

CNAM

 A C H I Z I Ţ I I P U B L I C E

CONTRACT Nr. 33/1 P
privind achiziția de servicii

I PARTEA GENERALĂ

Obiectul achiziției achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG și SIP
Cod CPV: 72200000-7

“31” decembrie 2025

mun. Chișinău

Prestator	Autoritatea contractantă
<p>Das Soft Plus SRL, reprezentată prin administrator, dl. Afanasie BUTUCEA care acționează în baza Statutului denumit în continuare <i>Prestator</i>,</p> <p><u>IDNO 1019600011052</u></p> <p>pe de o parte,</p>	<p><u>Compania Națională de Asigurări în Medicină,</u> reprezentată prin director general, dl. Ion DODON, care acționează în baza <u>Statutului</u>,</p> <p>denumit în continuare <i>Beneficiar</i></p> <p><u>IDNO 1007601007778</u></p> <p>pe de o parte,</p>

ambii denumiți în continuare Părți, au încheiat prezentul Contract referitor la următoarele:

a. Achiziționarea serviciilor de mentenanță, suport și dezvoltare pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG și SIP

denumite în continuare Servicii, conform procedurii de achiziții publice de tip Licitatie deschisă nr. din ocds-b3wdp1-MD-1763716847767 din 21/11/2025, în baza deciziei grupului de lucru al Beneficiarului Nr. 15/25 din 22.12.2025.

b. Următoarele documente vor fi considerate părți componente ale Contractului:

- a) *Specificația tehnică..... Anexa nr.1;*
- b) *Specificația de preț..... Anexa nr.2;*

c) *Modelul Actului de predare-primirea serviciilor pentru luna raportatăAnexa nr.3*

- c. În cazul unor discrepanțe sau inconsecvențe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.
- d. În calitate de contravaloare a plăților care urmează a fi efectuate de Beneficiar, se obligă prin prezentul contract să presteze Beneficiarului Serviciile și 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 și modalitatea stabilite de Contract.

1. Obiectul Contractului

- 1.1. Prestatorul își asumă obligația de a presta Specificației tehnice *Anexa nr.1* și Specificației de preț *Anexa nr.2*, care este parte integrantă a prezentului Contract.
- 1.2. Beneficiarul se obligă, la rândul său, să achite și să recepționeze 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 și condiții de livrare

- 2.1. Prestarea Serviciilor se efectuează de către Prestator *01.01.2026-31.12.2026, inclusiv.*
- 2.2. Documentația de însoțire a Serviciilor include:
- 1) *Originalele facturilor fiscale2 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 târziu la momentul prestării Serviciilor la destinația finală. Prestarea Serviciilor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.



3. Prețul și condiții de plată

- 3.1. Prețul Serviciilor prestate conform prezentului Contract este stabilit în lei moldovenești, fiind indicat în Specificația de preț din *Anexa nr.2*.
- 3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabilește în lei moldovenești și constituie: **2 235 708,00** (două milioane două sute treizeci și cinci de mii șapte sute opt lei și 00 bani) lei MDL.
- 3.3. Achitarea plăților pentru Serviciile prestate se va efectua în lei moldovenești.
- 3.4. Metoda și condițiile de plată de către Beneficiar vor fi: în termen de 15 zile lucrătoare din momentul prezentării facturii lunare și Actului de predare-primire a serviciilor pentru luna raportată *Anexa nr.3*.
- 3.5. Plățile se vor efectua prin transfer bancar pe contul de decontare al Prestatorului indicat în prezentul Contract.

4. Condiții de predare-primire

- 4.1. Serviciile se consideră prestate de către Prestator și recepționate de către Beneficiar, dacă:
- a) cantitatea Serviciilor corespunde Specificației tehnice *Anexa nr.1* și Specificației de preț *Anexa nr.2* și informației indicate în documentele de însoțire conform punctului 2.2 al prezentului Contract;
 - b) calitatea Serviciilor corespunde informației indicate în Specificației 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 plății. Pentru nerespectarea de către Prestator a prezentei clauze, Beneficiarul își rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4 corespunzător numărului de zile de întârziere și de a fi exonerat de achitarea penalității 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. Obligațiile părților

6.1. În baza prezentului Contract, Prestatorul se obligă:

- a) să presteze Serviciile în condițiile prevăzute în Specificația tehnică din *Anexa nr.1*.
- b) să anunțe 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 condițiile corespunzătoare pentru recepționarea Serviciilor de către Beneficiar, în termenele stabilite, în corespundere cu cerințele prezentului Contract;
- d) să asigure integritatea și calitatea Serviciilor pe toată perioada de până la recepționarea lor de către Beneficiar.

6.2. În baza prezentului Contract, Beneficiarul se obligă:

- a) să întreprindă toate măsurile necesare pentru asigurarea recepționării în termenul stabilit a Serviciilor prestate în corespundere cu cerințele prezentului Contract;
- b) să asigure achitarea Serviciilor prestate, respectând modalitățile și termenele indicate în prezentul Contract.

7. Circumstanțe care justifică neexecutarea contractului

7.1. Părțile sunt exonerate de răspundere pentru neîndeplinirea parțială sau integrală a obligațiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanțe care justifică neexecutarea contractului (războaie, calamități naturale: incendii, inundații, cutremure de pământ, precum și alte circumstanțe care nu depind de voința Părților).

7.2. Partea care invocă clauza circumstanțelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai târziu de 10 zile) cealaltă Parte despre survenirea circumstanțelor care justifică neexecutarea contractului.

7.3. Survenirea circumstanțelor care justifică neexecutarea contractului, momentul declanșării și termenul de acțiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din țara Părții care invocă asemenea circumstanțe.

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 neîndeplinirea parțială sau integrală a obligațiilor, inclusiv modificarea termenilor în cazul suspendării și executării ulterioare a contractului.

8. Rezoluțiunea

8.1. Rezoluțiunea Contractului se poate realiza cu acordul comun al Părților.

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 Părți a pretențiilor înaintate conform prezentului Contract.

8.3. Beneficiarul are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situații:

- a) contractantul se afla, la momentul atribuirii lui, în una dintre situațiile 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 obligațiilor ce rezultă din Legea nr.131/2015 privind achizițiile publice și/sau tratatele internaționale 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 inițiatoare a rezoluțiunii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părți despre intențiile ei printr-o scrisoare motivată.

8.5. Partea înștiințată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluționat în termenele stabilite, partea inițiatoare va iniția rezoluțiunea.

