz, după soluționarea oricăror contestații, sau monitorizării conformității desfăşurării procedurilor de achiziţii publice de către Agenția Achiziții Publice, autoritatea contractantă încheie contractul de achiziții publice, în conformitate cu termenii și condițiile indicate în documentația de atribuire.

95. La data încheierii contractului de achiziție publică de bunuri/servicii se interzice modificarea unor elemente ale ofertei câștigătoare, impunerea de noi cerințe ofertantului câștigător sau implicarea oricărui alt ofertant decât cel care a prezentat oferta cea mai avantajoasă.

96. Contractul pentru care sursele financiare se alocă din bugetul de stat/bugetul local se înregistrează obligatoriu la una din trezoreriile regionale ale Ministerului Finanțelor și intră în vigoare la data înregistrării sau la o altă dată ulterioară prevăzută de acesta după înregistrare la una din trezoreriile regionale ale Ministerului Finanțelor.

97. Autoritatea contractantă utilizează contractul - model (anexa nr. 24) din prezenta documentație-standard, inclusiv pentru contracte subsecvente încheiate conform acordului-cadru (anexa nr. 26), pentru contracte de valoare mică, pentru contractele în urma desfășurării procedurii prin cererea ofertelor de prețuri, la fel și pentru contractele în urma desfășurării procedurilor negociate. Contractul poate fi încheiat între una sau mai multe autorități contractante și unul sau mai mulți operatori economici, care are ca obiect livrarea/prestarea bunurilor/serviciilor.

98. Contractul este compus din două părți: Partea I cea generală care este obligatorie, și care nu se modifică, doar cu excepția contractelor de achiziţii publice ce nu cad sub incidența Legii nr. 131/2015 privind achiziţiile publice și Partea II ceea ce ține de condițiile speciale al contractului care se completează doar la necesitate, unde autoritatea contractantă are dreptul de a stabili condiții/cerințe speciale în dependență de obiectul achiziției, de complexitatea procedurii, atât și de a stabili condițiile achitării (în special la achiziționarea combustibilului, energiei electrice, gaze, apa și canalizare, salubritate, servicii de comunicații electronice, etc.), atât și de a stabili condițiile achitării în avans. În cazul achizițiilor serviciilor din domeniul energetic și de alimentare cu apă și de canalizare, contractul de achiziții publice conțin clauzele obligatorii stabilite prin legile sectoriale și actele normative de reglementare aprobate de către ANRE. Totodată, prevederile obligatorii stabilite prin deciziile acesteia, care nu se regăsec în partea I cea generală al contractului, se indică în partea II ce ține de condițiile speciale al contractului.

99. Termenii de asumare a angajamentelor în contractele de achiziții publice de către autoritățile/instituțiile bugetare se stabilesc în conformitate cu prevederile art. 66 din Legea nr. 181/2015 finanțelor publice și responsabilității bugetar-fiscale.

100. În cazul serviciilor de audit, autoritatea contractantă indică în partea II ce ține de condițiile speciale al contractului drepturile/obligațiile Beneficiarului și drepturile/obligațiile Prestatorului, în conformitate cu prevederile Ordinului ministrului finanțelor nr. 160/2020 cu privire la aprobarea Regulamentului privind activitatea de audit intern pe bază de contract în sectorul public.

101. Nu se acceptă în cadrul achizițiilor publice proiectele contractelor ce deviază de la anexa nr. 24, întocmite de prestator/furnizor cu excepția cazurilor când serviciile sunt prestate în afara țării și sunt încheiate conform cadrului juridic local (de exemplu: serviciile de instruire, servicii hoteliere, etc.).

102. Orice operator economic care consideră că, în cadrul procedurilor de achiziţie, autoritatea contractantă, prin decizia emisă sau prin procedura de achiziţie aplicată cu încălcarea legii, a lezat un drept al său recunoscut de lege, în urma cărui fapt el a suportat sau poate suporta prejudicii, are dreptul să conteste decizia sau procedura aplicată de autoritatea contractantă, în modul stabilit de Legea nr. 131/2015 privind achiziţiile publice.

103. Contestaţiile se depun direct la Agenția Națională pentru Soluționare a Contestațiilor. Toate contestaţiile se depun, se examinează şi se soluţionează în modul stabilit de Legea nr. 131/2015 privind achiziţiile publice.

104. Operatorul economic, conform art. 83 al Legii nr. 131/2015 privind achizițiile publice, în termen de până la 5 zile, sau10 zile de la data la care a aflat despre circumstanţele ce au servit drept temei pentru contestaţie, are dreptul să depună la Agenția Națională pentru Soluționarea Contestațiilor o contestaţie argumentată a acţiunilor, a deciziei ori a procedurii aplicate de autoritatea contractantă.

105. Contestaţiile privind anunțurile de participare la licitaţie şi documentaţia de atribuire se depun în termenele indicate la pct. 104, însă nu mai târziu de deschiderea ofertelor de către autoritatea contractantă.

106. Fiecare ofertant care participă, în mod individual sau ca asociat, la procedura de atribuire a contractului de achiziție publică de bunuri/servicii are obligația să prezinte anexele prevăzute în prezenta documentație, completate în mod corespunzător şi semnate de persoanele autorizate, conform cerințelor stabilite în anexa nr.2.

Anexa nr. 2
la Documentația standard nr._____
din "____" _____ 202__

ANUNȚ DE PARTICIPARE

privind achiziționarea serviciilor de mentenanță şi suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG și SIP
prin procedura de achiziție *Licitație deschisă*

1. **Denumirea autorității contractante:** *Compania Națională de Asigurări în Medicină*
2. **IDNO:** *1007601007778*
3. **Adresa:** *mun. Chișinău, str. Vlaicu Pârcălab 46*
4. **Numărul de telefon/fax:** 022 780-263/264
5. **Adresa de e-mail și de internet a autorității contractante***: achizitii@cnam.gov.md*
6. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire:** ***documentația de atribuire este anexată în cadrul procedurii în SIA RSAP***
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** *Instituție publică / asigurare obligatorie de asistență medicală*
8. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea/prestarea/executarea următoarelor bunuri /servicii/lucrări:**

Nr. lotului	Cod CPV	Denumirea bunurilor/serviciilor/ lucrărilor solicitate	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată fără TVA (se va indica pentru fiecare lot în parte)
Lotul 1						
1	72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – **în bază de abonament**	Luni	12	Conform Caietului de sarcini din Anexa nr. 1	539 784,00
2	72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – **în bază de trouble**	Om/ore	900	Conform Caietului de sarcini din Anexa nr. 1	137 700,00

		ticket/ticketing				
					Valoarea estimată totală (fără TVA)	677 484.00

Nr. lotului	**Cod CPV**	**Denumirea bunurilor/serviciilor/ lucrărilor solicitate**	**Unitatea de măsură**	**Cantitatea**	**Specificarea tehnică deplină solicitată, Standarde de referință**	**Valoarea estimată fară TVA (se va indica pentru fiecare lot în parte)**
Lotul 2						
1	72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de abonament**. .	Luni	12	Conform Caietului de sarcini din Anexa nr. 2	539 784,00
2	72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de trouble ticket/ticketing.**	Om/ore	900	Conform Caietului de sarcini din Anexa nr. 2	137 700,00
	Valoarea estimată totală (fără TVA)					677 484.00

9. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):** *Pentru mai multe loturi*

10. **Admiterea sau interzicerea ofertelor alternative:** **nu se admite**
(indicați se admite sau nu se admite)

11. **Termenii și condițiile de livrare/prestare/executare solicitați:** 01.01.2025-31.12.2025

12. **Termenul de valabilitate a contractului:** *31.12.2025*

13. **Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz):** *NU*
(indicați da sau nu)

14. **Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz):** *NU*
(se menționează respectivele acte cu putere de lege și acte administrative)

15. **Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):**

Nr. d/o	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1.	Vor fi excluși operatorii economici care nu şi-au îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în ţara în care este stabilit.	Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertei) - eliberat de Inspectoratul Fiscal Principal de Stat, confirmat prin semnătura electronică, ori link-ul la accesarea unei baze de date naționale disponibile gratuit pentru autoritatea contractantă care deține informațiile privind lipsa/existența restanțelor. confirmată prin aplicarea semnăturii electronice a participantului	***Obligatoriu***
2.	Declaraţii privind cifra de afaceri în domeniul de activitate aferent obiectului contractului (prestarea serviciilor similare) într-o perioadă anterioară care vizează activitatea pentru ultimii 3 ani - a cîte min 1 000 000,00 lei pentru fiecare din ultimii 3 ani original confirmat prin semnătura electronică a participantului: (la solicitare se va prezenta documente primare de confirmare copiile contractelor, raport financiar etc.)	Declaraţie privind lista principalelor prestări de serviciul efectuate în ultimii 3 ani de activitate similare obiectului de achiziție conform ***Anexei nr. 12*** din Ordinul MF 115/2021 - confirmată prin semnătura electronică	***Obligatoriu***
3.	Demonstrarea accesului la personalul necesar pentru îndeplinirea corespunzătoare a obiectului contractului ce urmează a fi atribuit	Conform Caietului de sarcini (Anexa nr. 1 / Anexa nr.2)	***Obligatoriu***
4.	Declarație de garanție	Autoritatea Contractantă solicită o garanție a aplicației acordată de către ofertanți pentru o perioada de 12 luni de la încetarea contractului. Confirmată prin aplicarea semnăturii electronice a persoanei responsabile a ofertantului. Pe perioada desfășurării contractului, codul sursă al aplicației va fi supus modificărilor efectuate de către specialiștii prestatorului. Orice modificare în codul sursă are ca efect o nouă versiune a aplicației care este supusă garanției contractuale a ofertantului în baza cerințelor minime și obligatorii ale Caietului de Sarcini.	***Obligatoriu***
5.	Va fi exclus din procedura de atribuire a contractului de achiziţii publice orice ofertant sau candidat despre care are cunoştinţă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanţe judecătoreşti, pentru participare la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, pentru fraudă şi/sau pentru spălare de bani, pentru infracţiuni de terorism sau infracţiuni legate de activităţi teroriste, finanţarea terorismului, exploatarea prin muncă a copiilor şi alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	***Obligatoriu*** *Lipsa condamnării pe parcursul a ultimilor 5 ani.*
6.	Va fi exclus orice operator economic care se află în proces de insolvabilitate ca urmare a hotărârii judecătoreşti.	La depunerea ofertei prin declararea în DUAE	***Obligatoriu*** *Nu se află în*

			proces de insolvabilitate
7.	Garanția pentru ofertă în **valoare de 1%**	**Garanţia pentru ofertă emisă de către o bancă comercială *sau* prin transfer la contul autorităţii contractante, conform următoarelor date bancare:** Beneficiarul plăţii: **Compania Națională de Asigurări în Medicină** Denumirea Băncii: **Ministerul Finanțelor – Trezoreria de Stat** Codul fiscal: **1006601000037** IBAN: **MD30TRGAAC14513001300000** cu nota "Pentru garanţia pentru ofertă la licitaţia publică nr. _____ din _____" Dispoziția de plată va fi atașată în modul scanat *(se va prezenta la depunerea ofertei de către toți ofertanți)	***Obligatoriu***
8.	Garanția de bună execuție a Contractului **în valoare de 5%** din valoarea Contratului	**Contractul va fi însoţit de o Garanţie de bună execuţie (emisă de către o bancă comercială)** *sau* **Garanţia de bună execuţie prin transfer la contul autorităţii contractante, conform următoarelor date bancare:** Beneficiarul plăţii: **Compania Națională de Asigurări în Medicină** Denumirea Băncii: **Ministerul Finanțelor – Trezoreria de Stat** Codul fiscal: **1006601000037** IBAN: **MD30TRGAAC14513001300000** **cu nota "Pentru garanţia de buna execuţie a contractului nr. _____ din _____"** * (Se va prezenta doar de către ofertantul declarat cîștigător odată cu semnarea Contractului)	***Obligatoriu*** *pentru operatorul economic declarat câștigător*
9.	DECLARAŢIE privind confirmarea identităţii beneficiarilor efectivi şi neîncadrarea acestora în situaţia condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani	Declaraţie în conformitate cu **Anexa nr. 3** din documentul (Caiet de sarcini mentenanta 2025-DRG și SIP) autentificată prin aplicarea semnăturii electronice a Participantului – depunere obligatorie după desemnare în calitate de ofertant/ofertant asociat desemnat câștigător ;	***Da*** *– depunere obligatorie după desemnare în calitate de cîștigător*

CAIET DE SARCINI

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **DRG**

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	Descriere
Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG: • *Servicii de mentenanță preventivă și Suport – în bază de abonament;* • *Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.*	*Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.*

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG (în continuare – DRG) pentru o perioadă de **minim 12 luni** după încetarea contractului.

De asemenea, Prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta CNAM (Beneficiar) împreună cu codul sursă DRG, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Descriere generală a DRG

DRG reprezintă un sistem național pentru instituțiile medicale din Republica Moldova, cu ajutorul căruia sunt încărcate și gestionate informațiile la nivelul bazei de date a CNAM.

Obiectivele strategice ale CNAM și MS în ceea ce privește costurile asociate tratamentului conduce la obținerea unei **imagini mai bune a rezultatelor** și la realizarea de **comparații ale rezultatelor**. DRG este un **instrument util spitalelor în creșterea eficienței** (prin identificarea resurselor necesare fiecărui tip de pacient), în procesul de îmbunătățire a calității serviciilor furnizate (prin evaluarea calității și definirea unor modele de practică), în **modelarea activității** și a structurii spitalelor (personal, secții, etc.) și în realizarea unui **management bazat pe rezultate** și nu pe resurse sau procese.

Funcționarea continuă și operarea în sistemul DRG are următoarele obiective:

A. Creșterea eficienței serviciilor spitalicești

Prin finanțarea în sistem DRG, spitalele ce vor avea costuri pentru un anumit DRG mai mari decât tariful stabilit vor pierde resurse la acea categorie de pacienți, iar cele cu costuri, pentru un anumit DRG, mai mici decât tariful stabilit vor câștiga resurse la acea categorie de pacienți. Alocarea resurselor financiare are la baza rezultatele spitalului și mai puțin structura acestora.

B. Creșterea eficienței tehnice la nivelul furnizorului de serviciilor spitalicești

DRG permite spitalelor să-și evidențieze cu claritate tipurile de pacienți și resursele atrase pentru aceștia, iar prin compararea cu costurile necesare se generează cadrul de funcționare pentru o eficientă cât mai mare (economiile făcute fiind păstrate la nivelul spitalului).
Spitalele pot să-și cunoască tipurile de pacienți pentru care pierd resurse (și să intervină în procesele ce se desfășoară pentru a reduce cheltuielile) și pacienții la care sunt în beneficiu financiar (și să încerce să atragă cât mai mulți pacienți de acest tip).

Specificații tehnice DRG

Caracteristici generale de funcționare

DRG are o arhitectura 3-layer, arhitectura care permite funcționarea pe platforma guvernamentală comună MCloud. DRG funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă tot ce este necesar de automatizat;
- are posibilitatea reparației unui modul fără afectarea altora;
- respectă standardele în vigoare a tehnologiilor informaționale;
- asigură flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare;
- utilizează o arhitectură orientată pe servicii pentru a acomoda cu ușurință noi modificări;
- are o arhitectura modernă cu un grad înalt de performanță, structurată pe 3 niveluri (nivelul pentru baze de date, nivelul pentru aplicație și nivelul acces/utilizator). Fiecare nivel are în componență toate echipamentele necesare bunei funcționări;
- este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- poate fi utilizat împreună cu echipamente ce permit creșterea vitezei de înregistrare a datelor de identificare ale pacienților (nume, prenume, IDNP etc.);
- este scalabil pentru a acomoda modificările viitoare ale numărului de utilizatori ai soluției;
- recunoaște corect sursele informaționale, le acceptă și le integrează în sistem;

- întreține în limba de stat interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate;
- permite ca utilizatorul să se autentifice o singură dată pentru a accesa toate modulele aplicației;
- asigură o siguranță sporită în exploatare.

Interfața Utilizator

Această interfață este accesibilă pentru toți utilizatorii autorizați în DRG:

- ✓ DRG dispune de o interfață inteligentă, intuitivă și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browserul web și nu necesită instalarea de componente software suplimentare;
- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului;
- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:

- **Platforma hardware**, formata din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat pe platforma guvernamentală comună MCloud:
  - Servere protejate redundant pentru hosting al bazelor de date, softului de sistem și softului funcțional (aplicații și subsisteme);
  - Platforma hardware pusă la dispoziție de către beneficiar este dimensionată corespunzător pentru a permite funcționarea în bune condiții a sistemului;
  - Performanta optima, în limita normelor obiective de uzură, pentru realizarea structurii funcționale și asigurarea extinderii ulterioare a sistemului;
  - este flexibilă în utilizarea mijloacelor disponibile destinate recepționarii informației din surse externe (alte instituții publice);
  - asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date;
  - asigura normele de funcționare ale platformelor informatice guvernamentale.

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:
  - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
  - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server 2017, vers. 14.
  - Pe stațiile utilizatorilor există în mod implicit .NET Framework 3.5 SP1 sau mai nou și navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare și transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mașini virtuale, mijloacele de imprimare, rețele electronice locale (LAN – local area network) și de scara largă (WAN – wide area network). Pentru operare se folosesc stațiile de lucru ale beneficiarului, singura specificație impusă utilizatorilor fiind cea de a dispune de un calculator conectat la internet și un browser instalat, fiind recomandate și utilizate soluțiile Microsoft.

Sistemul de securitate

DRG funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.

Caracteristici:

- asigură accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de system;
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor;

Având în vedere natura specială a informațiilor gestionate în cadrul DRG, acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.

Sistemul are următoarele nivele de securitate care asigură confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație între stațiile clientului și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unică cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este asigurata automat, iar modificările de structura la nivelul acesteia se fac exclusiv în baza drepturilor corespunzătoare de administrator al bazei de date. În plus, baza de date deține propriul mecanism de backup care permite, în caz de dezastru, restaurarea unor versiuni anterioare recente (de ordinul zilelor).

Sistemul asigură dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori sunt create

module de acces și autentificare în sistem; sunt indicate volumul de informație și funcționalitatea pe care aceștia o accesează. Sistemul permite accesul la datele statistice pentru anumiți utilizatori și grupuri de utilizatori. Sistemul asigura verificarea automată a drepturilor în momentul intrării în sistem și în ulterioarele accesări a sistemului și creează un jurnal al accesărilor – jurnalul de audit.

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Operator**: permite introducerea și modificarea datelor specifice activității sale;
- nivelul **Administrator**: permite arhivarea datelor, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

La nivel aplicativ, sistemul generează o listă de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

- ✓ posibilitatea înregistrării, adăugării si ștergerii utilizatorilor din sistem;
- ✓ posibilitatea distribuției drepturilor utilizatorilor folosind grupuri de acces;
- ✓ posibilitatea pentru fiecare utilizator de a avea cel puțin următoarele atribute de autentificare: identificarea, autentificarea.
- ✓ posibilitatea intrării în sistem a unui utilizator în orice moment;
- ✓ asigurarea de către administrator a regimurilor de funcționare, deconectare, conectare, modificării regimului de autentificare și identificare, dirijarea cu drepturi și auditul.

Retenția datelor, acces securizat și audit

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale (consultații, fișe medicale și bilete de trimitere) în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.
- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respectă regulile de control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.
- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.
- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem și pe baza permisiunilor asociate rolului sau rolurilor atribuite utilizatorilor.
- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fișele electronice ale pacienților săi.
- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu că a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:

- unicitatea utilizatorilor în sistem;
- jurnalizarea tuturor operațiunilor efectuate de sistem;
- mecanism de control al versiunilor pentru înregistrările medicale.

- **Securitatea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit.** Toate operațiunile efectuate de utilizatori sau de către alte sisteme care accesează sistemul păstrează o înregistrare în componența auditului. Astfel, este permisă investigarea incidentelor de către un administrator.

Arhitectura DRG

DRG are o arhitectură bazată pe tehnologie web, folosind platforma Microsoft. Sistemul este conceput modular, dezvoltarea acestora putând fi realizată în paralel. Orice client se poate conecta la serverul de aplicație și poate utiliza sistemul conform drepturilor pe care le are. Comunicația între client și server se realizează exclusiv prin protocoale securizate de tip HTTPS folosind certificat de securitate integrat la nivelul serverului de aplicație. Schema arhitecturala este în figura următoare:

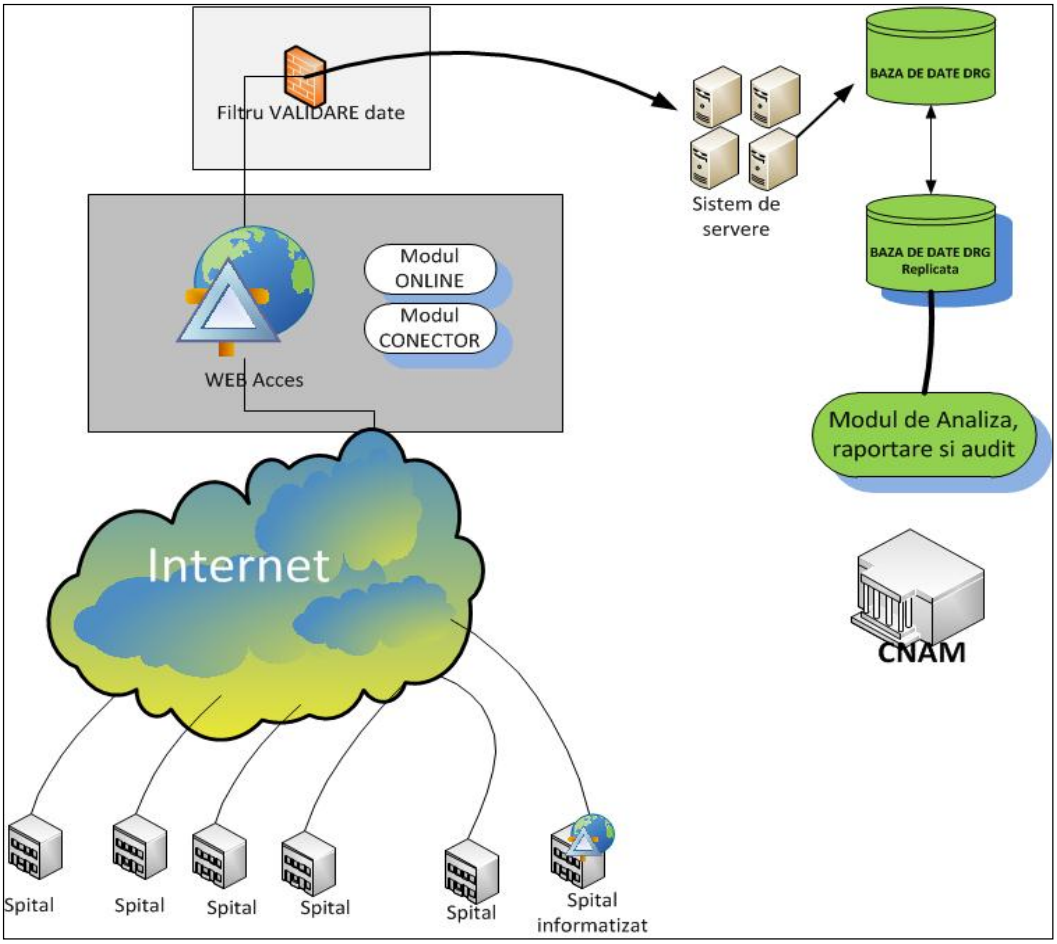


Figura 1. Schema arhitecturală DRG

Componentele DRG sunt operaționale și sunt prezente conform modulelor:

- ✓ Modulul de administrare sistem colector;

- ✓ Modulul de autentificare;
- ✓ Modulul colectare date Real Time;
- ✓ Modulul de nerepudiere;
- ✓ Modulul de validare;
- ✓ Modulul de înregistrare raportări;
- ✓ Modulul de setări, raportare și audit;
- ✓ Modulul Depozit (warehouse);
- ✓ Modulul de Analiză la nivel de Baza de Date;
- ✓ Modul conector pentru Auditul Codificării.

Modulul de administrare sistem colector

În cadrul acestui modul se execută:

- **Managementul utilizatorilor** (creare, ștergere, modificare date utilizatori). Fiecare instituție care execută raportare în DRG are desemnat cel puțin un utilizator al sistemului care transmite raportările; modalitatea de alocare a acestei resurse umane este răspunderea instituției.
- **Administrarea sistemului.** Administratorii sistemului pot efectua setări la nivelul celorlalte module și pot verifica funcționarea corectă a fiecărui modul. Nivelul de acces al administratorilor este corespunzător cerințelor de care aceștia răspund:
  - administratorii pot modifica informațiile de referință ale operatorilor sistemului (nume, prenume, locație, instituție, etc.);
  - administratorii pot modifica intervalele temporare în care transmiterea raportărilor este permisă;
  - administratorii pot vizualiza informații existente în modulul de nerepudiere (fișierele care conțin informațiile raportate trec prin modulul de nerepudiere);
  - administratorii pot vizualiza informațiile existente în modulul de înregistrare și să confirme funcționarea normală a acestuia;
  - administratorii pot vizualiza existenta rapoartelor transmise și stadiul în care se afla acestea față de modulul de validare;
  - administratorii pot face modificări asupra Modulului de Notificare și Raportare.
  - administratorii pot verifica transmiterea corectă a rapoartelor către Modulul Warehouse, unde sunt depozitate informațiile în vederea prelucrării.

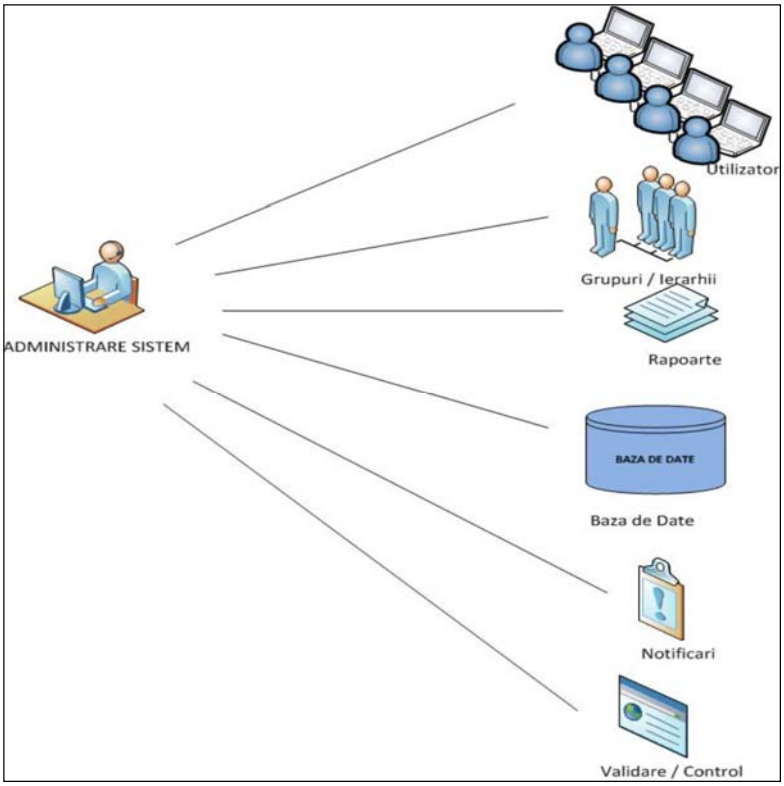


Figura 2. Schema Modulul de administrare sistem colector

Nivelul de acces al acestui modul:

- modulul care are acces la toate nivelurile sistemului;
- doar administratorii sistemului au acces la acest modul, în vederea efectuării operațiilor necesare funcționării normale a sistemului.

Modulul de administrare este singurul modul care permite accesul unui număr restrâns de persoane (administratorii sistemului) la toate elementele din sistem, fără să permită – prin procedura - modificarea conținutului rapoartelor.

Administratorii sistemului au rolul de a verifica fluxul normal al prelucrării datelor de către sistem și de a ajusta situațiile de excepție atunci când este cazul. Prin situații de excepție se înțeleg acele cazuri în care sistemul răspunde corect din punct de vedere al fluxului, dar cerințele unui utilizator sunt diferite și justificate.

Administratorii sistemului nu acționează asupra conținutului datelor transmise de către unitățile medicale, iar utilizatorii sunt instruiți asupra faptului că sunt direct răspunzători de conținutul informațiilor transmise. Conținutul datelor este confidențial și respectă normele de securitate din domeniu; sistemul informatic DRG poate opera cu fișierele de date fără a fi necesară intervenția administratorilor de sistem asupra conținutului. În situațiile în care utilizatorul corespunzător care a generat raportul cere explicit acest lucru, administratorul nu o prelucrează: conținutul datelor transmise rămâne exclusiv responsabilitatea instituțiilor medicale / operatorilor care folosesc sistemul.

Modulul de colectare date Real Time

Acest modul este cel care transformă operarea DRG într-o activitate aflată la dispoziția permanentă a oricărui spital: este un modul destinat acelor instituții care nu au un sistem informatic integrat al activității medicale, și care, în prezent lucrează cu diferite programe informatice în vederea generării raportărilor.

Acest modul are o interfață de lucru universală cu un aspect operațional intuitiv și ușor de urmărit, care nu necesită cunoștințe tehnice informatice avansate; orice medic sau asistent îl poate utiliza în activitatea curentă în vederea introducerii în sistemul național a informațiilor despre pacienții pe care îi tratează.

Informațiile pot fi introduse de către utilizatorii autorizați direct în sistem non-stop, la nivel național, într-o interfață accesibilă de pe orice calculator care dispune de un browser și de o legătura la serverul sistemului DRG: vârsta, sex, durata de spitalizare, diagnostice principale și secundare, proceduri, starea la externare și greutatea la naștere (în cazul nou-născuților), iar în funcție de acestea pacienții sunt clasificați într-o categorie distinctă (o grupă de diagnostice), în conformitate cu nomenclatoarele din domeniu.

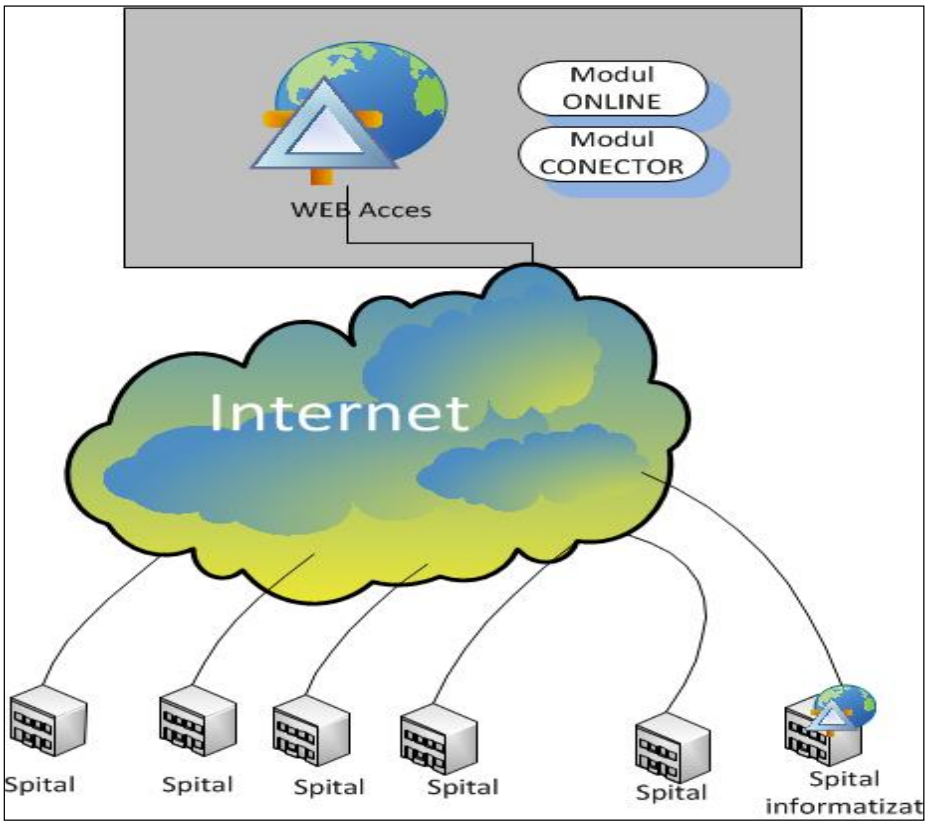


Figura 4. Modulul de colectare date Real Time

Avantajul major pe care îl oferă acest modul este că el este permanent updatat în conformitate cu cerințele CNAM, nomenclatoare noi sau alte dispoziții, iar acele instituții care aleg să îl folosească au siguranța actualizării informațiilor referitoare la raportările DRG. Informațiile sunt disponibile în timp real și pot fi analizate imediat, atât prin intermediul mecanismelor de analiză, audit și validare, cât și prin intermediul operatorilor CNAM.
Modulul preia informațiile, le validează și le introduce imediat în sistem. Datele despre pacient fiind de ultima ora, iar modificările asupra oricărui element care are legătura cu diagnosticul acestuia sunt trecute prin filtrele de validare; aceasta înseamnă că sistemul este capabil să calculeze imediat valoarea de complexitate a cazului tratat. Modul prenotat are capacitatea de a trece în analiza sau chiar să elimine activitățile suspecte sau lipsite de fond.

Modulul are și rolul de a elimina necesitatea spitalelor de a testa nenumărate programe informatice care generează rapoartele și care de multe ori au rezultate nesatisfăcătoare. Existența unui sistem informatic național dedicat acestui tip de raportare realizează o unificare și un control deosebit, ceea ce permite operatorilor generarea de rapoarte și identificarea prin auditare a zonelor sensibile din punct de vedere financiar.

Se elimină astfel obligativitatea existenței unui mecanism terțiar [de tip „3rd party”] la nivelul spitalelor pe care unele spitale îl utilizează în vederea raportării către CNAM. Aflat la dispoziția oricărui spital, DRG permite lucrul în timp real și la un înalt nivel de securitate, direct spre baza de date a CNAM.

Operațional, prin punerea la dispoziția personalului medical a unei interfețe de lucru în vederea acestui tip de raportare medicală cu puternice implicații financiare, sunt premisele unei colaborări eficiente inter / intra departamentale medical-administrativ cât și între spitale care sunt interesate să își modeleze activitatea în așa fel încât să eficientizeze activitatea.

Alegerea modului în care sunt efectuate raportările către CNAM este opțiunea instituțiilor medicale: acestea pot folosi fie modulul de colectare date Real Time sau software-ul intern și apoi mecanismul de transfer al rapoartelor real-time prin sistemul colector.

Modulul de nerepudiere

Modulul de nerepudiere are un rol important din punct de vedere al auditării: acest modul garantează pentru toți utilizatorii sistemului ca operarea se execută în mod unic și că nici un utilizator nu poate nega acțiunile legate de sistem.

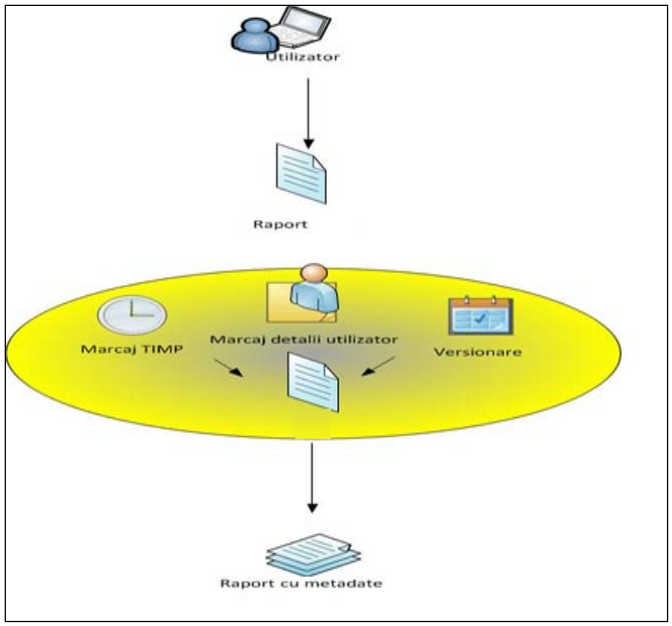


Figura 5. Modulul de nerepudiere

Fiecare utilizator este unic în sistem, lucru verificabil prin intermediul modulului de autentificare. Modulul de nerepudiere se referă la faptul că acțiunile pe care le efectuează un utilizator nu pot fi negate de acesta, deoarece fiecare acțiune are directă corespondență cu un utilizator. Orice fișier transferat de către un utilizator primește prin intermediul acestui modul un pachet de metadate care conține:

- ✓ Data și ora la care au fost transmise fișierele către sistem;
- ✓ Numele utilizatorului care a transmis fișierul; pentru fiecare fișier în parte se atașează metadatele corespunzătoare. Sistemul face automat asocierea între utilizator și fișierul transmis.
- ✓ Numele utilizatorului care a rescris ultima versiune a fișierului – va fi stabilit în faza de analiză, în funcție de particularitățile observate;

Aceste informații sunt disponibile atât administratorilor și, parțial, utilizatorilor. Adăugarea metadatelor la fișiere este o operațiune pe care modulul de nerepudiere o execută în mod automat și independent de opțiunile utilizatorilor. Orice raport transmis către sistem este însoțit de elemente de identificare unice: data, ora, nume utilizator etc. În cazul auditării sistemului, sunt disponibile date referitoare la acțiunile fiecărui utilizator, corelate integral cu informațiile introduse în sistem.

Modulul de validare

DRG reduce situațiile în care utilizatorii trimit setul minim de date la nivel de pacient al căror format este necorespunzător.

- Modulul de validare operează în mod minimal fișierele transmise (setul minim de date la nivel de pacient) și le acceptă doar pe cele care se încadrează în formatul dorit de către CNAM;
- Modulul de validare verifică, de asemenea, existența metadatelor de corespondența între utilizator și fișier înainte de trecerea în sistem a fișierelor al căror conținut îl constituie rapoartele. În cazul în care apar neconcordanțe între ceea ce așteaptă sistemul și ceea ce livrează utilizatorii, se trimit alerte către „Modulul de notificare, raportare și audit" care prelucrează situațiile în mod corespunzător, în sensul aducerii la forma standard a raportărilor.
- Modulul de validare este ultima componentă a sistemului care decide automat dacă un raport este valid sau nu; atenția acordată acestui modul este ridicată iar analiza situațiilor neconforme și alinierea acestora sunt urmărite permanent.
- Modulul de validare are capacitatea de a trata cât mai multe situații comune și elimina la timp cât mai multe cazuri în care apare eroarea umană.

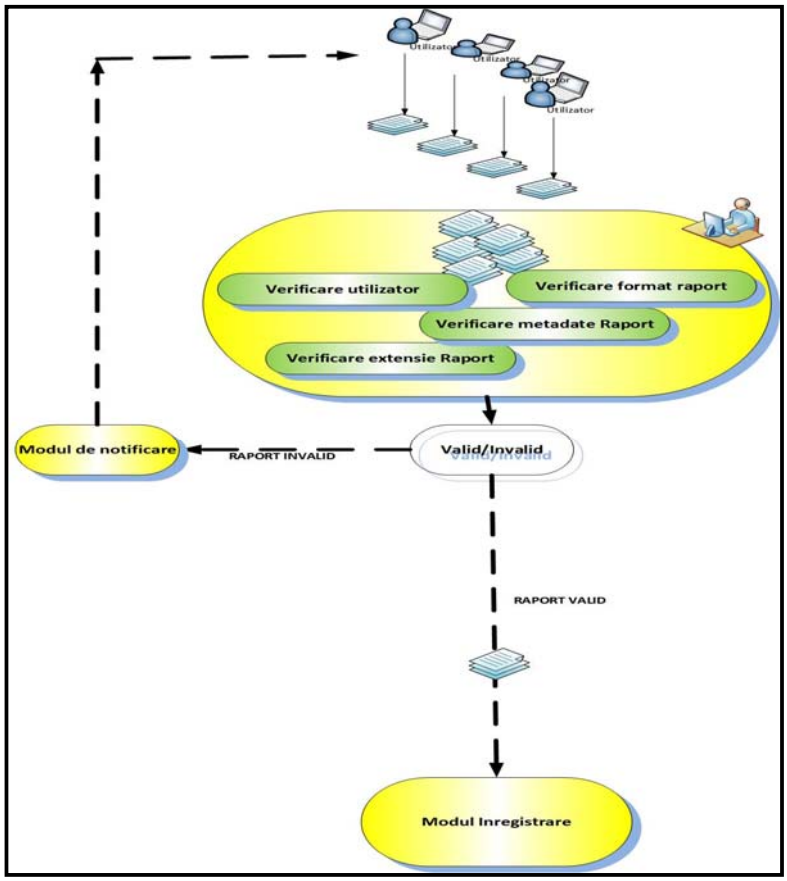


Figura 6. Schema Modulului de Validare

Modulul de înregistrare raportări

Modulul de înregistrare raportări este responsabil de depozitarea corectă a raportărilor trimise de către instituțiile medicale, în vederea transferului acestora către modulul depozit (data warehouse).

Modulul de înregistrare a raportări conține două componente:

1. Componenta „buffer", temporară, care colectează toate raportările utilizatorilor în toate versiunile pe care aceștia le transmit în intervalul alocat; această componentă dispune de un mecanism de ordonare care permite automatizarea procesului de transfer al versiunilor finale fără intervenția administratorilor sau a utilizatorilor. Componenta „buffer" are rolul de a colecta și organiza rapoartele trimise de către utilizatori în mod unic, astfel încât nu există pentru o instituție medicală rapoarte dublate.

2. Componenta „transfer" golește „bufferul" în momentul expirării termenului de transmitere a raportărilor și le mută în zona de depozitare a rapoartelor – forma definitivă, prelucrabilă – numita Modul Warehouse.

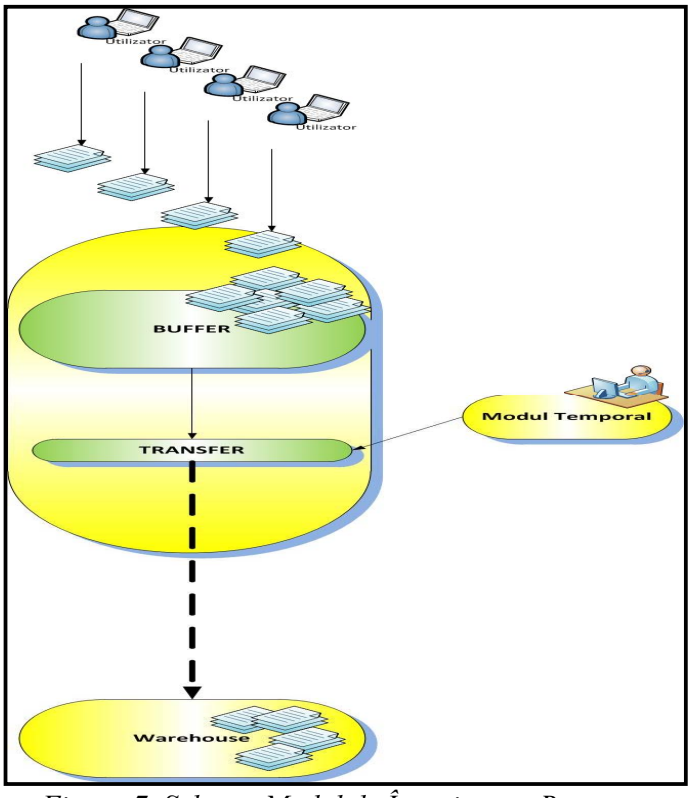


Figura 7. Schema Modul de Înregistrare Rapoarte

Informațiile de interes se limitează doar la ultimele versiuni ale raportărilor transmise:

- „Bufferul" permite unele modificări controlate de administratori asupra raportărilor în intervalul configurat în modulul de control temporal. La cerere administratorii de sistem pot vedea la nivel de *nume_raport* existența rapoartelor în buffer.

- „Transfer" acționează în mod programat, după expirarea termenului în care le este permis utilizatorilor să transmită raportările. Codul aplicației conține legătura directă între Modulul de Înregistrare și Modulul de control temporal.

Modulul de setări, raportare și audit

Modulul îndeplinește trei funcții: Setări, Raportare și Audit privind situația raportărilor din intervalul curent de timp în care este deschisă sesiunea de transfer a datelor. Fiecare dintre acestea este importantă la nivelul sistemului pentru că menține o comunicare permanenta între utilizatori, beneficiari și entitatea informatică:

✓ **Setări:** aceasta funcție a modulului este accesibila unui număr mic de utilizatori – administratori pentru introducerea datelor (inclusiv de autentificare) la nivel de CNAM și la nivel de instituție medicală. În cazul, în care modulul acționează în mod corect informațiile colectate și transmise sunt corecte și definesc informațiile ce pot afecta direct toate celelalte informații din baza de date.

✓ **Raportare:** aceasta funcție a modulului executa rapoarte în mod programat privind utilizarea sistemului.