9. Reclamații

9.1. Reclamațiile privind cantitatea Serviciilor prestate sunt înaintate Prestatorului la momentul recepționării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Prestatorului.

9.2. Pretențiile privind calitatea Serviciilor prestate sunt înaintate Prestatorului în termen de 5 zile de la depistarea deficiențelor de calitate și trebuie confirmate printr-un certificat eliberat de o organizație independentă neutră și autorizată în acest sens.

9.3. Prestatorul este obligat să examineze pretențiile înaintate în termen de 3 zile de la data primirii acestora și să comunice Beneficiarului despre decizia luată.

9.4. În caz de recunoaștere a pretențiilor, Prestatorul este obligat, în termen de 5 zile, să livreze suplimentar Beneficiarului cantitatea neprestată de Servicii, iar în caz de constatare a calității necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerințele 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 organizația independentă neutră sau autorizată în acest sens, cheltuielile pentru staționare sau întârziere sunt suportate de partea vinovată.

10. Sancțiuni

10.1. Forma de garanție de bună executare a contractului agreată de Beneficiar este în cuantum de 5% din valoarea contractului și se efectuează prin transfer la contul autorității contractante.

10.2. Pentru refuzul de a presta Serviciile prevăzute în prezentul Contract, se va reține garanția de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevederile 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 despăgubirii 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 penalității calculate Prestatorului conform prezentului Contract poate fi dedusă (reținută) de către Beneficiar din suma plății pentru Serviciile prestate.

11. Drepturi de proprietate intelectuală

11.1. Prestatorul are obligația să despăgubească achizitorul împotriva oricărui:

a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalațiile sau utilajele folosite pentru sau în legătură cu produsele achiziționate, și

b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către achizitor.

12. Dispoziții finale

12.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluționate de către Părți pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanța de judecată competentă conform legislației Republicii Moldova.

12.2. Părțile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin acord adițional, numai în cazul apariției unor circumstanțe care lezează interesele comerciale legitime ale acestora și care nu au putut fi prevăzute la data încheierii contractului. Modificările și completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris și au fost semnate de ambele Părți.

12.3. Nici una dintre Părți nu are dreptul să transmită obligațiile și drepturile sale stipulate în prezentul Contract unor terțe persoane fără acordul în scris al celeilalte părți.

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 Beneficiar.

12.5. Prezentul Contract este întocmit în două exemplare în limba de stat a Republicii Moldova, câte un exemplar pentru Prestator. Prezentul Contract se consideră încheiat la data semnării și 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 **31.12.2026**.

12.7. Prezentul Contract reprezintă acordul de voință al părților și se consideră semnat la data aplicării ultimei semnături de către una din părți.

12.8. Pentru confirmarea celor menționate mai sus, Părțile au semnat prezentul Contract în conformitate cu legislația 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
----------------------------	------------------

<p>Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG:</p> <ul style="list-style-type: none"> • <i>Servicii de mentenanță preventivă și Suport – în bază de abonament;</i> • <i>Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing.</i> 	<p><i>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.</i></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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, credențialele 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 eficiență cât mai mare (economii 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**, formată 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;

- 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);
 - asigură 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 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 scară 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 (înscrisoare, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structură 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 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 asigurată automat, iar modificările de structură 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 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 **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 și 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. Măsurile de securitate ajută 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 competență. 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 arhitecturală este în figura următoare:

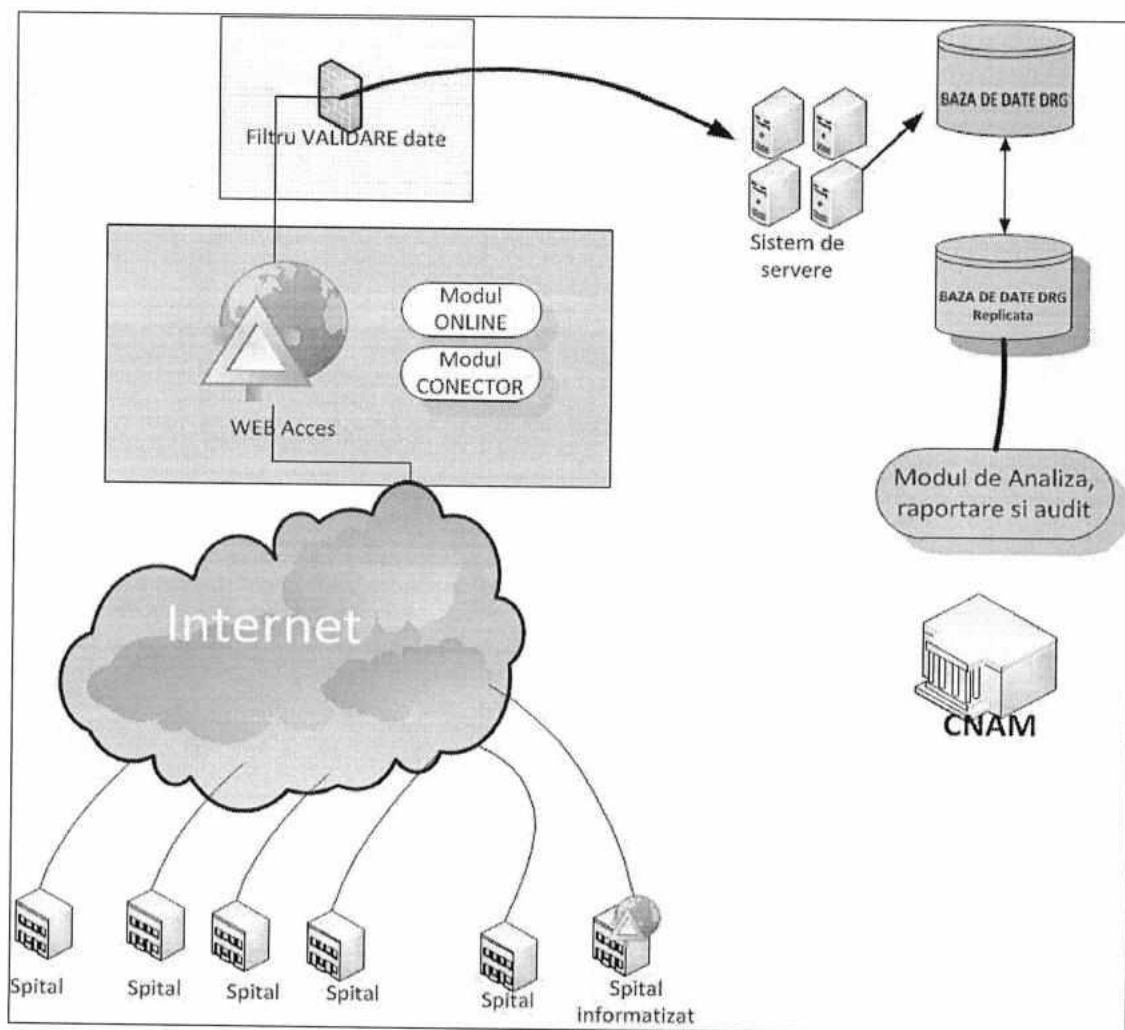


Figura 1. Schema arhitecturală DRG

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 existența 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.

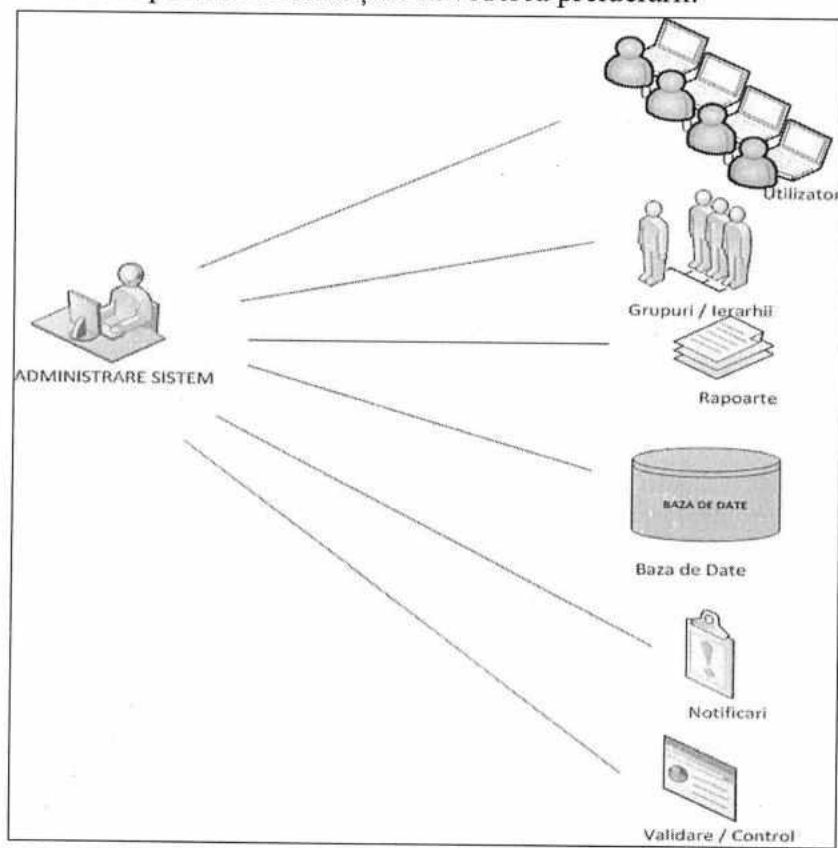


Figura 2. Schema Modulul de administrare sistem colector

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 legătură 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.

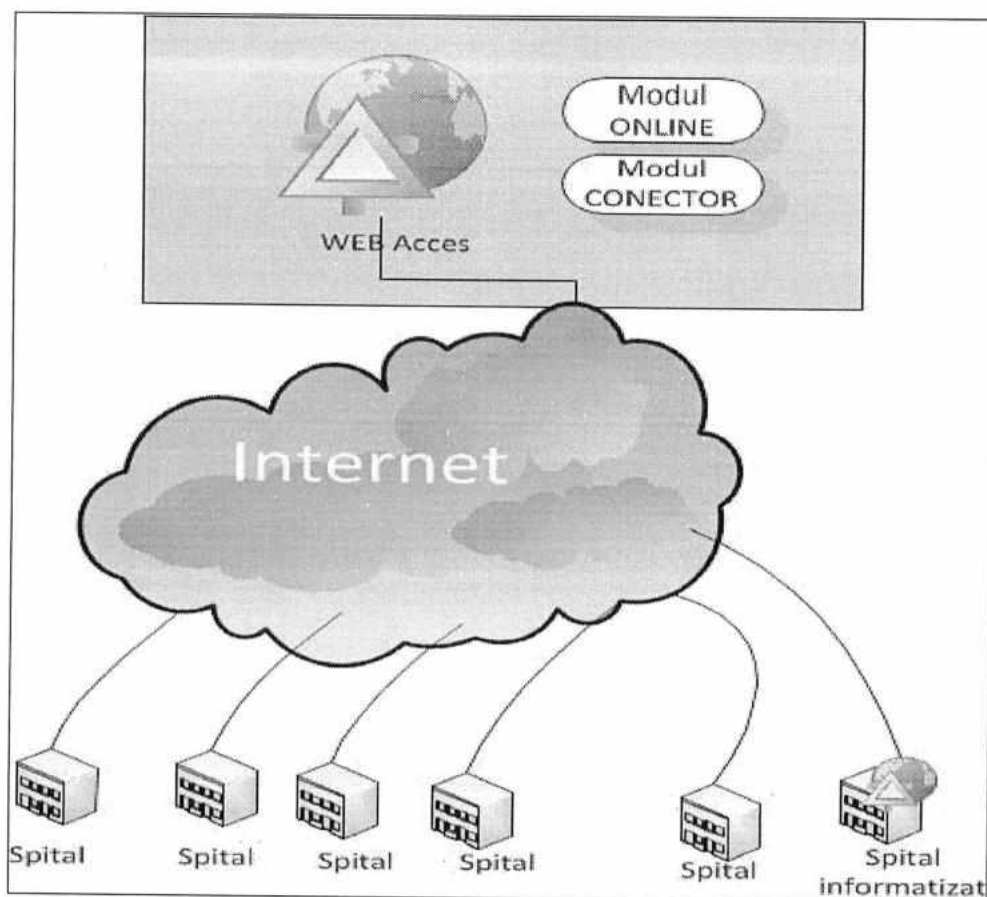


Figura 4. Modulul de colectare date Real Time

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.