✓ **Audit:** aceasta funcție a modulului identifică acțiunile desfășurate de către un utilizator, în mod cronologic; în cazul apariției unei probleme, la nivel de administrator de sistem, se poate vedea istoricul operațiilor desfășurate de orice utilizator în vederea

identificării și corectării problemei. Sunt vizibile atât informațiile referitoare la logarile în sistem cât și cele referitoare la fișierele cu care utilizatorul a operat. Funcția de audit folosește în mod implicit modulul de nerepudiere care asigura orice investigație ca datele existente în sistem sunt cele corecte și ca asocierea între conținutul informatic și activitatea umană este incontestabilă.

Modulul Depozit (Warehouse)

În cadrul fluxului de colectare de către sistem a raportărilor de la instituțiile medicale, Modulul Depozit (warehouse) este componenta finală, cea care deține datele necesare prelucrării. Aici se găsesc informațiile utile Beneficiarului, motiv pentru care acestea:

- ✓ sunt organizate într-o structură ierarhică care permite identificarea rapida a unui raport provenit de la orice instituție medicală la un anumit moment.
- ✓ conțin informațiile organizate într-o manieră care permite managementul rapoartelor fără a afecta conținutul acestora: există posibilitatea mutării datelor într-o arhivă; acest tip de operație necesită o analiză a graficului de încărcare a rapoartelor.
- ✓ modulul warehouse beneficiază de un spațiu de stocare protejat conform normelor de securitate ale Beneficiarului. Spațiul de stocare folosit de Modulul warehouse poate fi supus și altor cerințe de securitate decât cele ale sistemului implementat, în funcție de necesitățile beneficiarului: de ex. audit de urgență, investigații etc.
- ✓ Întreg spațiul alocat depozitarii rapoartelor este supus procedurilor de back-up.

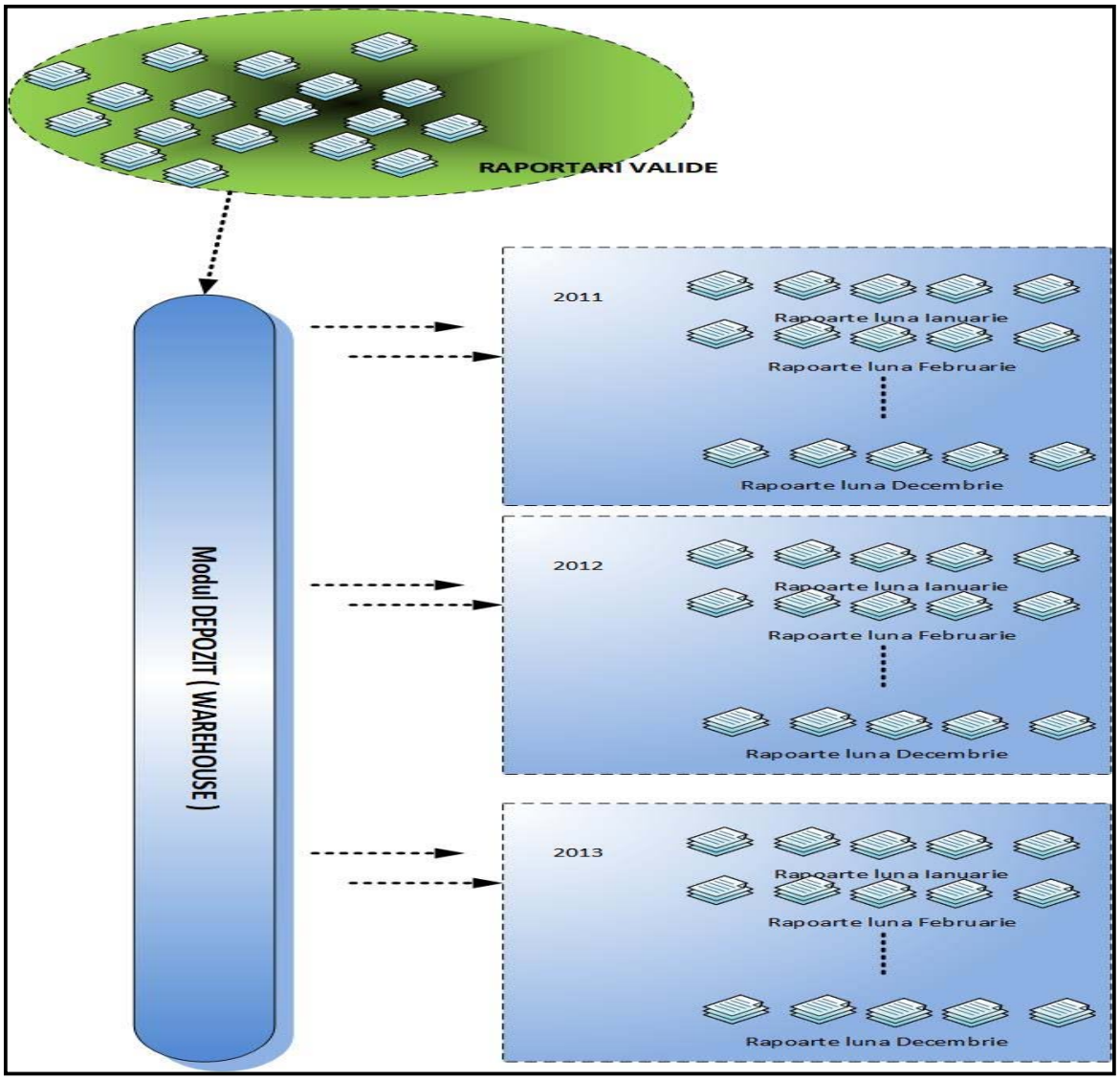


Figura 8. Schema Modul Depozit Rapoarte DRG (Warehouse)

Zona de stocare a Modulului Depozit (warehouse) poate fi controlată atât de administratorii sistemului DRG cât și de inginerii de sistem informatic MCloud.

Modulul de Analiză la nivel de Baza de Date

Sistemul DRG creează în mod dinamic o bază de date updatată permanent, cu informații consistente; sistemul este un instrument performant de interogare care permite extragerea de rapoarte necesare CNAM și MS, oferind o imagine clară a istoricului diagnosticelor pacienților; pe baza acestora se pot identifica eventualele neconcordante ulterioare în diagnosticarea pacientului.

Prin interogarea bazei de date temporare, în care sunt depozitate rapoartele trimise în vederea validării și închiderii, se pot obține statistici în timp real. Odată ce perioada de raportare este încheiată, baza de date Warehouse conține informațiile corecte și complete ale perioadei anterioare.

Modulul de analiza, raportare și audit poate fi utilizat de departamentele autorizate ale CNAM în vederea generării de rapoarte bazate pe template-uri, dar și ad-hoc, utile în activitatea curenta. Sistemul răspunde următoarelor solicitări:

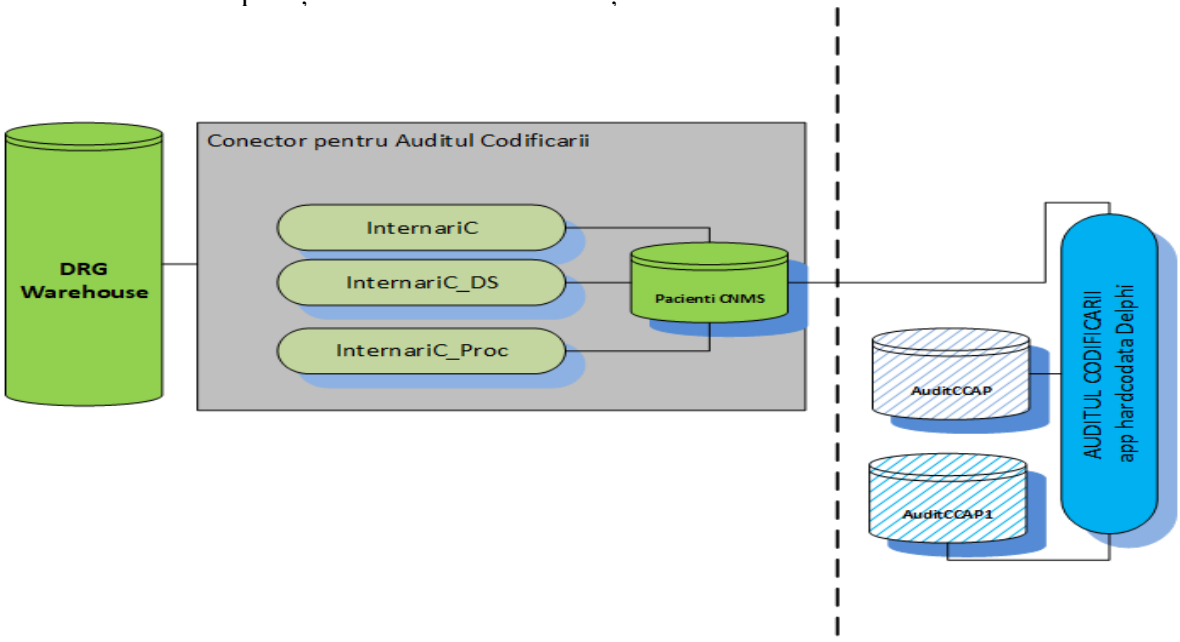
1) Evitarea fraudării. Sistemul SI DRG este un sistem operațional la nivel național, iar CNAM dispune de o baza de date unică, cu informații reale; veridicitatea informațiilor se verifica in doua feluri:

- în timp real: respingerea informațiilor eronate cu atenționarea celui care introduce datele; sistemul nu permite introducerea de date necorespunzătoare.
- în urma auditării: personalul CNAM poate genera rapoarte de audit și control prin care sunt identificate cazurile suspecte; aceste rapoarte pot fi organizate în template-uri pentru a fi reutilizate, dar pot fi customizate în așa fel încât echipele care executa auditarea și evaluare să obțină o lista consistentă și reală pe care sa o verifice și în teren. Prin utilizarea sistemului informatic pot fi identificate cazurile de fraudare.

2) Creșterea eficientei. Existenta modulului de analiză, raportare și audit la nivelul CNAM constituie un instrument pe care departamentele autorizate CNAM implicate în raportare îl folosesc în vederea creșterii eficientei de lucru. Căutările sunt rapide, rapoartele sunt generate cu mare ușurința în ciuda complexității deosebite a sistemului. Prin monitorizarea permanentă și corecția raportărilor se elimină cazurile în care spitalele execută raportări care necesită reanalizare și reverificare de către CNAM. Informațiile sunt corecte, validate și disponibile în timp real.

Modulul conector pentru Audit al codificării

Funcționalitatea de audit a codificării este acoperită de o aplicație pentru care CNAM nu deține codul sursa. Cea mai mare parte din informațiile prelucrate de către aplicația de Audit al codificării se găsesc actualizate în timp real în CCAP. În lipsa codului sursă, dezvoltatorii CCAP au reușit să atingă o parte din obiectivele funcționale ale operatorilor care executî auditul codificării prin operațiuni care nu afectează aplicația ci doar baza de date. Astfel operatorii Autorității Contractante care efectuează auditul codificării continuă să folosească vechea aplicație hardcodata care folosește date din warehouse-ul DRG.



CNAM va continua să emită fie solicitări de dezvoltare a sistemului CCAP, fie de execuție a unor proceduri la nivelul bazelor de date și conectorilor în scopul obținerii rezultatelor dorite pană la momentul includerii definitive în CCAP a funcționalităților de audit al codificării. În prezenta procedura de achiziție CNAM solicită operațiuni de mentenanță care se referă exclusiv la funcționalitățile asupra cărora deține codul sursă, urmand ca pe parcursul dezvoltării funcționalităților în cadrul CCAP, aria de mentenanță să se extindă corespunzător. Astfel, CNAM solicită analiza compartimentului

Menu=>„Rapoarte audit” privind verificarea corectitudinii regrupării cazurilor supuse auditului codificării.

Codul dezvoltat în sensul susținerii modului de conectare pentru auditul codificării permite operatorilor de audit să desfășoare în cadrul vechii aplicații două operațiuni:

- **Selectarea fișelor medicale a bolnavului spitalizat pentru audit (Database DRG).**
- **Importul fișelor medicale din "Database DRG" în aplicație și efectuarea auditului.**

CNAM deține codul sursa necesar pentru prelucrarea noii baze de date **Pacienți CNMS** și asupra **view-rilor de internări** [InternariC, InternariC_DS, InternariC_Proc] și **ListaSpitale**, care colectează și interpretează informațiile din baza de date Wodehouse a DRG, acestea intrând în obiectul operațiunilor de mentenanță pe care urmează să le desfășoare furnizorul serviciilor.

În prezent, la procedura de audit al codificarii prin intermediul aplicatiei CCAP nu este posibilă logarea/autentificarea concominentă a Auditorilor I/II în aplicaţie şi ca urmare nu este posibilă analiza concomitentă/independentă de către Auditor I și Auditor II a fișelor supuse auditului. În acest context, CNAM solicită analiza subiectului prenotat, şi ajustarea compartimentului conform solicitării. Totodată, CNAM subliniază faptul ca, în cazul în care nu este posibilă ajustarea propriu-zisă a conexiunii concomitente în CCAP, CNAM solicită reingineria modulului de audit al codificării în SI DRG.

A. Cerințe de Mentenanță preventivă și Suport

Cerinţele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanţă elaborat de Prestator şi aprobat de Beneficiar.

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanță sistemului DRG, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Actualizarea parametrilor existenți în partea utilizatorilor, conform cerințelor legislației în vigoare (spre exemplu: actualizarea/completarea nomenclatoarelor programelor special, diagnosticelor, procedurilor, spitalelor, rapoartelor, modificarea valorilor relative, aplicarea/anularea aplicării KP, completarea/modificarea algoritmelor de validare și excepțiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora,

conform formatului solicitat și menținerea posibilităților de extragere a datelor de către utilizator.

- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;
- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație pentru utilizatori:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM;
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistența tehnică pentru utilizatorii CNAM prin email și platforma Service Desk pusă la dispoziție de către Furnizor;
- Modalități de asigurare a suportului: email, telefon, acces la distanță;
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare - best effort.

Suport platforma software

Servicii dedicate Sistemelor de Operare

În această categorie se includ următoarele servicii minime relative de administrare şi mentenanță a sistemelor de operare ale SI DRG care vor fi desfășurate de către Furnizor:

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifestă transparent și înlăturarea cauzelor care le-au produs sau recomandarea măsurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- optimizarea configuratiei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanta și disponibilitate a sistemului;
- asigurarea funcționării continue a conectorilor;
- migrarea cazurilor medicale pe perioade definite de timp prin web-servicii pentru instituții medicale cu sisteme informatice proprii;
- mapare câmpuri, import cazuri medicale pe perioade definite de timp prin web-servicii instituții medicale cu sisteme informatice proprii.

Servicii dedicate sistemelor de gestiune a bazelor de date

În această categorie întra următoarele servicii minime relative la Microsoft SQL Server ale DRG care vor fi desfășurate de către Furnizor:

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corecta a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidenţialităţii şi securităţii datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerinţelor de securitate informaţională de către utilizatori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securităţii privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale DRG şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum şi restaurarea acestora.
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

Servicii dedicate componentelor, inclusiv a celor de interoperabilitate

În această categorie întră următoarele servicii minime relative la codul aplicației DRG care vor fi desfășurate de către Furnizor:

- verifică și optimizează secvențele de cod;
- identifică și analizează problemele și potențialele probleme de la nivelul codului;
- rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației;
- soluționează incidentele apărute la nivelul codului;
- modifică rapoartele, șabloanele, serviciile aplicative;
- comunică cu echipele de suport în scopul funcționarii corecte și permanente a sistemului.

Efectuarea testelor de penetrare

Teste de penetrare se referă la o metodă de evaluare a securității sistemului informațional prin simularea unor atacuri cibernetice. Scopul acestor teste este de a identifica și exploata vulnerabilitățile sistemului pentru a evalua cât de bine poate rezista sistemul informațional la atacuri reale. În această categorie întră următoarele servicii minime:

- Simulare a atacurilor;
- Identificarea vulnerabilităților;
- Evaluarea impactului;
- Raportare și recomandări.

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice DRG

DRG este un sistem automatizat care operează în condițiile legislației în vigoare. Prin serviciile prestate, ofertantul va asigura operațiuni de întreținere, suport și recomandări tehnice asupra aplicației, inclusiv în situația modificărilor legislative care afectează componentele software existente în DRG. CNAM precizează că modificarea funcționalităților existente în aplicație în corelație cu modificările legislative presupun în mod concret modificări în codul sursă al aplicației.

Orice modificare asupra codului sursa are ca efect o nouă versiune operațională a aplicației, conforma legislației. CNAM solicită ofertantului asumarea faptului că deține cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toată perioada desfășurării contractului.

Operațiunile tehnice de întreținere ce vor fi desfășurate de personalul care va asigura funcționarea continuă a DRG se referă la componentele majore ale sistemului, adică la:

- ✓ Interfața DRG prin care instituțiile medicale introduc datele;
- ✓ Conectorii de tip „web-services” cu instituțiile medicale care au propriile sisteme informatice;
- ✓ Regulile de validare a raportărilor. Tratarea excepțiilor;
- ✓ Bazele de date ale sistemului – servicii de întreținere;
- ✓ Rapoarte CNAM.

Pe lângă strânsă comunicare tehnică pe care echipa tehnică de suport aplicativ și platforma trebuie sa o aibă cu specialiștii M-Cloud, au fost identificate, fără a ne limita la acestea, următoarele operațiuni specifice care fac obiectul serviciilor de întreținere și suport specifice DRG:

Reguli de Validare

- ➢ Întreținerea modului de validare, a regulilor definite, conexiunilor cu baza de date și operațiuni de securitate specifice modulului.
- ➢ Actualizarea nomenclatoarelor DRG: Program Special, Diagnostice, Proceduri, Categorii Asigurat, Lista Spitale, KP, Criterii de Validare, etc.
- ➢ Modificarea criteriilor/regulilor de validare. Tratarea excepțiilor pentru criteriile de validare.
- ➢ Analize de impact pentru modificarea criteriilor/regulilor de validare la cerere. Recomandări și corectare situații neconforme.
- ➢ Actualizarea metodei de configurare a secțiilor. Păstrarea ID-urilor unice.

Întreținerea bazei de date a sistemului

- ➢ Operațiuni de administrare și optimizare a bazei de date pe infrastructura existentă.
- ➢ Operațiuni de migrare pe alte servere ale Beneficiarului care nu presupun modificarea arhitecturii sistemului.
- ➢ Operațiuni de întreținere a securității bazei de date.

- Operațiuni de analiza și auditare a securității bazei de date.

Rapoarte CNAM

- Generarea programată a rapoartelor.
- Îmbunătățirea, ajustarea și completarea rapoartelor CNAM. Raport complex, intern, etc.
- Implementarea restricțiilor CNAM: obligativitate câmpuri în dependența cu datele completate, eliminare cazuri medicale dublate, diagnostice secundare, proceduri secundare, etc.

B. Cerințe de mentenanță adaptivă şi corectivă a DRG

Asumarea contextului adaptării şi corecţiei software

În categoria serviciilor de mentenanță adaptivă şi corectivă a DRG intră acele servicii necesare pentru adaptarea şi corecţia sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul ”A. Cerințe de Mentenanță preventivă și Suport”.

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

- Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.
- Asumarea serviciilor din acest proiect implica acordarea garanției asupra DRG pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.
- În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.
- În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la DRG, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de DRG.
- Furnizorul este responsabil pentru eventualele incidente asupra DRG generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.
- Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.

➢ În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.

➢ Ofertanții trebuie sa demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport şi menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.

➢ Cererile de ajustări au termene relativ scurte și survin în general în urma unor modificări legislative sau în urma îmbunătățirilor funcționării business-proceselor. CNAM a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Pentru buna desfășurare a operațiunilor, dar și de consultanță în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnică a Furnizorului trebuie să fie pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și să dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului ajustărilor care sunt propuse de Beneficiar sau care sunt necesare în așa fel încât să asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie ajustări.

CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 900 de om/ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a DRG cum ar fi: ajustarea unor module ale DRG, ajustarea compartimentului Rapoarte, de asemenea, dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, etc. Rezervarea a 900 de om/ore la un preț prestabilit creează CNAM avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale DRG și asigură continuitatea serviciului în situațiile urgente.**

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

Serviciile de mentenanță adaptivă şi corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

Solicitarea serviciilor de mentenanță adaptivă şi corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului și a costului estimativ conform tarifelor.

Prestarea serviciilor de mentenanță adaptivă şi corectivă

Prestarea serviciilor de mentenanță adaptivă şi corectivă se va efectua cu aplicarea următoarelor reguli:

➢ Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului și acceptării rezultatului de către Beneficiar.

➢ Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.

➢ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condiţiile iniţiale ale solicitării (formularea problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.

➢ Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ţinînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.

➢ Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor și condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

DRG este găzduit în MCloud-ul guvernamental. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a Beneficiarului. Toate operațiunile se vor desfășura în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

➢ Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental

➢ Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.

➢ Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client "Hot-Line"

Suportul operaţional la utilizarea serviciilor este asigurat de către Prestator prin intermediul Serviciului de Suport Client "Hot-Line" (în continuare SSC) cu oferirea unei platforme de Service Desk. Beneficiarul va contacta SSC, prin întocmirea Cererilor, în următoarele scopuri:

➢ pentru soluționarea defectelor;

➢ pentru solicitarea modificărilor funcționalităților existente;

➢ pentru solicitarea informației şi consultanței în vederea soluționării defectelor legate de utilizarea sistemului;

➢ pentru solicitarea realizării anumitor activităţi şi acţiuni ce sunt în responsabilitatea Prestatorului;

➢ pentru solicitarea analizei unei solicitări de modificare.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități:

➢ expedierea unui e-mail la adresa SSC;

➢ efectuarea unui apel telefonic;

➢ crearea unui ticket în platforma de Service Desk.

Orice defect sau necesitate apărută la utilizarea serviciilor, Beneficiarul o va adresa inițial către SSC. În caz de necesitate, problema poate fi ulterior escaladată către Managerul de Proiect sau conducătorul Prestatorului. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului şi Beneficiarului, pentru a gestiona orice aspect ivit în relaţiile dintre aceştia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul.

Reguli privind prestare a serviciilor de suport

Serviciile de suport sunt orientate soluţionării incidentelor şi problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor şi actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul şi Beneficiarul vor conlucra strîns în vederea prevenirii incidentelor şi în vederea soluţionării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul şi prioritatea acordată pentru soluţionarea unui incident va ţine cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecinţele acestuia asupra disponibilităţii şi performanţei softului aplicativ. Urgenţa incidentului caracterizează operativitatea cu care acesta trebuie soluţionat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare şi soluţionare a incidentelor va fi în funcţie de impactul şi urgenţa incidentului. Algoritmul aplicat pentru stabilirea priorităţii unui incident este definit în continuare.

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

PRIORITATE		**Impact**		
		Înalt	*Mediu*	*Jos*
Urgenţă	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENŢĂ	**Descriere**
Înaltă	Un incident este estimat ca avînd nivelul urgenţei „Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activităţi şi operaţiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacţiunea imediată poate preveni riscuri legale majore şi de securitate (protecţie) a informaţiei.
Medie	Un incident este estimat ca avînd nivelul urgenţei „Mediu” în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activităţi şi operaţiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacţia operativă poate preveni riscuri legale moderate şi de securitate a informaţiei.
Joasă	Un incident este estimat ca avînd nivelul urgenţei „Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puţin în timp; - activităţile şi operaţiunile afectate nu trebuie continuate imediat; - nu există riscuri legale şi de securitate a informaţiei semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	**Descriere**
Înalt	Un incident este estimat ca avînd nivelul impactului „Înalt” în una sau mai multe din următoarele cazuri: - activităţile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizaţiei Beneficiarului şi afectează utilizatori

	externi, reputaţia şi imaginea Beneficiarului; - există riscuri legale şi financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca avînd nivelul impactului „Major" în una sau mai multe din următoarele cazuri: - activităţile importante ale Beneficiarului sunt întrerupte sau activităţile cheie sunt desfăşurate cu dificultate; - incidentul a afectat utilizatori interni şi un număr nesemnificativ de utilizatori externi; - există riscuri legale şi financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca avînd nivelul impactului „Jos" în una sau mai multe din următoarele cazuri: - activităţile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activităţile importante sunt desfăşurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru (8:00 – 17:00). În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort".

Prioritate incident	**Timpul de reacţie**	**Timpul de soluţionare**	**Timp maxim pentru corectare a cauzei***	**Raportare primară**
Critică	Timpul de reacţie al Prestatorului – imediat	pînă la 3 ore	8 ore	SSC (în afara orelor de lucru – Manager de Proiect)
Înaltă	Timpul de reacţie al Prestatorului – 15 minute	8 ore	ora 12 a zilei următoare	SSC (în afara orelor de lucru – Manager de Proiect)
Medie	Timpul de reacţie al Prestatorului – 4 ore	24 ore	5 zile	SSC (în afara orelor de lucru – Manager de Proiect)
Joasă	Timpul de reacţie al Prestatorului – 24 ore;	3 zile	10 zile	SSC
Neglijabilă	Timpul de reacţie al Prestatorului – 72 ore;	Cel mai bun efort	-	SSC

***Notă:** se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.*

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergenţe apărute între Părţi vor fi soluţionate cu efort comun şi prin strînsă conlucrare între Părţi. În acest scop, vor fi aplicate următoarele reguli:

- Părţile vor forma un grup comun de lucru în scopul soluţionării divergenţelor. De comun acord, în grupul de lucru pot fi acceptaţi reprezentanţi ai părţilor terţe, inclusiv experţi independenţi.
- La necesitate, părţile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergenţă.
- Grupul de lucru se va convoca şi va examina subiectul divergenţelor şi probele existente la subiect. Părţile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluţii echitabile pentru divergenţele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Prestatorul este responsabil pentru securitatea tehnologică şi funcţională a softului aplicativ în limitele sarcinilor de mentenanţă îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informaţiei, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părţile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;
- Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

După soluţionarea unui incident de securitate, părţile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acţiuni pentru prevenirea repetării incidentelor similare.

Livrabile

Prestatorul menține în stare actuală documentația tehnică. Documentaţia conţine suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni şi modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.

La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:

- Codul sursă final compilabil pe suport (DVD-R sau USB);
- Documentația tehnică;
- Ghidul utilizatorilor;
- Ghidul administratorului;
- Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Cerințe privind experiența personalului

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.

În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente mentenanței, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini și doar în baza acceptului Beneficiarului.

Ofertantul este obligat să informeze în prealabil Beneficiarul despre necesitatea modificării echipei de mentenanță, va transmite CV-ul persoanei care înlocuiește și va confirma recepționarea răspunsului (de acceptare sau refuz) expediat de către Beneficiar. Beneficiarul își rezervă dreptul de a refuza modificarea componenței minime a echipei în cazul în care pregătirea profesională și experiența noilor membri nu corespunde cerințelor stabilite în prezent caiet de sarcini sau solicitarea privind modificarea echipei nu este relevantă.

CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.
- Deținerea certificatului Project Manager sau documentului analogic de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor și/sau emis de o instituție publică sau privată competentă cu recunoaștere generală.
- Minim 3 ani de experiență în managementul proiectelor în domeniul tehnologiilor informaționale.
- Minim 3 proiecte în domeniul tehnologiilor informaționale realizate în calitate de Manager de proiect.
- Minim 3 ani de experiență în utilizarea metodologiilor de management de proiecte recunoscute pe plan internațional.
- Experiență specifică de Manager de Proiect în cel puțin 3 proiecte de complexitate similară, pe toată durata proiectului, realizate cu succes.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Business Analist *(minim 1 persoană)*

- Studii superioare în domeniul ingineriei sau tehnologiilor informaționale confirmate prin diploma de absolvire.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Cel puțin 3 ani de experiență în domeniul tehnologiilor informaționale.
- Cel puțin 3 ani de experiență în domeniul analizei și modelării Business-proceselor.
- Experiență profesională specifică, confirmată prin participarea în cel puțin 3 proiecte similare de implementare a unui sistem informatic integrat similar, în care el/ea s-a poziționat ca Business Analitic.
- Experiență în implementarea sistemelor informaționale complexe în instituțiile bugetare și/sau în domeniul medical.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist securitatea informațională (minim 1 persoană)

- Studii superioare Tehnice sau în domeniul TI.
- Cunoștințe privind securitatea sistemelor informatice și securitatea sistemelor ce conțin informații cu caracter personal, dovedite prin diplome/certificate obținute.
- Cunoștințe privind auditul sistemelor informatice dovedite prin diplome/certificate obținute (ISO27001, CISA sau echivalent*).
- Experiență de cel puțin 3 ani în domeniul securității sistemelor informatice.
- Participarea în ultimii 3 ani ca consultant sau auditor la cel puțin 3 contracte în domeniul securității informației.
- Participarea în cel puțin 3 contracte similare ca expert de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist infrastructură sistem (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență profesională generală în domeniul de specialitate de minim 3 ani;
- Experiență dobândită prin participarea în cel puțin 3 proiecte în activități IT complexe privind infrastructura software și hardware pe platforme în baza tehnologiei de „cloud computing"

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist programator (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență de minim 3 ani în programarea aplicațiilor web: Java, Java script, HTML, CSS, etc;
- Experiență dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de implementare a unui sistem informațional de complexitate similară

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist baze de date (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență de minim 3 ani în administrarea bazelor de date: MS SQL Server;
- Experiență dobândită prin participarea în calitate de specialist în baze de date în cel puțin 3 proiecte de implementare a unui sistem informatic de complexitate similară

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Software Tester (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Experiență demonstrată în testarea funcțională a sistemelor informaționale;
- Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale;
- Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din

partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Anexa nr.2

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **SIP**

CAIET DE SARCINI

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	Descriere
Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP: • *Servicii de mentenanță preventivă și Suport – în bază de abonament;* • *Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.*	*Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.*

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP (în continuare – SIP) pentru o perioadă de **minim 12 luni** după încetarea contractului.

De asemenea, Prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta CNAM (Beneficiar) împreună cu codul sursă DRG, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Descriere generală a SIP

SIP este destinat evidenței și raportării serviciilor medicale de înaltă performanța și urmărește automatizarea proceselor care au loc în activitatea prestatorilor de servicii medicale care se contractează după metoda "per serviciu", privind estimarea necesității de servicii medicale de înaltă performanță, posibilitatea de programare a persoanelor în IMS care prestează servicii medicale și evidența personificată a serviciilor medicale prestate. SIP oferă transparență în procesul de prestare a serviciilor medicale de înaltă performanta, astfel ca pacientul are dreptul de a alege la care prestator vrea să meargă pentru servicii medicale, iar modul în care sunt alocate aceste servicii este conform procedurilor CNAM.

Setul de date folosit în funcționalitatea sistemului cuprinde:

- IDNP al pacientului;
- IDNP al medicului prescriptor;
- IDNO prestatorului de servicii medicale în care activează medicul;
- Denumirea prestatorului de servicii medicale în care activează medicul;
- IDNO al prestatorului de servicii de înaltă performanță;
- Denumirea prestatorului de servicii de înaltă performanță;
- Data și ora trimiterii la serviciile medicale;
- Codul serviciilor medicale prescrise;
- Codul serviciilor medicale prestate;

- Denumirea deplină a serviciilor de înaltă performanță;
- Data și ora generării sloturilor pentru serviciile medicale;
- Data și ora efectuării programării serviciilor medicale;
- Data și ora prestării serviciilor medicale;
- Statutul/categoria serviciilor medicale
- Diagnosticul la trimitere (prin selectare din Lista Diagnosticelor);
- Numele și Prenumele Pacientului;
- Data nașterii;
- Adresa la domiciliu.

Beneficiarii direcți ai SIP sunt CNAM, pacientul asigurat, medic prescriptor (medic de familie sau medic specialist), prestator servicii medicale, care deține contract cu CNAM.

Specificații tehnice SIP

Caracteristici generale de funcționare

SIP are o arhitectură 3-layer, arhitectura care permite funcționarea pe platforma guvernamentală comună MCloud. SIP funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă tot ce este necesar de automatizat;
- are posibilitatea reparației unui modul fără afectarea altora;
- respecta standardele în vigoare a tehnologiilor informaționale;
- asigura flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare;
- utilizează o arhitectură orientată pe servicii pentru a acomoda cu ușurință noi modificări cu intervenții exclusiv asupra componentei de updatat, minimizând costurile și timpul necesar realizării modificărilor;
- are o arhitectură modernă cu un grad înalt de performanță, structurată pe 3 niveluri (nivelul pentru baze de date, nivelul pentru aplicație si nivelul acces/utilizator). Fiecare nivel are în componența toate echipamentele necesare bunei funcționări.
- SIP este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- poate fi utilizat împreună cu echipamente ce permit creșterea vitezei de înregistrare a datelor de identificare ale pacienților (nume, prenume, IDNP etc.)
- este scalabil pentru a acomoda modificările viitoare ale numărului de utilizatori ai soluției;
- recunoaște corect sursele informaționale, le acceptă și le integrează în sistem;
- întreține în limba de stat interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate;
- permite ca utilizatorul să se autentifice o singură data pentru a accesa toate modulele aplicației;
- Poate fi accesat de pe telefon, PC, notebook, etc.

Interfața Utilizator

Aceasta interfața este accesibilă pentru toți utilizatorii autorizați în SIP:

- ✓ SIP dispune de o interfață inteligenta, intuitiva și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browser-ul web și nu necesită instalarea de componente software suplimentare;

- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului
- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:

- **Platforma hardware**, formată din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat în sistemul MCloud:
  - Servere protejate redundant pentru hosting al bazelor de date, softului de sistem si softului funcțional (aplicații și subsisteme);
  - Platforma hardware pusă la dispoziție de către beneficiar este dimensionată corespunzător pentru a permite funcționarea în bune condiții a sistemului;
  - Performanța optimă, în limita normelor obiective de uzură, pentru realizarea structurii funcționale și asigurarea extinderii ulterioare a sistemului;
  - este flexibilă în utilizarea mijloacelor disponibile destinate recepționării informației din surse externe (alte instituții publice);
  - asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date;
  - asigură normele de funcționare ale platformelor informatice guvernamentale.

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:
  - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
  - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server.
  - Pe stațiile utilizatorilor există navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare si transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mijloacele de imprimare, cititoare, rețele electronice locale (LAN – local area network) și de scară largă (WAN – wide area network). Pentru operare se folosesc stațiile de lucru ale beneficiarului, singură specificație impusă utilizatorilor fiind cea de a dispune de un browser conectat la internet, fiind recomandate și utilizate soluțiile Microsoft.

Sistemul de securitate

SIP funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.

Caracteristici:

- asigura accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare si consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de sistem.
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor.

Având în vedere natura specială a informațiilor gestionate în cadrul SIP, acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.

Sistemul are următoarele nivele de securitate care asigura confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație intre stații si server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unica cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este asigurată automat, iar modificările de structura la nivelul acesteia se fac exclusiv în baza drepturilor corespunzătoare de administrator al bazei de date. În plus, baza de date deține propriul mecanism de backup care permite, în caz de dezastru, restaurarea unor versiuni anterioare recente (de ordinul zilelor).

Sistemul asigura dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori sunt create module de acces și autentificare în sistem; sunt indicate volumul de informație și funcționalitatea pe care aceștia o accesează. Sistemul permite accesul la datele statistice pentru anumiți utilizatori și grupuri de utilizatori. Sistemul asigură verificarea automată a drepturilor în momentul intrării în sistem și în ulterioarele accesări a sistemului și creează un jurnal al accesărilor – jurnalul de audit.

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Prestator/Prescriptor**: permite introducerea și modificarea datelor specifice activității sale;
- nivelul **Administrator**: permite înregistrarea și modificarea datelor specifice activității sale, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

La nivel aplicativ, sistemul generează o lista de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

- ✓ posibilitatea înregistrării, adăugării si dezactivării utilizatorilor din sistem;
- ✓ posibilitatea distribuției drepturilor utilizatorilor folosind grupuri de acces;
- ✓ posibilitatea pentru fiecare utilizator de a avea cel puțin următoarele atribute de autentificare: identificarea, autentificarea.
- ✓ posibilitatea intrării în sistem a unui utilizator în orice moment;
- ✓ asigurarea de către administrator a regimurilor de funcționare, deconectare, conectare, modificării regimului de autentificare și identificare, dirijarea cu drepturi și auditul.

Retenția datelor, acces securizat

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.

- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respecta regulile de control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.

- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.

- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați sa acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem si pe baza permisiunilor asociate rolului sau rolurilor din care fac parte utilizatorii.

- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați sa acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fisele electronice ale pacienților săi.

- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu ca a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:

  - Unicitatea utilizatorilor în sistem;

  - Mecanism de control al versiunilor pentru înregistrările medicale.

- **Securizarea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.

Arhitectura SIP

SIP are o arhitectură bazată pe tehnologie web, folosind platforma Microsoft/Linux Sistemul este conceput modular, dezvoltarea acestora putând fi realizata în paralel. Orice client se poate conecta la serverul de aplicație și poate utiliza sistemul conform drepturilor pe care le are. Comunicația între client și server se realizează exclusiv prin protocoale securizate de tip HTTPS folosind certificat de securitate integrat la nivelul serverului de aplicație. Schema arhitecturală este în figura următoare:

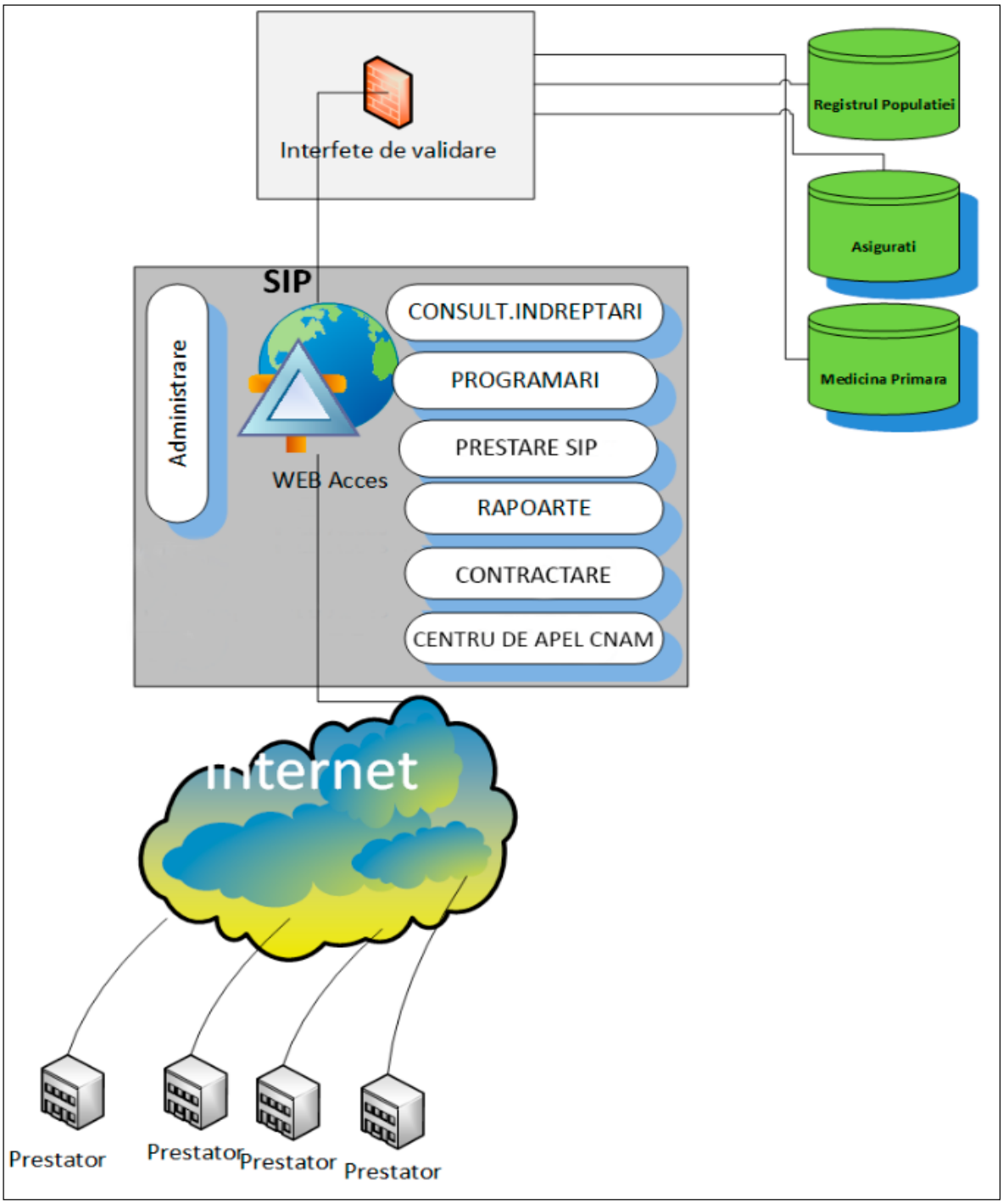


Figura 1. Schema arhitecturală SIP

Componente operaționale ale SIP sunt operaționale în următoarea structură modulară:

- ✓ Modulul de administrare roluri;
- ✓ Modulul consult/îndreptări (prescriere a biletului de trimitere);
- ✓ Modulul programări;
- ✓ Modulul prestare a serviciilor de înalta performanță;
- ✓ Modulul rapoarte;
- ✓ Modulul contractare;
- ✓ Interfețe.

Modulul de administrare roluri

Actorii implicați în circuitul informațional privind evidența serviciilor medicale de înaltă performanță sunt:

- Pacient asigurat;
- Administrator CNAM (administrare SIRSM);
- CNAM (responsabil CNAM);
- Medic prescriptor (medic de familie sau medic specialist);
- Prestator servicii medicale, care deține contract cu CNAM.

Administrarea sistemului informatic este realizată de către administratorul (reprezentantul) CNAM pentru partea de conținut a serviciilor medicale în colaborare cu Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) pentru partea de asistență și mijloacele tehnice necesare funcționării SIP extins în infrastructură hardware & software din cadrul MCloud.

Administratorul sistemului are acces deplin la toate funcționalitățile sistemului, fișiere și baze de date aferente sistemului, încăperile în care se află echipamentele pe care rulează aplicațiile software sau care asigură securitatea datelor.

Medicul prescriptor

În interfața de utilizare a sistemului medicul prescriptor (medic de familie sau specialist) are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului:

- Datele de identificare ale medicului de familie sau specialist cu drepturi de prescriere a serviciilor medicale;
- Adresa;
- IDNO al instituțiilor medicale în care medicul prestează servicii;
- Denumirea instituțiilor medicale în care medicul prestează servicii;
- Cod instituțiilor medicale în care medicul prestează servicii.

Pentru medicul de familie sau medicul specialist, interfața de utilizare a sistemului are o formă simplă care îi permite efectuarea rapida de prescriere, validare și programare servicii medicale a pacientului, după modelul descris în continuare.

Prestatorul de servicii medicale

În interfața de utilizare a sistemului, prestatorul de servicii medicale are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului, în directa corespondență cu contractul CNAM, pe care nu le poate modifica:

- IDNO al instituției prestatoare de servicii medicale;
- Adresa instituției;
- Numărul contractului;

- Lista de servicii medicale asumate pe grupuri și programe, inclusiv sumele contractuale specificate pentru perioadele pe care sunt programate aceste sume.

Pe lângă acestea, administratorul local al prestatorului are în cadrul interfeței:

- Câmpurile necesare definirii listei de servicii medicale ce pot fi executate;
- Opțiunile de alocare a serviciilor disponibile în lista pe sloturi libere (secvențe de timp);
- Posibilitatea de urmărire a atributelor la nivel de serviciu și slot.

Posibilitatea de urmărire a relației dintre serviciile medicale contractate și cele alocate în sloturi.

Modul consult/îndreptări

Modulul consult urmărește traseul prescrierii serviciului medical și programării pacientului la serviciile medicale de înaltă performanță. Sistemul dispune de mecanismele de restricție și control prin care acest flux va fi urmărit permanent:

- Pacientul se prezintă la medicul de familie sau la medicul specialist, unde prezintă datele de identificare. Identificatorul unic al pacientului este IDNP-ul.
- Medicul introduce în sistem IDNP-ul.
- Prin intermediul web-serviciilor sistemul verifica automat statutul de asigurat al pacientului și validează alocarea pacientului la medicul de familie care efectuează operațiunea curentă.
- Dacă asigurarea pacientului nu este validată de către sistem (pacientul nu are statut de asigurat), medicul nu poate prescrie biletul de trimitere. La fel, dacă sistemul nu confirmă că pacientul este alocat medicului de familie curent, atunci medicul nu poate îndrepta pacientul către servicii medicale.
- Scenariul favorabil pentru prescrierea biletului de trimitere la serviciul medical este cel în care pacientul este validat de sistem cu statut de asigurat și ulterior înregistrat la medicul de familie curent sau, în situații excepționale (concediu, boala) de înlocuitorul acestuia. În acest caz, medicul stabilește în baza consultului necesitatea unei investigații din lista de servicii medicale conform Programului.

Modul programări

Programarea efectivă a pacientului constă în alocarea unui slot (interval definit de timp în care un anumit serviciu este disponibil).