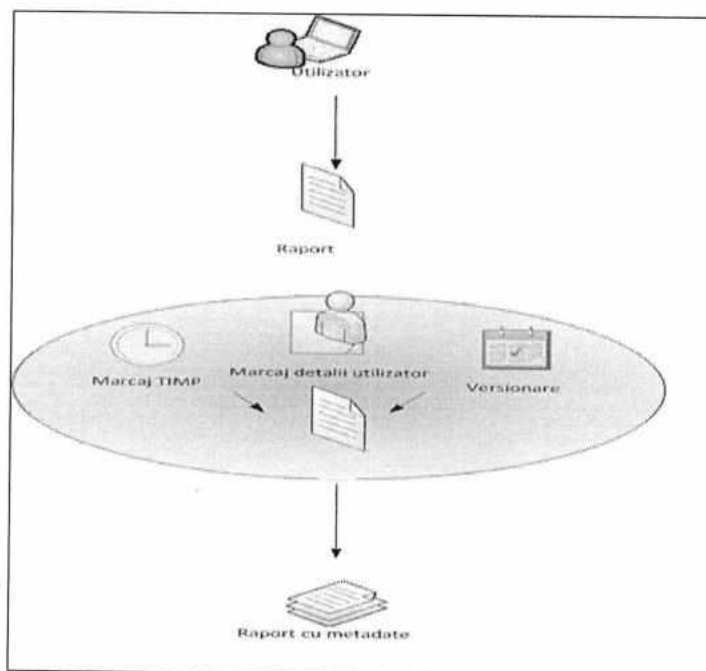


Figura 5. Modulul de nerepudiere

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 metadata 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 metadatale 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 corespondență 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.

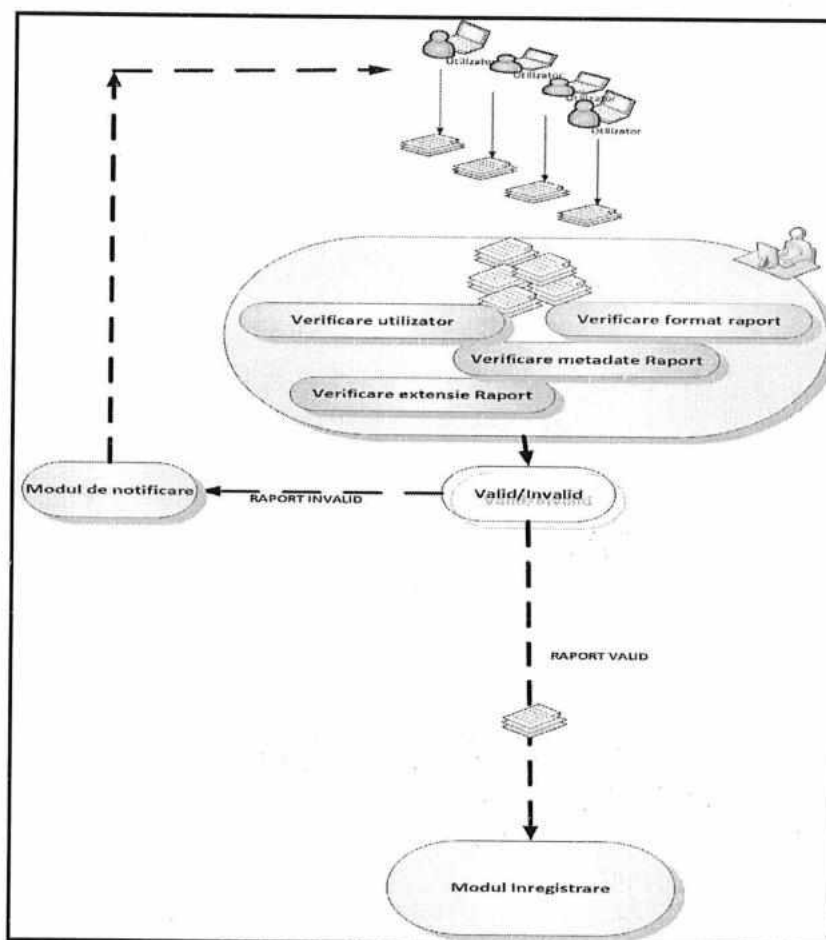


Figura 6. Schema Modulului de Validare

Modulul de înregistrare raportări

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

Modulul de înregistrare a rapoartări conține două componente:

1. Componenta „buffer”, temporară, care colectează toate rapoartărilor 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 rapoartărilor și le mută în zona de depozitare a rapoartelor – forma definitivă, prelucrabilă – numita Modul Warehouse.

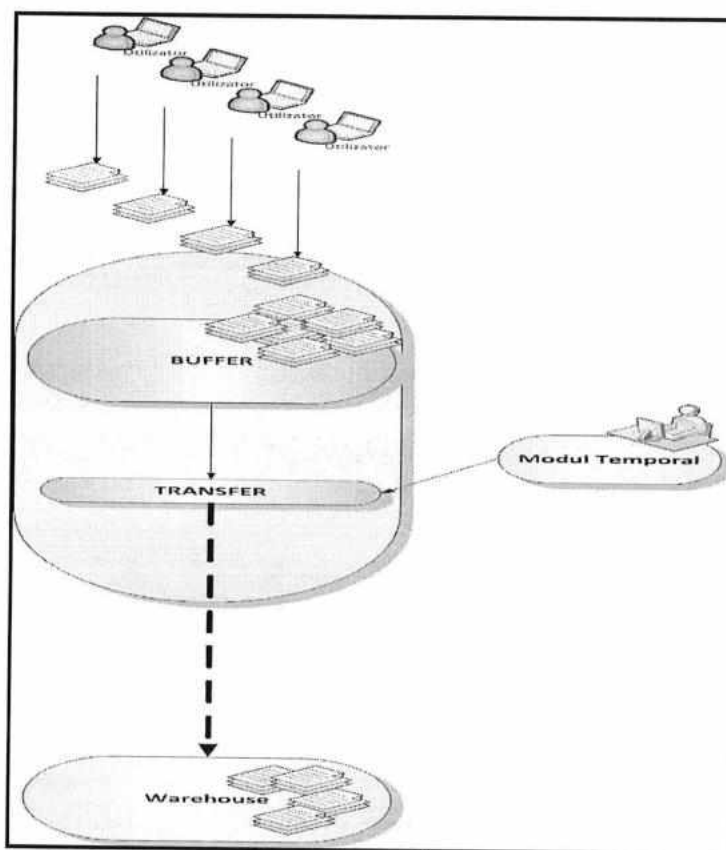


Figura 7. Schema Modul de Înregistrare Rapoarte

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

- „Bufferul” permite unele modificări controlate de administratori asupra rapoartărilor 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 rapoartărilor. 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 permanentă între utilizatori, beneficiari și entitatea informatică:

✓ **Setări:** aceasta funcție a modulului este accesibilă 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 execută 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 asigură 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 rapidă 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.