- Programarea pacientului la serviciul medical se bazează pe dreptul pacientului la libera alegere a prestatorului.
- Pacientul asigurat și înregistrat la medicul de familie care efectuează consultul are dreptul la servicii medicale plătite din fondul CNAM. Medicul de familie sau medicul specialist decid în baza consultului aceasta necesitate, iar sistemul emite un **cod unic al biletului de trimitere a pacientului către servicii medicale CNAM.**
- Codul unic al biletului de trimitere poate fi folosit în interesul pacientului în <u>următoarele</u> moduri:
  a) Medicul prescriptor se consultă cu pacientul în vederea programării în SIP a pacientului într-unul din sloturile libere declarate de către Prestatori, în funcție de distanța și disponibilitatea definite de Prescriptor.
  b) Pacientului îi este tipărit numărul de trimitere și detaliile consultului urmând sa își facă singur programarea la serviciul de înaltă performanță prin intermediul SIP.
  c) Pacientului îi este tipărit numărul de trimitere și detaliile consultului urmând să-și facă programarea prin intermediul Centrului de apel al CNAM.

Modulul prestare a serviciilor de înaltă performanță

Executarea efectivă a serviciilor de înaltă performanță este o operațiune a prestatorului care se încheie cu confirmarea prestării acestuia și completarea rezultatului. Prestarea se consideră încheiată doar în momentul în care pacientul are un rezultat în urma investigației.

- În interfața sistemului prestatorul declară sloturile libere pe grupe de servicii de înaltă performanță, în corespondență cu contractul CNAM. Aceste sloturi sunt completate automat în baza programărilor efectuate. Prestatorul are acces la datele de corespondență ale pacientului.
- După prezentarea pacientului pentru efectuarea investigației, prestatorul completează în sistem rezultatul și închide programarea.
- Pacientul primește rezultatul investigației în mod fizic (tipărit) și continuă investigațiile sau tratamentul la îndrumarea medicului care i-a prescris serviciul medical.
- Sistemul înregistrează încheierea prestării și confirmă CNAM că serviciul medical contractat de către prestator a fost prestat și ca poate fi plătit.

Modulul rapoarte

În cadrul interfeței de lucru sunt disponibile în timp real următoarele valori:

- Încărcarea prescriptorilor: în sistem sunt disponibile valorile per medic prescriptor. De asemenea în sistem apar valori adiacente: date despre prescrieri, prescriptor, pacient, servicii medicale etc. Sistemul poate folosi aceste informații în scop de analiză pentru realizarea de rapoarte statistice.
- Încărcarea prestatorilor: în sistem sunt disponibile listele de servicii medicale contractate, alocarea pe sloturi, executarea serviciilor de înaltă performanță în timp real în directă corespondență cu contractul CNAM.

Efectuarea programărilor. În sistem sunt disponibile în timp real toate informațiile despre programări, servicii medicale, prestatori, prescriptori și datele în corespondența cu contractul CNAM. În cadrul interfeței administratorul poate vedea efectuarea programărilor în timp real dar și pe intervale de timp definite ad-hoc.

Modulul contractare

În modulul contractare se înregistrează volumele contractuale în dependență de lista de servicii medicale, numărul de servicii, tarife, sumele contractate. În interfața acestui modul sunt disponibile următoarele funcționalități:

- Modificarea/actualizarea nomenclatorului serviciilor medicale din Anexa nr. 5 al PU (nr.de ordine, denumire serviciu, cod serviciu tarif serviciu) în dependență de modificare Programului Unic;
- Modificarea/actualizarea listei prestatorilor și prescriptorilor (denumire deplina și scurta a prestator/prescriptor, adresa/locația, IDNO, codul din 4 cifre);
- Introducerea și înregistrarea contractelor cu prestatorii în dependență de: număr contract, perioada de timp (lista serviciilor de înaltă performanță: nr.de ordine, denumire, cod, număr de servicii, tarif, sumă);
- Modificarea contractelor prin Acord adițional în dependență de: număr acord adițional, perioada de timp (lista serviciilor de înaltă performanță: nr.de ordine, denumire, cod, număr de servicii, tarif, sumă).

A. Cerințe de Mentenanță preventivă și Suport

Cerințele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se

manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanţă elaborat de Prestator şi aprobat de Beneficiar.

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanța SIP, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;
- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație pentru utilizatori:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM;
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistența tehnică pentru utilizatorii CNAM prin email și platforma Service Desk pusă la dispoziție de către Furnizor;
- Modalități de asigurare a suportului: email, telefon, acces la distanță;
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare - best effort.

Suport platforma software

Servicii dedicate Sistemelor de Operare

În aceasta categorie întră următoarele servicii minime relative la sistemele de operare pe care rulează SIP care vor fi desfășurate de către Furnizor:

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifesta transparent și înlăturarea cauzelor care le-au produs sau recomandarea masurilor ce trebuie luate pentru a nu mai apărea astfel de erori;

- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- creare și întreținere conturi de acces locale;
- optimizarea configuratei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanță și disponibilitate a sistemului.

Servicii dedicate sistemelor de gestiune a bazelor de date

În această categorie întră următoarele servicii minime relative la Microsoft SQL Server ale SIP care vor fi desfășurate de către Furnizor:

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corecta a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidenţialităţii şi securităţii datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerinţelor de securitate informaţională de către utilizatori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securităţii privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale SIP şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum şi restaurarea acestora.
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

Servicii dedicate componentelor, inclusiv a celor de interconectare

În această categorie întră următoarele servicii minime relative la codul SIP care vor fi desfășurate de către Furnizor:

- verifică și optimizează secvențele de cod;
- identifică și analizează problemele și potențialele probleme de la nivelul codului;
- rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației;
- soluționează incidentele apărute la nivelul codului;
- modifică rapoartele, șabloanele, serviciile aplicative;
- comunică cu echipele de suport în scopul funcționarii corecte și permanente a sistemului.

Efectuarea testelor de penetrare

Teste de penetrare se referă la o metodă de evaluare a securității sistemului informațional prin simularea unor atacuri cibernetice. Scopul acestor teste este de a identifica și exploata vulnerabilitățile sistemului pentru a evalua cât de bine poate rezista sistemul informațional la atacuri reale. În această categorie întră următoarele servicii minime:

- Simulare a atacurilor;
- Identificarea vulnerabilităților;
- Evaluarea impactului;
- Raportare și recomandări.

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice SIP

SIP este un sistem automatizat care operează în condițiile legislației în vigoare. Prin serviciile prestate, ofertantul va asigura operațiuni de întreținere, suport și recomandări tehnice asupra aplicației, inclusiv în situația modificărilor legislative care afectează componentele software existente în SIP. CNAM precizează că modificarea funcționalităților existente în aplicație în corelație cu modificările legislative presupun în mod concret modificări în codul sursa al aplicației.

Orice modificare asupra codului sursă are ca efect o noua versiune operațională a aplicației, conform legislației. CNAM solicită ofertantului asumarea faptului că, deține cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toata perioada desfășurării contractului.

Operațiunile tehnice de întreținere ce se vor desfășura de personalul care va asigura funcționarea continuă a SIP se referă la componentele majore ale sistemului, adică la:

- ✓ Interfața SIP prin care prescriptorii și prestatorii introduc datele;
- ✓ Bazele de date ale sistemului – servicii de întreținere;
- ✓ Rapoarte CNAM;

B. Cerințe de mentenanță adaptivă şi corectivă a SIP

Asumarea contextului adaptării şi corecţiei software

În categoria serviciilor de mentenanță adaptivă şi corectivă a SIP intră acele servicii necesare pentru adaptarea şi corecţia sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul ”A. Cerințe de Mentenanță preventivă și Suport”.

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

- Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației.

Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării

corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.

- Asumarea serviciilor din acest proiect implica acordarea garanției asupra SIP pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.
- În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.
- În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la SIP, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de SIP.
- Furnizorul este responsabil pentru eventualele incidente asupra SIP generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.
- Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.
- În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.
- Ofertanții trebuie sa demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport şi menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.
- Cererile de ajustări au termene relativ scurte și survin în general în urma unor modificări legislative sau în urma îmbunătățirilor funcționării business-proceselor. CNAM a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Pentru buna desfășurare a operațiunilor, dar și de consultanță în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnică a Furnizorului trebuie să fie pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și să dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului ajustărilor care sunt propuse de Beneficiar sau care sunt necesare în așa fel încât să asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie ajustări.

CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 900 de om/ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a SIP cum ar fi: ajustarea modulelor SIP, elaborarea modulului pentru Centrul de Apel „INFO CNAM”, , de asemenea, dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, etc. Rezervarea a 900 de om/ore la un preț prestabilit creează CNAM avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale SIP și asigură continuitatea serviciului în situațiile urgente.**

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

Serviciile de mentenanță adaptivă şi corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

Solicitarea serviciilor de mentenanță adaptivă şi corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului şi a costului estimativ conform tarifelor.

Prestarea serviciilor de mentenanță adaptivă şi corectivă

Prestarea serviciilor de mentenanță adaptivă şi corectivă se va efectua cu aplicarea următoarelor reguli:

- Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului şi acceptării rezultatului de către Beneficiar.
- Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.
- Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condiţiile iniţiale ale solicitării (formularea problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.
- Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ţinînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.
- Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor şi condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

SIP este găzduit în MCloud-ul guvernamental. În timpul desfăşurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului şi cea a Beneficiarului. Toate operațiunile se vor desfăşura în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar şi pentru operațiuni normale de întreținere:

- Intervenții de la distanță securizată. Se vor respecta recomandările specialiştilor cloud-ului guvernamental
- Intervenții tehnice şi recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.
- Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiştii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client "Hot-Line"

Suportul operaţional la utilizarea serviciilor este asigurat de către Prestator prin intermediul Serviciului de Suport Client "Hot-Line" (în continuare SSC) cu oferirea unei platforme de Service Desk. Beneficiarul va contacta SSC, prin întocmirea Cererilor, în următoarele scopuri:

- pentru soluționarea defectelor;
- pentru solicitarea modificărilor funcționalităților existente;
- pentru solicitarea informației şi consultanței în vederea soluționării defectelor legate de utilizarea sistemului;
- pentru solicitarea realizării anumitor activităţi şi acţiuni ce sunt în responsabilitatea Prestatorului;
- pentru solicitarea analizei unei solicitări de modificare.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități:

- expedierea unui e-mail la adresa SSC;
- efectuarea unui apel telefonic;
- crearea unui ticket în platforma de Service Desk.

Orice defect sau necesitate apărută la utilizarea serviciilor, Beneficiarul o va adresa inițial către SSC. În caz de necesitate, problema poate fi ulterior escaladată către Managerul de Proiect sau conducătorul Prestatorului. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului şi Beneficiarului, pentru a gestiona orice aspect ivit în relaţiile dintre aceştia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul.

Reguli privind prestare a serviciilor de suport

Serviciile de suport sunt orientate soluţionării incidentelor şi problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor şi actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul şi Beneficiarul vor conlucra strîns în vederea prevenirii incidentelor şi în vederea soluţionării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul şi prioritatea acordată pentru soluţionarea unui incident va ţine cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecinţele acestuia asupra disponibilităţii şi performanţei softului aplicativ. Urgenţa incidentului caracterizează operativitatea cu care acesta trebuie soluţionat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare şi soluţionare a incidentelor va fi în funcţie de impactul şi urgenţa incidentului. Algoritmul aplicat pentru stabilirea priorităţii unui incident este definit în continuare.

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

PRIORITATE		**Impact**		
		Înalt	*Mediu*	*Jos*
Urgenţă	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENȚĂ	Descriere
Înaltă	Un incident este estimat ca avînd nivelul urgenţei „Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activităţi şi operaţiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacţiunea imediată poate preveni riscuri legale majore şi de securitate (protecţie) a informaţiei.
Medie	Un incident este estimat ca avînd nivelul urgenţei „Mediu” în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activităţi şi operaţiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacţia operativă poate preveni riscuri legale moderate şi de securitate a informaţiei.
Joasă	Un incident este estimat ca avînd nivelul urgenţei „Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puţin în timp; - activităţile şi operaţiunile afectate nu trebuie continuate imediat; - nu există riscuri legale şi de securitate a informaţiei semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere
Înalt	Un incident este estimat ca avînd nivelul impactului „Înalt” în una sau mai multe din următoarele cazuri: - activităţile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizaţiei Beneficiarului şi afectează utilizatori externi, reputaţia şi imaginea Beneficiarului; - există riscuri legale şi financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca avînd nivelul impactului „Major” în una sau mai multe din următoarele cazuri: - activităţile importante ale Beneficiarului sunt întrerupte sau activităţile cheie sunt desfăşurate cu dificultate; - incidentul a afectat utilizatori interni şi un număr nesemnificativ de utilizatori externi; - există riscuri legale şi financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca avînd nivelul impactului „Jos” în una sau mai multe din următoarele cazuri: - activităţile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activităţile importante sunt desfăşurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru (8:00 – 17:00). În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort”.

Prioritate incident	Timpul de reacţie	Timpul de soluţionare	Timp maxim pentru corectare a cauzei*	Raportare primară
Critică	Timpul de reacţie al Prestatorului – imediat	pînă la 3 ore	8 ore	SSC (în afara orelor de lucru – Manager de Proiect)
Înaltă	Timpul de reacţie al Prestatorului – 15 minute	8 ore	ora 12 a zilei următoare	SSC (în afara orelor de lucru – Manager de Proiect)
Medie	Timpul de reacţie al Prestatorului – 4 ore	24 ore	5 zile	SSC (în afara orelor de lucru – Manager de Proiect)
Joasă	Timpul de reacţie al Prestatorului – 24 ore;	3 zile	10 zile	SSC
Neglijabilă	Timpul de reacţie al Prestatorului – 72 ore;	Cel mai bun efort	-	SSC

**Notă:* *se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.*

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergenţe apărute între Părţi vor fi soluţionate cu efort comun şi prin strînsă conlucrare între Părţi. În acest scop, vor fi aplicate următoarele reguli:

- Părţile vor forma un grup comun de lucru în scopul soluţionării divergenţelor. De comun acord, în grupul de lucru pot fi acceptaţi reprezentanţi ai părţilor terţe, inclusiv experţi independenţi.
- La necesitate, părţile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergenţă.
- Grupul de lucru se va convoca şi va examina subiectul divergenţelor şi probele existente la subiect. Părţile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluţii echitabile pentru divergenţele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informaţiei

Prestatorul este responsabil pentru securitatea tehnologică şi funcţională a softului aplicativ în limitele sarcinilor de mentenanţă îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informaţiei, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părţile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;
- Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

După soluţionarea unui incident de securitate, părţile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acţiuni pentru prevenirea repetării incidentelor similare.

Livrabile

Prestatorul menține în stare actuală documentația tehnică. Documentaţia conţine suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanţă.

Prestatorul va notifica Beneficiarul despre noile versiuni și modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.

La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:

- Codul sursă final compilabil pe suport (DVD-R sau USB);
- Documentația tehnică;
- Ghidul utilizatorilor;
- Ghidul administratorului;
- Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Cerințe privind experiența personalului

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.

În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente mentenanței, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini și doar în baza acceptului Beneficiarului.

Ofertantul este obligat să informeze în prealabil Beneficiarul despre necesitatea modificării echipei de mentenanță, va transmite CV-ul persoanei care înlocuiește și va confirma recepționarea răspunsului (de acceptare sau refuz) expediat de către Beneficiar. Beneficiarul își rezervă dreptul de a refuza modificarea componenței minime a echipei în cazul în care pregătirea profesională și experiența noilor membri nu corespunde cerințelor stabilite în prezent caiet de sarcini sau solicitarea privind modificarea echipei nu este relevantă.

CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.
- Deținerea certificatului Project Manager sau documentului analogic de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor și/sau emis de o instituție publică sau privată competentă cu recunoaștere generală.
- Minim 3 ani de experiență în managementul proiectelor în domeniul tehnologiilor informaționale.
- Minim 3 proiecte în domeniul tehnologiilor informaționale realizate în calitate de Manager de proiect.
- Minim 3 ani de experiență în utilizarea metodologiilor de management de proiecte recunoscute pe plan internațional.

- Experiență specifică de Manager de Proiect în cel puțin 3 proiecte de complexitate similară, pe toată durata proiectului, realizate cu succes.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Business Analist *(minim 1 persoană)*

- Studii superioare în domeniul ingineriei sau tehnologiilor informaționale confirmate prin diploma de absolvire.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Cel puțin 3 ani de experiență în domeniul tehnologiilor informaționale.
- Cel puțin 3 ani de experiență în domeniul analizei și modelării Business-proceselor.
- Experiență profesională specifică, confirmată prin participarea în cel puțin 3 proiecte similare de implementare a unui sistem informatic integrat similar, în care el/ea s-a poziționat ca Business Analitic.
- Experiență în implementarea sistemelor informaționale complexe în instituțiile bugetare și/sau în domeniul medical.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist securitatea informațională (minim 1 persoană)

- Studii superioare Tehnice sau în domeniul TI.
- Cunoștințe privind securitatea sistemelor informatice și securitatea sistemelor ce conțin informații cu caracter personal, dovedite prin diplome/certificate obținute.
- Cunoștințe privind auditul sistemelor informatice dovedite prin diplome/certificate obținute (ISO27001, CISA sau echivalent*).
- Experiență de cel puțin 3 ani în domeniul securității sistemelor informatice.
- Participarea în ultimii 3 ani ca consultant sau auditor la cel puțin 3 contracte în domeniul securității informației.
- Participarea în cel puțin 3 contracte similare ca expert de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist infrastructură sistem (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență profesională generală în domeniul de specialitate de minim 3 ani;
- Experiență dobândită prin participarea în cel puțin 3 proiecte în activități IT complexe privind infrastructura software și hardware pe platforme în baza tehnologiei de „cloud computing”

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist programator (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență de minim 3 ani în programarea aplicațiilor web: Java, Java script, HTML, CSS, etc;
- Experiență dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de

implementare a unui sistem informațional de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Specialist baze de date (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Cunoașterea limbii de stat; – Experiență de minim 3 ani în administrarea bazelor de date: MS SQL Server; – Experiență dobândită prin participarea în calitate de specialist în baze de date în cel puțin 3 proiecte de implementare a unui sistem informatic de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Software Tester (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Experiență demonstrată în testarea funcțională a sistemelor informaționale; – Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale; – Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*

16. Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrînse și al procedurii negociate), *NU*

17. Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): *NU*

18. Condiții speciale de care depinde îndeplinirea contractului *Nu se aplică*

19. Criteriul de evaluare aplicat pentru adjudecarea contractului: *prețul cel mai scăzut pentru fiecare lot în parte.*

20. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor: *nu se aplică*

21. Termenul limită de depunere/deschidere a ofertelor:

- **până la:** ***[ora exactă]*** Conform informației din SIA RSAP ”MTender”
- **pe:** ***[data]*** Conform informației din SIA RSAP ”MTender”

22. Adresa la care trebuie transmise ofertele sau cererile de participare:

Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP

23. Termenul de valabilitate a ofertelor: *40 zile*

24. Locul deschiderii ofertelor: SIA RSAP ”MTender”
Ofertele întîrziate vor fi respinse.

25. Persoanele autorizate să asiste la deschiderea ofertelor:
Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului cînd ofertele au fost depuse prin SIA “RSAP”.

26. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:
limba de stat

27. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: *NU*

(se specifică denumirea proiectului și/sau programului)

28. Denumirea și adresa organismului competent de soluționare a contestațiilor:
Agenția Națională pentru Soluționarea Contestațiilor
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md

29. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): *NU*

30. În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare: *NU*

31. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: *nu a fost publicat*

32. Data transmiterii spre publicare a anunțului de participare: Conform informației din SIA RSAP "MTender"

33. În cadrul procedurii de achiziție publică se va utiliza/accepta:

Denumirea instrumentului electronic	Se va utiliza/accepta sau nu
depunerea electronică a ofertelor sau a cererilor de participare	DA
sistemul de comenzi electronice	NU
facturarea electronică	DA
plățile electronice	DA

34. Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): *NU*

35. Alte informații relevante: *nu sunt*

Președintele grupului de lucru: _____ Ion DODON

Anexa nr. 7
la Documentația standard nr._____
din "____" _____ 20___

CERERE DE PARTICIPARE

Către _____
(denumirea autorității contractante şi adresa completă)

Stimaţi domni,

Ca urmare a anunțului/invitației de participare/de preselecție apărut în Buletinul achizițiilor publice și/sau Jurnalul Oficial al Uniunii Europene, nr. . . . . din . . . . . (ziua/luna/anul), privind aplicarea procedurii pentru atribuirea contractului . . . . . (denumirea contractului de achiziție publică), noi . . . . . (denumirea/numele ofertantului/candidatului), am luat cunoștință de condițiile și de cerințele expuse în documentația de atribuire și exprimăm prin prezenta interesul de a participa, în calitate de ofertant/candidat, neavînd obiecții la documentația de atribuire.

Data completării . . . . . Cu stimă,

Ofertant/candidat

. . . . . .

(semnătura autorizată)

Anexa nr. 8
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE
privind valabilitatea ofertei

Către_____
(*denumirea autorităţii contractante şi adresa completă*)

Stimaţi domni,

Ne angajăm să menținem oferta valabilă, **privind achiziționarea _____**
(se indică obiectul achiziției)
prin procedura de achiziție_____,
(tipul procedurii de achiziție)
pentru o durată de _____ zile, (durata în litere și cifre), respectiv până la data de _____ (ziua/luna/anul), și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

Data completării . . . . . Cu stimă,

Ofertant/candidat

. . . . . .

(semnătura autorizată)

Anexa nr. 9
la Documentația standard nr._____
din "____" _____ 20___

BANCA

_____
(denumirea)

SCRISOARE DE GARANŢIE BANCARĂ
pentru participare cu ofertă la procedura de atribuire a contractului de achiziţie publică

Către_____
(denumirea autorităţii contractante şi adresa completă)

_____
cu privire la procedura de atribuire a contractului
_____,
(denumirea contractului de achiziţie publică)
subsemnaţii_____,
(denumirea băncii)
Înregistrat la_____,
(adresa băncii)
ne obligăm faţă de _____să
(*denumirea autorităţii contractante*)
plătim suma de_____, la prima sa cerere scrisă şi
(suma în litere şi în cifre)

fără ca acesta să aibă obligaţia de a-şi motiva cererea respectivă, cu condiţia, ca în cererea sa autoritatea contractantă să specifice că suma cerută de ea şi datorată ei este din cauza existenţei uneia sau mai multora dintre situaţiile următoare:

1. Ofertantul _____
(denumirea ofertantului)
îşi retrage sau modifică oferta în perioada de valabilitate a acesteia;
Prezenta ofertă rămâne valabilă pentru perioada de timp specificată în Anexa nr.2 Anunțul de Participare, începînd cu data-limită pentru depunerea ofertei, în conformitate cu Anexa nr.2 Anunțul de Participare, și rămâne obligatorie şi poate fi acceptată în orice moment până la expirarea acestei perioade;
2. Oferta sa fiind stabilită câştigătoare, ofertantul _____
(denumirea ofertantului)
nu a constituit garanţia de bună execuție;
3. Oferta sa fiind stabilită câştigătoare, ofertantul _____
(denumirea ofertantului)
a refuzat să semneze contractul de achiziţie publică de bunuri/servicii;

Nu se execută vreo condiţie, specificată în documenația de atribuire înainte de semnarea contractului de achiziţie publică de bunuri/servicii.
Prezenta garanţie este valabilă până la data de _____
Parafată de Banca_____în ziua___luna____anul_____
(semnătura autorizată)

Anexa nr. 10
la Documentația standard nr._____
din "____" _____ 20___

[Banca comercială, la cererea ofertantului cîştigător, va completa acest formular pe foaie cu antet, în conformitate cu instrucţiunile de mai jos.]

Data: "___" _____ 20__

Procedura de achiziție Nr.: _____

Oficiul Băncii: _____
[introduceţi numele complet al garantului]

Beneficiar: _____
[introduceţi numele complet al autorităţii contractante]

GARANŢIA DE BUNĂ EXECUŢIE
Nr. _____

Noi, *[introduceţi numele legal şi adresa băncii],* am fost informaţi că firmei *[introduceţi numele deplin al Furnizorului/Prestatorului]* (numit în continuare „Furnizor/Prestator") i-a fost adjudecat Contractul de achiziție publică de livrare/prestare _____ [*obiectul achiziţiei, descrieţi bunurile/serviciile*] conform anunțului/invitaţiei la procedura de achiziție nr. din _____. 20_ [*numărul şi data procedurii de achiziţie*] (numit în continuare „Contract").

Prin urmare, noi înţelegem că Furnizorul/Prestatorul trebuie să depună o Garanţie de bună execuţie în conformitate cu prevederile documentației de atribuire.

În urma solicitării Furnizorul/Prestatorului, noi, prin prezenta, ne angajăm irevocabil să vă plătim orice sumă(e) ce nu depăşeşte *[introduceţi suma(ele) în cifre şi cuvinte]* la primirea primei cereri în scris din partea Dvs., prin care declaraţi că Furnizorul/Prestatorul nu îndeplineşte una sau mai multe obligaţii conform Contractului, fără discuţii sau clarificări şi fără necesitatea de a demonstra sau arăta temeiurile sau motivele pentru cererea Dvs. Sau pentru suma indicată în aceasta.

Această Garanţie va expira nu mai tîrziu de *[introduceţi numărul]* de la data de *[introduceţi luna][introduceţi anul]*, şi orice cerere de plată ce ţine de aceasta trebuie recepţionată de către noi la oficiu pînă la această dată inclusiv.

[semnăturile reprezentanţilor autorizaţi ai băncii şi ai Furnizorului/Prestatorului]

Anexa nr. 11
la Documentația standard nr._____
din "____" _____ 20___

INFORMAŢII PRIVIND ASOCIEREA

1.Părţi contractante (agenţi economici)
a) _____
b) _____
c) _____
2. Adrese, telefon, fax a oficiilor partenerilor (părţi contractante):
a) _____
b) _____
c) _____
3. Informaţii privind modul de asociere:
a) Data încheierii contractului de asociere _____
b) Locul şi data înregistrării asociaţiei_____
c)Activităţi economice ce se vor realiza în comun _____
d) Contribuţia fiecărei părţi la realizarea activităţilor economice comune convenite _____
_____
e) Valoarea și cota procentuală a bunurilor livrate/serviciilor prestate de fiecare asociat
f) Condiţii de administrare a asociaţiei_____
g)Modalitatea de împărţire a rezultatelor activităţii economice comune desfăşurate _____
h)Cauze de încetare a asociaţiei şi modul de împărţire a rezultatelor lichidării_____
i) Repartizarea fizică, valorică şi procentuală între fiecare asociat pentru executarea obiectivului supus licitaţiei_____
j) Alte cauze_____

Data completării _____
Semnat Liderul Asociației: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Semnat Asociatul secund: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr. 12
la Documentația standard nr._____
din "____" _____ 20___

DECLARAȚIE
privind lista principalelor livrari/prestări efectuate în ultimii 3 ani de activitate

Nr d/o	Obiectul contractului	Denumirea/ numele beneficiarului/Adresa	Calitatea Furnizorului/Prestatorului*)	Preţul contractului/ valoarea bunurilor/serviciilor livrate/prestate	Perioada de livrare/prestare (luni)
1					
2					
...					

*) Se precizează calitatea în care a participat la îndeplinirea contractului, care poate fi de: contractant unic sau lider de asociaţie; contractant asociat; subcontractant.
Semnat: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr. 13
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE
privind dotările specifice, utilajul şi echipamentul necesar pentru îndeplinirea corespunzătoare a contractului

Nr. d/o	**Denumirea principalelor utilaje, echipamente, mijloace de transport, baze de producţie (ateliere, depozite, spaţii de cazare) şi laboratoare propuse de ofertant ca necesare pentru prestarea serviciilor, rezultate în baza tehnologiilor pe care el urmează să le adopte**	**Unitatea de măsură (bucăţi şi seturi)**	**Asigurate din dotare**	**Asigurate de la terţi sau din alte surse**
0	**1**	**2**	**3**	**4**
1.				
2.				
3.				
.				
n				

Semnat: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr.15
la Documentația standard nr._____
din "____" _____ 20___

LISTA SUBCONTRACTANȚILOR
ŞI PARTEA/PĂRŢILE DIN CONTRACT CARE SUNT
ÎNDEPLINITE DE ACEŞTIA

Nr. d/o	**Numele şi adresa subantreprenorilor**	**Activităţi din contract**	**Valoarea aproximativă**	**% din valoarea contractului**
1.				
2.				
3.				
4.				

Semnat: _____
Nume: _____
Funcţia în cadrul firmei: _____
Denumirea firmei: _____

Anexa nr.16
la Documentaţia standard nr._____
din "____" _____ 20___

ANGAJAMENT TERŢ SUSŢINĂTOR FINANCIAR

Terţ susţinător financiar

.....(denumirea)

ANGAJAMENT
privind susţinerea financiară a ofertantului/candidatului

Către, ...
(denumirea autorităţii contractante şi adresa completă)
Cu privire la procedura pentru atribuirea contractului .....
(denumirea contractului de achiziţie publică), noi .....(*denumirea terţului susţinător financiar)*, având sediul înregistrat la ..... (*adresa terţului susţinător financiar)*, ne obligăm, în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia ..... (*denumirea ofertantului/candidatului*) toate resursele financiare necesare pentru îndeplinirea integrală şi la termen a tuturor obligaţiilor asumate de acesta conform ofertei prezentate şi contractului de achiziţie publică ce urmează a fi încheiat între ofertant şi autoritatea contractantă.
Acordarea susţinerii financiare nu implică alte costuri pentru achizitor, cu excepţia celor care au fost incluse în propunerea financiară.
În acest sens, ne obligăm în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia .....(*denumirea ofertantului/candidatului)* suma de .....(valoarea totală/parţială din propunerea financiară), necesară pentru îndeplinirea integrală, reglementară şi la termen a contractului de achiziţie publică.
Noi, ... (*denumirea terţului susţinător financiar),* declarăm că înţelegem să răspundem faţă de autoritatea contractantă pentru neexecutarea oricărei obligaţii asumate de ..... (*denumirea ofertantului)*, în baza contractului de achiziţie publică şi pentru care ..... (*denumirea ofertantului/candidatului)* a primit susţinerea financiară conform prezentului angajament, renunţând în acest sens, definitiv şi irevocabil, la invocarea beneficiului de diviziune.
Noi, ... *(denumirea terţului susţinător financiar)*, declarăm că înţelegem să renunţam definitiv şi irevocabil la dreptul de a invoca orice excepţie de neexecutare, atât faţă de autoritatea contractantă, cât şi faţă de ..... (*denumirea ofertantului/candidatului),* care ar putea conduce la neexecutarea, parţială sau totală, sau la executarea cu întârziere sau în mod necorespunzător a obligaţiilor asumate de noi prin prezentul angajament.
Noi,..... *(denumirea terţului susţinător financiar),* declarăm că înţelegem să răspundem pentru prejudiciile cauzate autorităţii contractante ca urmare a nerespectării obligaţiilor prevăzute în angajament.
Prezentul reprezintă angajamentul nostru ferm încheiat în conformitate cu prevederile art.21 alin.(6) al Legii nr.131/2015 privind achiziţiile publice, care dă dreptul autorităţii contractante de a solicita, în mod legitim, îndeplinirea de către noi a anumitor obligaţii care decurg din susţinerea financiară acordată ..... (*denumirea ofertantului/candidatului).*

Data completării,
.....

Terţ susţinător,
.....
(semnătură autorizată)

Anexa nr. 17
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE TERŢ SUSŢINĂTOR FINANCIAR

Terţ susţinător financiar

.....
(denumirea)

Declaraţie

Subsemnatul, reprezentant împuternicit al ..... (*denumirea terţului susţinător financiar),* declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că toate resursele financiare necesare pentru îndeplinirea integrală şi la termen a tuturor obligaţiilor contractului de achiziţie publică..... sunt reale.

Declar de asemenea că vom disponibiliza aceste resurse necondiţionat, în funcţie de necesităţile care vor apărea pe parcursul îndeplinirii contractului de achiziţie publică având ca obiect.....(*obiectul contractului).*

Data completării, Terţ susţinător,

(*semnătură autorizată*)

Anexa nr. 18
la Documentația standard nr._____
din "____" _____ 20___

ANGAJAMENT PRIVIND SUSŢINEREA TEHNICĂ ȘI PROFESIONALĂ A OFERTANTULUI/GRUPULUI DE OPERATORI ECONOMICI

.....
(denumirea)

ANGAJAMENT
privind susţinerea tehnică şi profesională
a ofertantului/candidatului

Către, ...
(denumirea autorităţii contractante şi adresa completă)
Cu privire la procedura pentru atribuirea contractului ..... *(denumirea contractului de achiziţie publică)*, noi ..... *(denumirea terţului susţinător tehnic şi profesional*), având sediul înregistrat la ....*(adresa terţului susţinător tehnic şi profesional)*, ne obligăm, în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia..... (*denumirea ofertantului)* toate resursele tehnice şi profesionale necesare pentru îndeplinirea integrală şi la termen a tuturor obligaţiilor asumate de acesta, conform ofertei prezentate şi contractului de achiziţie publică ce urmează a fi încheiat între ofertant şi autoritatea contractantă.
Acordarea susţinerii tehnice şi profesionale nu implică alte costuri pentru achizitor, cu excepţia celor care au fost incluse în propunerea financiară.
În acest sens, ne obligăm în mod ferm, necondiţionat şi irevocabil, să punem la dispoziţia ..... (*denumirea ofertantului/candidatului)* resursele tehnice şi/sau profesionale de ....necesare pentru îndeplinirea integrală, reglementară şi la termen a contractului de achiziţie publică.
Noi, ... *(denumirea terţului susţinător tehnic şi profesional),* declarăm că înţelegem să răspundem, în mod necondiţionat, faţă de autoritatea contractantă pentru neexecutarea oricărei obligaţii asumate de ..... *(denumire ofertantului/candidatului)*, în baza contractului de achiziţie publică, şi pentru care ..... *(denumirea operatorului/candidatului)* a primit susţinerea tehnică şi profesională conform prezentului angajament, renunţând în acest sens, definitiv şi irevocabil, la invocarea beneficiului de diviziune.
Noi, ... *(denumirea terţului susţinător tehnic şi profesional),* declarăm că înţelegem să renunţăm definitiv şi irevocabil la dreptul de a invoca orice excepţie de neexecutare, atât faţă de autoritatea contractantă, cât şi faţă de ..... (*denumire ofertant),* care ar putea conduce la neexecutarea, parţială sau totală, sau la executarea cu întârziere sau în mod necorespunzător a obligaţiilor asumate de noi prin prezentul angajament.
Noi,..... *(denumirea terţului susţinător tehnic şi profesional),* declarăm că înţelegem să răspundem pentru prejudiciile cauzate autorităţii contractante ca urmare a nerespectării obligaţiilor prevăzute în angajament.
Prezentul reprezintă angajamentul nostru ferm încheiat în conformitate cu prevederile art.22 alin.(6) al Legii nr.131/2015 privind achiziţiile publice, care dă dreptul autorităţii contractante de a solicita, în mod legitim, îndeplinirea de către noi a anumitor obligaţii care decurg din susţinerea tehnică şi profesională acordată ..... (*denumirea ofertantului/candidatului).*

Data completării,
.....

Terţ susţinător,
.....
(semnătură autorizată)

Anexa nr. 19
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE TERŢ SUSŢINĂTOR TEHNIC

Terţ susţinător tehnic

.....
(denumirea)

Declaraţie

Subsemnatul, reprezentant împuternicit al ..... (*denumirea terţului susţinător tehnic),* declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că datele prezentate în tabelul anexat privind logistica, utilajele, instalaţiile, echipamentele tehnice de care dispun şi care urmează a fi folosite efectiv pentru îndeplinirea contractului de achiziţie publică..... sunt reale.

Declar de asemenea că vom disponibiliza aceste resurse necondiţionat, în funcţie de necesităţile care vor apărea pe parcursul îndeplinirii contractului de achiziţie publică având ca obiect.....(*obiectul contractului).*

LISTA

privind logistica, utilajele, instalaţiile şi echipamentele tehnice aflate în dotare și care urmează a fi efectiv folosite pentru îndeplinirea contractului de achiziţie publică

Nr. crt	Denumire utilaj/echipament/instalaţie	Cantitate U.M.	Forma de deținere	
			Proprietate	În chirie

Prezenta declaraţie este anexă la „Angajamentul ferm" privind susţinerea noastră tehnică şi profesională oferită.....(*denumirea ofertantului/candidatului).*

Data completării,

Terţ susţinător,

(semnătură autorizată)

Anexa nr. 20
la Documentația standard nr._____
din "____" _____ 20___

DECLARAŢIE TERŢ SUSŢINĂTOR PROFESIONAL

Terţ susţinător profesional

.....
(denumirea)

Declaraţie

Subsemnatul, reprezentant împuternicit al .....(denumirea terţului susţinător profesional), declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că datele prezentate în tabelul anexat privind efectivul mediu anual al personalului de specialitate angajat care urmează a fi efectiv alocat pentru îndeplinirea contractului de achiziţie publică..... sunt reale.

LISTA

privind personalul de specialitate angajat care urmează a fi efectiv alocat pentru îndeplinirea contractului de achiziţie publică

	Anul 1	Anul 2	Anul 3
Personalul de specialitate			
……			
……			
…….			

Anexez declaraţiei, CV-urile personalului de specialitate, precum şi ale personalului care va fi alocat efectiv pentru îndeplinirea contractului de achiziţie publică.

Subsemnatul declar că informaţiile furnizate, referitoare la experienţa anterioară, capacităţile tehnice şi personalul de specialitate angajat sunt complete şi corecte în fiecare detaliu şi înţeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, situaţiilor şi documentelor care însoţesc oferta, orice informaţii suplimentare în scopul verificării datelor din prezenta declaraţie.

Subsemnatul autorizez prin prezenta orice instituţie, societate comercială, bancă, alte persoane juridice să furnizeze informaţii reprezentanţilor autorizaţi ai ..... (*denumirea şi adresa autorităţii contractante)* cu privire la orice aspect tehnic şi financiar în legătură cu activitatea noastră.

Prezenta declaraţie este anexă la „Angajamentul ferm" privind susţinerea noastră tehnică şi profesională oferită ....(*denumirea ofertantului/candidatului).*

Data completării,

Terţ susţinător,

(semnătură autorizată)

Anexa nr. 21
la Documentația standard nr._____
din "____" _____ 2023

CAIET DE SARCINI
Servicii

Obiectul: *achiziţionarea serviciilor de mentenanţă, suport şi dezvoltare pentru Sistemul Informaţional de Raportare şi Evidenţă a Serviciilor Medicale, componenta DRG şi SIP*
Autoritatea contractantă: *Compania Națională de Asigurări în Medicină*
(denumirea, adresa)

1. Descriere generală. Informaţii

Nr. lotului	Cod CPV	Denumirea bunurilor/serviciilor/ lucrărilor solicitate	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată fară TVA (se va indica pentru fiecare lot în parte)
Lotul 1						
1	72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – **în bază de abonament**	Luni	12	Conform Caietului de sarcini din Anexa nr. 1	539 784,00
2	72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – **în bază de trouble ticket/ticketing**	Om/ore	900	Conform Caietului de sarcini din Anexa nr. 1	137 700,00
	Valoarea estimată totală (fără TVA)					677 484.00

Nr. lotului	Cod CPV	Denumirea bunurilor/serviciilor/ lucrărilor solicitate	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată fară TVA (se va indica pentru fiecare lot în parte)
Lotul 2						
1	72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de abonament**. .	Luni	12	Conform Caietului de sarcini din Anexa nr. 2	539 784,00
2	72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de trouble ticket/ticketing.**	Om/ore	900	Conform Caietului de sarcini din Anexa nr. 2	137 700,00
	Valoarea estimată totală (fără TVA)					677 484.00

CAIET DE SARCINI

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **DRG**

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	Descriere
Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG: • *Servicii de mentenanță preventivă și Suport – în bază de abonament;* • *Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.*	*Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.*

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG (în continuare – DRG) pentru o perioadă de **minim 12 luni** după încetarea contractului.

De asemenea, Prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta CNAM (Beneficiar) împreună cu codul sursă DRG, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Descriere generală a DRG

DRG reprezintă un sistem național pentru instituțiile medicale din Republica Moldova, cu ajutorul căruia sunt încărcate și gestionate informațiile la nivelul bazei de date a CNAM.

Obiectivele strategice ale CNAM și MS în ceea ce privește costurile asociate tratamentului conduce la obținerea unei **imagini mai bune a rezultatelor** și la realizarea de **comparații ale rezultatelor**. DRG este un **instrument util spitalelor în creșterea eficienței** (prin identificarea resurselor necesare fiecărui tip de pacient), în procesul de îmbunătățire a calității serviciilor furnizate (prin evaluarea calității și definirea unor modele de practică), în **modelarea activității** și a structurii spitalelor (personal, secții, etc.) și în realizarea unui **management bazat pe rezultate** și nu pe resurse sau procese.

Funcționarea continuă și operarea în sistemul DRG are următoarele obiective:

A. Creșterea eficienței serviciilor spitalicești

Prin finanțarea în sistem DRG, spitalele ce vor avea costuri pentru un anumit DRG mai mari decât tariful stabilit vor pierde resurse la acea categorie de pacienți, iar cele cu costuri, pentru un anumit DRG, mai mici decât tariful stabilit vor câștiga resurse la acea categorie de pacienți. Alocarea resurselor financiare are la baza rezultatele spitalului și mai puțin structura acestora.

B. Creșterea eficienței tehnice la nivelul furnizorului de serviciilor spitalicești

DRG permite spitalelor să-și evidențieze cu claritate tipurile de pacienți și resursele atrase pentru aceștia, iar prin compararea cu costurile necesare se generează cadrul de funcționare pentru o eficientă cât mai mare (economiile făcute fiind păstrate la nivelul spitalului).
Spitalele pot să-și cunoască tipurile de pacienți pentru care pierd resurse (și să intervină în procesele ce se desfășoară pentru a reduce cheltuielile) și pacienții la care sunt în beneficiu financiar (și să încerce să atragă cât mai mulți pacienți de acest tip).

Specificații tehnice DRG

Caracteristici generale de funcționare

DRG are o arhitectura 3-layer, arhitectura care permite funcționarea pe platforma guvernamentală comună MCloud. DRG funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă tot ce este necesar de automatizat;
- are posibilitatea reparației unui modul fără afectarea altora;
- respectă standardele în vigoare a tehnologiilor informaționale;
- asigură flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare;
- utilizează o arhitectură orientată pe servicii pentru a acomoda cu ușurință noi modificări;
- are o arhitectura modernă cu un grad înalt de performanță, structurată pe 3 niveluri (nivelul pentru baze de date, nivelul pentru aplicație și nivelul acces/utilizator). Fiecare nivel are în componență toate echipamentele necesare bunei funcționări;
- este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- poate fi utilizat împreună cu echipamente ce permit creșterea vitezei de înregistrare a datelor de identificare ale pacienților (nume, prenume, IDNP etc.);
- este scalabil pentru a acomoda modificările viitoare ale numărului de utilizatori ai soluției;
- recunoaște corect sursele informaționale, le acceptă și le integrează în sistem;

- întreține în limba de stat interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate;
- permite ca utilizatorul să se autentifice o singură dată pentru a accesa toate modulele aplicației;
- asigură o siguranță sporită în exploatare.

Interfața Utilizator

Această interfață este accesibilă pentru toți utilizatorii autorizați în DRG:

- ✓ DRG dispune de o interfață inteligentă, intuitivă și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browserul web și nu necesită instalarea de componente software suplimentare;
- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului;
- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:

- **Platforma hardware**, formata din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat pe platforma guvernamentală comună MCloud:
  - Servere protejate redundant pentru hosting al bazelor de date, softului de sistem și softului funcțional (aplicații și subsisteme);
  - Platforma hardware pusă la dispoziție de către beneficiar este dimensionată corespunzător pentru a permite funcționarea în bune condiții a sistemului;
  - Performanta optima, în limita normelor obiective de uzură, pentru realizarea structurii funcționale și asigurarea extinderii ulterioare a sistemului;
  - este flexibilă în utilizarea mijloacelor disponibile destinate recepționarii informației din surse externe (alte instituții publice);
  - asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date;
  - asigura normele de funcționare ale platformelor informatice guvernamentale.

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:
  - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
  - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server 2017, vers. 14.
  - Pe stațiile utilizatorilor există în mod implicit .NET Framework 3.5 SP1 sau mai nou și navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare și transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mașini virtuale, mijloacele de imprimare, rețele electronice locale (LAN – local area network) și de scara largă (WAN – wide area network). Pentru operare se folosesc stațiile de lucru ale beneficiarului, singura specificație impusă utilizatorilor fiind cea de a dispune de un calculator conectat la internet și un browser instalat, fiind recomandate și utilizate soluțiile Microsoft.

Sistemul de securitate

DRG funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.

Caracteristici:

- asigură accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de system;
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor;

Având în vedere natura specială a informațiilor gestionate în cadrul DRG, acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.

Sistemul are următoarele nivele de securitate care asigură confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație între stațiile clientului și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unică cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este asigurata automat, iar modificările de structura la nivelul acesteia se fac exclusiv în baza drepturilor corespunzătoare de administrator al bazei de date. În plus, baza de date deține propriul mecanism de backup care permite, în caz de dezastru, restaurarea unor versiuni anterioare recente (de ordinul zilelor).

Sistemul asigură dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori sunt create

module de acces și autentificare în sistem; sunt indicate volumul de informație și funcționalitatea pe care aceștia o accesează. Sistemul permite accesul la datele statistice pentru anumiți utilizatori și grupuri de utilizatori. Sistemul asigura verificarea automată a drepturilor în momentul intrării în sistem și în ulterioarele accesări a sistemului și creează un jurnal al accesărilor – jurnalul de audit.

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Operator**: permite introducerea și modificarea datelor specifice activității sale;
- nivelul **Administrator**: permite arhivarea datelor, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

La nivel aplicativ, sistemul generează o listă de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

- ✓ posibilitatea înregistrării, adăugării si ștergerii utilizatorilor din sistem;
- ✓ posibilitatea distribuției drepturilor utilizatorilor folosind grupuri de acces;
- ✓ posibilitatea pentru fiecare utilizator de a avea cel puțin următoarele atribute de autentificare: identificarea, autentificarea.
- ✓ posibilitatea intrării în sistem a unui utilizator în orice moment;
- ✓ asigurarea de către administrator a regimurilor de funcționare, deconectare, conectare, modificării regimului de autentificare și identificare, dirijarea cu drepturi și auditul.

Retenția datelor, acces securizat și audit

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale (consultații, fișe medicale și bilete de trimitere) în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.
- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respectă regulile de control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.
- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.
- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem și pe baza permisiunilor asociate rolului sau rolurilor atribuite utilizatorilor.
- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fișele electronice ale pacienților săi.
- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu că a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:

- unicitatea utilizatorilor în sistem;
- jurnalizarea tuturor operațiunilor efectuate de sistem;
- mecanism de control al versiunilor pentru înregistrările medicale.

- **Securitatea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit.** Toate operațiunile efectuate de utilizatori sau de către alte sisteme care accesează sistemul păstrează o înregistrare în componența auditului. Astfel, este permisă investigarea incidentelor de către un administrator.

Arhitectura DRG

DRG are o arhitectură bazată pe tehnologie web, folosind platforma Microsoft. Sistemul este conceput modular, dezvoltarea acestora putând fi realizată în paralel. Orice client se poate conecta la serverul de aplicație și poate utiliza sistemul conform drepturilor pe care le are. Comunicația între client și server se realizează exclusiv prin protocoale securizate de tip HTTPS folosind certificat de securitate integrat la nivelul serverului de aplicație. Schema arhitecturala este în figura următoare:

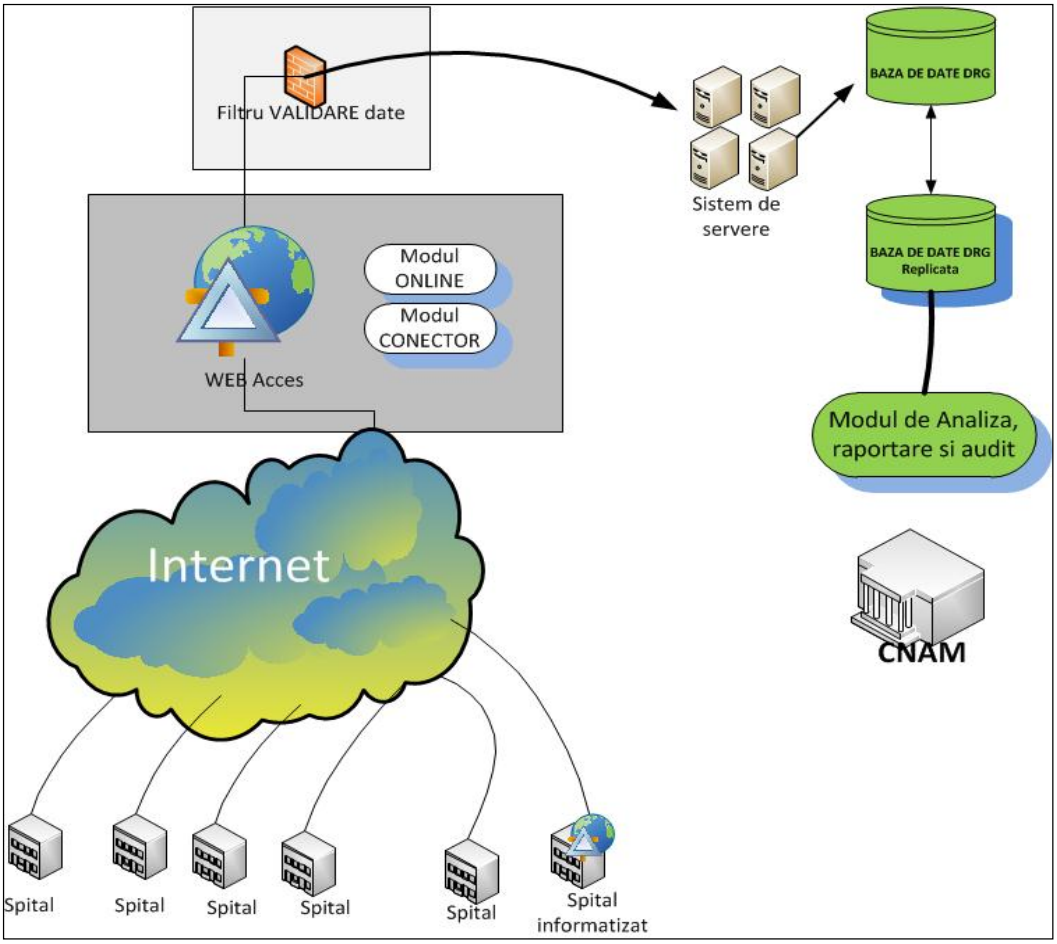


Figura 1. Schema arhitecturală DRG

Componentele DRG sunt operaționale și sunt prezente conform modulelor:

- ✓ Modulul de administrare sistem colector;

- ✓ Modulul de autentificare;
- ✓ Modulul colectare date Real Time;
- ✓ Modulul de nerepudiere;
- ✓ Modulul de validare;
- ✓ Modulul de înregistrare raportări;
- ✓ Modulul de setări, raportare și audit;
- ✓ Modulul Depozit (warehouse);
- ✓ Modulul de Analiză la nivel de Baza de Date;
- ✓ Modul conector pentru Auditul Codificării.

Modulul de administrare sistem colector

În cadrul acestui modul se execută:

- **Managementul utilizatorilor** (creare, ștergere, modificare date utilizatori). Fiecare instituție care execută raportare în DRG are desemnat cel puțin un utilizator al sistemului care transmite raportările; modalitatea de alocare a acestei resurse umane este răspunderea instituției.
- **Administrarea sistemului.** Administratorii sistemului pot efectua setări la nivelul celorlalte module și pot verifica funcționarea corectă a fiecărui modul. Nivelul de acces al administratorilor este corespunzător cerințelor de care aceștia răspund:
  - administratorii pot modifica informațiile de referință ale operatorilor sistemului (nume, prenume, locație, instituție, etc.);
  - administratorii pot modifica intervalele temporare în care transmiterea raportărilor este permisă;
  - administratorii pot vizualiza informații existente în modulul de nerepudiere (fișierele care conțin informațiile raportate trec prin modulul de nerepudiere);
  - administratorii pot vizualiza informațiile existente în modulul de înregistrare și să confirme funcționarea normală a acestuia;
  - administratorii pot vizualiza existenta rapoartelor transmise și stadiul în care se afla acestea față de modulul de validare;
  - administratorii pot face modificări asupra Modulului de Notificare și Raportare.
  - administratorii pot verifica transmiterea corectă a rapoartelor către Modulul Warehouse, unde sunt depozitate informațiile în vederea prelucrării.

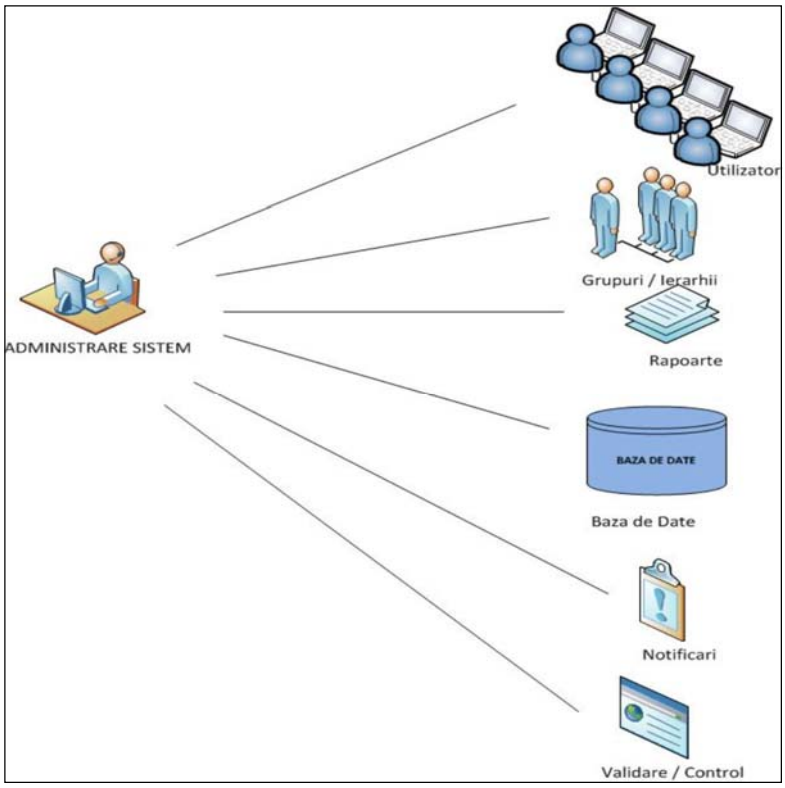


Figura 2. Schema Modulul de administrare sistem colector

Nivelul de acces al acestui modul:

- modulul care are acces la toate nivelurile sistemului;
- doar administratorii sistemului au acces la acest modul, în vederea efectuării operațiilor necesare funcționării normale a sistemului.

Modulul de administrare este singurul modul care permite accesul unui număr restrâns de persoane (administratorii sistemului) la toate elementele din sistem, fără să permită – prin procedura - modificarea conținutului rapoartelor.

Administratorii sistemului au rolul de a verifica fluxul normal al prelucrării datelor de către sistem și de a ajusta situațiile de excepție atunci când este cazul. Prin situații de excepție se înțeleg acele cazuri în care sistemul răspunde corect din punct de vedere al fluxului, dar cerințele unui utilizator sunt diferite și justificate.

Administratorii sistemului nu acționează asupra conținutului datelor transmise de către unitățile medicale, iar utilizatorii sunt instruiți asupra faptului că sunt direct răspunzători de conținutul informațiilor transmise. Conținutul datelor este confidențial și respectă normele de securitate din domeniu; sistemul informatic DRG poate opera cu fișierele de date fără a fi necesară intervenția administratorilor de sistem asupra conținutului. În situațiile în care utilizatorul corespunzător care a generat raportul cere explicit acest lucru, administratorul nu o prelucrează: conținutul datelor transmise rămâne exclusiv responsabilitatea instituțiilor medicale / operatorilor care folosesc sistemul.

Modulul de colectare date Real Time

Acest modul este cel care transformă operarea DRG într-o activitate aflată la dispoziția permanentă a oricărui spital: este un modul destinat acelor instituții care nu au un sistem informatic integrat al activității medicale, și care, în prezent lucrează cu diferite programe informatice în vederea generării raportărilor.

Acest modul are o interfață de lucru universală cu un aspect operațional intuitiv și ușor de urmărit, care nu necesită cunoștințe tehnice informatice avansate; orice medic sau asistent îl poate utiliza în activitatea curentă în vederea introducerii în sistemul național a informațiilor despre pacienții pe care îi tratează.

Informațiile pot fi introduse de către utilizatorii autorizați direct în sistem non-stop, la nivel național, într-o interfață accesibilă de pe orice calculator care dispune de un browser și de o legătura la serverul sistemului DRG: vârsta, sex, durata de spitalizare, diagnostice principale și secundare, proceduri, starea la externare și greutatea la naștere (în cazul nou-născuților), iar în funcție de acestea pacienții sunt clasificați într-o categorie distinctă (o grupă de diagnostice), în conformitate cu nomenclatoarele din domeniu.

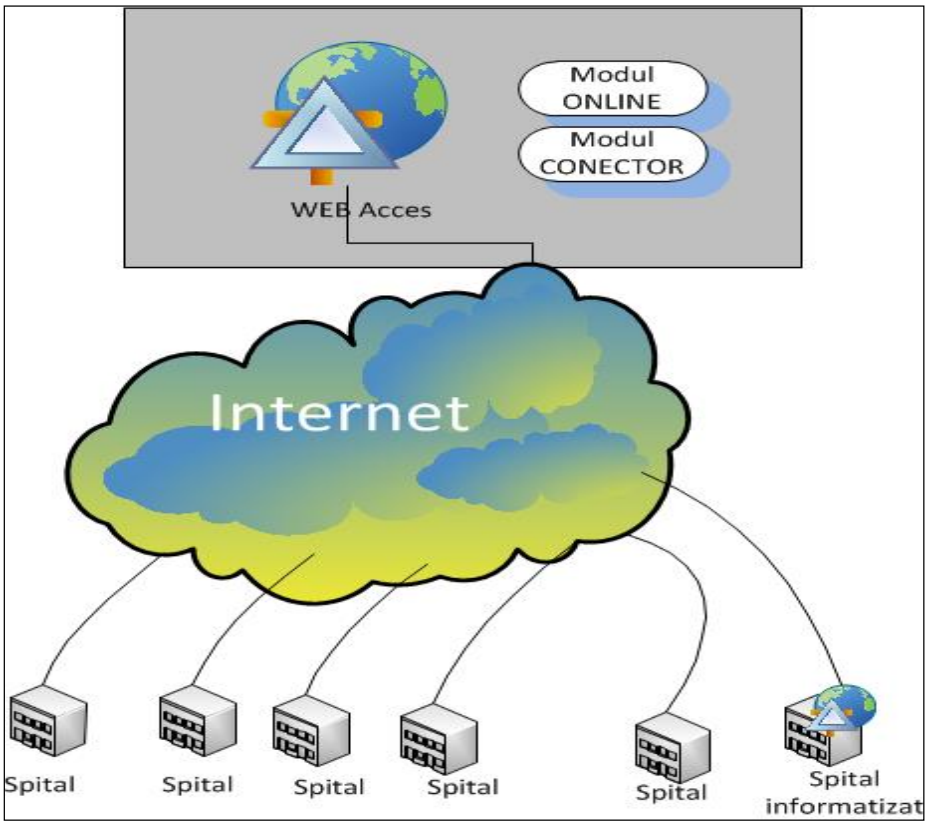


Figura 4. Modulul de colectare date Real Time

Avantajul major pe care îl oferă acest modul este că el este permanent updatat în conformitate cu cerințele CNAM, nomenclatoare noi sau alte dispoziții, iar acele instituții care aleg să îl folosească au siguranța actualizării informațiilor referitoare la raportările DRG. Informațiile sunt disponibile în timp real și pot fi analizate imediat, atât prin intermediul mecanismelor de analiză, audit și validare, cât și prin intermediul operatorilor CNAM.
Modulul preia informațiile, le validează și le introduce imediat în sistem. Datele despre pacient fiind de ultima ora, iar modificările asupra oricărui element care are legătura cu diagnosticul acestuia sunt trecute prin filtrele de validare; aceasta înseamnă că sistemul este capabil să calculeze imediat valoarea de complexitate a cazului tratat. Modul prenotat are capacitatea de a trece în analiza sau chiar să elimine activitățile suspecte sau lipsite de fond.

Modulul are și rolul de a elimina necesitatea spitalelor de a testa nenumărate programe informatice care generează rapoartele și care de multe ori au rezultate nesatisfăcătoare. Existența unui sistem informatic național dedicat acestui tip de raportare realizează o unificare și un control deosebit, ceea ce permite operatorilor generarea de rapoarte și identificarea prin auditare a zonelor sensibile din punct de vedere financiar.

Se elimină astfel obligativitatea existenței unui mecanism terțiar [de tip „3rd party”] la nivelul spitalelor pe care unele spitale îl utilizează în vederea raportării către CNAM. Aflat la dispoziția oricărui spital, DRG permite lucrul în timp real și la un înalt nivel de securitate, direct spre baza de date a CNAM.

Operațional, prin punerea la dispoziția personalului medical a unei interfețe de lucru în vederea acestui tip de raportare medicală cu puternice implicații financiare, sunt premisele unei colaborări eficiente inter / intra departamentale medical-administrativ cât și între spitale care sunt interesate să își modeleze activitatea în așa fel încât să eficientizeze activitatea.

Alegerea modului în care sunt efectuate raportările către CNAM este opțiunea instituțiilor medicale: acestea pot folosi fie modulul de colectare date Real Time sau software-ul intern și apoi mecanismul de transfer al rapoartelor real-time prin sistemul colector.

Modulul de nerepudiere

Modulul de nerepudiere are un rol important din punct de vedere al auditării: acest modul garantează pentru toți utilizatorii sistemului ca operarea se execută în mod unic și că nici un utilizator nu poate nega acțiunile legate de sistem.

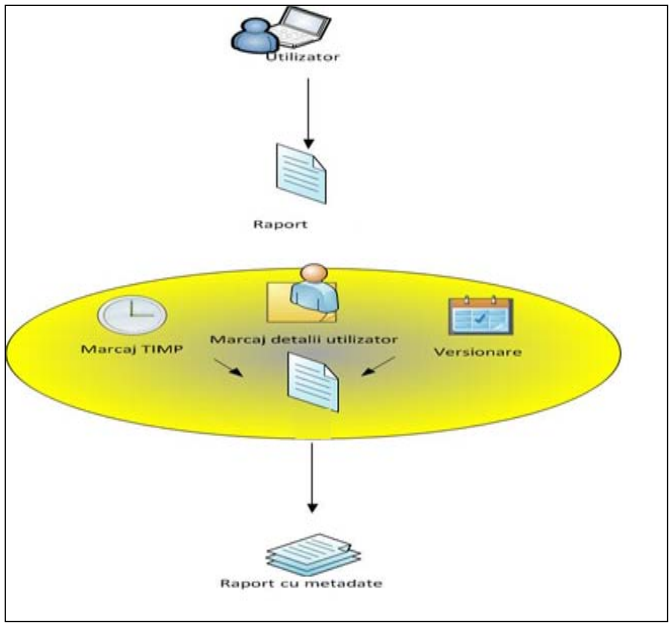


Figura 5. Modulul de nerepudiere

Fiecare utilizator este unic în sistem, lucru verificabil prin intermediul modulului de autentificare. Modulul de nerepudiere se referă la faptul că acțiunile pe care le efectuează un utilizator nu pot fi negate de acesta, deoarece fiecare acțiune are directă corespondență cu un utilizator. Orice fișier transferat de către un utilizator primește prin intermediul acestui modul un pachet de metadate care conține:

- ✓ Data și ora la care au fost transmise fișierele către sistem;
- ✓ Numele utilizatorului care a transmis fișierul; pentru fiecare fișier în parte se atașează metadatele corespunzătoare. Sistemul face automat asocierea între utilizator și fișierul transmis.
- ✓ Numele utilizatorului care a rescris ultima versiune a fișierului – va fi stabilit în faza de analiză, în funcție de particularitățile observate;

Aceste informații sunt disponibile atât administratorilor și, parțial, utilizatorilor. Adăugarea metadatelor la fișiere este o operațiune pe care modulul de nerepudiere o execută în mod automat și independent de opțiunile utilizatorilor. Orice raport transmis către sistem este însoțit de elemente de identificare unice: data, ora, nume utilizator etc. În cazul auditării sistemului, sunt disponibile date referitoare la acțiunile fiecărui utilizator, corelate integral cu informațiile introduse în sistem.

Modulul de validare

DRG reduce situațiile în care utilizatorii trimit setul minim de date la nivel de pacient al căror format este necorespunzător.

- Modulul de validare operează în mod minimal fișierele transmise (setul minim de date la nivel de pacient) și le acceptă doar pe cele care se încadrează în formatul dorit de către CNAM;
- Modulul de validare verifică, de asemenea, existența metadatelor de corespondența între utilizator și fișier înainte de trecerea în sistem a fișierelor al căror conținut îl constituie rapoartele. În cazul în care apar neconcordanțe între ceea ce așteaptă sistemul și ceea ce livrează utilizatorii, se trimit alerte către „Modulul de notificare, raportare și audit” care prelucrează situațiile în mod corespunzător, în sensul aducerii la forma standard a raportărilor.
- Modulul de validare este ultima componentă a sistemului care decide automat dacă un raport este valid sau nu; atenția acordată acestui modul este ridicată iar analiza situațiilor neconforme și alinierea acestora sunt urmărite permanent.
- Modulul de validare are capacitatea de a trata cât mai multe situații comune și elimina la timp cât mai multe cazuri în care apare eroarea umană.

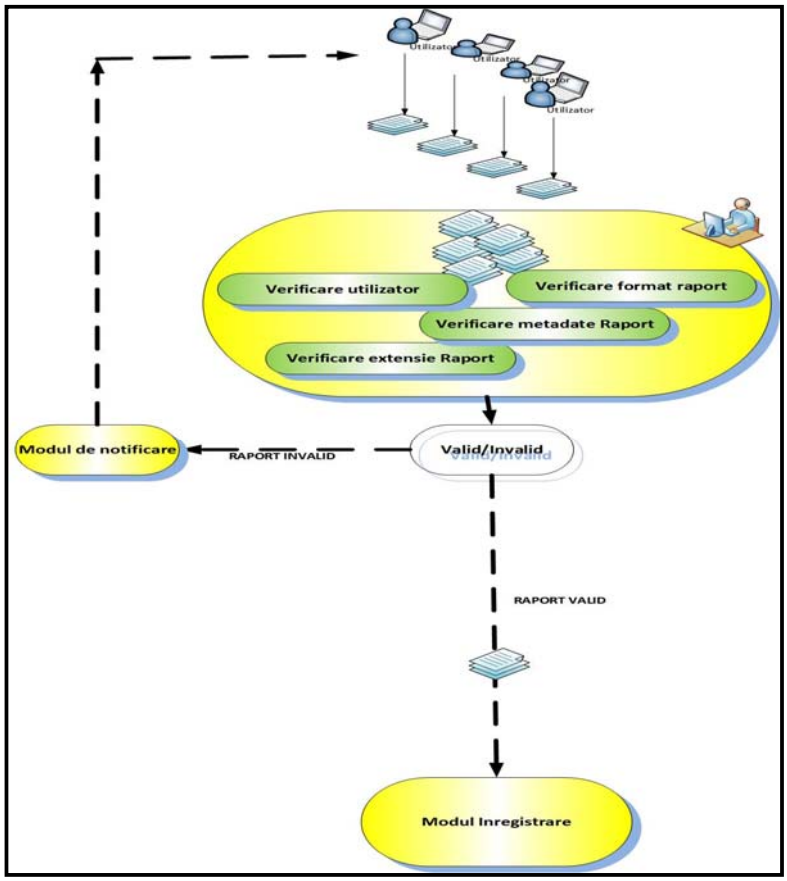


Figura 6. Schema Modulului de Validare

Modulul de înregistrare raportări

Modulul de înregistrare raportări este responsabil de depozitarea corectă a raportărilor trimise de către instituțiile medicale, în vederea transferului acestora către modulul depozit (data warehouse).

Modulul de înregistrare a raportări conține două componente:

1. Componenta „buffer”, temporară, care colectează toate raportările utilizatorilor în toate versiunile pe care aceștia le transmit în intervalul alocat; această componentă dispune de un mecanism de ordonare care permite automatizarea procesului de transfer al versiunilor finale fără intervenția administratorilor sau a utilizatorilor. Componenta „buffer” are rolul de a colecta și organiza rapoartele trimise de către utilizatori în mod unic, astfel încât nu există pentru o instituție medicală rapoarte dublate.

2. Componenta „transfer” golește „bufferul” în momentul expirării termenului de transmitere a raportărilor și le mută în zona de depozitare a rapoartelor – forma definitivă, prelucrabilă – numita Modul Warehouse.

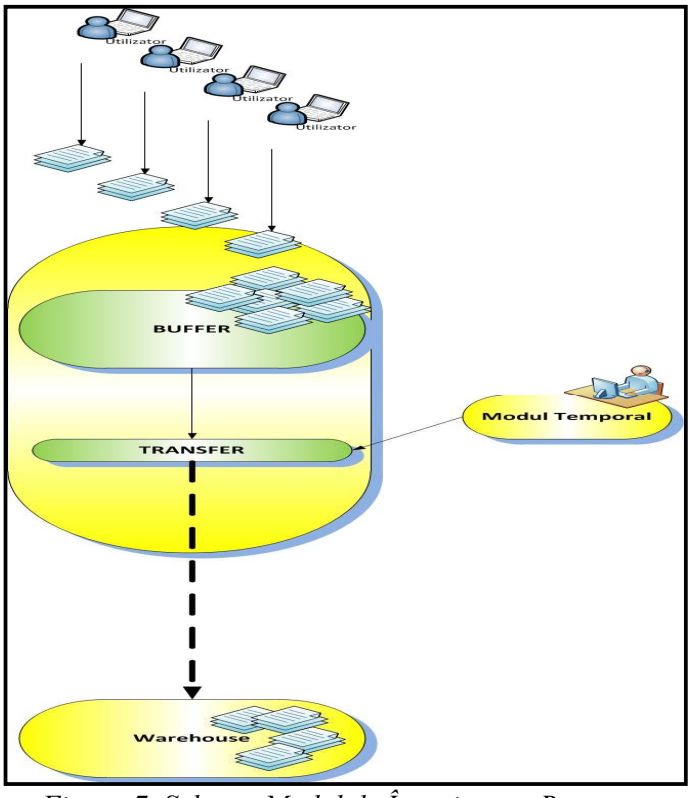


Figura 7. Schema Modul de Înregistrare Rapoarte

Informațiile de interes se limitează doar la ultimele versiuni ale raportărilor transmise:

- „Bufferul" permite unele modificări controlate de administratori asupra raportărilor în intervalul configurat în modulul de control temporal. La cerere administratorii de sistem pot vedea la nivel de *nume_raport* existența rapoartelor în buffer.

- „Transfer" acționează în mod programat, după expirarea termenului în care le este permis utilizatorilor să transmită raportările. Codul aplicației conține legătura directă între Modulul de Înregistrare și Modulul de control temporal.

Modulul de setări, raportare și audit

Modulul îndeplinește trei funcții: Setări, Raportare și Audit privind situația raportărilor din intervalul curent de timp în care este deschisă sesiunea de transfer a datelor. Fiecare dintre acestea este importantă la nivelul sistemului pentru că menține o comunicare permanenta între utilizatori, beneficiari și entitatea informatică:

✓ **Setări:** aceasta funcție a modulului este accesibila unui număr mic de utilizatori – administratori pentru introducerea datelor (inclusiv de autentificare) la nivel de CNAM și la nivel de instituție medicală. În cazul, în care modulul acționează în mod corect informațiile colectate și transmise sunt corecte și definesc informațiile ce pot afecta direct toate celelalte informații din baza de date.

✓ **Raportare:** aceasta funcție a modulului executa rapoarte în mod programat privind utilizarea sistemului.

✓ **Audit:** aceasta funcție a modulului identifică acțiunile desfășurate de către un utilizator, în mod cronologic; în cazul apariției unei probleme, la nivel de administrator de sistem, se poate vedea istoricul operațiilor desfășurate de orice utilizator în vederea

identificării și corectării problemei. Sunt vizibile atât informațiile referitoare la logarile în sistem cât și cele referitoare la fișierele cu care utilizatorul a operat. Funcția de audit folosește în mod implicit modulul de nerepudiere care asigura orice investigație ca datele existente în sistem sunt cele corecte și ca asocierea între conținutul informatic și activitatea umană este incontestabilă.

Modulul Depozit (Warehouse)

În cadrul fluxului de colectare de către sistem a raportărilor de la instituțiile medicale, Modulul Depozit (warehouse) este componenta finală, cea care deține datele necesare prelucrării. Aici se găsesc informațiile utile Beneficiarului, motiv pentru care acestea:

- ✓ sunt organizate într-o structură ierarhică care permite identificarea rapida a unui raport provenit de la orice instituție medicală la un anumit moment.
- ✓ conțin informațiile organizate într-o manieră care permite managementul rapoartelor fără a afecta conținutul acestora: există posibilitatea mutării datelor într-o arhivă; acest tip de operație necesită o analiză a graficului de încărcare a rapoartelor.
- ✓ modulul warehouse beneficiază de un spațiu de stocare protejat conform normelor de securitate ale Beneficiarului. Spațiul de stocare folosit de Modulul warehouse poate fi supus și altor cerințe de securitate decât cele ale sistemului implementat, în funcție de necesitățile beneficiarului: de ex. audit de urgență, investigații etc.
- ✓ Întreg spațiul alocat depozitarii rapoartelor este supus procedurilor de back-up.

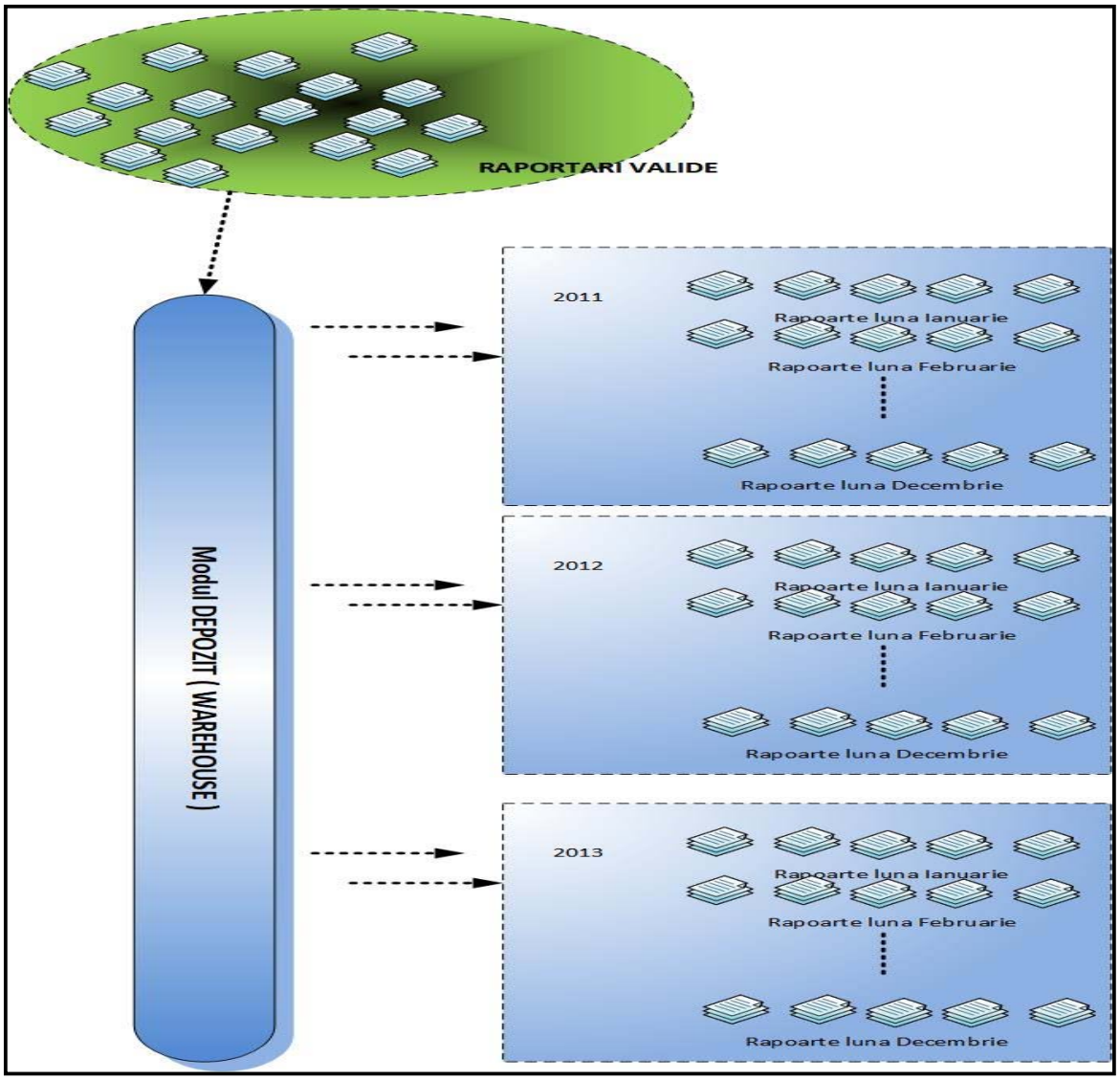


Figura 8. Schema Modul Depozit Rapoarte DRG (Warehouse)

Zona de stocare a Modulului Depozit (warehouse) poate fi controlată atât de administratorii sistemului DRG cât și de inginerii de sistem informatic MCloud.

Modulul de Analiză la nivel de Baza de Date

Sistemul DRG creează în mod dinamic o bază de date updatată permanent, cu informații consistente; sistemul este un instrument performant de interogare care permite extragerea de rapoarte necesare CNAM și MS, oferind o imagine clară a istoricului diagnosticelor pacienților; pe baza acestora se pot identifica eventualele neconcordante ulterioare în diagnosticarea pacientului.

Prin interogarea bazei de date temporare, în care sunt depozitate rapoartele trimise în vederea validării și închiderii, se pot obține statistici în timp real. Odată ce perioada de raportare este încheiată, baza de date Warehouse conține informațiile corecte și complete ale perioadei anterioare.

Modulul de analiza, raportare și audit poate fi utilizat de departamentele autorizate ale CNAM în vederea generării de rapoarte bazate pe template-uri, dar și ad-hoc, utile în activitatea curenta. Sistemul răspunde următoarelor solicitări:

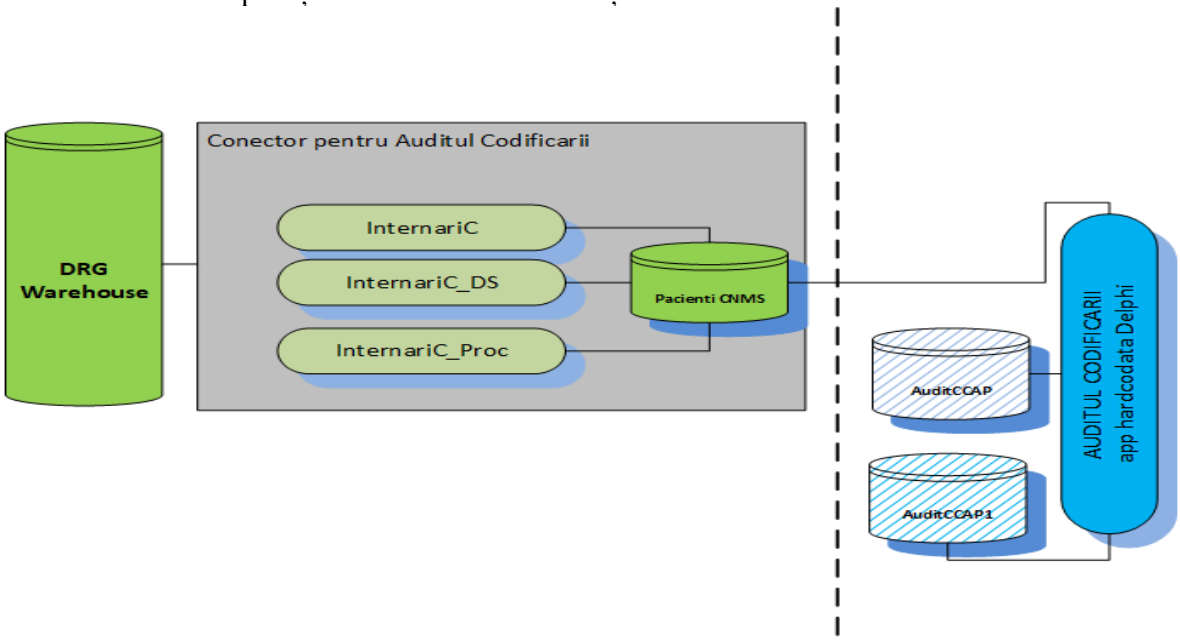
1) Evitarea fraudării. Sistemul SI DRG este un sistem operațional la nivel național, iar CNAM dispune de o baza de date unică, cu informații reale; veridicitatea informațiilor se verifica in doua feluri:

- în timp real: respingerea informațiilor eronate cu atenționarea celui care introduce datele; sistemul nu permite introducerea de date necorespunzătoare.
- în urma auditării: personalul CNAM poate genera rapoarte de audit și control prin care sunt identificate cazurile suspecte; aceste rapoarte pot fi organizate în template-uri pentru a fi reutilizate, dar pot fi customizate în așa fel încât echipele care executa auditarea și evaluare să obțină o lista consistentă și reală pe care sa o verifice și în teren. Prin utilizarea sistemului informatic pot fi identificate cazurile de fraudare.

2) Creșterea eficientei. Existenta modulului de analiză, raportare și audit la nivelul CNAM constituie un instrument pe care departamentele autorizate CNAM implicate în raportare îl folosesc în vederea creșterii eficientei de lucru. Căutările sunt rapide, rapoartele sunt generate cu mare ușurința în ciuda complexității deosebite a sistemului. Prin monitorizarea permanentă și corecția raportărilor se elimină cazurile în care spitalele execută raportări care necesită reanalizare și reverificare de către CNAM. Informațiile sunt corecte, validate și disponibile în timp real.

Modulul conector pentru Audit al codificării

Funcționalitatea de audit a codificării este acoperită de o aplicație pentru care CNAM nu deține codul sursa. Cea mai mare parte din informațiile prelucrate de către aplicația de Audit al codificării se găsesc actualizate în timp real în CCAP. În lipsa codului sursă, dezvoltatorii CCAP au reușit să atingă o parte din obiectivele funcționale ale operatorilor care executî auditul codificării prin operațiuni care nu afectează aplicația ci doar baza de date. Astfel operatorii Autorității Contractante care efectuează auditul codificării continuă să folosească vechea aplicație hardcodata care folosește date din warehouse-ul DRG.



CNAM va continua să emită fie solicitări de dezvoltare a sistemului CCAP, fie de execuție a unor proceduri la nivelul bazelor de date și conectorilor în scopul obținerii rezultatelor dorite pană la momentul includerii definitive în CCAP a funcționalităților de audit al codificării. În prezenta procedura de achiziție CNAM solicită operațiuni de mentenanță care se referă exclusiv la funcționalitățile asupra cărora deține codul sursă, urmand ca pe parcursul dezvoltării funcționalităților în cadrul CCAP, aria de mentenanță să se extindă corespunzător. Astfel, CNAM solicită analiza compartimentului

Menu=>„Rapoarte audit” privind verificarea corectitudinii regrupării cazurilor supuse auditului codificării.

Codul dezvoltat în sensul susținerii modului de conectare pentru auditul codificării permite operatorilor de audit să desfășoare în cadrul vechii aplicații două operațiuni:

- **Selectarea fișelor medicale a bolnavului spitalizat pentru audit (Database DRG).**
- **Importul fișelor medicale din "Database DRG" în aplicație şi efectuarea auditului.**

CNAM deține codul sursa necesar pentru prelucrarea noii baze de date **Pacienți CNMS** și asupra **view-rilor de internări** [InternariC, InternariC_DS, InternariC_Proc] și **ListaSpitale**, care colectează și interpretează informațiile din baza de date Wodehouse a DRG, acestea intrând în obiectul operațiunilor de mentenanță pe care urmează să le desfășoare furnizorul serviciilor.

În prezent, la procedura de audit al codificarii prin intermediul aplicatiei CCAP nu este posibilă logarea/autentificarea concominentă a Auditorilor I/II în aplicaţie şi ca urmare nu este posibilă analiza concomitentă/independentă de către Auditor I și Auditor II a fişelor supuse auditului. În acest context, CNAM solicită analiza subiectului prenotat, şi ajustarea compartimentului conform solicitării. Totodată, CNAM subliniază faptul ca, în cazul în care nu este posibilă ajustarea propriu-zisă a conexiunii concomitente în CCAP, CNAM solicită reingineria modulului de audit al codificării în SI DRG.

A. Cerințe de Mentenanță preventivă și Suport

Cerinţele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanţă elaborat de Prestator şi aprobat de Beneficiar.

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanță sistemului DRG, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Actualizarea parametrilor existenți în partea utilizatorilor, conform cerințelor legislației în vigoare (spre exemplu: actualizarea/completarea nomenclatoarelor programelor special, diagnosticelor, procedurilor, spitalelor, rapoartelor, modificarea valorilor relative, aplicarea/anularea aplicării KP, completarea/modificarea algoritmelor de validare și excepțiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora,

conform formatului solicitat și menținerea posibilităților de extragere a datelor de către utilizator.

- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;
- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație pentru utilizatori:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM;
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistența tehnică pentru utilizatorii CNAM prin email și platforma Service Desk pusă la dispoziție de către Furnizor;
- Modalități de asigurare a suportului: email, telefon, acces la distanță;
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare - best effort.

Suport platforma software

Servicii dedicate Sistemelor de Operare

În această categorie se includ următoarele servicii minime relative de administrare şi mentenanță a sistemelor de operare ale SI DRG care vor fi desfășurate de către Furnizor:

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifestă transparent și înlăturarea cauzelor care le-au produs sau recomandarea măsurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- optimizarea configuratiei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanta și disponibilitate a sistemului;
- asigurarea funcționării continue a conectorilor;
- migrarea cazurilor medicale pe perioade definite de timp prin web-servicii pentru instituții medicale cu sisteme informatice proprii;
- mapare câmpuri, import cazuri medicale pe perioade definite de timp prin web-servicii instituții medicale cu sisteme informatice proprii.

Servicii dedicate sistemelor de gestiune a bazelor de date

În această categorie întra următoarele servicii minime relative la Microsoft SQL Server ale DRG care vor fi desfășurate de către Furnizor:

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corecta a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidenţialităţii şi securităţii datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerinţelor de securitate informaţională de către utilizatori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securităţii privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale DRG şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum şi restaurarea acestora.
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

Servicii dedicate componentelor, inclusiv a celor de interoperabilitate

În această categorie întră următoarele servicii minime relative la codul aplicației DRG care vor fi desfășurate de către Furnizor:

- verifică și optimizează secvențele de cod;
- identifică și analizează problemele și potențialele probleme de la nivelul codului;
- rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației;
- soluționează incidentele apărute la nivelul codului;
- modifică rapoartele, șabloanele, serviciile aplicative;
- comunică cu echipele de suport în scopul funcționarii corecte și permanente a sistemului.

Efectuarea testelor de penetrare

Teste de penetrare se referă la o metodă de evaluare a securității sistemului informațional prin simularea unor atacuri cibernetice. Scopul acestor teste este de a identifica și exploata vulnerabilitățile sistemului pentru a evalua cât de bine poate rezista sistemul informațional la atacuri reale. În această categorie întră următoarele servicii minime:

- Simulare a atacurilor;
- Identificarea vulnerabilităților;
- Evaluarea impactului;
- Raportare și recomandări.

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice DRG

DRG este un sistem automatizat care operează în condițiile legislației în vigoare. Prin serviciile prestate, ofertantul va asigura operațiuni de întreținere, suport și recomandări tehnice asupra aplicației, inclusiv în situația modificărilor legislative care afectează componentele software existente în DRG. CNAM precizează că modificarea funcționalităților existente în aplicație în corelație cu modificările legislative presupun în mod concret modificări în codul sursă al aplicației.

Orice modificare asupra codului sursa are ca efect o nouă versiune operațională a aplicației, conforma legislației. CNAM solicită ofertantului asumarea faptului că deține cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toată perioada desfășurării contractului.

Operațiunile tehnice de întreținere ce vor fi desfășurate de personalul care va asigura funcționarea continuă a DRG se referă la componentele majore ale sistemului, adică la:

B. Interfața DRG prin care instituțiile medicale introduc datele;

C. Conectorii de tip „web-services” cu instituțiile medicale care au propriile sisteme informatice;

D. Regulile de validare a raportărilor. Tratarea excepțiilor;

E. Bazele de date ale sistemului – servicii de întreținere;

F. Rapoarte CNAM.

Pe lângă strânsă comunicare tehnică pe care echipa tehnică de suport aplicativ și platforma trebuie sa o aibă cu specialiștii M-Cloud, au fost identificate, fără a ne limita la acestea, următoarele operațiuni specifice care fac obiectul serviciilor de întreținere și suport specifice DRG:

Reguli de Validare

- Întreținerea modului de validare, a regulilor definite, conexiunilor cu baza de date și operațiuni de securitate specifice modulului.
- Actualizarea nomenclatoarelor DRG: Program Special, Diagnostice, Proceduri, Categorii Asigurat, Lista Spitale, KP, Criterii de Validare, etc.
- Modificarea criteriilor/regulilor de validare. Tratarea excepțiilor pentru criteriile de validare.
- Analize de impact pentru modificarea criteriilor/regulilor de validare la cerere. Recomandări și corectare situații neconforme.
- Actualizarea metodei de configurare a secțiilor. Păstrarea ID-urilor unice.