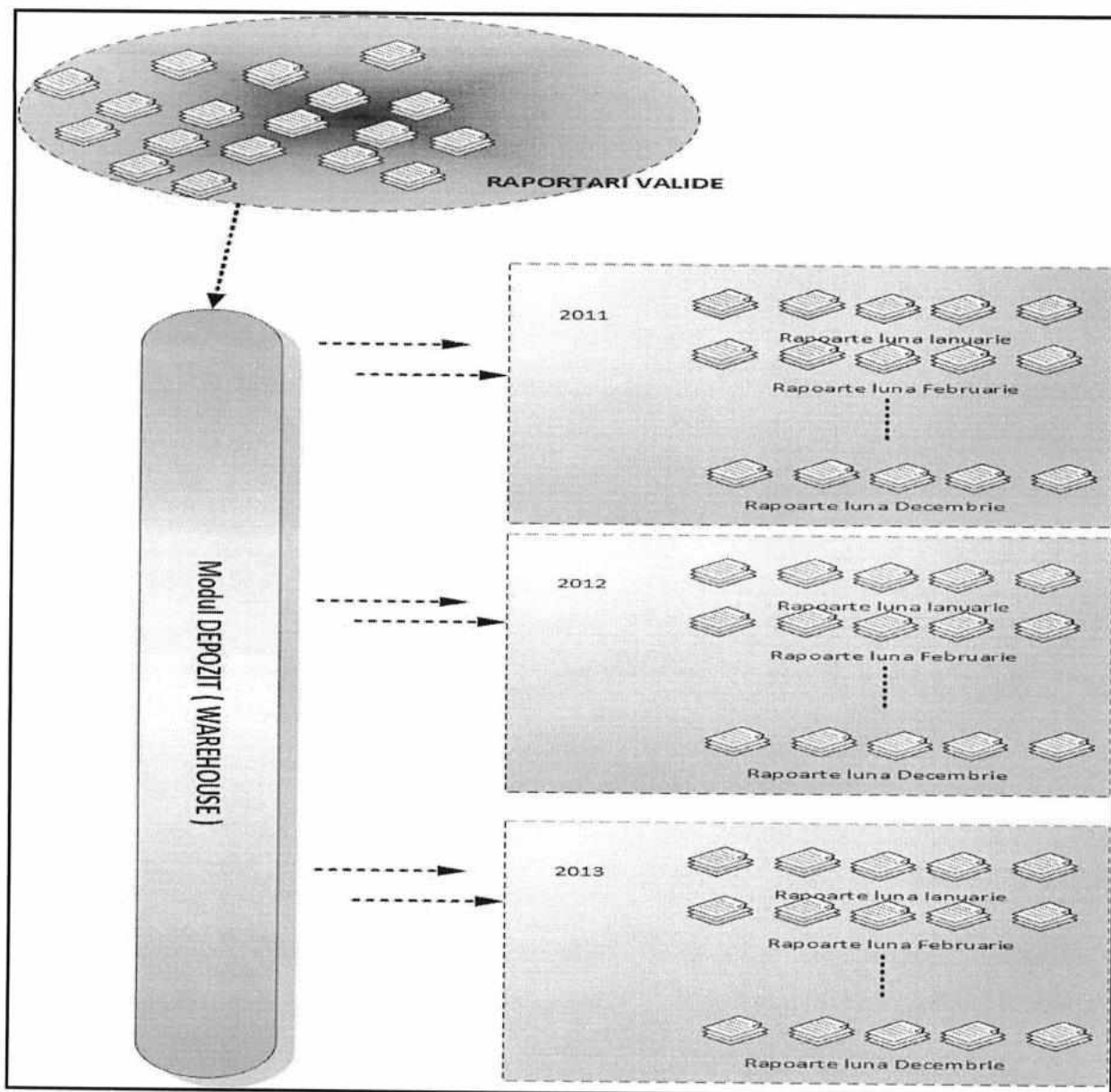


Figura 8. Schema Modul Depozit Rapoarte DRG (Warehouse)

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 diagnosticilor pacienților; pe baza acestora se pot identifica eventualele neconcordanțe 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 curentă. Sistemul răspunde următoarelor solicitări:

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

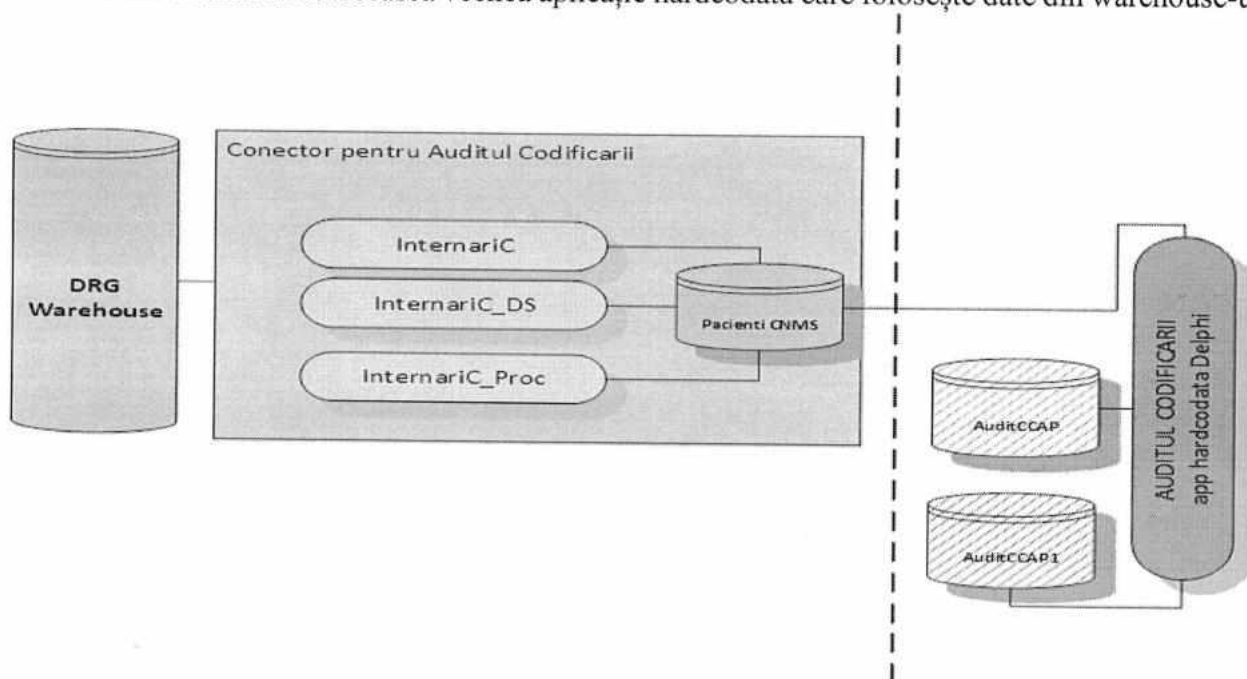
- în timp real: respingerea informațiilor eronate cu atenționarea celui care introduce datele; sistemul nu permite introducerea de date necorespunzătoare.