Întreținerea bazei de date a sistemului

- Operațiuni de administrare și optimizare a bazei de date pe infrastructura existentă.
- Operațiuni de migrare pe alte servere ale Beneficiarului care nu presupun modificarea arhitecturii sistemului.
- Operațiuni de întreținere a securității bazei de date.

- Operațiuni de analiza și auditare a securității bazei de date.

Rapoarte CNAM

- Generarea programată a rapoartelor.
- Îmbunătățirea, ajustarea și completarea rapoartelor CNAM. Raport complex, intern, etc.
- Implementarea restricțiilor CNAM: obligativitate câmpuri în dependența cu datele completate, eliminare cazuri medicale dublate, diagnostice secundare, proceduri secundare, etc.

B.Cerințe de mentenanță adaptivă şi corectivă a DRG

Asumarea contextului adaptării şi corecţiei software

În categoria serviciilor de mentenanță adaptivă şi corectivă a DRG intră acele servicii necesare pentru adaptarea şi corecţia sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul ”A. Cerințe de Mentenanță preventivă și Suport”.

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

- Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.
- Asumarea serviciilor din acest proiect implica acordarea garanției asupra DRG pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.
- În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.
- În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la DRG, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de DRG.
- Furnizorul este responsabil pentru eventualele incidente asupra DRG generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.
- Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.

➢ În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.

➢ Ofertanții trebuie sa demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport şi menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.

➢ Cererile de ajustări au termene relativ scurte și survin în general în urma unor modificări legislative sau în urma îmbunătățirilor funcționării business-proceselor. CNAM a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Pentru buna desfășurare a operațiunilor, dar și de consultanță în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnică a Furnizorului trebuie să fie pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și să dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului ajustărilor care sunt propuse de Beneficiar sau care sunt necesare în așa fel încât să asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie ajustări.

CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 900 de om/ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a DRG cum ar fi: ajustarea unor module ale DRG, ajustarea compartimentului Rapoarte, de asemenea, dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, etc. Rezervarea a 900 de om/ore la un preț prestabilit creează CNAM avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale DRG și asigură continuitatea serviciului în situațiile urgente.**

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

Serviciile de mentenanță adaptivă și corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

Solicitarea serviciilor de mentenanță adaptivă şi corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului și a costului estimativ conform tarifelor.

Prestarea serviciilor de mentenanță adaptivă şi corectivă

Prestarea serviciilor de mentenanță adaptivă şi corectivă se va efectua cu aplicarea următoarelor reguli:

➢ Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului și acceptării rezultatului de către Beneficiar.

➢ Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.

➢ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condiţiile iniţiale ale solicitării (formularea problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.

➢ Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ţinînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.

➢ Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor și condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

DRG este găzduit în MCloud-ul guvernamental. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a Beneficiarului. Toate operațiunile se vor desfășura în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

➢ Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental

➢ Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.

➢ Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client "Hot-Line"

Suportul operaţional la utilizarea serviciilor este asigurat de către Prestator prin intermediul Serviciului de Suport Client "Hot-Line" (în continuare SSC) cu oferirea unei platforme de Service Desk. Beneficiarul va contacta SSC, prin întocmirea Cererilor, în următoarele scopuri:

➢ pentru soluționarea defectelor;

➢ pentru solicitarea modificărilor funcționalităților existente;

➢ pentru solicitarea informației şi consultanței în vederea soluționării defectelor legate de utilizarea sistemului;

➢ pentru solicitarea realizării anumitor activităţi şi acţiuni ce sunt în responsabilitatea Prestatorului;

➢ pentru solicitarea analizei unei solicitări de modificare.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități:

➢ expedierea unui e-mail la adresa SSC;

➢ efectuarea unui apel telefonic;

➢ crearea unui ticket în platforma de Service Desk.

Orice defect sau necesitate apărută la utilizarea serviciilor, Beneficiarul o va adresa inițial către SSC. În caz de necesitate, problema poate fi ulterior escaladată către Managerul de Proiect sau conducătorul Prestatorului. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului şi Beneficiarului, pentru a gestiona orice aspect ivit în relaţiile dintre aceştia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul.

Reguli privind prestare a serviciilor de suport

Serviciile de suport sunt orientate soluţionării incidentelor şi problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor şi actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul şi Beneficiarul vor conlucra strîns în vederea prevenirii incidentelor şi în vederea soluţionării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul şi prioritatea acordată pentru soluţionarea unui incident va ţine cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecinţele acestuia asupra disponibilităţii şi performanţei softului aplicativ. Urgenţa incidentului caracterizează operativitatea cu care acesta trebuie soluţionat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare şi soluţionare a incidentelor va fi în funcţie de impactul şi urgenţa incidentului. Algoritmul aplicat pentru stabilirea priorităţii unui incident este definit în continuare.

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

PRIORITATE		**Impact**		
		Înalt	*Mediu*	*Jos*
Urgenţă	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENŢĂ	**Descriere**
Înaltă	Un incident este estimat ca avînd nivelul urgenţei „Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activităţi şi operaţiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacţiunea imediată poate preveni riscuri legale majore şi de securitate (protecţie) a informaţiei.
Medie	Un incident este estimat ca avînd nivelul urgenţei „Mediu” în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activităţi şi operaţiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacţia operativă poate preveni riscuri legale moderate şi de securitate a informaţiei.
Joasă	Un incident este estimat ca avînd nivelul urgenţei „Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puţin în timp; - activităţile şi operaţiunile afectate nu trebuie continuate imediat; - nu există riscuri legale şi de securitate a informaţiei semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	**Descriere**
Înalt	Un incident este estimat ca avînd nivelul impactului „Înalt” în una sau mai multe din următoarele cazuri: - activităţile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizaţiei Beneficiarului şi afectează utilizatori

	externi, reputaţia şi imaginea Beneficiarului; - există riscuri legale şi financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca avînd nivelul impactului „Major" în una sau mai multe din următoarele cazuri: - activităţile importante ale Beneficiarului sunt întrerupte sau activităţile cheie sunt desfăşurate cu dificultate; - incidentul a afectat utilizatori interni şi un număr nesemnificativ de utilizatori externi; - există riscuri legale şi financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca avînd nivelul impactului „Jos" în una sau mai multe din următoarele cazuri: - activităţile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activităţile importante sunt desfăşurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru (8:00 – 17:00). În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort".

Prioritate incident	**Timpul de reacţie**	**Timpul de soluţionare**	**Timp maxim pentru corectare a cauzei***	**Raportare primară**
Critică	Timpul de reacţie al Prestatorului – imediat	pînă la 3 ore	8 ore	SSC (în afara orelor de lucru – Manager de Proiect)
Înaltă	Timpul de reacţie al Prestatorului – 15 minute	8 ore	ora 12 a zilei următoare	SSC (în afara orelor de lucru – Manager de Proiect)
Medie	Timpul de reacţie al Prestatorului – 4 ore	24 ore	5 zile	SSC (în afara orelor de lucru – Manager de Proiect)
Joasă	Timpul de reacţie al Prestatorului – 24 ore;	3 zile	10 zile	SSC
Neglijabilă	Timpul de reacţie al Prestatorului – 72 ore;	Cel mai bun efort	-	SSC

***Notă:** se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.*

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergenţe apărute între Părţi vor fi soluţionate cu efort comun şi prin strînsă conlucrare între Părţi. În acest scop, vor fi aplicate următoarele reguli:

- Părţile vor forma un grup comun de lucru în scopul soluţionării divergenţelor. De comun acord, în grupul de lucru pot fi acceptaţi reprezentanţi ai părţilor terţe, inclusiv experţi independenţi.
- La necesitate, părţile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergenţă.
- Grupul de lucru se va convoca şi va examina subiectul divergenţelor şi probele existente la subiect. Părţile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluţii echitabile pentru divergenţele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Prestatorul este responsabil pentru securitatea tehnologică şi funcţională a softului aplicativ în limitele sarcinilor de mentenanţă îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informaţiei, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părţile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;
- Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

După soluţionarea unui incident de securitate, părţile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acţiuni pentru prevenirea repetării incidentelor similare.

Livrabile

Prestatorul menține în stare actuală documentația tehnică. Documentaţia conţine suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni şi modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.

La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:

- Codul sursă final compilabil pe suport (DVD-R sau USB);
- Documentația tehnică;
- Ghidul utilizatorilor;
- Ghidul administratorului;
- Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Cerințe privind experiența personalului

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.

În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente mentenanței, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini și doar în baza acceptului Beneficiarului.

Ofertantul este obligat să informeze în prealabil Beneficiarul despre necesitatea modificării echipei de mentenanță, va transmite CV-ul persoanei care înlocuiește și va confirma recepționarea răspunsului (de acceptare sau refuz) expediat de către Beneficiar. Beneficiarul își rezervă dreptul de a refuza modificarea componenței minime a echipei în cazul în care pregătirea profesională și experiența noilor membri nu corespunde cerințelor stabilite în prezent caiet de sarcini sau solicitarea privind modificarea echipei nu este relevantă.

CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.
- Deținerea certificatului Project Manager sau documentului analogic de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor și/sau emis de o instituție publică sau privată competentă cu recunoaștere generală.
- Minim 3 ani de experiență în managementul proiectelor în domeniul tehnologiilor informaționale.
- Minim 3 proiecte în domeniul tehnologiilor informaționale realizate în calitate de Manager de proiect.
- Minim 3 ani de experiență în utilizarea metodologiilor de management de proiecte recunoscute pe plan internațional.
- Experiență specifică de Manager de Proiect în cel puțin 3 proiecte de complexitate similară, pe toată durata proiectului, realizate cu succes.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Business Analist *(minim 1 persoană)*

- Studii superioare în domeniul ingineriei sau tehnologiilor informaționale confirmate prin diploma de absolvire.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Cel puțin 3 ani de experiență în domeniul tehnologiilor informaționale.
- Cel puțin 3 ani de experiență în domeniul analizei și modelării Business-proceselor.
- Experiență profesională specifică, confirmată prin participarea în cel puțin 3 proiecte similare de implementare a unui sistem informatic integrat similar, în care el/ea s-a poziționat ca Business Analitic.
- Experiență în implementarea sistemelor informaționale complexe în instituțiile bugetare și/sau în domeniul medical.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist securitatea informațională (minim 1 persoană)

- Studii superioare Tehnice sau în domeniul TI.
- Cunoștințe privind securitatea sistemelor informatice și securitatea sistemelor ce conțin informații cu caracter personal, dovedite prin diplome/certificate obținute.
- Cunoștințe privind auditul sistemelor informatice dovedite prin diplome/certificate obținute (ISO27001, CISA sau echivalent*).
- Experiență de cel puțin 3 ani în domeniul securității sistemelor informatice.
- Participarea în ultimii 3 ani ca consultant sau auditor la cel puțin 3 contracte în domeniul securității informației.
- Participarea în cel puțin 3 contracte similare ca expert de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist infrastructură sistem (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență profesională generală în domeniul de specialitate de minim 3 ani;
- Experiență dobândită prin participarea în cel puțin 3 proiecte în activități IT complexe privind infrastructura software și hardware pe platforme în baza tehnologiei de „cloud computing"

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist programator (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență de minim 3 ani în programarea aplicațiilor web: Java, Java script, HTML, CSS, etc;
- Experiență dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de implementare a unui sistem informațional de complexitate similară

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist baze de date (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență de minim 3 ani în administrarea bazelor de date: MS SQL Server;
- Experiență dobândită prin participarea în calitate de specialist în baze de date în cel puțin 3 proiecte de implementare a unui sistem informatic de complexitate similară

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Software Tester (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Experiență demonstrată în testarea funcțională a sistemelor informaționale;
- Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale;
- Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din

partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Anexa nr.2

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **SIP**

CAIET DE SARCINI

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	Descriere
Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP: • *Servicii de mentenanță preventivă și Suport – în bază de abonament;* • *Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.*	*Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.*

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP (în continuare – SIP) pentru o perioadă de **minim 12 luni** după încetarea contractului.

De asemenea, Prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta CNAM (Beneficiar) împreună cu codul sursă DRG, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Descriere generală a SIP

SIP este destinat evidenței și raportării serviciilor medicale de înaltă performanța și urmărește automatizarea proceselor care au loc în activitatea prestatorilor de servicii medicale care se contractează după metoda "per serviciu", privind estimarea necesității de servicii medicale de înaltă performanță, posibilitatea de programare a persoanelor în IMS care prestează servicii medicale și evidența personificată a serviciilor medicale prestate. SIP oferă transparență în procesul de prestare a serviciilor medicale de înaltă performanta, astfel ca pacientul are dreptul de a alege la care prestator vrea să meargă pentru servicii medicale, iar modul în care sunt alocate aceste servicii este conform procedurilor CNAM.

Setul de date folosit în funcționalitatea sistemului cuprinde:

- IDNP al pacientului;
- IDNP al medicului prescriptor;
- IDNO prestatorului de servicii medicale în care activează medicul;
- Denumirea prestatorului de servicii medicale în care activează medicul;
- IDNO al prestatorului de servicii de înaltă performanță;
- Denumirea prestatorului de servicii de înaltă performanță;
- Data și ora trimiterii la serviciile medicale;
- Codul serviciilor medicale prescrise;
- Codul serviciilor medicale prestate;

- Denumirea deplină a serviciilor de înaltă performanță;
- Data și ora generării sloturilor pentru serviciile medicale;
- Data și ora efectuării programării serviciilor medicale;
- Data și ora prestării serviciilor medicale;
- Statutul/categoria serviciilor medicale
- Diagnosticul la trimitere (prin selectare din Lista Diagnosticelor);
- Numele și Prenumele Pacientului;
- Data nașterii;
- Adresa la domiciliu.

Beneficiarii direcți ai SIP sunt CNAM, pacientul asigurat, medic prescriptor (medic de familie sau medic specialist), prestator servicii medicale, care deține contract cu CNAM.

Specificații tehnice SIP

Caracteristici generale de funcționare

SIP are o arhitectură 3-layer, arhitectura care permite funcționarea pe platforma guvernamentală comună MCloud. SIP funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă tot ce este necesar de automatizat;
- are posibilitatea reparației unui modul fără afectarea altora;
- respecta standardele în vigoare a tehnologiilor informaționale;
- asigura flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare;
- utilizează o arhitectură orientată pe servicii pentru a acomoda cu ușurință noi modificări cu intervenții exclusiv asupra componentei de updatat, minimizând costurile și timpul necesar realizării modificărilor;
- are o arhitectură modernă cu un grad înalt de performanță, structurată pe 3 niveluri (nivelul pentru baze de date, nivelul pentru aplicație si nivelul acces/utilizator). Fiecare nivel are în componența toate echipamentele necesare bunei funcționări.
- SIP este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- poate fi utilizat împreună cu echipamente ce permit creșterea vitezei de înregistrare a datelor de identificare ale pacienților (nume, prenume, IDNP etc.)
- este scalabil pentru a acomoda modificările viitoare ale numărului de utilizatori ai soluției;
- recunoaște corect sursele informaționale, le acceptă și le integrează în sistem;
- întreține în limba de stat interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate;
- permite ca utilizatorul să se autentifice o singură data pentru a accesa toate modulele aplicației;
- Poate fi accesat de pe telefon, PC, notebook, etc.

Interfața Utilizator

Aceasta interfața este accesibilă pentru toți utilizatorii autorizați în SIP:

- ✓ SIP dispune de o interfață inteligenta, intuitiva și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browser-ul web și nu necesită instalarea de componente software suplimentare;

- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului
- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:

- **Platforma hardware**, formată din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat în sistemul MCloud:
  - Servere protejate redundant pentru hosting al bazelor de date, softului de sistem si softului funcțional (aplicații și subsisteme);
  - Platforma hardware pusă la dispoziție de către beneficiar este dimensionată corespunzător pentru a permite funcționarea în bune condiții a sistemului;
  - Performanța optimă, în limita normelor obiective de uzură, pentru realizarea structurii funcționale și asigurarea extinderii ulterioare a sistemului;
  - este flexibilă în utilizarea mijloacelor disponibile destinate recepționării informației din surse externe (alte instituții publice);
  - asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date;
  - asigură normele de funcționare ale platformelor informatice guvernamentale.

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:
  - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
  - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server.
  - Pe stațiile utilizatorilor există navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare si transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mijloacele de imprimare, cititoare, rețele electronice locale (LAN – local area network) și de scară largă (WAN – wide area network). Pentru operare se folosesc stațiile de lucru ale beneficiarului, singură specificație impusă utilizatorilor fiind cea de a dispune de un browser conectat la internet, fiind recomandate și utilizate soluțiile Microsoft.

Sistemul de securitate

SIP funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.

Caracteristici:

- asigura accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare si consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de sistem.
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor.

Având în vedere natura specială a informațiilor gestionate în cadrul SIP, acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.

Sistemul are următoarele nivele de securitate care asigura confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație intre stații si server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unica cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este asigurată automat, iar modificările de structura la nivelul acesteia se fac exclusiv în baza drepturilor corespunzătoare de administrator al bazei de date. În plus, baza de date deține propriul mecanism de backup care permite, în caz de dezastru, restaurarea unor versiuni anterioare recente (de ordinul zilelor).

Sistemul asigura dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori sunt create module de acces și autentificare în sistem; sunt indicate volumul de informație și funcționalitatea pe care aceștia o accesează. Sistemul permite accesul la datele statistice pentru anumiți utilizatori și grupuri de utilizatori. Sistemul asigură verificarea automată a drepturilor în momentul intrării în sistem și în ulterioarele accesări a sistemului și creează un jurnal al accesărilor – jurnalul de audit.

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Prestator/Prescriptor**: permite introducerea și modificarea datelor specifice activității sale;
- nivelul **Administrator**: permite înregistrarea și modificarea datelor specifice activității sale, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

La nivel aplicativ, sistemul generează o lista de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

- ✓ posibilitatea înregistrării, adăugării si dezactivării utilizatorilor din sistem;
- ✓ posibilitatea distribuției drepturilor utilizatorilor folosind grupuri de acces;
- ✓ posibilitatea pentru fiecare utilizator de a avea cel puțin următoarele atribute de autentificare: identificarea, autentificarea.
- ✓ posibilitatea intrării în sistem a unui utilizator în orice moment;
- ✓ asigurarea de către administrator a regimurilor de funcționare, deconectare, conectare, modificării regimului de autentificare și identificare, dirijarea cu drepturi și auditul.

Retenția datelor, acces securizat

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.

- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respecta regulile de control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.

- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.

- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați sa acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem si pe baza permisiunilor asociate rolului sau rolurilor din care fac parte utilizatorii.

- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați sa acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fisele electronice ale pacienților săi.

- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu ca a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:

    - Unicitatea utilizatorilor în sistem;

    - Mecanism de control al versiunilor pentru înregistrările medicale.

- **Securizarea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.

Arhitectura SIP

SIP are o arhitectură bazată pe tehnologie web, folosind platforma Microsoft/Linux Sistemul este conceput modular, dezvoltarea acestora putând fi realizata în paralel. Orice client se poate conecta la serverul de aplicație și poate utiliza sistemul conform drepturilor pe care le are. Comunicația între client și server se realizează exclusiv prin protocoale securizate de tip HTTPS folosind certificat de securitate integrat la nivelul serverului de aplicație. Schema arhitecturală este în figura următoare:

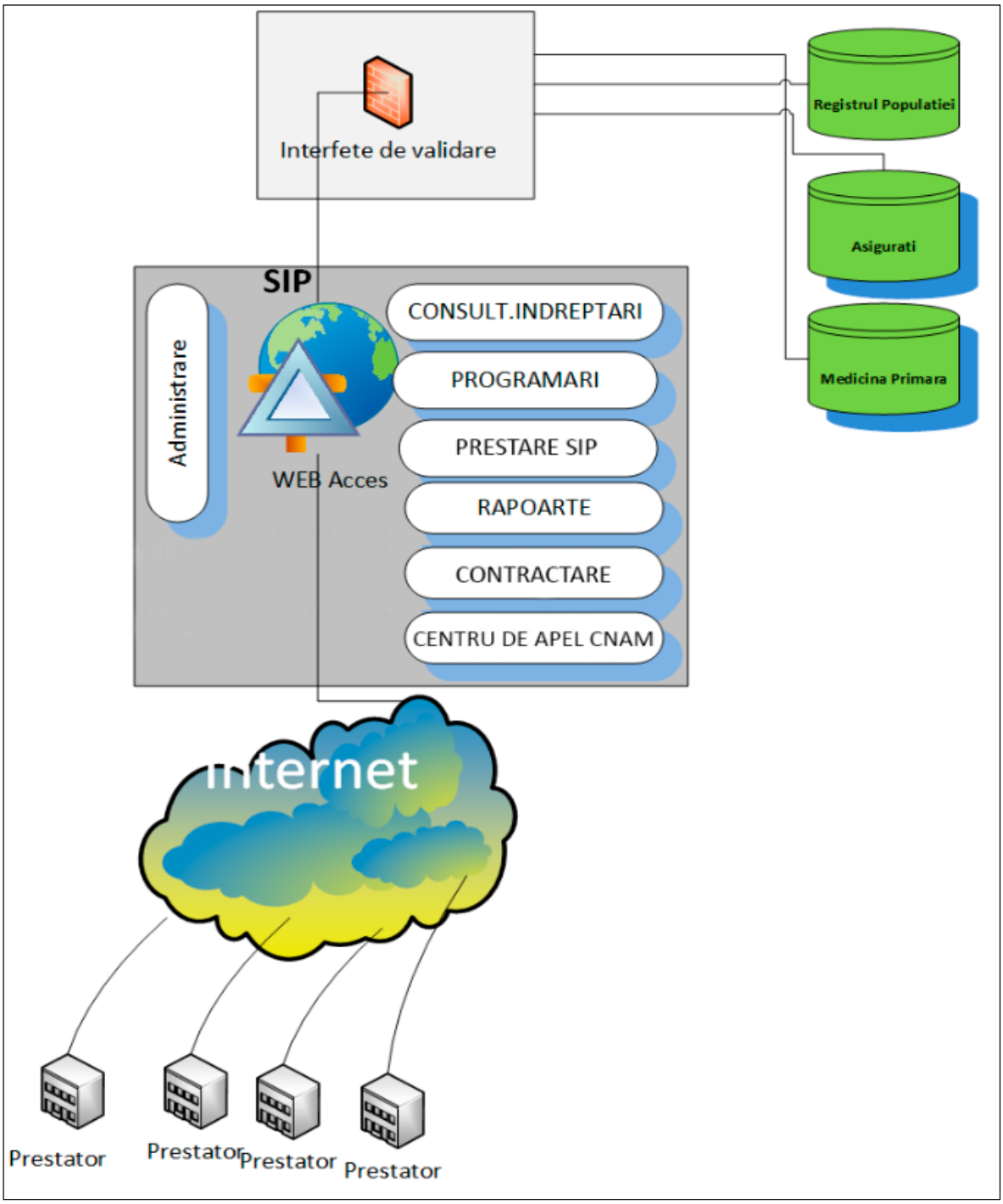


Figura 1. Schema arhitecturală SIP

Componente operaționale ale SIP sunt operaționale în următoarea structură modulară:

- ✓ Modulul de administrare roluri;
- ✓ Modulul consult/îndreptări (prescriere a biletului de trimitere);
- ✓ Modulul programări;
- ✓ Modulul prestare a serviciilor de înalta performanță;
- ✓ Modulul rapoarte;
- ✓ Modulul contractare;
- ✓ Interfețe.

Modulul de administrare roluri

Actorii implicați în circuitul informațional privind evidența serviciilor medicale de înaltă performanță sunt:

- Pacient asigurat;
- Administrator CNAM (administrare SIRSM);
- CNAM (responsabil CNAM);
- Medic prescriptor (medic de familie sau medic specialist);
- Prestator servicii medicale, care deține contract cu CNAM.

Administrarea sistemului informatic este realizată de către administratorul (reprezentantul) CNAM pentru partea de conținut a serviciilor medicale în colaborare cu Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) pentru partea de asistență și mijloacele tehnice necesare funcționării SIP extins în infrastructură hardware & software din cadrul MCloud.

Administratorul sistemului are acces deplin la toate funcționalitățile sistemului, fișiere și baze de date aferente sistemului, încăperile în care se află echipamentele pe care rulează aplicațiile software sau care asigură securitatea datelor.

Medicul prescriptor

În interfața de utilizare a sistemului medicul prescriptor (medic de familie sau specialist) are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului:

- Datele de identificare ale medicului de familie sau specialist cu drepturi de prescriere a serviciilor medicale;
- Adresa;
- IDNO al instituțiilor medicale în care medicul prestează servicii;
- Denumirea instituțiilor medicale în care medicul prestează servicii;
- Cod instituțiilor medicale în care medicul prestează servicii.

Pentru medicul de familie sau medicul specialist, interfața de utilizare a sistemului are o formă simplă care îi permite efectuarea rapida de prescriere, validare și programare servicii medicale a pacientului, după modelul descris în continuare.

Prestatorul de servicii medicale

În interfața de utilizare a sistemului, prestatorul de servicii medicale are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului, în directa corespondență cu contractul CNAM, pe care nu le poate modifica:

- IDNO al instituției prestatoare de servicii medicale;
- Adresa instituției;
- Numărul contractului;

- Lista de servicii medicale asumate pe grupuri și programe, inclusiv sumele contractuale specificate pentru perioadele pe care sunt programate aceste sume.

Pe lângă acestea, administratorul local al prestatorului are în cadrul interfeței:

- Câmpurile necesare definirii listei de servicii medicale ce pot fi executate;
- Opțiunile de alocare a serviciilor disponibile în lista pe sloturi libere (secvențe de timp);
- Posibilitatea de urmărire a atributelor la nivel de serviciu și slot.

Posibilitatea de urmărire a relației dintre serviciile medicale contractate și cele alocate în sloturi.

Modul consult/îndreptări

Modulul consult urmărește traseul prescrierii serviciului medical și programării pacientului la serviciile medicale de înaltă performanță. Sistemul dispune de mecanismele de restricție și control prin care acest flux va fi urmărit permanent:

- Pacientul se prezintă la medicul de familie sau la medicul specialist, unde prezintă datele de identificare. Identificatorul unic al pacientului este IDNP-ul.
- Medicul introduce în sistem IDNP-ul.
- Prin intermediul web-serviciilor sistemul verifica automat statutul de asigurat al pacientului și validează alocarea pacientului la medicul de familie care efectuează operațiunea curentă.
- Dacă asigurarea pacientului nu este validată de către sistem (pacientul nu are statut de asigurat), medicul nu poate prescrie biletul de trimitere. La fel, dacă sistemul nu confirmă că pacientul este alocat medicului de familie curent, atunci medicul nu poate îndrepta pacientul către servicii medicale.
- Scenariul favorabil pentru prescrierea biletului de trimitere la serviciul medical este cel în care pacientul este validat de sistem cu statut de asigurat și ulterior înregistrat la medicul de familie curent sau, în situații excepționale (concediu, boala) de înlocuitorul acestuia. În acest caz, medicul stabilește în baza consultului necesitatea unei investigații din lista de servicii medicale conform Programului.

Modul programări

Programarea efectivă a pacientului constă în alocarea unui slot (interval definit de timp în care un anumit serviciu este disponibil).

- Programarea pacientului la serviciul medical se bazează pe dreptul pacientului la libera alegere a prestatorului.
- Pacientul asigurat și înregistrat la medicul de familie care efectuează consultul are dreptul la servicii medicale plătite din fondul CNAM. Medicul de familie sau medicul specialist decid în baza consultului aceasta necesitate, iar sistemul emite un **cod unic al biletului de trimitere a pacientului către servicii medicale CNAM.**
- Codul unic al biletului de trimitere poate fi folosit în interesul pacientului în <u>următoarele</u> moduri:
  a) Medicul prescriptor se consultă cu pacientul în vederea programării în SIP a pacientului într-unul din sloturile libere declarate de către Prestatori, în funcție de distanța și disponibilitatea definite de Prescriptor.
  b) Pacientului îi este tipărit numărul de trimitere și detaliile consultului urmând sa își facă singur programarea la serviciul de înaltă performanță prin intermediul SIP.
  c) Pacientului îi este tipărit numărul de trimitere și detaliile consultului urmând să-și facă programarea prin intermediul Centrului de apel al CNAM.

Modulul prestare a serviciilor de înaltă performanță

Executarea efectivă a serviciilor de înaltă performanță este o operațiune a prestatorului care se încheie cu confirmarea prestării acestuia și completarea rezultatului. Prestarea se consideră încheiată doar în momentul în care pacientul are un rezultat în urma investigației.

- În interfața sistemului prestatorul declară sloturile libere pe grupe de servicii de înaltă performanță, în corespondență cu contractul CNAM. Aceste sloturi sunt completate automat în baza programărilor efectuate. Prestatorul are acces la datele de corespondență ale pacientului.
- După prezentarea pacientului pentru efectuarea investigației, prestatorul completează în sistem rezultatul și închide programarea.
- Pacientul primește rezultatul investigației în mod fizic (tipărit) și continuă investigațiile sau tratamentul la îndrumarea medicului care i-a prescris serviciul medical.
- Sistemul înregistrează încheierea prestării și confirmă CNAM că serviciul medical contractat de către prestator a fost prestat și ca poate fi plătit.

Modulul rapoarte

În cadrul interfeței de lucru sunt disponibile în timp real următoarele valori:

- Încărcarea prescriptorilor: în sistem sunt disponibile valorile per medic prescriptor. De asemenea în sistem apar valori adiacente: date despre prescrieri, prescriptor, pacient, servicii medicale etc. Sistemul poate folosi aceste informații în scop de analiză pentru realizarea de rapoarte statistice.
- Încărcarea prestatorilor: în sistem sunt disponibile listele de servicii medicale contractate, alocarea pe sloturi, executarea serviciilor de înaltă performanță în timp real în directă corespondență cu contractul CNAM.

Efectuarea programărilor. În sistem sunt disponibile în timp real toate informațiile despre programări, servicii medicale, prestatori, prescriptori și datele în corespondența cu contractul CNAM. În cadrul interfeței administratorul poate vedea efectuarea programărilor în timp real dar și pe intervale de timp definite ad-hoc.

Modulul contractare

În modulul contractare se înregistrează volumele contractuale în dependență de lista de servicii medicale, numărul de servicii, tarife, sumele contractate. În interfața acestui modul sunt disponibile următoarele funcționalități:

- Modificarea/actualizarea nomenclatorului serviciilor medicale din Anexa nr. 5 al PU (nr.de ordine, denumire serviciu, cod serviciu tarif serviciu) în dependență de modificare Programului Unic;
- Modificarea/actualizarea listei prestatorilor și prescriptorilor (denumire deplina și scurta a prestator/prescriptor, adresa/locația, IDNO, codul din 4 cifre);
- Introducerea și înregistrarea contractelor cu prestatorii în dependență de: număr contract, perioada de timp (lista serviciilor de înaltă performanță: nr.de ordine, denumire, cod, număr de servicii, tarif, sumă);
- Modificarea contractelor prin Acord adițional în dependență de: număr acord adițional, perioada de timp (lista serviciilor de înaltă performanță: nr.de ordine, denumire, cod, număr de servicii, tarif, sumă).

A. Cerințe de Mentenanță preventivă și Suport

Cerințele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se

manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanţă elaborat de Prestator şi aprobat de Beneficiar.

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanța SIP, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;
- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație pentru utilizatori:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM;
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistența tehnică pentru utilizatorii CNAM prin email și platforma Service Desk pusă la dispoziție de către Furnizor;
- Modalități de asigurare a suportului: email, telefon, acces la distanță;
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare - best effort.

Suport platforma software

Servicii dedicate Sistemelor de Operare

În aceasta categorie întră următoarele servicii minime relative la sistemele de operare pe care rulează SIP care vor fi desfășurate de către Furnizor:

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifesta transparent și înlăturarea cauzelor care le-au produs sau recomandarea masurilor ce trebuie luate pentru a nu mai apărea astfel de erori;

- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- creare și întreținere conturi de acces locale;
- optimizarea configuratei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanță și disponibilitate a sistemului.

Servicii dedicate sistemelor de gestiune a bazelor de date

În această categorie întră următoarele servicii minime relative la Microsoft SQL Server ale SIP care vor fi desfășurate de către Furnizor:

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corecta a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidenţialităţii şi securităţii datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerinţelor de securitate informaţională de către utilizatori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securităţii privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale SIP şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum şi restaurarea acestora.
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

Servicii dedicate componentelor, inclusiv a celor de interconectare

În această categorie întră următoarele servicii minime relative la codul SIP care vor fi desfășurate de către Furnizor:

- verifică și optimizează secvențele de cod;
- identifică și analizează problemele și potențialele probleme de la nivelul codului;
- rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației;
- soluționează incidentele apărute la nivelul codului;
- modifică rapoartele, șabloanele, serviciile aplicative;
- comunică cu echipele de suport în scopul funcționarii corecte și permanente a sistemului.

Efectuarea testelor de penetrare

Teste de penetrare se referă la o metodă de evaluare a securității sistemului informațional prin simularea unor atacuri cibernetice. Scopul acestor teste este de a identifica și exploata vulnerabilitățile sistemului pentru a evalua cât de bine poate rezista sistemul informațional la atacuri reale. În această categorie întră următoarele servicii minime:

- Simulare a atacurilor;
- Identificarea vulnerabilităților;
- Evaluarea impactului;
- Raportare și recomandări.

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice SIP

SIP este un sistem automatizat care operează în condițiile legislației în vigoare. Prin serviciile prestate, ofertantul va asigura operațiuni de întreținere, suport și recomandări tehnice asupra aplicației, inclusiv în situația modificărilor legislative care afectează componentele software existente în SIP. CNAM precizează că modificarea funcționalităților existente în aplicație în corelație cu modificările legislative presupun în mod concret modificări în codul sursa al aplicației.

Orice modificare asupra codului sursă are ca efect o noua versiune operațională a aplicației, conform legislației. CNAM solicită ofertantului asumarea faptului că, deține cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toata perioada desfășurării contractului.

Operațiunile tehnice de întreținere ce se vor desfășura de personalul care va asigura funcționarea continuă a SIP se referă la componentele majore ale sistemului, adică la:

- ✓ Interfața SIP prin care prescriptorii și prestatorii introduc datele;
- ✓ Bazele de date ale sistemului – servicii de întreținere;
- ✓ Rapoarte CNAM;

B.Cerințe de mentenanță adaptivă şi corectivă a SIP

Asumarea contextului adaptării şi corecţiei software

În categoria serviciilor de mentenanță adaptivă şi corectivă a SIP intră acele servicii necesare pentru adaptarea şi corecţia sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul ”A. Cerințe de Mentenanță preventivă și Suport”.

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

- Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului.

Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.

- Asumarea serviciilor din acest proiect implica acordarea garanției asupra SIP pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.
- În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.
- În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la SIP, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de SIP.
- Furnizorul este responsabil pentru eventualele incidente asupra SIP generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.
- Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.
- În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.
- Ofertanții trebuie sa demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport şi menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.
- Cererile de ajustări au termene relativ scurte și survin în general în urma unor modificări legislative sau în urma îmbunătățirilor funcționării business-proceselor. CNAM a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Pentru buna desfășurare a operațiunilor, dar și de consultanță în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnică a Furnizorului trebuie să fie pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și să dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului ajustărilor care sunt propuse de Beneficiar sau care sunt necesare în așa fel încât să asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie ajustări.

CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 900 de om/ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a SIP cum ar fi: ajustarea modulelor SIP, elaborarea modulului pentru Centrul de Apel „INFO CNAM”, , de asemenea, dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, etc. Rezervarea a 900 de om/ore la un preț prestabilit creează CNAM**

avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale SIP și asigură continuitatea serviciului în situațiile urgente.

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

Serviciile de mentenanță adaptivă şi corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

Solicitarea serviciilor de mentenanță adaptivă şi corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului şi a costului estimativ conform tarifelor.

Prestarea serviciilor de mentenanță adaptivă şi corectivă

Prestarea serviciilor de mentenanță adaptivă şi corectivă se va efectua cu aplicarea următoarelor reguli:

- Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului şi acceptării rezultatului de către Beneficiar.
- Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.
- Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condiţiile iniţiale ale solicitării (formularea problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.
- Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ţinînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.
- Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor şi condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

SIP este găzduit în MCloud-ul guvernamental. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a Beneficiarului. Toate operațiunile se vor desfășura în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

- Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental
- Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.
- Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client "Hot-Line"

Suportul operaţional la utilizarea serviciilor este asigurat de către Prestator prin intermediul Serviciului de Suport Client "Hot-Line" (în continuare SSC) cu oferirea unei platforme de Service Desk. Beneficiarul va contacta SSC, prin întocmirea Cererilor, în următoarele scopuri:

- pentru soluționarea defectelor;
- pentru solicitarea modificărilor funcționalităților existente;
- pentru solicitarea informației şi consultanței în vederea soluționării defectelor legate de utilizarea sistemului;
- pentru solicitarea realizării anumitor activităţi şi acţiuni ce sunt în responsabilitatea Prestatorului;
- pentru solicitarea analizei unei solicitări de modificare.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități:

- expedierea unui e-mail la adresa SSC;
- efectuarea unui apel telefonic;
- crearea unui ticket în platforma de Service Desk.

Orice defect sau necesitate apărută la utilizarea serviciilor, Beneficiarul o va adresa inițial către SSC. În caz de necesitate, problema poate fi ulterior escaladată către Managerul de Proiect sau conducătorul Prestatorului. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului şi Beneficiarului, pentru a gestiona orice aspect ivit în relaţiile dintre aceştia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul.

Reguli privind prestare a serviciilor de suport

Serviciile de suport sunt orientate soluţionării incidentelor şi problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor şi actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul şi Beneficiarul vor conlucra strîns în vederea prevenirii incidentelor şi în vederea soluţionării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul şi prioritatea acordată pentru soluţionarea unui incident va ţine cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecinţele acestuia asupra disponibilităţii şi performanţei softului aplicativ. Urgenţa incidentului caracterizează operativitatea cu care acesta trebuie soluţionat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare şi soluţionare a incidentelor va fi în funcţie de impactul şi urgenţa incidentului. Algoritmul aplicat pentru stabilirea priorităţii unui incident este definit în continuare.

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

PRIORITATE		**Impact**		
		Înalt	*Mediu*	*Jos*
Urgenţă	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENŢĂ	Descriere
Înaltă	Un incident este estimat ca avînd nivelul urgenţei „Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activităţi şi operaţiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacţiunea imediată poate preveni riscuri legale majore şi de securitate (protecţie) a informaţiei.
Medie	Un incident este estimat ca avînd nivelul urgenţei „Mediu” în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activităţi şi operaţiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacţia operativă poate preveni riscuri legale moderate şi de securitate a informaţiei.
Joasă	Un incident este estimat ca avînd nivelul urgenţei „Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puţin în timp; - activităţile şi operaţiunile afectate nu trebuie continuate imediat; - nu există riscuri legale şi de securitate a informaţiei semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere
Înalt	Un incident este estimat ca avînd nivelul impactului „Înalt” în una sau mai multe din următoarele cazuri: - activităţile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizaţiei Beneficiarului şi afectează utilizatori externi, reputaţia şi imaginea Beneficiarului; - există riscuri legale şi financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca avînd nivelul impactului „Major” în una sau mai multe din următoarele cazuri: - activităţile importante ale Beneficiarului sunt întrerupte sau activităţile cheie sunt desfăşurate cu dificultate; - incidentul a afectat utilizatori interni şi un număr nesemnificativ de utilizatori externi; - există riscuri legale şi financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca avînd nivelul impactului „Jos” în una sau mai multe din următoarele cazuri: - activităţile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activităţile importante sunt desfăşurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru (8:00 – 17:00). În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort”.

Prioritate incident	Timpul de reacţie	Timpul de soluţionare	Timp maxim pentru corectare a cauzei*	Raportare primară
Critică	Timpul de reacţie al Prestatorului – imediat	pînă la 3 ore	8 ore	SSC (în afara orelor de lucru – Manager de Proiect)
Înaltă	Timpul de reacţie al Prestatorului – 15 minute	8 ore	ora 12 a zilei următoare	SSC (în afara orelor de lucru – Manager de Proiect)
Medie	Timpul de reacţie al Prestatorului – 4 ore	24 ore	5 zile	SSC (în afara orelor de lucru – Manager de Proiect)
Joasă	Timpul de reacţie al Prestatorului – 24 ore;	3 zile	10 zile	SSC

Neglijabilă	Timpul de reacţie al Prestatorului – 72 ore;	Cel mai bun efort	-	SSC

***Notă:** se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.*

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergenţe apărute între Părţi vor fi soluţionate cu efort comun şi prin strînsă conlucrare între Părţi. În acest scop, vor fi aplicate următoarele reguli:

- Părţile vor forma un grup comun de lucru în scopul soluţionării divergenţelor. De comun acord, în grupul de lucru pot fi acceptaţi reprezentanţi ai părţilor terţe, inclusiv experţi independenţi.
- La necesitate, părţile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergenţă.
- Grupul de lucru se va convoca şi va examina subiectul divergenţelor şi probele existente la subiect. Părţile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluţii echitabile pentru divergenţele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informaţiei

Prestatorul este responsabil pentru securitatea tehnologică şi funcţională a softului aplicativ în limitele sarcinilor de mentenanţă îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informaţiei, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părţile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;
- Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

După soluţionarea unui incident de securitate, părţile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acţiuni pentru prevenirea repetării incidentelor similare.

Livrabile

Prestatorul menține în stare actuală documentația tehnică. Documentaţia conţine suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni şi modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.

La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:

- Codul sursă final compilabil pe suport (DVD-R sau USB);
- Documentația tehnică;
- Ghidul utilizatorilor;
- Ghidul administratorului;
- Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Cerințe privind experiența personalului

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.

În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente mentenanței, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini și doar în baza acceptului Beneficiarului.

Ofertantul este obligat să informeze în prealabil Beneficiarul despre necesitatea modificării echipei de mentenanță, va transmite CV-ul persoanei care înlocuiește și va confirma recepționarea răspunsului (de acceptare sau refuz) expediat de către Beneficiar. Beneficiarul își rezervă dreptul de a refuza modificarea componenței minime a echipei în cazul în care pregătirea profesională și experiența noilor membri nu corespunde cerințelor stabilite în prezent caiet de sarcini sau solicitarea privind modificarea echipei nu este relevantă.

CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.
- Deținerea certificatului Project Manager sau documentului analogic de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor și/sau emis de o instituție publică sau privată competentă cu recunoaștere generală.
- Minim 3 ani de experiență în managementul proiectelor în domeniul tehnologiilor informaționale.
- Minim 3 proiecte în domeniul tehnologiilor informaționale realizate în calitate de Manager de

proiect.

- Minim 3 ani de experiență în utilizarea metodologiilor de management de proiecte recunoscute pe plan internațional.
- Experiență specifică de Manager de Proiect în cel puțin 3 proiecte de complexitate similară, pe toată durata proiectului, realizate cu succes.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Business Analist *(minim 1 persoană)*

- Studii superioare în domeniul ingineriei sau tehnologiilor informaționale confirmate prin diploma de absolvire.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Cel puțin 3 ani de experiență în domeniul tehnologiilor informaționale.
- Cel puțin 3 ani de experiență în domeniul analizei și modelării Business-proceselor.
- Experiență profesională specifică, confirmată prin participarea în cel puțin 3 proiecte similare de implementare a unui sistem informatic integrat similar, în care el/ea s-a poziționat ca Business Analitic.
- Experiență în implementarea sistemelor informaționale complexe în instituțiile bugetare și/sau în domeniul medical.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist securitatea informațională (minim 1 persoană)

- Studii superioare Tehnice sau în domeniul TI.
- Cunoștințe privind securitatea sistemelor informatice și securitatea sistemelor ce conțin informații cu caracter personal, dovedite prin diplome/certificate obținute.
- Cunoștințe privind auditul sistemelor informatice dovedite prin diplome/certificate obținute (ISO27001, CISA sau echivalent*).
- Experiență de cel puțin 3 ani în domeniul securității sistemelor informatice.
- Participarea în ultimii 3 ani ca consultant sau auditor la cel puțin 3 contracte în domeniul securității informației.
- Participarea în cel puțin 3 contracte similare ca expert de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist infrastructură sistem (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență profesională generală în domeniul de specialitate de minim 3 ani;
- Experiență dobândită prin participarea în cel puțin 3 proiecte în activități IT complexe privind infrastructura software și hardware pe platforme în baza tehnologiei de „cloud computing”

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist programator (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;

– Experiență de minim 3 ani în programarea aplicațiilor web: Java, Java script, HTML, CSS, etc; – Experiență dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de implementare a unui sistem informațional de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Specialist baze de date (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Cunoașterea limbii de stat; – Experiență de minim 3 ani în administrarea bazelor de date: MS SQL Server; – Experiență dobândită prin participarea în calitate de specialist în baze de date în cel puțin 3 proiecte de implementare a unui sistem informatic de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Software Tester (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Experiență demonstrată în testarea funcțională a sistemelor informaționale; – Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale; – Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*

2. Documente obligatorii la depunerea ofertei

Nr. d/o	Descrierea documentului	Mod de demonstrare a îndeplinirii:	Nivelul minim/ Obligativitatea
1.	Prezentarea Declarației privind valabilitatea ofertei conform ***Anexei nr.8*** din Ordinul MF 115/2021	Declarația privind valabilitatea ofertei confirmată prin semnătura electronică	***Da***
2.	Prezentarea Specificații de preț conform ***Anexei nr.23*** din Ordinul MF 115/2021	Specificații de preț, confirmat prin semnătura electronică	***Da***
3.	Prezentarea Specificații tehnice conform ***Anexei nr.22*** din Ordinul MF 115/2021	Specificații tehnice, confirmată prin semnătura electronică .	***Da***
4.	Prezentarea Formularul standard al Documentului Unic de Achiziții European completat	Formularul standard al Documentului Unic de Achiziții European confirmat prin semnătura electronică	***Da***

3. Documente obligatorii la evaluarea ofertelor

- în cazul existenței datelor cu caracter personal informația se remite direct autorității contractante pe poșta electronică achizitii@cnam.gov.md

Nr. d/o	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1.	Vor fi excluși operatorii economici care nu şi-au îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale în conformitate cu	Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertei) - eliberat de Inspectoratul Fiscal Principal de Stat, confirmat prin	***Obligatoriu***

	prevederile legale în vigoare în Republica Moldova sau în ţara în care este stabilit.	semnătura electronică, ori link-ul la accesarea unei baze de date naționale disponibile gratuit pentru autoritatea contractantă care deține informațiile privind lipsa/existența restanțelor. confirmată prin aplicarea semnăturii electronice a participantului	
2.	Declaraţii privind cifra de afaceri în domeniul de activitate aferent obiectului contractului (prestarea serviciilor similare) într-o perioadă anterioară care vizează activitatea pentru ultimii 3 ani - a cîte min 1 000 000,00 lei pentru fiecare din ultimii 3 ani original confirmat prin semnătura electronică a participantului: (la solicitare se va prezenta documente primare de confirmare copiile contractelor, raport financiar etc.)	Declaraţie privind lista principalelor prestări de serviciul efectuate în ultimii 3 ani de activitate similare obiectului de achiziție conform ***Anexei nr. 12*** din Ordinul MF 115/2021 - confirmată prin semnătura electronică	***Obligatoriu***
3.	Demonstrarea accesului la personalul necesar pentru îndeplinirea corespunzătoare a obiectului contractului ce urmează a fi atribuit	Conform Caietului de sarcini (Anexa nr. 1 / Anexa nr.2)	***Obligatoriu***
4.	Declarație de garanție	Autoritatea Contractantă solicită o garanție a aplicației acordată de către ofertanți pentru o perioada de 12 luni de la încetarea contractului. Confirmată prin aplicarea semnăturii electronice a persoanei responsabile a ofertantului. Pe perioada desfășurării contractului, codul sursă al aplicației va fi supus modificărilor efectuate de către specialiștii prestatorului. Orice modificare în codul sursă are ca efect o nouă versiune a aplicației care este supusă garanției contractuale a ofertantului în baza cerințelor minime și obligatorii ale Caietului de Sarcini.	***Obligatoriu***
5.	Va fi exclus din procedura de atribuire a contractului de achiziţii publice orice ofertant sau candidat despre care are cunoştinţă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanţe judecătoreşti, pentru participare la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, pentru fraudă şi/sau pentru spălare de bani, pentru infracţiuni de terorism sau infracţiuni legate de activităţi teroriste, finanţarea terorismului, exploatarea prin muncă a copiilor şi alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	***Obligatoriu*** *Lipsa condamnării pe parcursul a ultimilor 5 ani.*
6.	Va fi exclus orice operator economic care se află în proces de insolvabilitate ca urmare a hotărârii judecătoreşti.	La depunerea ofertei prin declararea în DUAE	***Obligatoriu*** *Nu se află în proces de insolvabilitate*
7.	Garanția pentru ofertă în **valoare de 1%**	**Garanţia pentru ofertă emisă de către o bancă comercială *sau* prin transfer la contul autorităţii contractante, conform următoarelor date bancare:**	***Obligatoriu***

		Beneficiarul plăţii: **Compania Națională de Asigurări în Medicină** Denumirea Băncii: **Ministerul Finanțelor – Trezoreria de Stat** Codul fiscal: **1006601000037** IBAN: **MD30TRGAAC14513001300000** cu nota "Pentru garanţia pentru ofertă la licitaţia publică nr. _____ din _____" Dispoziția de plată va fi atașată în modul scanat *(se va prezenta la depunerea ofertei de către toți ofertanți)	
8.	Garanția de bună execuție a Contractului **în valoare de 5%** din valoarea Contratului	**Contractul va fi însoţit de o Garanţie de bună execuţie (emisă de către o bancă comercială)** *sau* **Garanţia de bună execuţie prin transfer la contul autorităţii contractante, conform următoarelor date bancare:** Beneficiarul plăţii: **Compania Națională de Asigurări în Medicină** Denumirea Băncii: **Ministerul Finanțelor – Trezoreria de Stat** Codul fiscal: **1006601000037** IBAN: **MD30TRGAAC14513001300000** **cu nota "Pentru garanţia de buna execuţie a contractului nr. _____ din _____"** * (Se va prezenta doar de către ofertantul declarat cîștigător odată cu semnarea Contractului)	***Obligatoriu*** *pentru operatorul economic declarat câștigător*
9.	DECLARAŢIE privind confirmarea identităţii beneficiarilor efectivi şi neîncadrarea acestora în situaţia condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani	Declaraţie în conformitate cu **Anexa nr. 3** din documentul (Caiet de sarcini mentenanta 2025-DRG și SIP) autentificată prin aplicarea semnăturii electronice a Participantului – depunere obligatorie după desemnare în calitate de ofertant/ofertant asociat desemnat câștigător ;	***Da*** *– depunere obligatorie după desemnare în calitate de cîștigător*

Președintele grupului de lucru:_____Ion DODON

L.Ș

Anexa nr. 3

APROBAT
prin Ordinul
Ministrului Finanțelor
nr. 145 din 24 noiembrie 2020

DECLARAŢIE
privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

Subsemnatul, _____ reprezentant împuternicit al _____ *(denumirea operatorului economic)* în calitate de ofertant/ofertant asociat desemnat câștigător în cadrul procedurii de achiziție publică nr. _____ din data __/__/___, declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că beneficiarul/beneficiarii efectivi ai operatorului economic în ultimii 5 ani nu au fost condamnați prin hotărâre judecătorească definitivă pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

Numele și prenumele beneficiarului efectiv	IDNP al beneficiarului efectiv

Data completării: _____
Semnat: _____
Nume/prenume: _____
Funcţia: _____
Denumirea operatorului economic _____
IDNO al operatorului economic _____

Anexa nr.22
la Documentația standard nr._____
din "____" _____ 20___

Anexa nr. nr.22.
Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziție_____ din _____
Obiectul achiziției: *achiziţionarea serviciilor de mentenanţă, suport şi dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG și SIP* _____

Denumirea serviciilor	**Denumirea modelului bunului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Lotul 1						
Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG**) – în bază de abonament**				Conform Caietului de sarcini din Anexa nr. 1		**Moldova Standard**
Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG**) – în bază de trouble ticket/ticketing**				Conform Caietului de sarcini din Anexa nr. 1		**Moldova Standard**
Lotul 2						
Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de abonament**. .				Conform Caietului de sarcini din Anexa nr. 2		**Moldova Standard**
Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de trouble ticket/ticketing.**				Conform Caietului de sarcini din Anexa nr. 2		**Moldova Standard**

Anexa nr.23
la Documentația standard nr._____
din "____" _____ 20___

Anexa nr. 33
Specificații de preț

[Acest tabel va fi completat de către ofertant în coloanele 5,6,7,8 și 11 la necesitate, iar de către autoritatea contractantă – în coloanele 1,2,3,4,9,10]

Numărul procedurii de achiziție_____din_____

Obiectul de achiziției *achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,componenta DRG și SIP*

Cod CPV	Denumirea bunurilor/ serviciilor	Unitatea de măsură	Canti-tatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Termenul de livrare/prestare	Clasificație bugetară (IBAN)	
1	2	3	4	5	6	7	8	9	10	
Lotul 1 *achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG*										
72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – **în bază de abonament**	Luni	12					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	
72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) **– în bază de trouble ticket/ticketing**	Om/ore	900					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	
Lotul 2 *achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,componenta SIP*										
72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de abonament**. .	Luni	12					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	

72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de trouble ticket/ticketing.**	Om/ore	900					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	

Semnat:_____ Numele, Prenumele:_____ În calitate de: _____
Ofertantul: _____ Adresa: _____

Anexa nr. 24
la Documentaţia standard nr._____
din "____" _____ 20___

A C H I Z I Ţ I I P U B L I C E

CONTRACT Nr.
privind achiziţia de servicii

I PARTEA GENERALĂ

Obiectul achiziţiei achiziţionarea serviciilor de mentenanţă, suport şi dezvoltare pentru Sistemul Informaţional de Raportare şi Evidenţă a Serviciilor Medicale, componenta DRG
Cod CPV: 72200000-7

"___"_____20__ *mun. Chişinău*

Prestator	**Autoritatea contractantă**
_____, *(denumirea completă a întreprinderii, asociaţiei, organizaţiei)* reprezentată prin _____, *(funcţia, numele, prenumele)* care acţionează în baza _____, *(statut, regulament, hotărîre etc.)* denumit(a) în continuare *Vînzător,* _____, *(se indică nr. şi data de înregistrare în Registrul de Stat)* pe de o parte,	**Compania Naţională de Asigurări în Medicină,** *(denumirea completă a întreprinderii, asociaţiei, organizaţiei)* reprezentată prin **director general, dl. Ion DODON** *(funcţia, numele, prenumele)* care acţionează în baza **Statutului**, *(statut, regulament, hotărâre etc.)* denumit(a) în continuare ***Beneficiar*** **IDNO 1007601007778** *(se indică nr. şi data de înregistrare în Registrul de Stat)* pe de o parte,

ambii (denumiţi(te) în continuare Părţi), au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea *serviciilor de mentenanţă, suport şi dezvoltare pentru Sistemul Informaţional de Raportare şi Evidenţă a Serviciilor Medicale, componenta DRG*

(denumirea bunului/serviciului)

denumite în continuare Servicii, conform procedurii de achiziţii publice de tip _____ nr._____ din_____,
în baza deciziei grupului de lucru al Beneficiarului din „___” _____20__.

b. Următoarele documente vor fi considerate părţi componente ale Contractului:

*a) Specificaţia tehnică..... **Anexa nr.1**;*
*b) Specificaţia de preţ..... **Anexa nr.2**;*
*c) Modelul Actului de predare-primirea serviciilor pentru luna raportată .....**Anexa nr.3***

c. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Beneficiar, se obligă prin prezentul contract să presteze Beneficiarului Serviciile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

e. Beneficiarul se obligă prin prezentul contract să plătească Prestatorului, în calitate de contravaloare a prestării serviciilor, preţul Contractului în termenele şi modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1.Prestatorul îşi asumă obligaţia de a presta Specificaţiei tehnice ***Anexa nr.1*** și Specificaţiei de preț ***Anexa nr.2*****,** care este parte integrantă a prezentului Contract.

1.2. Benificiarul se obligă, la rândul său, să achite şi să recepţioneze Serviciile prestate de Prestator.

1.3 Serviciile prestate în baza contractului vor respecta standardele indicate în Partea II ”Condițiile speciale a contractului”.

1.4 Serviciile prestate în baza Contractului vor respecta standardele și normativele de domeniu sau alte reglementări autorizate.

2. Termeni şi condiţii de livrare

2.1. Prestarea Serviciilor se efectuează de către Prestator ***01.01.2025-31.12.2025***

2.2. Documentaţia de însoţire a Serviciilor include:

1) Originalele facturilor fiscale .....2 ex

2) Act de predare-primire.....2 ex conform **Anexei *nr.3***

2.3. Originalele documentelor prevăzute în punctul 2.2 se vor prezenta Beneficiarului cel tîrziu la momentul prestării Serviciilor la destinaţia finală. Prestarea Serviciilor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.

3. Preţul şi condiţii de plată

3.1. Preţul Serviciilor prestate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat în Specificaţia de preț din ***Anexa nr.2***.

3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabileşte în lei moldoveneşti şi constituie: _____lei MD.

(suma cu cifre şi litere)

3.3. Achitarea plăţilor pentru Serviciile prestate se va efectua în lei moldoveneşti.

3.4. Metoda şi condiţiile de plată de către Beneficiar vor fi:

în termen de 15 zile lucrătoare din momentul prezentării facturii lunare şi Actului de predare-primire a serviciilor pentru luna raportată ***Anexa nr.3***.

3.5. Plăţile se vor efectua prin transfer bancar pe contul de decontare al Prestatorului indicat în prezentul Contract.

4. Condiţii de predare-primire

4.1. Serviciile se consideră prestate de către Prestator şi recepţionate de către Beneficiar, dacă:

a) cantitatea Serviciilor corespunde Specificaţiei tehnice ***Anexa nr.1***și Specificaţiei de preț ***Anexa nr.2*** și informaţiei indicate în documentele de însoţire conform punctului 2.2 al prezentului Contract;

b) calitatea Serviciilor corespunde informaţiei indicate în Specificaţiei tehnice ***Anexa nr.1***;

4.2. Prestatorul este obligat să prezinte la sfârșitul lunii raportate Beneficiarului un exemplar original al facturii fiscale și Actului de predare-primire a serviciilor pentru luna raportată ***Anexa nr.3***, pentru efectuarea plăţii. Pentru nerespectarea de către Prestator a prezentei clauze, Beneficiarul îşi rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4 corespunzător numărului de zile de întîrziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 10.3.

5. Standarde

5.1. Serviciile prestate în baza contractului vor respecta standardele și normativele de domeniu sau alte reglementări autorizate.

6. Obligaţiile părţilor

6.1. În baza prezentului Contract, Prestatorul se obligă:

a) să presteze Serviciile în condiţiile prevăzute în Specificaţia tehnică din ***Anexa nr.1***.

b) să anunţe Beneficiarul după semnarea prezentului Contract, în decurs de __5__ zile calendaristice, prin telefon/fax sau poșta electronică achizitii@cnam.gov.md, despre disponibilitatea prestării Serviciilor;

c) să asigure condiţiile corespunzătoare pentru recepţionarea Serviciilor de către Beneficiar, în termenele stabilite, în corespundere cu cerinţele prezentului Contract;

d) să asigure integritatea şi calitatea Serviciilor pe toată perioada de până la recepţionarea lor de către Beneficiar.

6.2. În baza prezentului Contract, Beneficiarul se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepţionării în termenul stabilit a Serviciilor prestate în corespundere cu cerinţele prezentului Contract;

b) să asigure achitarea Serviciilor prestate, respectînd modalităţile şi termenele indicate în prezentul Contract.

7. Circumstanţe care justifică neexecutarea contractului

7.1. Părţile sunt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanţe care justifică neexecutarea contractului (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pământ, precum şi alte circumstanţe care nu depind de voinţa Părţilor).

7.2. Partea care invocă clauza circumstanţelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai tîrziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor care justifică neexecutarea contractului.

7.3. Survenirea circumstanţelor care justifică neexecutarea contractului, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.

7.4 În cazul în care în circumstanțele care justifică neexecutarea contractului, acesta se modifică prin acordul adițional, inclusiv modificarea termenilor de executare, în cazul unei executări ulterioare a contractului. Când se execută pct.7.1 și pct. 7.3, părțile modifică contractul prin acord - adițional, privind neîndeplinerea parțială sau integrală a obligațiunilor, inclusiv modificarea termenilor în cazul suspendării și executării ulterioare a contractului.

8. Rezoluţiunea

8.1. Rezoluțiunea Contractului se poate realiza cu acordul comun al Părţilor.

8.2. Contractul poate fi rezolvit în mod unilateral de către:

a) Beneficiarul în caz de refuz al Prestatorului de a presta Serviciile prevăzute în prezentul

Contract;
b) Beneficiarul în caz de nerespectare de către Prestator a termenelor de prestare stabilite;
c) Prestatorul în caz de nerespectare de către Beneficiar a termenelor de plată a Serviciilor;
d) Prestatorul sau Beneficiarul în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.
8.3 Beneficiarul are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situaţii:
a) contractantul se afla, la momentul atribuirii lui, în una dintre situaţiile care ar fi determinat excluderea sa din procedura de atribuire potrivit art. 19 al Legii nr.131/2015 privind achizițiile publice;
b) contractul a făcut obiectul unei modificări substanțiale care necesita o nouă procedură de achiziție publică în conformitate cu art. 76 al Legii nr.131/2015 privind achizițiile publice;
c) contractul nu ar fi trebuit să fie atribuit contractantului respectiv, avînd în vedere o încălcare gravă a obligaţiilor ce rezultă din Legea nr.131/2015 privind achizițiile publice și/sau tratatele internaţionale la care Republica Moldova este parte, care a fost constatată printr-o decizie a unei instanțe judecătorești naționale sau, după caz, internaționale.
8.4. Partea iniţiatoare a rezoluțiunii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.
8.5. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluţionat în termenele stabilite, partea iniţiatoare va iniția rezoluțiunea.

9. Reclamaţii

9.1. Reclamaţiile privind cantitatea Serviciilor prestate sunt înaintate Prestatorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Prestatorului.
9.2. Pretenţiile privind calitatea Serviciilor prestate sunt înaintate Prestatorului în termen de 5 zile de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o organizaţie independentă neutră şi autorizată în acest sens.
9.3. Prestatorul este obligat să examineze pretenţiile înaintate în termen de 3 zile de la data primirii acestora şi să comunice Beneficiarului despre decizia luată.
9.4. În caz de recunoaştere a pretenţiilor, Prestatorul este obligat, în termen de 5 zile, să livreze suplimentar Beneficiarului cantitatea neprestată de Servicii, iar în caz de constatare a calităţii necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.
9.5. Prestatorul poartă răspundere pentru calitatea Serviciilor în limitele stabilite, inclusiv pentru viciile ascunse.
9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizaţia independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întîrziere sunt suportate de partea vinovată.

10. Sancţiuni

10.1. Forma de garanţie de bună executare a contractului agreată de Beneficiar este _____, în cuantum de 5% din valoarea contractului.
10.2. Pentru refuzul de a presta Serviciile prevăzute în prezentul Contract, se va reține garanţia de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevedrile punctului 10.1., în caz contrar Prestatorul suportă o penalitate în valoare de 5 % din suma totală a contractului.
10.3. Pentru achitarea cu întârziere, Beneficiarul poartă plata despăgubirei în valoare de 0,1% din suma Serviciilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 5 % din suma totală a prezentului contract.
10.4. Suma penalităţii calculate Prestatorului conform prezentului Contract poate fi dedusă (reţinută) de către Beneficiar din suma plăţii pentru Serviciile prestate.

11. Drepturi de proprietate intelectuală

11.1. Prestatorul are obligaţia să despăgubească achizitorul împotriva oricăror:

a) reclamaţii şi acţiuni în justiţie, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile sau utilajele folosite pentru sau în legătură cu produsele achiziţionate, şi

b) daune-interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către achizitor.

12. Dispoziţii finale

12.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluţionate de către Părţi pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanţa de judecată competentă conform legislaţiei Republicii Moldova.

12.2. Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin acord adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului. Modificările şi completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris şi au fost semnate de ambele Părţi.

12.3. Nici una dintre Părţi nu are dreptul să transmită obligaţiile şi drepturile sale stipulate în prezentul Contract unor terţe persoane fără acordul în scris al celeilalte părţi.

12.4. Prezentul Contract în cazul în care este semnat electronic, de către ambele părți, acesta este remis în mod automat prin mijloacele electronice, dar în cazul când contractul este semnat olografic se întocmește în două exemplare în limba română, câte un exemplar pentru Prestator și Benefeciar.

12.5. Prezentul Contract este întocmit în două exemplare în limba de stat a Republicii Moldova, cîte un exemplar pentru Prestator. Prezentul Contract se consideră încheiat la data semnării şi intră în vigoare din data comunicării către Prestator privind transmiterea către Agenția de Achiziții Publice a dării de seamă**.**

12.6. Prezentul contract este valabil până la **31.12.2025.**

12.7. Prezentul Contract reprezintă acordul de voinţă al părţilor şi se consideră semnat la data aplicării ultimei semnături de către una din părți.

12.8. Pentru confirmarea celor menţionate mai sus, Părţile au semnat prezentul Contract în conformitate cu legislaţia Republicii Moldova.

CONDIȚIILE
SPECIALE A CONTRACTULUI

CAIET DE SARCINI

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **DRG**

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	Descriere
Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG: • *Servicii de mentenanță preventivă și Suport – în bază de abonament;* • *Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.*	*Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.*

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG (în continuare – DRG) pentru o perioadă de **minim 12 luni** după încetarea contractului.

De asemenea, Prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta CNAM (Beneficiar) împreună cu codul sursă DRG, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Descriere generală a DRG

DRG reprezintă un sistem național pentru instituțiile medicale din Republica Moldova, cu ajutorul căruia sunt încărcate și gestionate informațiile la nivelul bazei de date a CNAM.

Obiectivele strategice ale CNAM și MS în ceea ce privește costurile asociate tratamentului conduce la obținerea unei **imagini mai bune a rezultatelor** și la realizarea de **comparații ale rezultatelor**. DRG este un **instrument util spitalelor în creșterea eficienței** (prin identificarea resurselor necesare fiecărui tip de pacient), în procesul de îmbunătățire a calității serviciilor furnizate (prin evaluarea calității și definirea unor modele de practică), în **modelarea activității** și a structurii spitalelor (personal, secții, etc.) și în realizarea unui **management bazat pe rezultate** și nu pe resurse sau procese.

Funcționarea continuă și operarea în sistemul DRG are următoarele obiective:

A. Creșterea eficienței serviciilor spitalicești

Prin finanțarea în sistem DRG, spitalele ce vor avea costuri pentru un anumit DRG mai mari decât tariful stabilit vor pierde resurse la acea categorie de pacienți, iar cele cu costuri, pentru un anumit DRG, mai mici decât tariful stabilit vor câștiga resurse la acea categorie de pacienți. Alocarea resurselor financiare are la baza rezultatele spitalului și mai puțin structura acestora.

B. Creșterea eficienței tehnice la nivelul furnizorului de serviciilor spitalicești

DRG permite spitalelor să-și evidențieze cu claritate tipurile de pacienți și resursele atrase pentru aceștia, iar prin compararea cu costurile necesare se generează cadrul de funcționare pentru o eficientă cât mai mare (economiile făcute fiind păstrate la nivelul spitalului).
Spitalele pot să-și cunoască tipurile de pacienți pentru care pierd resurse (și să intervină în procesele ce se desfășoară pentru a reduce cheltuielile) și pacienții la care sunt în beneficiu financiar (și să încerce să atragă cât mai mulți pacienți de acest tip).

Specificații tehnice DRG

Caracteristici generale de funcționare

DRG are o arhitectura 3-layer, arhitectura care permite funcționarea pe platforma guvernamentală comună MCloud. DRG funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă tot ce este necesar de automatizat;
- are posibilitatea reparației unui modul fără afectarea altora;
- respectă standardele în vigoare a tehnologiilor informaționale;
- asigură flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare;
- utilizează o arhitectură orientată pe servicii pentru a acomoda cu ușurință noi modificări;
- are o arhitectura modernă cu un grad înalt de performanță, structurată pe 3 niveluri (nivelul pentru baze de date, nivelul pentru aplicație și nivelul acces/utilizator). Fiecare nivel are în componență toate echipamentele necesare bunei funcționări;
- este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- poate fi utilizat împreună cu echipamente ce permit creșterea vitezei de înregistrare a datelor de identificare ale pacienților (nume, prenume, IDNP etc.);
- este scalabil pentru a acomoda modificările viitoare ale numărului de utilizatori ai soluției;
- recunoaște corect sursele informaționale, le acceptă și le integrează în sistem;
- întreține în limba de stat interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate;
- permite ca utilizatorul să se autentifice o singură dată pentru a accesa toate modulele aplicației;
- asigură o siguranță sporită în exploatare.

Interfața Utilizator

Această interfață este accesibilă pentru toți utilizatorii autorizați în DRG:

- ✓ DRG dispune de o interfață inteligentă, intuitivă și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browserul web și nu necesită instalarea de componente software suplimentare;
- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului;
- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:

- **Platforma hardware**, formata din Complexul tehnic de prelucrare și transportare a datelor,

acesta fiind asigurat pe platforma guvernamentală comună MCloud:

- Servere protejate redundant pentru hosting al bazelor de date, softului de sistem și softului funcțional (aplicații și subsisteme);
- Platforma hardware pusă la dispoziție de către beneficiar este dimensionată corespunzător pentru a permite funcționarea în bune condiții a sistemului;
- Performanta optima, în limita normelor obiective de uzură, pentru realizarea structurii funcționale și asigurarea extinderii ulterioare a sistemului;
- este flexibilă în utilizarea mijloacelor disponibile destinate recepționarii informației din surse externe (alte instituții publice);
- asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date;
- asigura normele de funcționare ale platformelor informatice guvernamentale.

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:

  - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
  - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server 2017, vers. 14.
  - Pe stațiile utilizatorilor există în mod implicit .NET Framework 3.5 SP1 sau mai nou și navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare și transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mașini virtuale, mijloacele de imprimare, rețele electronice locale (LAN – local area network) și de scara largă (WAN – wide area network). Pentru operare se folosesc stațiile de lucru ale beneficiarului, singura specificație impusă utilizatorilor fiind cea de a dispune de un calculator conectat la internet și un browser instalat, fiind recomandate și utilizate soluțiile Microsoft.

Sistemul de securitate

DRG funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.

Caracteristici:

- asigură accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de system;
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;

- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor;

Având în vedere natura specială a informațiilor gestionate în cadrul DRG, acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.

Sistemul are următoarele nivele de securitate care asigură confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație între stațiile clientului și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unică cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este asigurata automat, iar modificările de structura la nivelul acesteia se fac exclusiv în baza drepturilor corespunzătoare de administrator al bazei de date. În plus, baza de date deține propriul mecanism de backup care permite, în caz de dezastru, restaurarea unor versiuni anterioare recente (de ordinul zilelor).

Sistemul asigură dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori sunt create module de acces și autentificare în sistem; sunt indicate volumul de informație și funcționalitatea pe care aceștia o accesează. Sistemul permite accesul la datele statistice pentru anumiți utilizatori și grupuri de utilizatori. Sistemul asigura verificarea automată a drepturilor în momentul intrării în sistem și în ulterioarele accesări a sistemului și creează un jurnal al accesărilor – jurnalul de audit.

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Operator**: permite introducerea și modificarea datelor specifice activității sale;

- nivelul **Administrator**: permite arhivarea datelor, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

La nivel aplicativ, sistemul generează o listă de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

- ✓ posibilitatea înregistrării, adăugării si ștergerii utilizatorilor din sistem;
- ✓ posibilitatea distribuției drepturilor utilizatorilor folosind grupuri de acces;
- ✓ posibilitatea pentru fiecare utilizator de a avea cel puțin următoarele atribute de autentificare: identificarea, autentificarea.
- ✓ posibilitatea intrării în sistem a unui utilizator în orice moment;
- ✓ asigurarea de către administrator a regimurilor de funcționare, deconectare, conectare, modificării regimului de autentificare și identificare, dirijarea cu drepturi și auditul.

Retenția datelor, acces securizat și audit

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale (consultații, fișe medicale și bilete de trimitere) în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.
- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respectă regulile de

control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.

- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.
- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem și pe baza permisiunilor asociate rolului sau rolurilor atribuite utilizatorilor.
- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fișele electronice ale pacienților săi.
- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu că a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:
  - unicitatea utilizatorilor în sistem;
  - jurnalizarea tuturor operațiunilor efectuate de sistem;
  - mecanism de control al versiunilor pentru înregistrările medicale.
- **Securitatea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit.** Toate operațiunile efectuate de utilizatori sau de către alte sisteme care accesează sistemul păstrează o înregistrare în componența auditului. Astfel, este permisă investigarea incidentelor de către un administrator.

Arhitectura DRG

DRG are o arhitectură bazată pe tehnologie web, folosind platforma Microsoft. Sistemul este conceput modular, dezvoltarea acestora putând fi realizată în paralel. Orice client se poate conecta la serverul de aplicație și poate utiliza sistemul conform drepturilor pe care le are. Comunicația între client și server se realizează exclusiv prin protocoale securizate de tip HTTPS folosind certificat de securitate integrat la nivelul serverului de aplicație. Schema arhitecturala este în figura următoare:

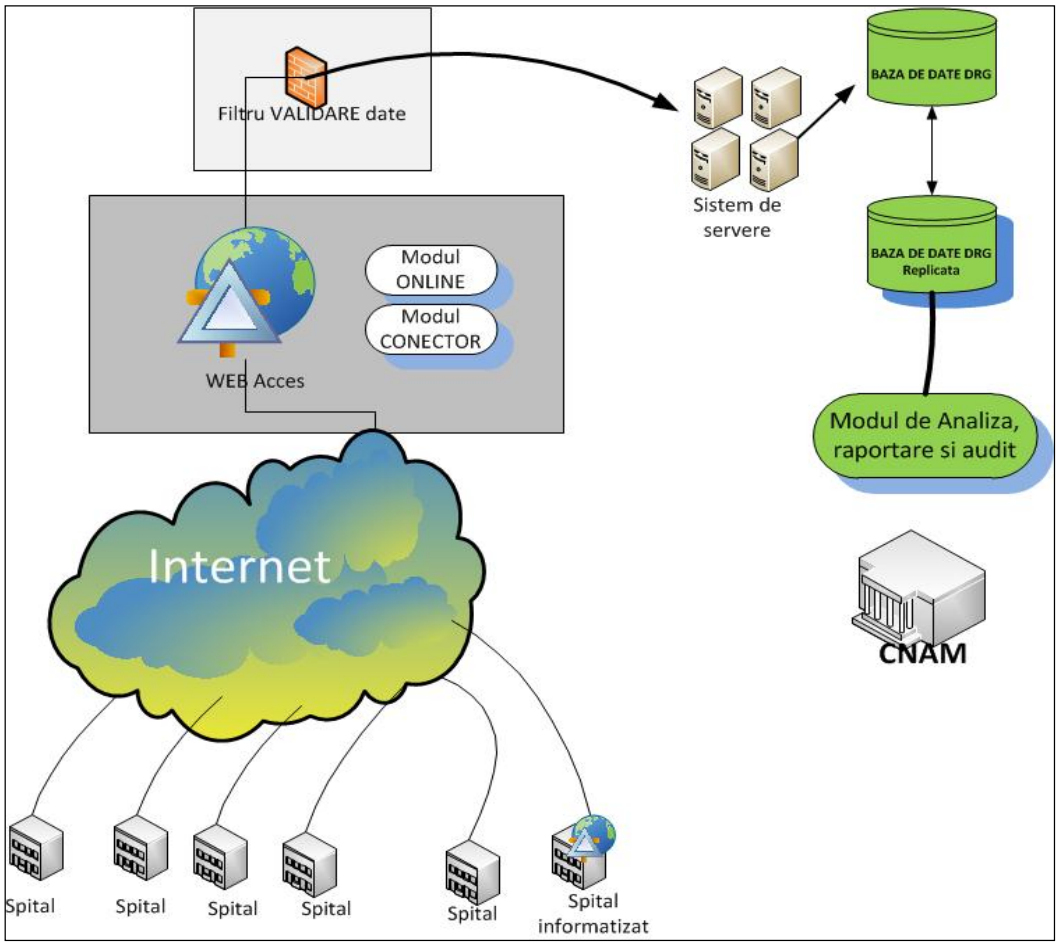


Figura 1. Schema arhitecturală DRG

Componentele DRG sunt operaționale și sunt prezente conform modulelor:

- ✓ Modulul de administrare sistem colector;
- ✓ Modulul de autentificare;
- ✓ Modulul colectare date Real Time;
- ✓ Modulul de nerepudiere;
- ✓ Modulul de validare;
- ✓ Modulul de înregistrare raportări;
- ✓ Modulul de setări, raportare și audit;
- ✓ Modulul Depozit (warehouse);
- ✓ Modulul de Analiză la nivel de Baza de Date;
- ✓ Modul conector pentru Auditul Codificării.

Modulul de administrare sistem colector

În cadrul acestui modul se execută:

- ➢ **Managementul utilizatorilor** (creare, ștergere, modificare date utilizatori). Fiecare instituție care execută raportare în DRG are desemnat cel puțin un utilizator al sistemului care transmite raportările; modalitatea de alocare a acestei resurse umane este răspunderea instituției.

- **Administrarea sistemului.** Administratorii sistemului pot efectua setări la nivelul celorlalte module și pot verifica funcționarea corectă a fiecărui modul. Nivelul de acces al administratorilor este corespunzător cerințelor de care aceștia răspund:
  - administratorii pot modifica informațiile de referință ale operatorilor sistemului (nume, prenume, locație, instituție, etc.);
  - administratorii pot modifica intervalele temporare în care transmiterea raportărilor este permisă;
  - administratorii pot vizualiza informații existente în modulul de nerepudiere (fișierele care conțin informațiile raportate trec prin modulul de nerepudiere);
  - administratorii pot vizualiza informațiile existente în modulul de înregistrare și să confirme funcționarea normală a acestuia;
  - administratorii pot vizualiza existenta rapoartelor transmise și stadiul în care se afla acestea față de modulul de validare;
  - administratorii pot face modificări asupra Modulului de Notificare și Raportare.
  - administratorii pot verifica transmiterea corectă a rapoartelor către Modulul Warehouse, unde sunt depozitate informațiile în vederea prelucrării.

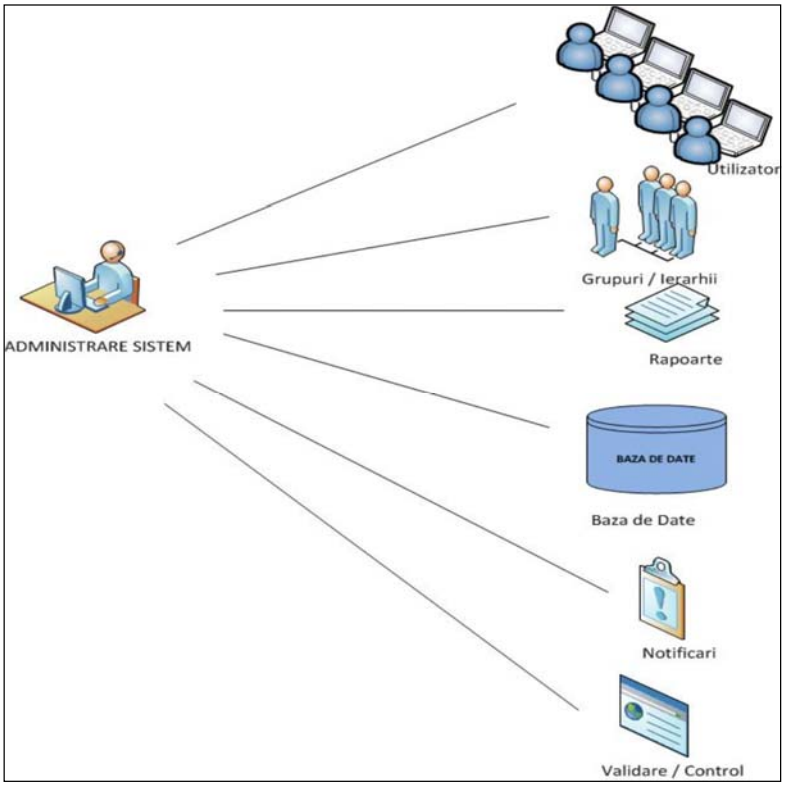


Figura 2. Schema Modulul de administrare sistem colector

Nivelul de acces al acestui modul:

- modulul care are acces la toate nivelurile sistemului;
- doar administratorii sistemului au acces la acest modul, în vederea efectuării operațiilor necesare funcționării normale a sistemului.

Modulul de administrare este singurul modul care permite accesul unui număr restrâns de persoane (administratorii sistemului) la toate elementele din sistem, fără să permită – prin procedura - modificarea conținutului rapoartelor.

Administratorii sistemului au rolul de a verifica fluxul normal al prelucrării datelor de către sistem și de a ajusta situațiile de excepție atunci când este cazul. Prin situații de excepție se înțeleg

acele cazuri în care sistemul răspunde corect din punct de vedere al fluxului, dar cerințele unui utilizator sunt diferite și justificate.

Administratorii sistemului nu acționează asupra conținutului datelor transmise de către unitățile medicale, iar utilizatorii sunt instruiți asupra faptului că sunt direct răspunzători de conținutul informațiilor transmise. Conținutul datelor este confidențial și respectă normele de securitate din domeniu; sistemul informatic DRG poate opera cu fișierele de date fără a fi necesară intervenția administratorilor de sistem asupra conținutului. În situațiile în care utilizatorul corespunzător care a generat raportul cere explicit acest lucru, administratorul nu o prelucrează: conținutul datelor transmise rămâne exclusiv responsabilitatea instituțiilor medicale / operatorilor care folosesc sistemul.

Modulul de colectare date Real Time

Acest modul este cel care transformă operarea DRG într-o activitate aflată la dispoziția permanentă a oricărui spital: este un modul destinat acelor instituții care nu au un sistem informatic integrat al activității medicale, și care, în prezent lucrează cu diferite programe informatice în vederea generării raportărilor.

Acest modul are o interfață de lucru universală cu un aspect operațional intuitiv și ușor de urmărit, care nu necesită cunoștințe tehnice informatice avansate; orice medic sau asistent îl poate utiliza în activitatea curentă în vederea introducerii în sistemul național a informațiilor despre pacienții pe care îi tratează.

Informațiile pot fi introduse de către utilizatorii autorizați direct în sistem non-stop, la nivel național, într-o interfață accesibilă de pe orice calculator care dispune de un browser și de o legătura la serverul sistemului DRG: vârsta, sex, durata de spitalizare, diagnostice principale și secundare, proceduri, starea la externare și greutatea la naștere (în cazul nou-născuților), iar în funcție de acestea pacienții sunt clasificați într-o categorie distinctă (o grupă de diagnostice), în conformitate cu nomenclatoarele din domeniu.

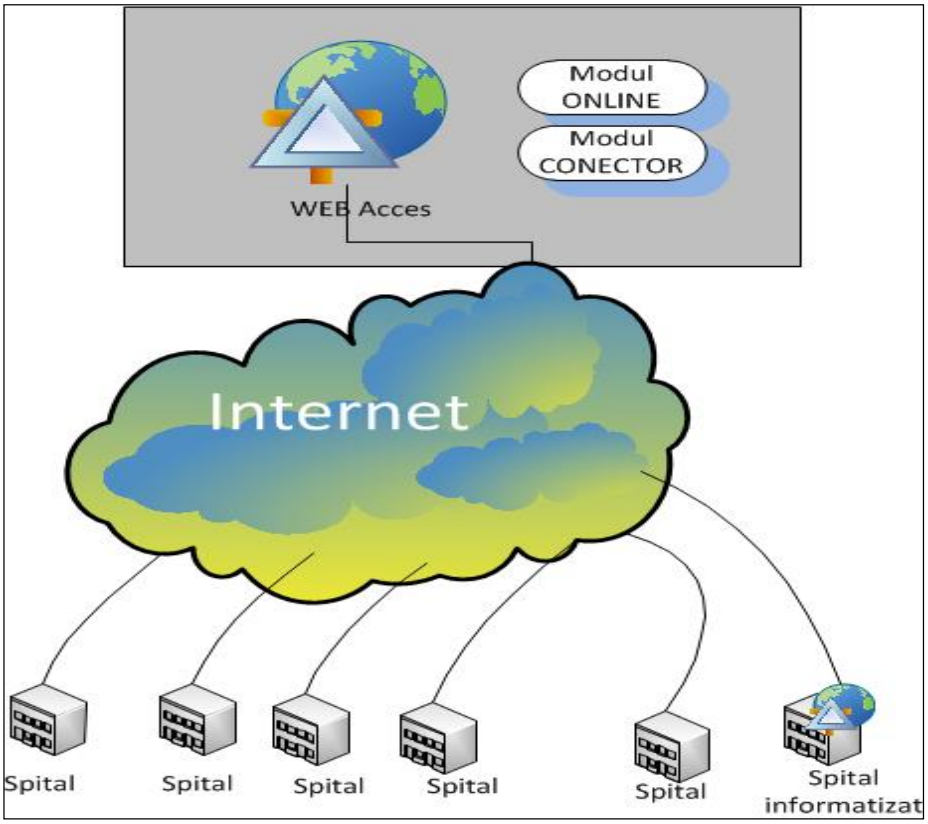


Figura 4. Modulul de colectare date Real Time

Avantajul major pe care îl oferă acest modul este că el este permanent updatat în conformitate cu cerințele CNAM, nomenclatoare noi sau alte dispoziții, iar acele instituții care aleg să îl folosească au siguranța actualizării informațiilor referitoare la raportările DRG. Informațiile sunt disponibile în timp real și pot fi analizate imediat, atât prin intermediul mecanismelor de analiză, audit și validare, cât și prin intermediul operatorilor CNAM.
Modulul preia informațiile, le validează și le introduce imediat în sistem. Datele despre pacient fiind de ultima ora, iar modificările asupra oricărui element care are legătura cu diagnosticul acestuia sunt trecute prin filtrele de validare; aceasta înseamnă că sistemul este capabil să calculeze imediat valoarea de complexitate a cazului tratat. Modul prenotat are capacitatea de a trece în analiza sau chiar să elimine activitățile suspecte sau lipsite de fond.

Modulul are și rolul de a elimina necesitatea spitalelor de a testa nenumărate programe informatice care generează rapoartele și care de multe ori au rezultate nesatisfăcătoare. Existența unui sistem informatic național dedicat acestui tip de raportare realizează o unificare și un control deosebit, ceea ce permite operatorilor generarea de rapoarte și identificarea prin auditare a zonelor sensibile din punct de vedere financiar.

Se elimină astfel obligativitatea existenței unui mecanism terțiar [de tip „3rd party”] la nivelul spitalelor pe care unele spitale îl utilizează în vederea raportării către CNAM. Aflat la dispoziția oricărui spital, DRG permite lucrul în timp real și la un înalt nivel de securitate, direct spre baza de date a CNAM.

Operațional, prin punerea la dispoziția personalului medical a unei interfețe de lucru în vederea acestui tip de raportare medicală cu puternice implicații financiare, sunt premisele unei colaborări eficiente inter / intra departamentale medical-administrativ cât și între spitale care sunt interesate să își modeleze activitatea în așa fel încât să eficientizeze activitatea.

Alegerea modului în care sunt efectuate raportările către CNAM este opțiunea instituțiilor medicale: acestea pot folosi fie modulul de colectare date Real Time sau software-ul intern și apoi mecanismul de transfer al rapoartelor real-time prin sistemul colector.

Modulul de nerepudiere

Modulul de nerepudiere are un rol important din punct de vedere al auditării: acest modul garantează pentru toți utilizatorii sistemului ca operarea se execută în mod unic și că nici un utilizator nu poate nega acțiunile legate de sistem.

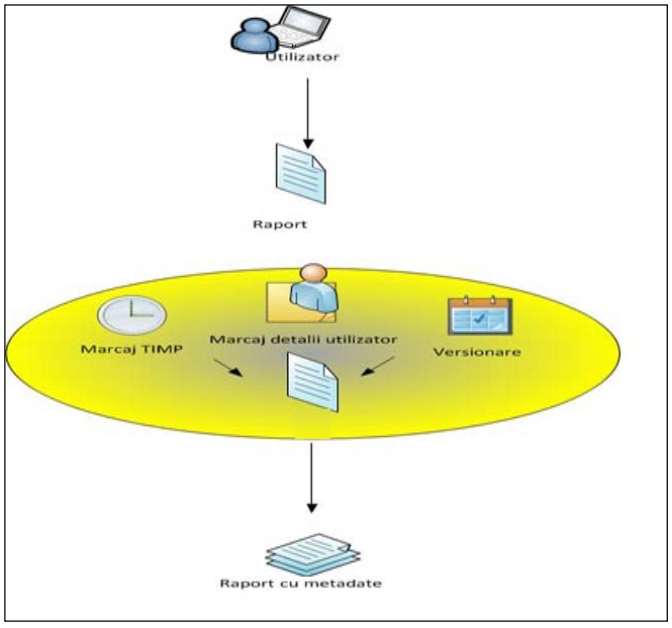


Figura 5. Modulul de nerepudiere

Fiecare utilizator este unic în sistem, lucru verificabil prin intermediul modulului de autentificare. Modulul de nerepudiere se referă la faptul că acțiunile pe care le efectuează un utilizator nu pot fi negate de acesta, deoarece fiecare acțiune are directă corespondență cu un utilizator. Orice fișier transferat de către un utilizator primește prin intermediul acestui modul un pachet de metadate care conține:

- ✓ Data și ora la care au fost transmise fișierele către sistem;
- ✓ Numele utilizatorului care a transmis fișierul; pentru fiecare fișier în parte se atașează metadatele corespunzătoare. Sistemul face automat asocierea între utilizator și fișierul transmis.
- ✓ Numele utilizatorului care a rescris ultima versiune a fișierului – va fi stabilit în faza de analiză, în funcție de particularitățile observate;

Aceste informații sunt disponibile atât administratorilor și, parțial, utilizatorilor. Adăugarea metadatelor la fișiere este o operațiune pe care modulul de nerepudiere o execută în mod automat și independent de opțiunile utilizatorilor. Orice raport transmis către sistem este însoțit de elemente de identificare unice: data, ora, nume utilizator etc. În cazul auditării sistemului, sunt disponibile date referitoare la acțiunile fiecărui utilizator, corelate integral cu informațiile introduse în sistem.