- 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 execută auditarea și evaluare să obțină o listă consistentă și reală pe care să o verifice și în teren. Prin utilizarea sistemului informatic pot fi identificate cazurile de fraudare.

2) Creșterea eficienței. Existența modului de analiză, raportare și audit la nivelul CNAM constituie un instrument pe care departamentele autorizate CNAM implicate în raportare îl folosesc în vederea creșterii eficienței de lucru. Căutările sunt rapide, rapoartele sunt generate cu mare ușurință 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 sursă. 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 execută 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 hardcodată 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 procedură de achiziție CNAM solicită operațiuni de mentenanță care se referă exclusiv la funcționalitățile asupra cărora deține codul sursă, urmând 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-urilor 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 codificării prin intermediul aplicației CCAP nu este posibilă logarea/autentificarea concomitentă a Auditorilor I/II în aplicație și 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, și 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 mentenanță elaborat de Prestator și aprobat de Beneficiar.

De menționat că prin procesul de mentenanță se controlează funcționarea produsului software, se înregistrează problemele pentru analiză, se întreprind acțiuni de avertizare și de corecție, precum și acțiuni de adaptare și de perfecționare a produsului software. Scopul procesului de mentenanță constă în menținerea capacității sistemului software de a presta servicii, precum și în modificarea produsului software, păstrând 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 intermediului unei *platforme Service Desk (ticketing) gestionată și deținută de Furnizor*;
 - Identificarea, investigarea, analiza și soluționarea 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 algoritmilor 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 și 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 performanțelor 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 configurației sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanță 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 intra 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 corectă a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidențialității și 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 cerințelor de securitate informațională de către utilizatori, să documenteze și să raporteze cazurile și tentativele de încălcare a acestora, să întreprindă

măsurile necesare pentru prevenirea, limitarea și lichidarea consecințelor 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 securității 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 și mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum și 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 intră 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 funcționării 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 intră 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 să 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 să 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 și corectivă a DRG

Activități în contextul adaptării și corecției software

În categoria serviciilor de mentenanță adaptivă și corectivă a DRG intră acele servicii necesare pentru adaptarea și corecția 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 perioadă 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 să 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 acordă 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 (actualizarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.

➤ Ofertanții trebuie să demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport și 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 și 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 și corectivă

Solicitarea serviciilor de mentenanță adaptivă și 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 și corectivă

Prestarea serviciilor de mentenanță adaptivă și 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 condițiile inițiale ale solicitării (formularea problemei și 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 și acceptate, și a standardelor agreeate de Beneficiar, ținând cont și de ultimele cerințe în materie de elaborare, și calculate în baza tarifelor convenite de părți.
- 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"

Supportul operațional 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 și consultanței în vederea soluționării defectelor legate de utilizarea sistemului;
- pentru solicitarea realizării anumitor activități și acțiuni 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 și Beneficiarului, pentru a gestiona orice aspect ivit în relațiile dintre aceștia.

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 soluționării incidentelor și problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor și actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul și Beneficiarul vor conlucra strâns în vederea prevenirii incidentelor și în vederea soluționării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul și prioritatea acordată pentru soluționarea unui incident va ține cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecințele acestuia asupra disponibilității și performanței softului aplicativ. Urgența incidentului caracterizează operativitatea cu care acesta trebuie soluționat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare și soluționare a incidentelor va fi în funcție de impactul și urgența incidentului. Algoritmul aplicat pentru stabilirea priorității unui incident este definit în continuare.

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

PRIORITATE		Impact		
		Înalt	Mediu	Jos
Urgență	Înalt	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenței incidentului

URGENȚĂ	Descriere
Înaltă	Un incident este estimat ca având nivelul urgenței „Înalt” în una sau mai multe din următoarele cazuri:

	<ul style="list-style-type: none"> - pagubele provocate de incident cresc extrem de rapid; - există activități și operațiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea imediată poate preveni riscuri legale majore și de securitate (protecție) a informației.
Medie	<p>Un incident este estimat ca avînd nivelul urgenței „Mediu” în una sau mai multe din următoarele cazuri:</p> <ul style="list-style-type: none"> -pagubele provocate de incident cresc considerabil în timp; -există activități și operațiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; -reacția operativă poate preveni riscuri legale moderate și de securitate a informației.
Joasă	<p>Un incident este estimat ca avînd nivelul urgenței „Jos” în una sau mai multe din următoarele cazuri:</p> <ul style="list-style-type: none"> - pagubele provocate de incident cresc relativ puțin în timp; - activitățile și operațiunile afectate nu trebuie continuate imediat; - nu există riscuri legale și de securitate a informației semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere
Înalt	<p>Un incident este estimat ca avînd nivelul impactului „Înalt” în una sau mai multe din următoarele cazuri:</p> <ul style="list-style-type: none"> - activitățile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizației Beneficiarului și afectează utilizatori externi, reputația și imaginea Beneficiarului; - există riscuri legale și financiare majore pentru Beneficiar;
Mediu	<p>Un incident este estimat ca avînd nivelul impactului „Major” în una sau mai multe din următoarele cazuri:</p> <ul style="list-style-type: none"> - activitățile importante ale Beneficiarului sunt întrerupte sau activitățile cheie sunt desfășurate cu dificultate; - incidentul a afectat utilizatori interni și un număr nesemnificativ de utilizatori externi; - există riscuri legale și financiare semnificative pentru Beneficiar;
Jos	<p>Un incident este estimat ca avînd nivelul impactului „Jos” în una sau mai multe din următoarele cazuri:</p> <ul style="list-style-type: none"> - activitățile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activitățile importante sunt desfășurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea și 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 și reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergențe apărute între Părți vor fi soluționate cu efort comun și prin strânsă conlucrare între Părți. În acest scop, vor fi aplicate următoarele reguli:

➤ Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv experți independenți.