Modulul de validare

DRG reduce situațiile în care utilizatorii trimit setul minim de date la nivel de pacient al căror format este necorespunzător.

- ➢ Modulul de validare operează în mod minimal fișierele transmise (setul minim de date la nivel de pacient) și le acceptă doar pe cele care se încadrează în formatul dorit de către CNAM;

- ➢ Modulul de validare verifică, de asemenea, existența metadatelor de corespondența între utilizator și fișier înainte de trecerea în sistem a fișierelor al căror conținut îl constituie rapoartele. În cazul în care apar neconcordanțe între ceea ce așteaptă sistemul și ceea ce livrează utilizatorii, se trimit alerte către „Modulul de notificare, raportare și audit” care prelucrează situațiile în mod corespunzător, în sensul aducerii la forma standard a raportărilor.

- ➢ Modulul de validare este ultima componentă a sistemului care decide automat dacă un raport este valid sau nu; atenția acordată acestui modul este ridicată iar analiza situațiilor neconforme și alinierea acestora sunt urmărite permanent.

- ➢ Modulul de validare are capacitatea de a trata cât mai multe situații comune și elimina la timp cât mai multe cazuri în care apare eroarea umană.

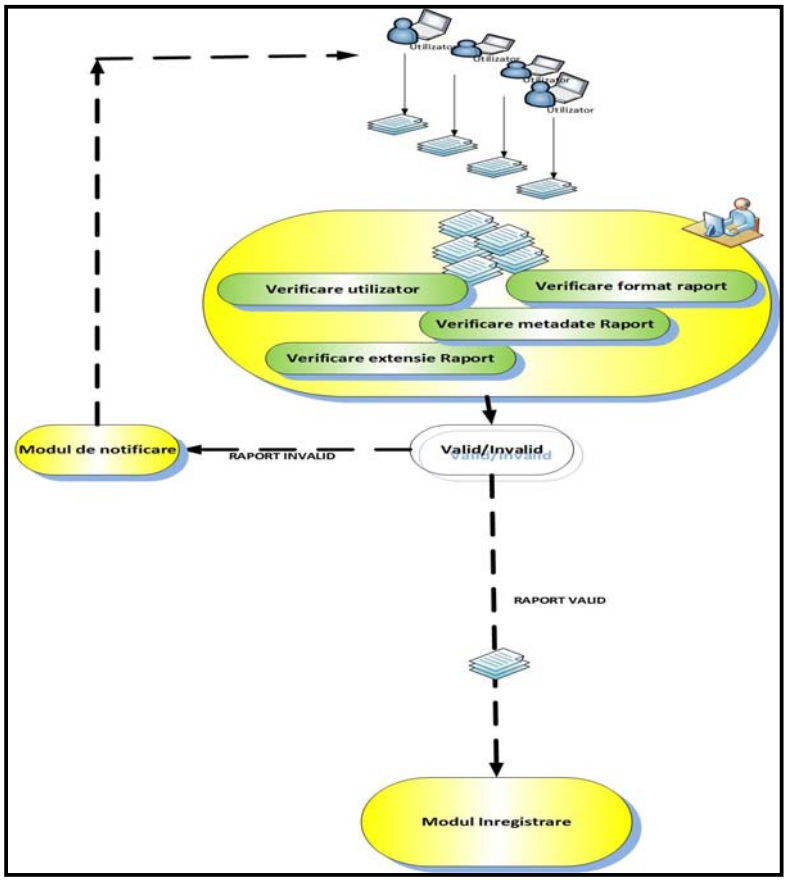


Figura 6. Schema Modulului de Validare

Modulul de înregistrare raportări

Modulul de înregistrare raportări este responsabil de depozitarea corectă a raportărilor trimise de către instituțiile medicale, în vederea transferului acestora către modulul depozit (data warehouse).

Modulul de înregistrare a raportări conține două componente:

1. Componenta „buffer", temporară, care colectează toate raportările utilizatorilor în toate versiunile pe care aceștia le transmit în intervalul alocat; această componentă dispune de un mecanism de ordonare care permite automatizarea procesului de transfer al versiunilor finale fără intervenția administratorilor sau a utilizatorilor. Componenta „buffer" are rolul de a colecta și organiza rapoartele trimise de către utilizatori în mod unic, astfel încât nu există pentru o instituție medicală rapoarte dublate.

2. Componenta „transfer" golește „bufferul" în momentul expirării termenului de transmitere a raportărilor și le mută în zona de depozitare a rapoartelor – forma definitivă, prelucrabilă – numita Modul Warehouse.

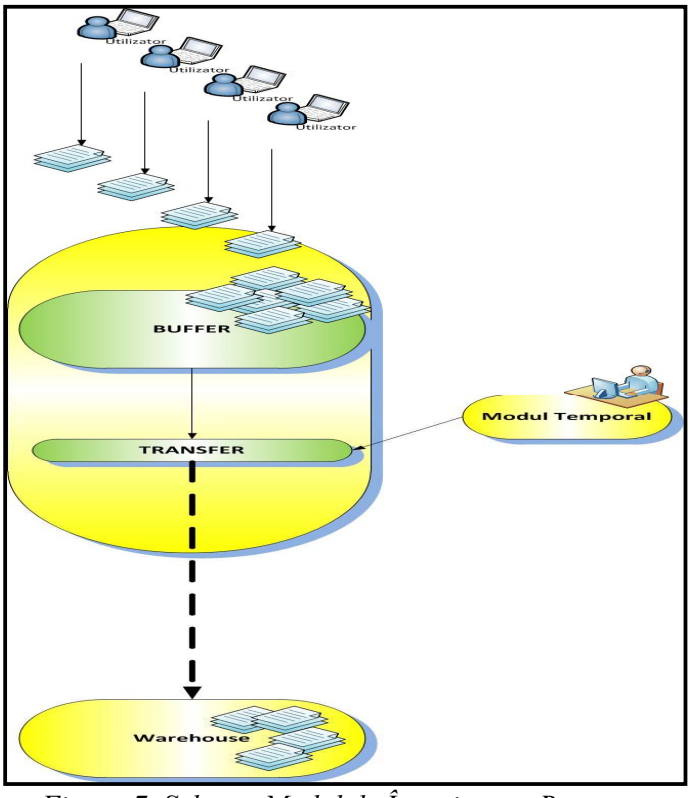


Figura 7. Schema Modul de Înregistrare Rapoarte

Informațiile de interes se limitează doar la ultimele versiuni ale raportărilor transmise:

- „Bufferul" permite unele modificări controlate de administratori asupra raportărilor în intervalul configurat în modulul de control temporal. La cerere administratorii de sistem pot vedea la nivel de *nume_raport* existența rapoartelor în buffer.
- „Transfer" acționează în mod programat, după expirarea termenului în care le este permis utilizatorilor să transmită raportările. Codul aplicației conține legătura directă între Modulul de Înregistrare și Modulul de control temporal.

Modulul de setări, raportare și audit

Modulul îndeplinește trei funcții: Setări, Raportare și Audit privind situația raportărilor din intervalul curent de timp în care este deschisă sesiunea de transfer a datelor. Fiecare dintre acestea este importantă la nivelul sistemului pentru că menține o comunicare permanenta între utilizatori, beneficiari și entitatea informatică:

✓ **Setări:** aceasta funcție a modulului este accesibila unui număr mic de utilizatori – administratori pentru introducerea datelor (inclusiv de autentificare) la nivel de CNAM și la nivel de instituție medicală. În cazul, în care modulul acționează în mod corect informațiile colectate și transmise sunt corecte și definesc informațiile ce pot afecta direct toate celelalte informații din baza de date.

✓ **Raportare:** aceasta funcție a modulului executa rapoarte în mod programat privind utilizarea sistemului.

✓ **Audit:** aceasta funcție a modulului identifică acțiunile desfășurate de către un utilizator, în mod cronologic; în cazul apariției unei probleme, la nivel de administrator de sistem, se poate vedea istoricul operațiilor desfășurate de orice utilizator în vederea identificării și corectării problemei. Sunt vizibile atât informațiile referitoare la logarile în sistem cât și cele referitoare la fișierele cu care

utilizatorul a operat. Funcția de audit folosește în mod implicit modulul de nerepudiere care asigura orice investigație ca datele existente în sistem sunt cele corecte și ca asocierea între conținutul informatic și activitatea umană este incontestabilă.

Modulul Depozit (Warehouse)

În cadrul fluxului de colectare de către sistem a raportărilor de la instituțiile medicale, Modulul Depozit (warehouse) este componenta finală, cea care deține datele necesare prelucrării. Aici se găsesc informațiile utile Beneficiarului, motiv pentru care acestea:

- ✓ sunt organizate într-o structură ierarhică care permite identificarea rapida a unui raport provenit de la orice instituție medicală la un anumit moment.
- ✓ conțin informațiile organizate într-o manieră care permite managementul rapoartelor fără a afecta conținutul acestora: există posibilitatea mutării datelor într-o arhivă; acest tip de operație necesită o analiză a graficului de încărcare a rapoartelor.
- ✓ modulul warehouse beneficiază de un spațiu de stocare protejat conform normelor de securitate ale Beneficiarului. Spațiul de stocare folosit de Modulul warehouse poate fi supus și altor cerințe de securitate decât cele ale sistemului implementat, în funcție de necesitățile beneficiarului: de ex. audit de urgență, investigații etc.
- ✓ Întreg spațiul alocat depozitarii rapoartelor este supus procedurilor de back-up.

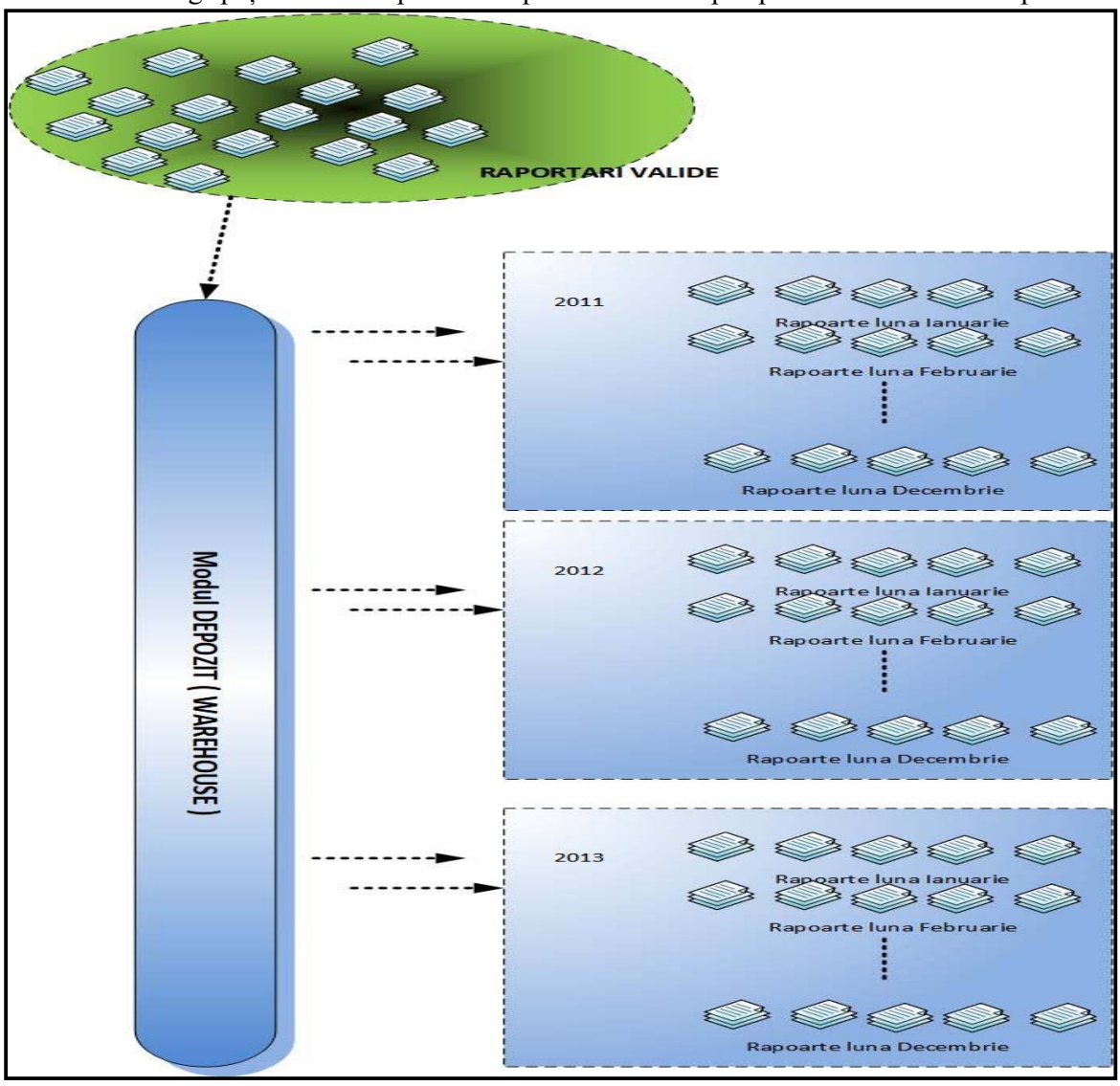


Figura 8. Schema Modul Depozit Rapoarte DRG (Warehouse)

Zona de stocare a Modulului Depozit (warehouse) poate fi controlată atât de administratorii sistemului DRG cât și de inginerii de sistem informatic MCloud.

Modulul de Analiză la nivel de Baza de Date

Sistemul DRG creează în mod dinamic o bază de date updatată permanent, cu informații consistente; sistemul este un instrument performant de interogare care permite extragerea de rapoarte necesare CNAM și MS, oferind o imagine clară a istoricului diagnosticelor pacienților; pe baza acestora se pot identifica eventualele neconcordante ulterioare în diagnosticarea pacientului.

Prin interogarea bazei de date temporare, în care sunt depozitate rapoartele trimise în vederea validării și închiderii, se pot obține statistici în timp real. Odată ce perioada de raportare este încheiată, baza de date Warehouse conține informațiile corecte și complete ale perioadei anterioare.

Modulul de analiza, raportare și audit poate fi utilizat de departamentele autorizate ale CNAM în vederea generării de rapoarte bazate pe template-uri, dar și ad-hoc, utile în activitatea curenta. Sistemul răspunde următoarelor solicitări:

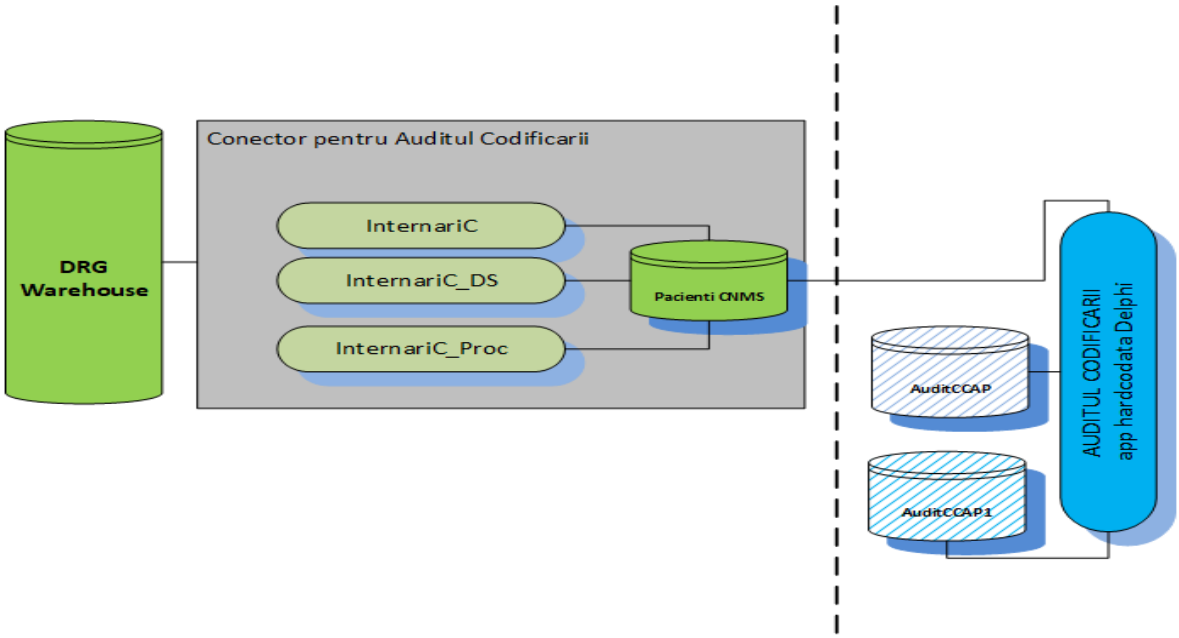
1) Evitarea fraudării. Sistemul SI DRG este un sistem operațional la nivel național, iar CNAM dispune de o baza de date unică, cu informații reale; veridicitatea informațiilor se verifica in doua feluri:

- în timp real: respingerea informațiilor eronate cu atenționarea celui care introduce datele; sistemul nu permite introducerea de date necorespunzătoare.
- în urma auditării: personalul CNAM poate genera rapoarte de audit și control prin care sunt identificate cazurile suspecte; aceste rapoarte pot fi organizate în template-uri pentru a fi reutilizate, dar pot fi customizate în așa fel încât echipele care executa auditarea și evaluare să obțină o lista consistentă și reală pe care sa o verifice și în teren. Prin utilizarea sistemului informatic pot fi identificate cazurile de fraudare.

2) Creșterea eficientei. Existenta modulului de analiză, raportare și audit la nivelul CNAM constituie un instrument pe care departamentele autorizate CNAM implicate în raportare îl folosesc în vederea creșterii eficientei de lucru. Căutările sunt rapide, rapoartele sunt generate cu mare ușurința în ciuda complexității deosebite a sistemului. Prin monitorizarea permanentă și corecția raportărilor se elimină cazurile în care spitalele execută raportări care necesită reanalizare și reverificare de către CNAM. Informațiile sunt corecte, validate și disponibile în timp real.

Modulul conector pentru Audit al codificării

Funcționalitatea de audit a codificării este acoperită de o aplicație pentru care CNAM nu deține codul sursa. Cea mai mare parte din informațiile prelucrate de către aplicația de Audit al codificării se găsesc actualizate în timp real în CCAP. În lipsa codului sursă, dezvoltatorii CCAP au reușit să atingă o parte din obiectivele funcționale ale operatorilor care executî auditul codificării prin operațiuni care nu afectează aplicația ci doar baza de date. Astfel operatorii Autorității Contractante care efectuează auditul codificării continuă să folosească vechea aplicație hardcodata care folosește date din warehouse-ul DRG.



CNAM va continua să emită fie solicitări de dezvoltare a sistemului CCAP, fie de execuție a unor proceduri la nivelul bazelor de date și conectorilor în scopul obținerii rezultatelor dorite până la momentul includerii definitive în CCAP a funcționalităților de audit al codificării. În prezenta procedura de achiziție CNAM solicită operațiuni de mentenanță care se referă exclusiv la funcționalitățile asupra cărora deține codul sursă, urmand ca pe parcursul dezvoltării funcționalităților în cadrul CCAP, aria de mentenanță să se extindă corespunzător. Astfel, CNAM solicită analiza compartimentului Menu=>„Rapoarte audit" privind verificarea corectitudinii regrupării cazurilor supuse auditului codificării.

Codul dezvoltat în sensul susținerii modului de conectare pentru auditul codificării permite operatorilor de audit să desfășoare în cadrul vechii aplicații două operațiuni:

- **Selectarea fișelor medicale a bolnavului spitalizat pentru audit (Database DRG).**
- **Importul fișelor medicale din "Database DRG" în aplicație şi efectuarea auditului.**

CNAM deține codul sursa necesar pentru prelucrarea noii baze de date **Pacienți CNMS** și asupra **view-rilor de internări** [InternariC, InternariC_DS, InternariC_Proc] și **ListaSpitale**, care colectează și interpretează informațiile din baza de date Wodehouse a DRG, acestea intrând în obiectul operațiunilor de mentenanță pe care urmează să le desfășoare furnizorul serviciilor.

În prezent, la procedura de audit al codificarii prin intermediul aplicatiei CCAP nu este posibilă logarea/autentificarea concominentă a Auditorilor I/II în aplicație şi ca urmare nu este posibilă analiza concomitentă/independentă de către Auditor I și Auditor II a fişelor supuse auditului. În acest context, CNAM solicită analiza subiectului prenotat, şi ajustarea compartimentului conform solicitării. Totodată, CNAM subliniază faptul ca, în cazul în care nu este posibilă ajustarea propriu-zisă a conexiunii concomitente în CCAP, CNAM solicită reingineria modulului de audit al codificării în SI DRG.

A. Cerințe de Mentenanță preventivă și Suport

Cerințele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanţă elaborat de Prestator şi aprobat de Beneficiar.

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi

acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanță sistemului DRG, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Actualizarea parametrilor existenți în partea utilizatorilor, conform cerințelor legislației în vigoare (spre exemplu: actualizarea/completarea nomenclatoarelor programelor special, diagnosticelor, procedurilor, spitalelor, rapoartelor, modificarea valorilor relative, aplicarea/anularea aplicării KP, completarea/modificarea algoritmelor de validare și excepțiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora, conform formatului solicitat și menținerea posibilităților de extragere a datelor de către utilizator.
- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;
- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație pentru utilizatori:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM;
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistența tehnică pentru utilizatorii CNAM prin email și platforma Service Desk pusă la dispoziție de către Furnizor;
- Modalități de asigurare a suportului: email, telefon, acces la distanță;
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare - best effort.

Suport platforma software

Servicii dedicate Sistemelor de Operare

În această categorie se includ următoarele servicii minime relative de administrare şi mentenanţă a sistemelor de operare ale SI DRG care vor fi desfășurate de către Furnizor:

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifestă transparent și înlăturarea cauzelor care le-au produs sau recomandarea măsurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- verificarea stării de funcționare a driverelor și a componentelor aferente;

- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- optimizarea configuratiei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanta și disponibilitate a sistemului;
- asigurarea funcționării continue a conectorilor;
- migrarea cazurilor medicale pe perioade definite de timp prin web-servicii pentru instituții medicale cu sisteme informatice proprii;
- mapare câmpuri, import cazuri medicale pe perioade definite de timp prin web-servicii instituții medicale cu sisteme informatice proprii.

Servicii dedicate sistemelor de gestiune a bazelor de date

În această categorie întra următoarele servicii minime relative la Microsoft SQL Server ale DRG care vor fi desfășurate de către Furnizor:

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corecta a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidenţialităţii şi securităţii datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerinţelor de securitate informaţională de către utilizatori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securităţii privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale DRG şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum şi restaurarea acestora.
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

Servicii dedicate componentelor, inclusiv a celor de interoperabilitate

În această categorie întră următoarele servicii minime relative la codul aplicației DRG care vor fi desfășurate de către Furnizor:

- verifică și optimizează secvențele de cod;
- identifică și analizează problemele și potențialele probleme de la nivelul codului;
- rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației;
- soluționează incidentele apărute la nivelul codului;
- modifică rapoartele, șabloanele, serviciile aplicative;
- comunică cu echipele de suport în scopul funcționarii corecte și permanente a sistemului.

Efectuarea testelor de penetrare

Teste de penetrare se referă la o metodă de evaluare a securității sistemului informațional prin simularea unor atacuri cibernetice. Scopul acestor teste este de a identifica și exploata vulnerabilitățile sistemului pentru a evalua cât de bine poate rezista sistemul informațional la atacuri reale. În această categorie întră următoarele servicii minime:

- Simulare a atacurilor;
- Identificarea vulnerabilităților;
- Evaluarea impactului;
- Raportare și recomandări.

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice DRG

DRG este un sistem automatizat care operează în condițiile legislației în vigoare. Prin serviciile prestate, ofertantul va asigura operațiuni de întreținere, suport și recomandări tehnice asupra aplicației, inclusiv în situația modificărilor legislative care afectează componentele software existente în DRG. CNAM precizează că modificarea funcționalităților existente în aplicație în corelație cu modificările legislative presupun în mod concret modificări în codul sursă al aplicației.

Orice modificare asupra codului sursa are ca efect o nouă versiune operațională a aplicației, conforma legislației. CNAM solicită ofertantului asumarea faptului că deține cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toată perioada desfășurării contractului.

Operațiunile tehnice de întreținere ce vor fi desfășurate de personalul care va asigura funcționarea continuă a DRG se referă la componentele majore ale sistemului, adică la:

- ✓ Interfața DRG prin care instituțiile medicale introduc datele;
- ✓ Conectorii de tip „web-services” cu instituțiile medicale care au propriile sisteme informatice;
- ✓ Regulile de validare a raportărilor. Tratarea excepțiilor;
- ✓ Bazele de date ale sistemului – servicii de întreținere;
- ✓ Rapoarte CNAM.

Pe lângă strânsă comunicare tehnică pe care echipa tehnică de suport aplicativ și platforma trebuie sa o aibă cu specialiștii M-Cloud, au fost identificate, fără a ne limita la acestea, următoarele operațiuni specifice care fac obiectul serviciilor de întreținere și suport specifice DRG:

Reguli de Validare

- Întreținerea modului de validare, a regulilor definite, conexiunilor cu baza de date și operațiuni de securitate specifice modulului.
- Actualizarea nomenclatoarelor DRG: Program Special, Diagnostice, Proceduri, Categorii Asigurat, Lista Spitale, KP, Criterii de Validare, etc.
- Modificarea criteriilor/regulilor de validare. Tratarea excepțiilor pentru criteriile de validare.
- Analize de impact pentru modificarea criteriilor/regulilor de validare la cerere. Recomandări și corectare situații neconforme.
- Actualizarea metodei de configurare a secțiilor. Păstrarea ID-urilor unice.

Întreținerea bazei de date a sistemului

- Operațiuni de administrare și optimizare a bazei de date pe infrastructura existentă.
- Operațiuni de migrare pe alte servere ale Beneficiarului care nu presupun modificarea arhitecturii sistemului.
- Operațiuni de întreținere a securității bazei de date.
- Operațiuni de analiza și auditare a securității bazei de date.

Rapoarte CNAM

- Generarea programată a rapoartelor.
- Îmbunătățirea, ajustarea și completarea rapoartelor CNAM. Raport complex, intern, etc.
- Implementarea restricțiilor CNAM: obligativitate câmpuri în dependența cu datele completate, eliminare cazuri medicale dublate, diagnostice secundare, proceduri secundare, etc.

B.Cerințe de mentenanță adaptivă şi corectivă a DRG

Asumarea contextului adaptării şi corecţiei software

În categoria serviciilor de mentenanță adaptivă şi corectivă a DRG intră acele servicii necesare pentru adaptarea şi corecţia sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul ”A. Cerințe de Mentenanță preventivă și Suport”.

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

- Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.
- Asumarea serviciilor din acest proiect implica acordarea garanției asupra DRG pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.
- În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.
- În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la DRG, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de DRG.
- Furnizorul este responsabil pentru eventualele incidente asupra DRG generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.
- Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.

➢ În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.

➢ Ofertanții trebuie sa demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport şi menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.

➢ Cererile de ajustări au termene relativ scurte și survin în general în urma unor modificări legislative sau în urma îmbunătățirilor funcționării business-proceselor. CNAM a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Pentru buna desfășurare a operațiunilor, dar și de consultanță în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnică a Furnizorului trebuie să fie pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și să dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului ajustărilor care sunt propuse de Beneficiar sau care sunt necesare în așa fel încât să asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie ajustări.

CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 900 de om/ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a DRG cum ar fi: ajustarea unor module ale DRG, ajustarea compartimentului Rapoarte, de asemenea, dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, etc. Rezervarea a 900 de om/ore la un preț prestabilit creează CNAM avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale DRG și asigură continuitatea serviciului în situațiile urgente.**

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

Serviciile de mentenanță adaptivă şi corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

Solicitarea serviciilor de mentenanță adaptivă şi corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului şi a costului estimativ conform tarifelor.

Prestarea serviciilor de mentenanță adaptivă şi corectivă

Prestarea serviciilor de mentenanță adaptivă şi corectivă se va efectua cu aplicarea următoarelor reguli:

➢ Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului şi acceptării rezultatului de către Beneficiar.

➢ Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.

➢ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.

➢ Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ţinînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.

➢ Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor şi condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

DRG este găzduit în MCloud-ul guvernamental. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a Beneficiarului. Toate operațiunile se vor desfășura în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

➢ Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental

➢ Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.

➢ Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client "Hot-Line"

Suportul operaţional la utilizarea serviciilor este asigurat de către Prestator prin intermediul Serviciului de Suport Client "Hot-Line" (în continuare SSC) cu oferirea unei platforme de Service Desk. Beneficiarul va contacta SSC, prin întocmirea Cererilor, în următoarele scopuri:

➢ pentru soluționarea defectelor;

➢ pentru solicitarea modificărilor funcționalităților existente;

➢ pentru solicitarea informaţiei şi consultanței în vederea soluționării defectelor legate de utilizarea sistemului;

➢ pentru solicitarea realizării anumitor activităţi şi acţiuni ce sunt în responsabilitatea Prestatorului;

➢ pentru solicitarea analizei unei solicitări de modificare.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități:

➢ expedierea unui e-mail la adresa SSC;

➢ efectuarea unui apel telefonic;

➢ crearea unui ticket în platforma de Service Desk.

Orice defect sau necesitate apărută la utilizarea serviciilor, Beneficiarul o va adresa inițial către SSC. În caz de necesitate, problema poate fi ulterior escaladată către Managerul de Proiect sau conducătorul Prestatorului. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului şi Beneficiarului, pentru a gestiona orice aspect ivit în relaţiile dintre aceştia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul.

Reguli privind prestare a serviciilor de suport

Serviciile de suport sunt orientate soluţionării incidentelor şi problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor şi actualizarea

documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul şi Beneficiarul vor conlucra strîns în vederea prevenirii incidentelor şi în vederea soluţionării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul şi prioritatea acordată pentru soluţionarea unui incident va ţine cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecinţele acestuia asupra disponibilităţii şi performanţei softului aplicativ. Urgenţa incidentului caracterizează operativitatea cu care acesta trebuie soluţionat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare şi soluţionare a incidentelor va fi în funcţie de impactul şi urgenţa incidentului. Algoritmul aplicat pentru stabilirea priorităţii unui incident este definit în continuare.

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

PRIORITATE		**Impact**		
		Înalt	*Mediu*	*Jos*
Urgenţă	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENŢĂ	**Descriere**
Înaltă	Un incident este estimat ca avînd nivelul urgenţei „Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activităţi şi operaţiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacţiunea imediată poate preveni riscuri legale majore şi de securitate (protecţie) a informaţiei.
Medie	Un incident este estimat ca avînd nivelul urgenţei „Mediu” în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activităţi şi operaţiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacţia operativă poate preveni riscuri legale moderate şi de securitate a informaţiei.
Joasă	Un incident este estimat ca avînd nivelul urgenţei „Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puţin în timp; - activităţile şi operaţiunile afectate nu trebuie continuate imediat; - nu există riscuri legale şi de securitate a informaţiei semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	**Descriere**
Înalt	Un incident este estimat ca avînd nivelul impactului „Înalt” în una sau mai multe din următoarele cazuri: - activităţile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizaţiei Beneficiarului şi afectează utilizatori externi, reputaţia şi imaginea Beneficiarului; - există riscuri legale şi financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca avînd nivelul impactului „Major” în una sau mai multe din următoarele cazuri: - activităţile importante ale Beneficiarului sunt întrerupte sau activităţile cheie sunt desfăşurate cu dificultate; - incidentul a afectat utilizatori interni şi un număr nesemnificativ de utilizatori externi; - există riscuri legale şi financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca avînd nivelul impactului „Jos” în una sau mai multe din următoarele cazuri: - activităţile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activităţile importante sunt desfăşurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru (8:00 – 17:00). În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort".

Prioritate incident	Timpul de reacție	Timpul de soluționare	Timp maxim pentru corectare a cauzei*	Raportare primară
Critică	Timpul de reacție al Prestatorului – imediat	pînă la 3 ore	8 ore	SSC (în afara orelor de lucru – Manager de Proiect)
Înaltă	Timpul de reacție al Prestatorului – 15 minute	8 ore	ora 12 a zilei următoare	SSC (în afara orelor de lucru – Manager de Proiect)
Medie	Timpul de reacție al Prestatorului – 4 ore	24 ore	5 zile	SSC (în afara orelor de lucru – Manager de Proiect)
Joasă	Timpul de reacție al Prestatorului – 24 ore;	3 zile	10 zile	SSC
Neglijabilă	Timpul de reacție al Prestatorului – 72 ore;	Cel mai bun efort	-	SSC

***Notă:** se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.*

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergenţe apărute între Părţi vor fi soluţionate cu efort comun şi prin strînsă conlucrare între Părţi. În acest scop, vor fi aplicate următoarele reguli:

- Părţile vor forma un grup comun de lucru în scopul soluţionării divergenţelor. De comun acord, în grupul de lucru pot fi acceptaţi reprezentanţi ai părţilor terţe, inclusiv experţi independenţi.
- La necesitate, părţile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergenţă.
- Grupul de lucru se va convoca şi va examina subiectul divergenţelor şi probele existente la subiect. Părţile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluţii echitabile pentru divergenţele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informaţiei

Prestatorul este responsabil pentru securitatea tehnologică şi funcţională a softului aplicativ în limitele sarcinilor de mentenanţă îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informaţiei, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părţile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce

asigură integritatea copiilor de rezervă efectuate;

- Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

După soluţionarea unui incident de securitate, părţile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acţiuni pentru prevenirea repetării incidentelor similare.

Livrabile

Prestatorul menține în stare actuală documentația tehnică. Documentaţia conţine suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni şi modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.

La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:

- Codul sursă final compilabil pe suport (DVD-R sau USB);
- Documentația tehnică;
- Ghidul utilizatorilor;
- Ghidul administratorului;
- Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Cerințe privind experiența personalului

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.

În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente mentenanței, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini și doar în baza acceptului Beneficiarului.

Ofertantul este obligat să informeze în prealabil Beneficiarul despre necesitatea modificării echipei de mentenanță, va transmite CV-ul persoanei care înlocuiește și va confirma recepționarea răspunsului (de acceptare sau refuz) expediat de către Beneficiar. Beneficiarul își rezervă dreptul de a refuza modificarea componenței minime a echipei în cazul în care pregătirea profesională și experiența noilor membri nu corespunde cerințelor stabilite în prezent caiet de sarcini sau solicitarea privind modificarea echipei nu este relevantă.

CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.
- Deținerea certificatului Project Manager sau documentului analogic de o instituție recunoscută

la nivel internațional în domeniul managementului proiectelor și/sau emis de o instituție publică sau privată competentă cu recunoaștere generală.
- Minim 3 ani de experiență în managementul proiectelor în domeniul tehnologiilor informaționale.
- Minim 3 proiecte în domeniul tehnologiilor informaționale realizate în calitate de Manager de proiect.
- Minim 3 ani de experiență în utilizarea metodologiilor de management de proiecte recunoscute pe plan internațional.
- Experiență specifică de Manager de Proiect în cel puțin 3 proiecte de complexitate similară, pe toată durata proiectului, realizate cu succes.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Business Analist *(minim 1 persoană)*
- Studii superioare în domeniul ingineriei sau tehnologiilor informaționale confirmate prin diploma de absolvire.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Cel puțin 3 ani de experiență în domeniul tehnologiilor informaționale.
- Cel puțin 3 ani de experiență în domeniul analizei și modelării Business-proceselor.
- Experiență profesională specifică, confirmată prin participarea în cel puțin 3 proiecte similare de implementare a unui sistem informatic integrat similar, în care el/ea s-a poziționat ca Business Analitic.
- Experiență în implementarea sistemelor informaționale complexe în instituțiile bugetare și/sau în domeniul medical.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist securitatea informațională (minim 1 persoană)
- Studii superioare Tehnice sau în domeniul TI.
- Cunoștințe privind securitatea sistemelor informatice și securitatea sistemelor ce conțin informații cu caracter personal, dovedite prin diplome/certificate obținute.
- Cunoștințe privind auditul sistemelor informatice dovedite prin diplome/certificate obținute (ISO27001, CISA sau echivalent*).
- Experiență de cel puțin 3 ani în domeniul securității sistemelor informatice.
- Participarea în ultimii 3 ani ca consultant sau auditor la cel puțin 3 contracte în domeniul securității informației.
- Participarea în cel puțin 3 contracte similare ca expert de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist infrastructură sistem (minim 1 persoană)
- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență profesională generală în domeniul de specialitate de minim 3 ani;
- Experiență dobândită prin participarea în cel puțin 3 proiecte în activități IT complexe privind infrastructura software și hardware pe platforme în baza tehnologiei de „cloud computing”

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a

fost).
Specialist programator (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Cunoașterea limbii de stat; – Experiență de minim 3 ani în programarea aplicațiilor web: Java, Java script, HTML, CSS, etc; – Experiență dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de implementare a unui sistem informațional de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Specialist baze de date (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Cunoașterea limbii de stat; – Experiență de minim 3 ani în administrarea bazelor de date: MS SQL Server; – Experiență dobândită prin participarea în calitate de specialist în baze de date în cel puțin 3 proiecte de implementare a unui sistem informatic de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Software Tester (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Experiență demonstrată în testarea funcțională a sistemelor informaționale; – Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale; – Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*

RECHIZITELE JURIDICE, POŞTALE ŞI DE PLĂŢI ALE PĂRŢILOR

Prestatorul	**Benefeciarul**
Adresa poştală:	Adresa poştală: mun. Chişinău, bd. Vlaicu Pîrcălab,46
Telefon:	Telefon/fax: 022 780-295, 022 780-240
Cod fiscal:	IBAN: MD58TRPEAD518720A01857AA Banca: Ministerul Finanțelor – Trezoreria de Stat
Banca:	Cod: TREZMD2X
Cod:	Cod fiscal: 1007601007778
IBAN	Adresa poştală: mun. Chişinău, bd. Vlaicu Pîrcălab,46

SEMNĂTURILE PĂRŢILOR

Prestatorul	**Benefeciarul** **Director general**

Ion DODON

Anexa nr. 1
la contractul nr. _____
Din „____” _____ 2023

SPECIFICAŢII TEHNICE

Denumirea serviciilor	**Denumirea modelului bunului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Lotul 1						
Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG**) – în bază de abonament**				Conform Caietului de sarcini din Capitolul II Condiții speciale ale contractului		**Moldova Standard**
Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG**) – în bază de trouble ticket/ticketing**				Conform Caietului de sarcini din Capitolul II Condiții speciale ale contractului		**Moldova Standard**

SEMNĂTURILE PĂRŢILOR

Prestatorul

Benefeciarul
Director general
Ion DODON

Anexa nr. 2
la contractul nr._____
din "____" _____ 2023

SPECIFICAŢII DE PREŢ

Cod CPV	Denumirea bunurilor/ serviciilor	Unitatea de măsură	Canti-tatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Termenul de livrare/prestare	Clasificație bugetară (IBAN)	
1	2	3	4	5	6	7	8	9	10	
Lotul 1 *achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG*										
72200000-7	Servicii de mentenanță preventivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – **în bază de abonament**	Luni	12					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	
72200000-7	Servicii de mentenanță corectivă și adaptivă (de suport) a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) **– în bază de trouble ticket/ticketing**	Om/ore	900					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	

SEMNĂTURILE PĂRŢILOR

Prestatorul

Benefeciarul
Director general
Ion DODON

Anexa nr.3
la contractul nr._____
din _ _____ 2023

Model de act de primire predare serviciilor pentru luna raportată

ACT
de primire-predare serviciilor pentru luna raportată

Prin prezentul act se confirmă prestarea serviciilor prevăzute de contractul

Nr._____ din ”_____”_____20__.

Se confirmă faptul că **operatorul economic_____**
a prestat servicii
_____
_____
_____
_____
_____
_____

la data de _____20__.

Prestatorul _____ *Beneficiarul*_____
Semnătura, F.N.P. **Semnătura, F.N.P**

Contrasemnat:

„____”_____202_ _____ _____
Semnătura F.N.P. și funcția persoanei care a recepționat bunuri

SEMNĂTURILE PĂRŢILOR

Prestatorul

Benefeciarul
Director general
Ion DODON

Anexa nr. 24
la Documentația standard nr._____
din "____" _____ 20___

A C H I Z I Ţ I I P U B L I C E

CONTRACT Nr.
privind achiziţia de servicii

I PARTEA GENERALĂ

Obiectul achiziţiei achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP
Cod CPV: 72200000-7

"___"_____20__ *mun. Chişinău*

Prestator	**Autoritatea contractantă**
_____ __, *(denumirea completă a întreprinderii, asociaţiei, organizaţiei)* reprezentată prin _____, *(funcţia, numele, prenumele)* care acţionează în baza _____, *(statut, regulament, hotărîre etc.)* denumit(a) în continuare *Vînzător,* _____	**Compania Națională de Asigurări în Medicină,** *(denumirea completă a întreprinderii, asociaţiei, organizaţiei)* reprezentată prin **director general,** **dl. Ion DODON** *(funcţia, numele, prenumele)* care acţionează în baza **Statutului**, *(statut, regulament, hotărâre etc.)* denumit(a) în continuare ***Beneficiar*** **IDNO 1007601007778** *(se indică nr. şi data de înregistrare în Registrul de Stat)* pe de o parte,

—, *(se indică nr. şi data de înregistrare în Registrul de Stat)* pe de o parte,	

ambii (denumiţi(te) în continuare Părţi), au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea *serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP*

(denumirea bunului/serviciului)

denumite în continuare Servicii, conform procedurii de achiziţii publice de tip _____ nr._____ din_____,
în baza deciziei grupului de lucru al Beneficiarului din „___” _____20__.

b. Următoarele documente vor fi considerate părţi componente ale Contractului:

*a) Specificaţia tehnică..... **Anexa nr.1**;*
*b) Specificația de preț..... **Anexa nr.2**;*
*c) Modelul Actului de predare-primirea serviciilor pentru luna raportată .....**Anexa nr.3***

c. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.
d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Beneficiar, se obligă prin prezentul contract să presteze Beneficiarului Serviciile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.
e. Beneficiarul se obligă prin prezentul contract să plătească Prestatorului, în calitate de contravaloare a prestării serviciilor, prețul Contractului în termenele şi modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1.Prestatorul îşi asumă obligaţia de a presta Specificaţiei tehnice ***Anexa nr.1*** și Specificaţiei de preț ***Anexa nr.2*****,** care este parte integrantă a prezentului Contract.
1.2. Benificiarul se obligă, la rândul său, să achite şi să recepţioneze Serviciile prestate de Prestator.
1.3 Serviciile prestate în baza contractului vor respecta standardele indicate în Partea II ”Condițiile speciale a contractului”.
1.4 Serviciile prestate în baza Contractului vor respecta standardele și normativele de domeniu sau alte reglementări autorizate.

2. Termeni şi condiţii de livrare

2.1. Prestarea Serviciilor se efectuează de către Prestator ***01.01.2025-31.12.2025.***
2.2. Documentaţia de însoţire a Serviciilor include:
1) *Originalele facturilor fiscale* .....2 ex
2) Act de predare-primire.....2 ex conform **Anexei *nr.3***
2.3. Originalele documentelor prevăzute în punctul 2.2 se vor prezenta Beneficiarului cel tîrziu la momentul prestării Serviciilor la destinaţia finală. Prestarea Serviciilor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.

3. Preţul şi condiţii de plată

3.1. Preţul Serviciilor prestate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat în Specificația de preț din ***Anexa nr.2***.

3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabileşte în lei moldoveneşti şi constituie: _____lei MD.

(suma cu cifre şi litere)

3.3. Achitarea plăţilor pentru Serviciile prestate se va efectua în lei moldoveneşti.

3.4. Metoda şi condiţiile de plată de către Beneficiar vor fi:

în termen de 15 zile lucrătoare din momentul prezentării facturii lunare şi Actului de predare-primire a serviciilor pentru luna raportată ***Anexa nr.3***.

3.5. Plăţile se vor efectua prin transfer bancar pe contul de decontare al Prestatorului indicat în prezentul Contract.

4. Condiţii de predare-primire

4.1. Serviciile se consideră prestate de către Prestator şi recepţionate de către Beneficiar, dacă:

a) cantitatea Serviciilor corespunde Specificaţiei tehnice ***Anexa nr.1***și Specificaţiei de preț ***Anexa nr.2*** și informaţiei indicate în documentele de însoţire conform punctului 2.2 al prezentului Contract;

b) calitatea Serviciilor corespunde informaţiei indicate în Specificaţiei tehnice ***Anexa nr.1***;

4.2. Prestatorul este obligat să prezinte la sfârșitul lunii raportate Beneficiarului un exemplar original al facturii fiscale și Actului de predare-primire a serviciilor pentru luna raportată ***Anexa nr.3***, pentru efectuarea plăţii. Pentru nerespectarea de către Prestator a prezentei clauze, Beneficiarul îşi rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4 corespunzător numărului de zile de întîrziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 10.3.

5. Standarde

5.1. Serviciile prestate în baza contractului vor respecta standardele și normativele de domeniu sau alte reglementări autorizate.

6. Obligaţiile părţilor

6.1. În baza prezentului Contract, Prestatorul se obligă:

a) să presteze Serviciile în condiţiile prevăzute în Specificaţia tehnică din ***Anexa nr.1***.

b) să anunţe Beneficiarul după semnarea prezentului Contract, în decurs de __5__ zile calendaristice, prin telefon/fax sau poșta electronică achizitii@cnam.gov.md, despre disponibilitatea prestării Serviciilor;

c) să asigure condiţiile corespunzătoare pentru recepţionarea Serviciilor de către Beneficiar, în termenele stabilite, în corespundere cu cerinţele prezentului Contract;

d) să asigure integritatea şi calitatea Serviciilor pe toată perioada de până la recepţionarea lor de către Beneficiar.

6.2. În baza prezentului Contract, Beneficiarul se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepţionării în termenul stabilit a Serviciilor prestate în corespundere cu cerinţele prezentului Contract;

b) să asigure achitarea Serviciilor prestate, respectînd modalităţile şi termenele indicate în prezentul Contract.

7. Circumstanțe care justifică neexecutarea contractului

7.1. Părţile sunt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanțe care justifică neexecutarea contractului (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pământ, precum şi alte circumstanţe care nu depind de voinţa Părţilor).

7.2. Partea care invocă clauza circumstanțelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai tîrziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor care justifică neexecutarea contractului.

7.3. Survenirea circumstanţelor care justifică neexecutarea contractului, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.
7.4 În cazul în care în circumstanțele care justifică neexecutarea contractului, acesta se modifică prin acordul adițional, inclusiv modificarea termenilor de executare, în cazul unei executări ulterioare a contractului. Când se execută pct.7.1 și pct. 7.3, părțile modifică contractul prin acord - adițional, privind neîndeplinerea parțială sau integrală a obligațiunilor, inclusiv modificarea termenilor în cazul suspendării și executării ulterioare a contractului.

8. Rezoluțiunea

8.1. Rezoluțiunea Contractului se poate realiza cu acordul comun al Părţilor.
8.2. Contractul poate fi rezolvit în mod unilateral de către:
a) Beneficiarul în caz de refuz al Prestatorului de a presta Serviciile prevăzute în prezentul Contract;
b) Beneficiarul în caz de nerespectare de către Prestator a termenelor de prestare stabilite;
c) Prestatorul în caz de nerespectare de către Beneficiar a termenelor de plată a Serviciilor;
d) Prestatorul sau Beneficiarul în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.
8.3 Beneficiarul are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situaţii:
a) contractantul se afla, la momentul atribuirii lui, în una dintre situaţiile care ar fi determinat excluderea sa din procedura de atribuire potrivit art. 19 al Legii nr.131/2015 privind achizițiile publice;
b) contractul a făcut obiectul unei modificări substanțiale care necesita o nouă procedură de achiziție publică în conformitate cu art. 76 al Legii nr.131/2015 privind achizițiile publice;
c) contractul nu ar fi trebuit să fie atribuit contractantului respectiv, avînd în vedere o încălcare gravă a obligaţiilor ce rezultă din Legea nr.131/2015 privind achizițiile publice și/sau tratatele internaţionale la care Republica Moldova este parte, care a fost constatată printr-o decizie a unei instanțe judecătorești naționale sau, după caz, internaționale.
8.4. Partea iniţiatoare a rezoluțiunii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.
8.5. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluţionat în termenele stabilite, partea iniţiatoare va iniția rezoluțiunea.

9. Reclamaţii

9.1. Reclamaţiile privind cantitatea Serviciilor prestate sunt înaintate Prestatorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Prestatorului.
9.2. Pretenţiile privind calitatea Serviciilor prestate sunt înaintate Prestatorului în termen de 5 zile de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o organizaţie independentă neutră şi autorizată în acest sens.
9.3. Prestatorul este obligat să examineze pretenţiile înaintate în termen de 3 zile de la data primirii acestora şi să comunice Beneficiarului despre decizia luată.
9.4. În caz de recunoaştere a pretenţiilor, Prestatorul este obligat, în termen de 5 zile, să livreze suplimentar Beneficiarului cantitatea neprestată de Servicii, iar în caz de constatare a calităţii necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.
9.5. Prestatorul poartă răspundere pentru calitatea Serviciilor în limitele stabilite, inclusiv pentru viciile ascunse.
9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizaţia independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întîrziere sunt suportate de partea vinovată.

10. Sancţiuni

10.1. Forma de garanţie de bună executare a contractului agreată de Beneficiar este _____, în cuantum de 5% din valoarea contractului.
10.2. Pentru refuzul de a presta Serviciile prevăzute în prezentul Contract, se va reține garanţia de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevedrile punctului 10.1., în caz contrar Prestatorul suportă o penalitate în valoare de 5 % din suma totală a contractului.
10.3. Pentru achitarea cu întârziere, Beneficiarul poartă plata despăgubirei în valoare de 0,1% din suma Serviciilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 5 % din suma totală a prezentului contract.
10.4. Suma penalităţii calculate Prestatorului conform prezentului Contract poate fi dedusă (reţinută) de către Beneficiar din suma plăţii pentru Serviciile prestate.

11. Drepturi de proprietate intelectuală

11.1. Prestatorul are obligaţia să despăgubească achizitorul împotriva oricăror:
a) reclamaţii şi acţiuni în justiţie, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile sau utilajele folosite pentru sau în legătură cu produsele achiziţionate, şi
b) daune-interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către achizitor.

12. Dispoziţii finale

12.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluţionate de către Părţi pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanţa de judecată competentă conform legislaţiei Republicii Moldova.
12.2. Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin acord adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului. Modificările şi completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris şi au fost semnate de ambele Părţi.
12.3. Nici una dintre Părţi nu are dreptul să transmită obligaţiile şi drepturile sale stipulate în prezentul Contract unor terţe persoane fără acordul în scris al celeilalte părţi.
12.4. Prezentul Contract în cazul în care este semnat electronic, de către ambele părți, acesta este remis în mod automat prin mijloacele electronice, dar în cazul când contractul este semnat olografic se întocmește în două exemplare în limba română, câte un exemplar pentru Prestator și Benefeciar.
12.5. Prezentul Contract este întocmit în două exemplare în limba de stat a Republicii Moldova, cîte un exemplar pentru Prestator. Prezentul Contract se consideră încheiat la data semnării şi intră în vigoare din data comunicării către Prestator privind transmiterea către Agenția de Achiziții Publice a dării de seamă**.**
12.6. Prezentul contract este valabil până la **31.12.2025.**
12.7. Prezentul Contract reprezintă acordul de voinţă al părţilor şi se consideră semnat la data aplicării ultimei semnături de către una din părți.
12.8. Pentru confirmarea celor menţionate mai sus, Părţile au semnat prezentul Contract în conformitate cu legislaţia Republicii Moldova.

CONDIȚIILE
SPECIALE A CONTRACTULUI

CAIET DE SARCINI

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **SIP**

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	Descriere
Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP: • *Servicii de mentenanță preventivă și Suport – în bază de abonament;* • *Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.*	*Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.*

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP (în continuare – SIP) pentru o perioadă de **minim 12 luni** după încetarea contractului.

De asemenea, Prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta CNAM (Beneficiar) împreună cu codul sursă DRG, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Descriere generală a SIP

SIP este destinat evidenței și raportării serviciilor medicale de înaltă performanța și urmărește automatizarea proceselor care au loc în activitatea prestatorilor de servicii medicale care se contractează după metoda "per serviciu", privind estimarea necesității de servicii medicale de înaltă performanță, posibilitatea de programare a persoanelor în IMS care prestează servicii medicale și evidența personificată a serviciilor medicale prestate. SIP oferă transparență în procesul de prestare a serviciilor medicale de înaltă performanta, astfel ca pacientul are dreptul de a alege la care prestator vrea să meargă pentru servicii medicale, iar modul în care sunt alocate aceste servicii este conform procedurilor CNAM.

Setul de date folosit în funcționalitatea sistemului cuprinde:

- IDNP al pacientului;
- IDNP al medicului prescriptor;
- IDNO prestatorului de servicii medicale în care activează medicul;

- Denumirea prestatorului de servicii medicale în care activează medicul;
- IDNO al prestatorului de servicii de înaltă performanță;
- Denumirea prestatorului de servicii de înaltă performanță;
- Data și ora trimiterii la serviciile medicale;
- Codul serviciilor medicale prescrise;
- Codul serviciilor medicale prestate;
- Denumirea deplină a serviciilor de înaltă performanță;
- Data și ora generării sloturilor pentru serviciile medicale;
- Data și ora efectuării programării serviciilor medicale;
- Data și ora prestării serviciilor medicale;
- Statutul/categoria serviciilor medicale
- Diagnosticul la trimitere (prin selectare din Lista Diagnosticelor);
- Numele și Prenumele Pacientului;
- Data nașterii;
- Adresa la domiciliu.

Beneficiarii direcți ai SIP sunt CNAM, pacientul asigurat, medic prescriptor (medic de familie sau medic specialist), prestator servicii medicale, care deține contract cu CNAM.

Specificații tehnice SIP

Caracteristici generale de funcționare

SIP are o arhitectură 3-layer, arhitectura care permite funcționarea pe platforma guvernamentală comună MCloud. SIP funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă tot ce este necesar de automatizat;
- are posibilitatea reparației unui modul fără afectarea altora;
- respecta standardele în vigoare a tehnologiilor informaționale;
- asigura flexibilitate în vederea adaptării permanente la normele juridice și în vederea dezvoltării softului după implementare;
- utilizează o arhitectură orientată pe servicii pentru a acomoda cu ușurință noi modificări cu intervenții exclusiv asupra componentei de updatat, minimizând costurile și timpul necesar realizării modificărilor;
- are o arhitectură modernă cu un grad înalt de performanță, structurată pe 3 niveluri (nivelul pentru baze de date, nivelul pentru aplicație si nivelul acces/utilizator). Fiecare nivel are în componența toate echipamentele necesare bunei funcționări.
- SIP este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- poate fi utilizat împreună cu echipamente ce permit creșterea vitezei de înregistrare a datelor de identificare ale pacienților (nume, prenume, IDNP etc.)
- este scalabil pentru a acomoda modificările viitoare ale numărului de utilizatori ai soluției;
- recunoaște corect sursele informaționale, le acceptă și le integrează în sistem;
- întreține în limba de stat interfața utilizator, conținutul registrelor, bazelor de date și documentelor generate;
- permite ca utilizatorul să se autentifice o singură data pentru a accesa toate modulele aplicației;
- Poate fi accesat de pe telefon, PC, notebook, etc.

Interfața Utilizator

Aceasta interfața este accesibilă pentru toți utilizatorii autorizați în SIP:

- ✓ SIP dispune de o interfață inteligenta, intuitiva și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browser-ul web și nu necesită instalarea de componente software suplimentare;
- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului
- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:

- **Platforma hardware**, formată din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat în sistemul MCloud:
  - Servere protejate redundant pentru hosting al bazelor de date, softului de sistem si softului funcțional (aplicații și subsisteme);
  - Platforma hardware pusă la dispoziție de către beneficiar este dimensionată corespunzător pentru a permite funcționarea în bune condiții a sistemului;
  - Performanța optimă, în limita normelor obiective de uzură, pentru realizarea structurii funcționale și asigurarea extinderii ulterioare a sistemului;
  - este flexibilă în utilizarea mijloacelor disponibile destinate recepționării informației din surse externe (alte instituții publice);
  - asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date;
  - asigură normele de funcționare ale platformelor informatice guvernamentale.

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:
  - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
  - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server.
  - Pe stațiile utilizatorilor există navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare si transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mijloacele de imprimare, cititoare, rețele electronice locale (LAN – local area network) și de scară largă (WAN – wide area network). Pentru operare se folosesc stațiile de lucru ale beneficiarului, singură specificație impusă utilizatorilor fiind cea de a dispune de un browser conectat la internet, fiind recomandate și utilizate soluțiile Microsoft.

Sistemul de securitate

SIP funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.

Caracteristici:

- asigura accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare si consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de sistem.
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor.

Având în vedere natura specială a informațiilor gestionate în cadrul SIP, acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.

Sistemul are următoarele nivele de securitate care asigura confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație intre stații si server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unica cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este asigurată automat, iar modificările de structura la nivelul acesteia se fac exclusiv în baza drepturilor corespunzătoare de administrator al bazei de date. În plus, baza de date deține propriul mecanism de backup care permite, în caz de dezastru, restaurarea unor versiuni anterioare recente (de ordinul zilelor).

Sistemul asigura dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori sunt create module de acces și autentificare în sistem; sunt indicate volumul de informație și funcționalitatea pe care aceștia o accesează. Sistemul permite accesul la datele statistice pentru anumiți utilizatori și grupuri de utilizatori. Sistemul asigură verificarea automată a drepturilor în momentul intrării în sistem și în ulterioarele accesări a sistemului și creează un jurnal al accesărilor – jurnalul de audit.

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Prestator/Prescriptor**: permite introducerea și modificarea datelor specifice activității sale;
- nivelul **Administrator**: permite înregistrarea și modificarea datelor specifice activității sale, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

La nivel aplicativ, sistemul generează o lista de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

- ✓ posibilitatea înregistrării, adăugării si dezactivării utilizatorilor din sistem;
- ✓ posibilitatea distribuției drepturilor utilizatorilor folosind grupuri de acces;
- ✓ posibilitatea pentru fiecare utilizator de a avea cel puțin următoarele atribute de autentificare:

identificarea, autentificarea.

- ✓ posibilitatea intrării în sistem a unui utilizator în orice moment;
- ✓ asigurarea de către administrator a regimurilor de funcționare, deconectare, conectare, modificării regimului de autentificare și identificare, dirijarea cu drepturi și auditul.

Retenția datelor, acces securizat

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.

- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respecta regulile de control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.

- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.

- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați sa acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem si pe baza permisiunilor asociate rolului sau rolurilor din care fac parte utilizatorii.

- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați sa acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fisele electronice ale pacienților săi.

- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu ca a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:

  - Unicitatea utilizatorilor în sistem;

  - Mecanism de control al versiunilor pentru înregistrările medicale.

- **Securizarea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.

Arhitectura SIP

SIP are o arhitectură bazată pe tehnologie web, folosind platforma Microsoft/Linux Sistemul este conceput modular, dezvoltarea acestora putând fi realizata în paralel. Orice client se poate conecta la serverul de aplicație și poate utiliza sistemul conform drepturilor pe care le are. Comunicația între client și server se realizează exclusiv prin protocoale securizate de tip HTTPS folosind certificat de securitate integrat la nivelul serverului de aplicație. Schema arhitecturală este în figura următoare:

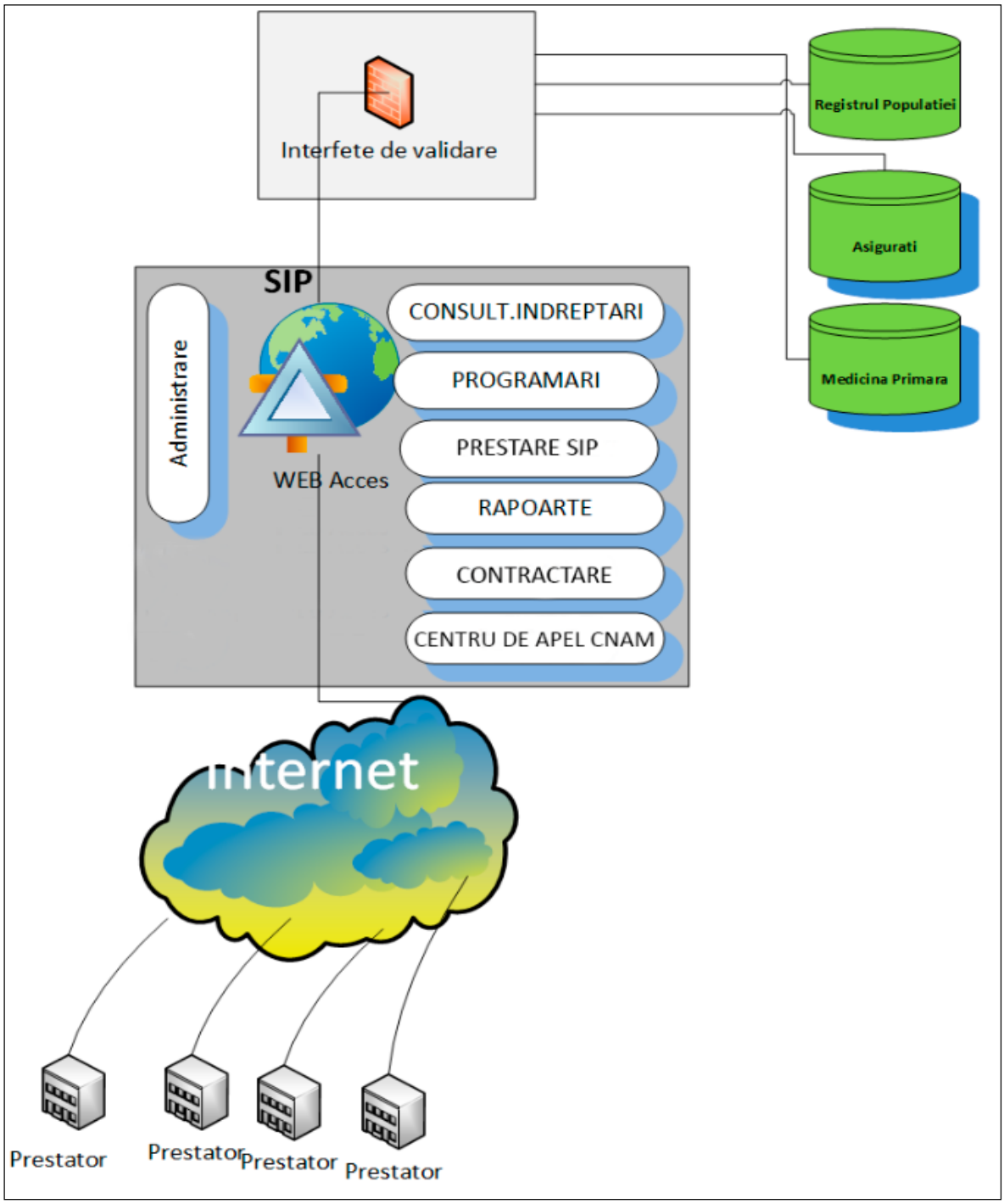


Figura 1. Schema arhitecturală SIP

Componente operaționale ale SIP sunt operaționale în următoarea structură modulară:

- ✓ Modulul de administrare roluri;
- ✓ Modulul consult/îndreptări (prescriere a biletului de trimitere);
- ✓ Modulul programări;
- ✓ Modulul prestare a serviciilor de înalta performanță;
- ✓ Modulul rapoarte;
- ✓ Modulul contractare;
- ✓ Interfețe.

Modulul de administrare roluri

Actorii implicați în circuitul informațional privind evidența serviciilor medicale de înaltă performanță sunt:

- Pacient asigurat;
- Administrator CNAM (administrare SIRSM);
- CNAM (responsabil CNAM);
- Medic prescriptor (medic de familie sau medic specialist);
- Prestator servicii medicale, care deține contract cu CNAM.

Administrarea sistemului informatic este realizată de către administratorul (reprezentantul) CNAM pentru partea de conținut a serviciilor medicale în colaborare cu Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) pentru partea de asistență și mijloacele tehnice necesare funcționării SIP extins în infrastructură hardware & software din cadrul MCloud.

Administratorul sistemului are acces deplin la toate funcționalitățile sistemului, fișiere și baze de date aferente sistemului, încăperile în care se află echipamentele pe care rulează aplicațiile software sau care asigură securitatea datelor.

Medicul prescriptor

În interfața de utilizare a sistemului medicul prescriptor (medic de familie sau specialist) are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului:

- Datele de identificare ale medicului de familie sau specialist cu drepturi de prescriere a serviciilor medicale;
- Adresa;
- IDNO al instituțiilor medicale în care medicul prestează servicii;
- Denumirea instituțiilor medicale în care medicul prestează servicii;
- Cod instituțiilor medicale în care medicul prestează servicii.

Pentru medicul de familie sau medicul specialist, interfața de utilizare a sistemului are o formă simplă care îi permite efectuarea rapida de prescriere, validare și programare servicii medicale a pacientului, după modelul descris în continuare.

Prestatorul de servicii medicale

În interfața de utilizare a sistemului, prestatorul de servicii medicale are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului, în directa corespondență cu contractul CNAM, pe care nu le poate modifica:

- IDNO al instituției prestatoare de servicii medicale;
- Adresa instituției;
- Numărul contractului;
- Lista de servicii medicale asumate pe grupuri și programe, inclusiv sumele contractuale specificate pentru perioadele pe care sunt programate aceste sume.

Pe lângă acestea, administratorul local al prestatorului are în cadrul interfeței:

- Câmpurile necesare definirii listei de servicii medicale ce pot fi executate;
- Opțiunile de alocare a serviciilor disponibile în lista pe sloturi libere (secvențe de timp);
- Posibilitatea de urmărire a atributelor la nivel de serviciu și slot.

Posibilitatea de urmărire a relației dintre serviciile medicale contractate și cele alocate în sloturi.

Modul consult/îndreptări

Modulul consult urmărește traseul prescrierii serviciului medical și programării pacientului la serviciile medicale de înaltă performanță. Sistemul dispune de mecanismele de restricție și control prin care acest flux va fi urmărit permanent:

- Pacientul se prezintă la medicul de familie sau la medicul specialist, unde prezintă datele de identificare. Identificatorul unic al pacientului este IDNP-ul.
- Medicul introduce în sistem IDNP-ul.
- Prin intermediul web-serviciilor sistemul verifica automat statutul de asigurat al pacientului și validează alocarea pacientului la medicul de familie care efectuează operațiunea curentă.
- Dacă asigurarea pacientului nu este validată de către sistem (pacientul nu are statut de asigurat), medicul nu poate prescrie biletul de trimitere. La fel, dacă sistemul nu confirmă că pacientul este alocat medicului de familie curent, atunci medicul nu poate îndrepta pacientul către servicii medicale.
- Scenariul favorabil pentru prescrierea biletului de trimitere la serviciul medical este cel în care pacientul este validat de sistem cu statut de asigurat și ulterior înregistrat la medicul de familie curent sau, în situații excepționale (concediu, boala) de înlocuitorul acestuia. În acest caz, medicul stabilește în baza consultului necesitatea unei investigații din lista de servicii medicale conform Programului.

Modul programări

Programarea efectivă a pacientului constă în alocarea unui slot (interval definit de timp în care un anumit serviciu este disponibil).

- Programarea pacientului la serviciul medical se bazează pe dreptul pacientului la libera alegere a prestatorului.
- Pacientul asigurat și înregistrat la medicul de familie care efectuează consultul are dreptul la servicii medicale plătite din fondul CNAM. Medicul de familie sau medicul specialist decid în baza consultului aceasta necesitate, iar sistemul emite un **cod unic al biletului de trimitere a pacientului către servicii medicale CNAM.**
- Codul unic al biletului de trimitere poate fi folosit în interesul pacientului în <u>următoarele</u> moduri:
  a) Medicul prescriptor se consultă cu pacientul în vederea programării în SIP a pacientului într-unul din sloturile libere declarate de către Prestatori, în funcție de distanța și disponibilitatea definite de Prescriptor.
  b) Pacientului îi este tipărit numărul de trimitere și detaliile consultului urmând sa își facă singur programarea la serviciul de înaltă performanță prin intermediul SIP.
  c) Pacientului îi este tipărit numărul de trimitere și detaliile consultului urmând să-și facă programarea prin intermediul Centrului de apel al CNAM.

Modulul prestare a serviciilor de înaltă performanță

Executarea efectivă a serviciilor de înaltă performanță este o operațiune a prestatorului care se încheie cu confirmarea prestării acestuia și completarea rezultatului. Prestarea se consideră încheiată doar în momentul în care pacientul are un rezultat în urma investigației.

- În interfața sistemului prestatorul declară sloturile libere pe grupe de servicii de înaltă performanță, în corespondență cu contractul CNAM. Aceste sloturi sunt completate automat în baza programărilor efectuate. Prestatorul are acces la datele de corespondență ale pacientului.
- După prezentarea pacientului pentru efectuarea investigației, prestatorul completează în sistem rezultatul și închide programarea.
- Pacientul primește rezultatul investigației în mod fizic (tipărit) și continuă investigațiile sau tratamentul la îndrumarea medicului care i-a prescris serviciul medical.
- Sistemul înregistrează încheierea prestării și confirmă CNAM că serviciul medical contractat de către prestator a fost prestat și ca poate fi plătit.

Modulul rapoarte

În cadrul interfeței de lucru sunt disponibile în timp real următoarele valori:

- Încărcarea prescriptorilor: în sistem sunt disponibile valorile per medic prescriptor. De asemenea în sistem apar valori adiacente: date despre prescrieri, prescriptor, pacient, servicii medicale etc. Sistemul poate folosi aceste informații în scop de analiză pentru realizarea de rapoarte statistice.
- Încărcarea prestatorilor: în sistem sunt disponibile listele de servicii medicale contractate, alocarea pe sloturi, executarea serviciilor de înaltă performanță în timp real în directă corespondență cu contractul CNAM.

Efectuarea programărilor. În sistem sunt disponibile în timp real toate informațiile despre programări, servicii medicale, prestatori, prescriptori și datele în corespondența cu contractul CNAM. În cadrul interfeței administratorul poate vedea efectuarea programărilor în timp real dar și pe intervale de timp definite ad-hoc.

Modulul contractare

În modulul contractare se înregistrează volumele contractuale în dependență de lista de servicii medicale, numărul de servicii, tarife, sumele contractate. În interfața acestui modul sunt disponibile următoarele funcționalități:

- Modificarea/actualizarea nomenclatorului serviciilor medicale din Anexa nr. 5 al PU (nr.de ordine, denumire serviciu, cod serviciu tarif serviciu) în dependență de modificare Programului Unic;
- Modificarea/actualizarea listei prestatorilor și prescriptorilor (denumire deplina și scurta a prestator/prescriptor, adresa/locația, IDNO, codul din 4 cifre);
- Introducerea și înregistrarea contractelor cu prestatorii în dependență de: număr contract, perioada de timp (lista serviciilor de înaltă performanță: nr.de ordine, denumire, cod, număr de servicii, tarif, sumă);
- Modificarea contractelor prin Acord adițional în dependență de: număr acord adițional, perioada de timp (lista serviciilor de înaltă performanță: nr.de ordine, denumire, cod, număr de servicii, tarif, sumă).

A. Cerințe de Mentenanță preventivă și Suport

Cerinţele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanţă elaborat de Prestator şi aprobat de Beneficiar.

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanța SIP, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;

- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

Prin ofertă, furnizorul serviciilor achiziționate de către Beneficiar asumă următoarele condiții minime de suport tehnic pe aplicație pentru utilizatori:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM;
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistența tehnică pentru utilizatorii CNAM prin email și platforma Service Desk pusă la dispoziție de către Furnizor;
- Modalități de asigurare a suportului: email, telefon, acces la distanță;
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare - best effort.

Suport platforma software

Servicii dedicate Sistemelor de Operare

În aceasta categorie întră următoarele servicii minime relative la sistemele de operare pe care rulează SIP care vor fi desfășurate de către Furnizor:

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifesta transparent și înlăturarea cauzelor care le-au produs sau recomandarea masurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- creare și întreținere conturi de acces locale;
- optimizarea configuratei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanță și disponibilitate a sistemului.

Servicii dedicate sistemelor de gestiune a bazelor de date

În această categorie întră următoarele servicii minime relative la Microsoft SQL Server ale SIP care vor fi desfășurate de către Furnizor:

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corecta a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidenţialităţii şi securității datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;

- supravegherea respectării cerinţelor de securitate informaţională de către utilizatori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securităţii privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale SIP şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum şi restaurarea acestora.
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

Servicii dedicate componentelor, inclusiv a celor de interconectare

În această categorie întră următoarele servicii minime relative la codul SIP care vor fi desfășurate de către Furnizor:

- verifică și optimizează secvențele de cod;
- identifică și analizează problemele și potențialele probleme de la nivelul codului;
- rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației;
- soluționează incidentele apărute la nivelul codului;
- modifică rapoartele, șabloanele, serviciile aplicative;
- comunică cu echipele de suport în scopul funcționarii corecte și permanente a sistemului.

Efectuarea testelor de penetrare

Teste de penetrare se referă la o metodă de evaluare a securității sistemului informațional prin simularea unor atacuri cibernetice. Scopul acestor teste este de a identifica și exploata vulnerabilitățile sistemului pentru a evalua cât de bine poate rezista sistemul informațional la atacuri reale. În această categorie întră următoarele servicii minime:

- Simulare a atacurilor;
- Identificarea vulnerabilităților;
- Evaluarea impactului;
- Raportare și recomandări.

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice SIP

SIP este un sistem automatizat care operează în condițiile legislației în vigoare. Prin serviciile prestate, ofertantul va asigura operațiuni de întreținere, suport și recomandări tehnice asupra aplicației, inclusiv în situația modificărilor legislative care afectează componentele software existente în SIP. CNAM precizează că modificarea funcționalităților existente în aplicație în corelație cu modificările

legislative presupun în mod concret modificări în codul sursa al aplicației.

Orice modificare asupra codului sursă are ca efect o noua versiune operațională a aplicației, conform legislației. CNAM solicită ofertantului asumarea faptului că, deține cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toata perioada desfășurării contractului.

Operațiunile tehnice de întreținere ce se vor desfășura de personalul care va asigura funcționarea continuă a SIP se referă la componentele majore ale sistemului, adică la:

- ✓ Interfața SIP prin care prescriptorii și prestatorii introduc datele;
- ✓ Bazele de date ale sistemului – servicii de întreținere;
- ✓ Rapoarte CNAM;

B.Cerințe de mentenanță adaptivă şi corectivă a SIP

Asumarea contextului adaptării şi corecţiei software

În categoria serviciilor de mentenanță adaptivă şi corectivă a SIP intră acele servicii necesare pentru adaptarea şi corecţia sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul ”A. Cerințe de Mentenanță preventivă și Suport”.

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

➢ Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.

➢ Asumarea serviciilor din acest proiect implica acordarea garanției asupra SIP pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.

➢ În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.

➢ În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la SIP, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de SIP.

➢ Furnizorul este responsabil pentru eventualele incidente asupra SIP generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.

➢ Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.

➢ În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.

➢ Ofertanții trebuie sa demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport şi menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.

➢ Cererile de ajustări au termene relativ scurte și survin în general în urma unor modificări

legislative sau în urma îmbunătățirilor funcționării business-proceselor. CNAM a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Pentru buna desfășurare a operațiunilor, dar și de consultanță în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnică a Furnizorului trebuie să fie pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și să dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului ajustărilor care sunt propuse de Beneficiar sau care sunt necesare în așa fel încât să asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie ajustări.

CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 900 de om/ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a SIP cum ar fi: ajustarea modulelor SIP, elaborarea modulului pentru Centrul de Apel „INFO CNAM”, , de asemenea, dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, etc. Rezervarea a 900 de om/ore la un preț prestabilit creează CNAM avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale SIP și asigură continuitatea serviciului în situațiile urgente.**

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

Serviciile de mentenanță adaptivă şi corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

Solicitarea serviciilor de mentenanță adaptivă şi corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului şi a costului estimativ conform tarifelor.

Prestarea serviciilor de mentenanță adaptivă şi corectivă

Prestarea serviciilor de mentenanță adaptivă şi corectivă se va efectua cu aplicarea următoarelor reguli:

- Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului şi acceptării rezultatului de către Beneficiar.
- Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.
- Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.
- Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ținînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părți.
- Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor şi condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

SIP este găzduit în MCloud-ul guvernamental. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a Beneficiarului. Toate operațiunile se vor desfășura în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

- Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental
- Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.
- Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client "Hot-Line"

Suportul operaţional la utilizarea serviciilor este asigurat de către Prestator prin intermediul Serviciului de Suport Client "Hot-Line" (în continuare SSC) cu oferirea unei platforme de Service Desk. Beneficiarul va contacta SSC, prin întocmirea Cererilor, în următoarele scopuri:

- pentru soluționarea defectelor;
- pentru solicitarea modificărilor funcționalităților existente;
- pentru solicitarea informației şi consultanței în vederea soluționării defectelor legate de utilizarea sistemului;
- pentru solicitarea realizării anumitor activităţi şi acţiuni ce sunt în responsabilitatea Prestatorului;
- pentru solicitarea analizei unei solicitări de modificare.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități:

- expedierea unui e-mail la adresa SSC;
- efectuarea unui apel telefonic;
- crearea unui ticket în platforma de Service Desk.

Orice defect sau necesitate apărută la utilizarea serviciilor, Beneficiarul o va adresa inițial către SSC. În caz de necesitate, problema poate fi ulterior escaladată către Managerul de Proiect sau conducătorul Prestatorului. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului şi Beneficiarului, pentru a gestiona orice aspect ivit în relaţiile dintre aceştia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul.

Reguli privind prestare a serviciilor de suport

Serviciile de suport sunt orientate soluţionării incidentelor şi problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor şi actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul şi Beneficiarul vor conlucra strîns în vederea prevenirii incidentelor şi în vederea soluţionării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul şi prioritatea acordată pentru soluţionarea unui incident va ţine cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecinţele acestuia asupra disponibilităţii şi performanţei softului aplicativ. Urgenţa incidentului caracterizează operativitatea cu care acesta trebuie soluţionat

pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare şi soluţionare a incidentelor va fi în funcţie de impactul şi urgenţa incidentului. Algoritmul aplicat pentru stabilirea priorităţii unui incident este definit în continuare.

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

PRIORITATE		**Impact**		
		Înalt	*Mediu*	*Jos*
Urgenţă	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENŢĂ	**Descriere**
Înaltă	Un incident este estimat ca având nivelul urgenţei „Înalt" în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activităţi şi operaţiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacţiunea imediată poate preveni riscuri legale majore şi de securitate (protecţie) a informaţiei.
Medie	Un incident este estimat ca având nivelul urgenţei „Mediu" în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activităţi şi operaţiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacţia operativă poate preveni riscuri legale moderate şi de securitate a informaţiei.
Joasă	Un incident este estimat ca având nivelul urgenţei „Jos" în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puţin în timp; - activităţile şi operaţiunile afectate nu trebuie continuate imediat; - nu există riscuri legale şi de securitate a informaţiei semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	**Descriere**
Înalt	Un incident este estimat ca având nivelul impactului „Înalt" în una sau mai multe din următoarele cazuri: - activităţile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizaţiei Beneficiarului şi afectează utilizatori externi, reputaţia şi imaginea Beneficiarului; - există riscuri legale şi financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca având nivelul impactului „Major" în una sau mai multe din următoarele cazuri: - activităţile importante ale Beneficiarului sunt întrerupte sau activităţile cheie sunt desfăşurate cu dificultate; - incidentul a afectat utilizatori interni şi un număr nesemnificativ de utilizatori externi; - există riscuri legale şi financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca având nivelul impactului „Jos" în una sau mai multe din următoarele cazuri: - activităţile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activităţile importante sunt desfăşurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru (8:00 – 17:00). În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort".

Prioritate incident	**Timpul de reacţie**	**Timpul de soluţionare**	**Timp maxim pentru corectare a cauzei***	**Raportare primară**

Critică	Timpul de reacţie al Prestatorului – imediat	pînă la 3 ore	8 ore	SSC (în afara orelor de lucru – Manager de Proiect)
Înaltă	Timpul de reacţie al Prestatorului – 15 minute	8 ore	ora 12 a zilei următoare	SSC (în afara orelor de lucru – Manager de Proiect)
Medie	Timpul de reacţie al Prestatorului – 4 ore	24 ore	5 zile	SSC (în afara orelor de lucru – Manager de Proiect)
Joasă	Timpul de reacţie al Prestatorului – 24 ore;	3 zile	10 zile	SSC
Neglijabilă	Timpul de reacţie al Prestatorului – 72 ore;	Cel mai bun efort	-	SSC

***Notă:** se aplică pentru situaţia când soluţionarea incidentului se face prin aplicarea unor măsuri de ocolire.*

Alte cerinţe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergenţe apărute între Părţi vor fi soluţionate cu efort comun şi prin strînsă conlucrare între Părţi. În acest scop, vor fi aplicate următoarele reguli:

- Părţile vor forma un grup comun de lucru în scopul soluţionării divergenţelor. De comun acord, în grupul de lucru pot fi acceptaţi reprezentanţi ai părţilor terţe, inclusiv experţi independenţi.
- La necesitate, părţile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergenţă.
- Grupul de lucru se va convoca şi va examina subiectul divergenţelor şi probele existente la subiect. Părţile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluţii echitabile pentru divergenţele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informaţiei

Prestatorul este responsabil pentru securitatea tehnologică şi funcţională a softului aplicativ în limitele sarcinilor de mentenanţă îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informaţiei, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părţile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acţiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilităţii pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;
- Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

După soluţionarea unui incident de securitate, părţile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acţiuni pentru prevenirea repetării incidentelor similare.

Livrabile

Prestatorul menține în stare actuală documentația tehnică. Documentaţia conţine suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni şi modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.

La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:

- Codul sursă final compilabil pe suport (DVD-R sau USB);
- Documentația tehnică;
- Ghidul utilizatorilor;
- Ghidul administratorului;
- Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțială a uneia dintre cerințe va duce automat la declararea ofertei ca fiind neconformă și, implicit, la descalificarea ei. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Cerințe privind experiența personalului

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.

În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente mentenanței, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini și doar în baza acceptului Beneficiarului.

Ofertantul este obligat să informeze în prealabil Beneficiarul despre necesitatea modificării echipei de mentenanță, va transmite CV-ul persoanei care înlocuiește și va confirma recepționarea răspunsului (de acceptare sau refuz) expediat de către Beneficiar. Beneficiarul își rezervă dreptul de a refuza modificarea componenței minime a echipei în cazul în care pregătirea profesională și experiența noilor membri nu corespunde cerințelor stabilite în prezent caiet de sarcini sau solicitarea privind modificarea echipei nu este relevantă.

CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.
- Deținerea certificatului Project Manager sau documentului analogic de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor și/sau emis de o instituție publică sau privată competentă cu recunoaștere generală.
- Minim 3 ani de experiență în managementul proiectelor în domeniul tehnologiilor informaționale.
- Minim 3 proiecte în domeniul tehnologiilor informaționale realizate în calitate de Manager de proiect.

- Minim 3 ani de experiență în utilizarea metodologiilor de management de proiecte recunoscute pe plan internațional.
- Experiență specifică de Manager de Proiect în cel puțin 3 proiecte de complexitate similară, pe toată durata proiectului, realizate cu succes.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Business Analist *(minim 1 persoană)*

- Studii superioare în domeniul ingineriei sau tehnologiilor informaționale confirmate prin diploma de absolvire.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Cel puțin 3 ani de experiență în domeniul tehnologiilor informaționale.
- Cel puțin 3 ani de experiență în domeniul analizei și modelării Business-proceselor.
- Experiență profesională specifică, confirmată prin participarea în cel puțin 3 proiecte similare de implementare a unui sistem informatic integrat similar, în care el/ea s-a poziționat ca Business Analitic.
- Experiență în implementarea sistemelor informaționale complexe în instituțiile bugetare și/sau în domeniul medical.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist securitatea informațională (minim 1 persoană)

- Studii superioare Tehnice sau în domeniul TI.
- Cunoștințe privind securitatea sistemelor informatice și securitatea sistemelor ce conțin informații cu caracter personal, dovedite prin diplome/certificate obținute.
- Cunoștințe privind auditul sistemelor informatice dovedite prin diplome/certificate obținute (ISO27001, CISA sau echivalent*).
- Experiență de cel puțin 3 ani în domeniul securității sistemelor informatice.
- Participarea în ultimii 3 ani ca consultant sau auditor la cel puțin 3 contracte în domeniul securității informației.
- Participarea în cel puțin 3 contracte similare ca expert de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate.

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist infrastructură sistem (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență profesională generală în domeniul de specialitate de minim 3 ani;
- Experiență dobândită prin participarea în cel puțin 3 proiecte în activități IT complexe privind infrastructura software și hardware pe platforme în baza tehnologiei de „cloud computing”

(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).

Specialist programator (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Cunoașterea limbii de stat;
- Experiență de minim 3 ani în programarea aplicațiilor web: Java, Java script, HTML, CSS, etc;

– Experiență dobândită prin participarea în calitate de specialist IT în cel puțin 3 proiecte de implementare a unui sistem informațional de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Specialist baze de date (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Cunoașterea limbii de stat; – Experiență de minim 3 ani în administrarea bazelor de date: MS SQL Server; – Experiență dobândită prin participarea în calitate de specialist în baze de date în cel puțin 3 proiecte de implementare a unui sistem informatic de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*
Software Tester (minim 1 persoană) – Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe; – Experiență demonstrată în testarea funcțională a sistemelor informaționale; – Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale; – Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară *(se justifică prin documente, ex: CV-uri, descrierea proiectelor și/sau scrisori de recomandare din partea beneficiarilor de proiecte, remise pe numele operatorului economic, angajatul căruia a fost).*

RECHIZITELE JURIDICE, POŞTALE ŞI DE PLĂŢI ALE PĂRŢILOR

Prestatorul	**Benefeciarul**
Adresa poştală:	Adresa poştală: mun. Chişinău, bd. Vlaicu Pîrcălab,46
Telefon:	Telefon/fax: 022 780-295, 022 780-240
	IBAN: MD58TRPEAD518720A01857AA
Cod fiscal:	Banca: Ministerul Finanţelor – Trezoreria de Stat
Banca:	Cod: TREZMD2X
Cod:	Cod fiscal: 1007601007778
IBAN	Adresa poştală: mun. Chişinău, bd. Vlaicu Pîrcălab,46

SEMNĂTURILE PĂRŢILOR

Prestatorul	**Benefeciarul** **Director general** **Ion DODON**

Anexa nr. 1
la contractul nr. _____
Din „____” _____ 2023

SPECIFICAŢII TEHNICE

Denumirea serviciilor	**Denumirea modelului bunului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Lotul 2						
Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de abonament**. .				Conform Caietului de sarcini din Capitolul II Condiții speciale ale Contractului		**Moldova Standard**
Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de trouble ticket/ticketing.**				Conform Caietului de sarcini din Capitolul II Condiții speciale ale Contractului		**Moldova Standard**

SEMNĂTURILE PĂRŢILOR

Prestatorul

Benefeciarul
Director general
Ion DODON

Anexa nr. 2
la contractul nr._____
din "____" _____ 2023

SPECIFICAŢII DE PREŢ

Cod CPV	Denumirea bunurilor/ serviciilor	Unitatea de măsură	Canti-tatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Termenul de livrare/prestare	Clasificație bugetară (IBAN)	
1	2	3	4	5	6	7	8	9	10	
Lotul 2 *achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP*										
72200000-7	Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de abonament**. .	Luni	12					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	
72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – **în bază de trouble ticket/ticketing.**	Om/ore	900					01.01.2025-31.12.2025	MD58TRPEAD518720A01857AA	

SEMNĂTURILE PĂRŢILOR

Prestatorul

Benefeciarul
Director general
Ion DODON

Anexa nr.3
la contractul nr._____
din _ _____ 2023

Model de act de primire predare serviciilor pentru luna raportată

ACT
de primire-predare serviciilor pentru luna raportată

Prin prezentul act se confirmă prestarea serviciilor prevăzute de contractul

Nr._____ din ”_____”_____20__.

Se confirmă faptul că **operatorul economic_____**
a prestat servicii
_____
_____
_____
_____
_____
_____

la data de _____20__.

Prestatorul _____ *Beneficiarul*_____
Semnătura, F.N.P. **Semnătura, F.N.P**

Contrasemnat:

„____”_____202_ _____ _____
Semnătura F.N.P. și funcția persoanei care a recepționat bunuri

SEMNĂTURILE PĂRŢILOR

Prestatorul

Benefeciarul
Director general
Ion DODON