➤ La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.

➤ Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite.

➤ Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informației

Prestatorul este responsabil pentru securitatea tehnologică și funcțională a softului aplicativ în limitele sarcinilor de mentenanță îndeplinite.

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

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

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

➤ Colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea;

➤ Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiții ce asigură integritatea copiilor de rezervă efectuate;

➤ Menținerea formalizată a Registrului privind deținerea probelor conservate (chain of custody).

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

Livrabile

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

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).

**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
----------------------------	------------------

<p>Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP:</p> <ul style="list-style-type: none"> • Servicii de mentenanță preventivă și Suport – în bază de abonament; • Servicii de mentenanță corectivă și adaptivă – la cerere. 	<p>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.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 SIP, 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 performanță precum și serviciilor paraclinice în cadrul AMP și AMSA 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 performanță, 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 utilizat la evidența serviciilor de înaltă performanță 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.

Setul de date utilizat la evidența serviciilor paraclinice cuprinde:

- Data și ora prestării;
- Nume și prenume pacient;
- IDNP al pacientului;
- Vârsta calculată automat la data prestării;
- Denumirea instituției medicale și codul IDNO a prestatorului;
- Serviciu medical (Denumire completă și cod unic);
- Locație / filială (Adresa instituției medicale);
- Tarif reglementat (Valoarea serviciului conform HG 1020/2011);
- Tarif real (Valoarea serviciului prestat);
- Numele persoanei care a introdus serviciul în sistem.

Beneficiarii ai SIRSM sunt CNAM, pacientul asigurat, 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;
- 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 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 și 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 dată pentru a accesa toate modulele aplicației;
- Poate fi accesat de pe telefon, PC, notebook, etc.

Interfața Utilizator

Această interfață este accesibilă pentru toți utilizatorii autorizați în SIP:

- ✓ SIP dispune de o interfață inteligentă, intuitivă 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 redundante 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;
 - 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);
 - asigură 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 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 și 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 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 (înscrisoare, 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 între stații 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 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 și 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. Măsurile de securitate ajută 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 din care fac parte utilizatorii.
- **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 competență. 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;
 - 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 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 arhitecturală este în figura următoare:

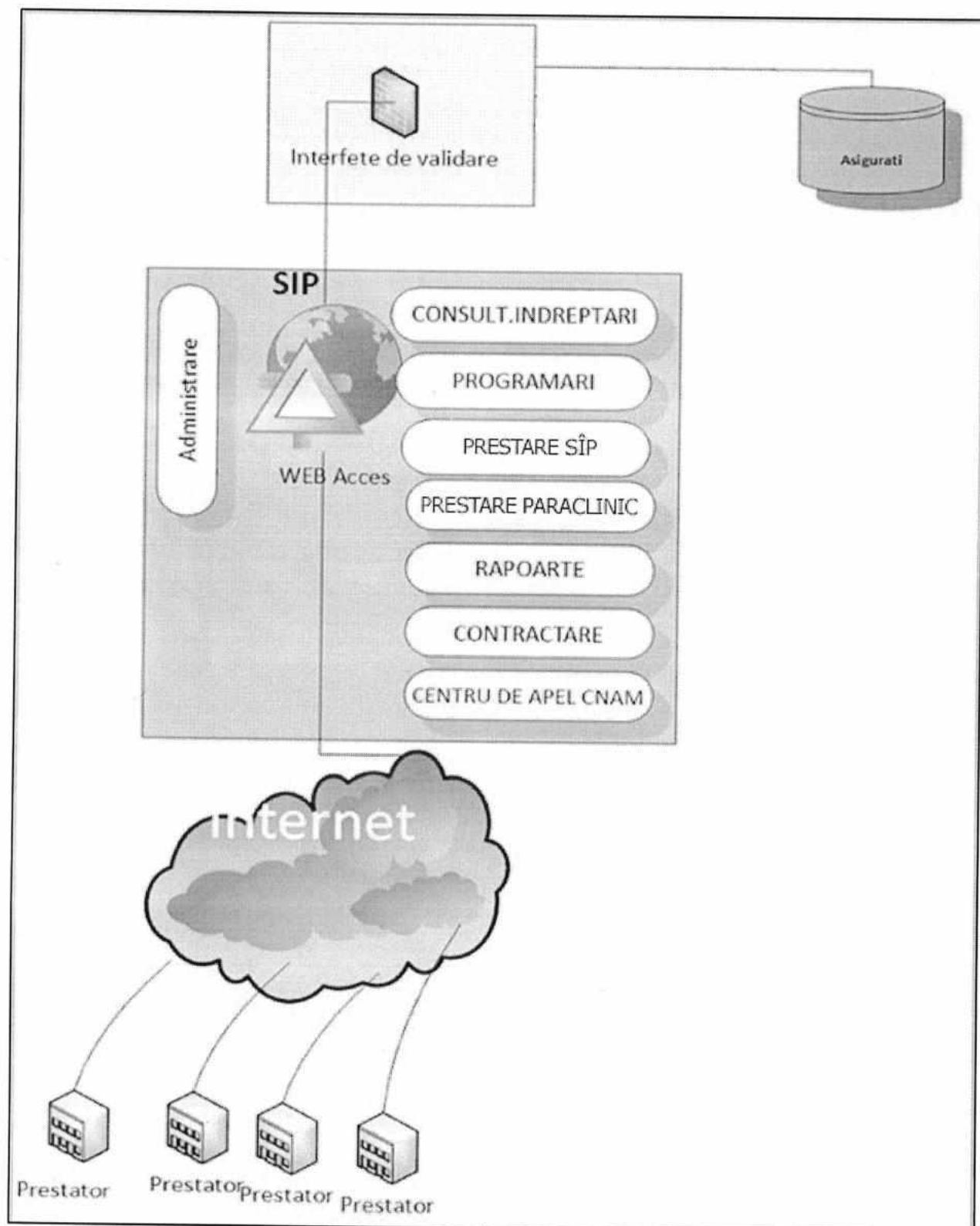


Figura 1. Schema arhitecturală SIP

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 prestare a serviciilor paraclinice;
- ✓ Modulul rapoarte;
- ✓ Modulul contractare;
- ✓ Interfețe.

Modulul de administrare roluri

Actorii implicați în circuitul informațional sunt:

- Pacient asigurat;
- Administrator CNAM (administrare SIRSM);
- CNAM (responsabil CNAM);
- Medic prescriptor (medic de familie sau medic specialist);
- Prestator servicii de înaltă performanță;
- Prestator paraclinic.

Administrarea sistemului informatic este realizată de către administratorul (reprezentantul) CNAM pentru partea de conținut a serviciilor medicale.

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 rapidă de prescriere, validare și programare servicii medicale a pacientului, după modelul descris în continuare.

Prestatorul de servicii de înaltă performanță

În interfața de utilizare a sistemului, prestatorul de servicii de înaltă performanță are acces la modulele operaționale în conformitate cu informațiile completate de către administratorul sistemului, în directă 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 următoarele 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 să 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 corespondență 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 conform Anexei nr.4 și Anexei nr. 5 din Normele metodologice de aplicare a PU (nr.de ordine, denumire serviciu, cod serviciu tarif serviciu) în dependență de modificările operate;
- 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).

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 mentenanță elaborat de Prestator și aprobat de Beneficiar.

De menționat că prin procesul de mentenanță se controlează funcționarea produsului software, se înregistrează problemele pentru analiză, se întreprind acțiuni de avertizare și de corecție, precum și

acțiuni de adaptare și de perfecționare a produsului software. Scopul procesului de mentenanță constă în menținerea capacității sistemului software de a presta servicii, precum și în modificarea produsului software, păstrând 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 intermediului unei *platforme Service Desk (ticketing) gestionate și oferite de Furnizor*;
 - Identificarea, investigarea, analiza și soluționarea 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 intră 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 performanțelor 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 măsurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- 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 intră 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 corectă a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidențialității și 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 cerințelor de securitate informațională de către utilizatori, să documenteze și să raporteze cazurile și tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea și lichidarea consecințelor 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 securității 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, generarea copii de rezervă ale SIP și mijloacelor software folosite pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum și 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 intră 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 funcționării 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 intră 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 să 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 sursă al aplicației.

Orice modificare asupra codului sursă are ca efect o nouă 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 toată 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;

Cerințe de mentenanță adaptivă și corectivă a SIP (la cerere)

Asumarea contextului adaptării și corecției software

În categoria serviciilor de mentenanță adaptivă și corectivă a SIP intră acele servicii necesare pentru adaptarea și corecția 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 perioadă 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 să 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 (actualizarea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.

➤ Ofertanții trebuie să demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport și 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 că, 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.

➤ Prestatorul va asigura un sistem de tip Service Desk/ticketing (sistem propriu sau agreat cu CNAM) pentru gestiunea cererilor de suport și a solicitărilor de mentenanță adaptivă/corectivă, prin care vor fi înregistrate toate intervențiile, inclusiv timpul alocat fiecărui ticket, cu permiterea accesului CNAM la sistem (pentru monitorizare, aprobare și raportare), respectând condiții stricte de confidențialitate și securitate a datelor.

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, ajustarea modulelor paraclinică și 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 prestarea a serviciilor de mentenanță adaptivă și 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 și corectivă

Solicitarea serviciilor de mentenanță adaptivă și 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 și corectivă

Prestarea serviciilor de mentenanță adaptivă și 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 tarificare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei și 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 și acceptate, și a standardelor agreeate de Beneficiar, ținând cont și de ultimele cerințe în materie de elaborare, și calculate în baza tarifelor convenite de părți.
- 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

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 operațional 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 și consultanței în vederea soluționării defectelor legate de utilizarea sistemului;
- pentru solicitarea realizării anumitor activități și acțiuni 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 și Beneficiarului, pentru a gestiona orice aspect ivit în relațiile dintre aceștia.

Reguli față de procesul de aplicare a modificărilor

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a căroră 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 soluționării incidentelor și problemelor de utilizare a softului aplicativ prin: analiza defectelor, introducerea corectărilor, documentarea corectărilor și actualizarea documentelor pentru softul aplicativ.

Clasificarea incidentelor

Prestatorul și Beneficiarul vor conlucra strâns în vederea prevenirii incidentelor și în vederea soluționării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul și prioritatea acordată pentru soluționarea unui incident va ține cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecințele acestuia asupra disponibilității și performanței softului aplicativ. Urgența incidentului caracterizează operativitatea cu care acesta trebuie soluționat pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare și soluționare a incidentelor va fi în funcție de impactul și urgența incidentului. Algoritmul aplicat pentru stabilirea priorității unui incident este definit în continuare.

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

PRIORITATE		Impact		
		Înalt	Mediu	Jos
Urgență	Înalt	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenței incidentului

URGENȚĂ	Descriere
Înaltă	Un incident este estimat ca avînd nivelul urgenței „Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activități și operațiuni critice pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea imediată poate preveni riscuri legale majore și de securitate (protecție) a informației.
Medie	Un incident este estimat ca avînd nivelul urgenței „Mediu” în una sau mai multe din următoarele cazuri: -pagubele provocate de incident cresc considerabil în timp; -există activități și operațiuni importante pentru business procesele Beneficiarului ce trebuie să fie efectuate imediat;

	-reacția operativă poate preveni riscuri legale moderate și de securitate a informației.
Joasă	Un incident este estimat ca avînd nivelul urgenței „Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puțin în timp; - activitățile și operațiunile afectate nu trebuie continuate imediat; - nu există riscuri legale și de securitate a informației 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: - activitățile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizației Beneficiarului și afectează utilizatori externi, reputația și imaginea Beneficiarului; - există riscuri legale și financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca avînd nivelul impactului „Major” în una sau mai multe din următoarele cazuri: - activitățile importante ale Beneficiarului sunt întrerupte sau activitățile cheie sunt desfășurate cu dificultate; - incidentul a afectat utilizatori interni și un număr nesemnificativ de utilizatori externi; - există riscuri legale și financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca avînd nivelul impactului „Jos” în una sau mai multe din următoarele cazuri: - activitățile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activitățile importante sunt desfășurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea și 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 și reguli privind prestarea serviciilor

Soluționarea divergențelor

Orice divergențe apărute între Părți vor fi soluționate cu efort comun și prin strânsă conlucrare între Părți. În acest scop, vor fi aplicate următoarele reguli:

➤ Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv experți independenți.

➤ La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.

➤ Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite.

➤ Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informației

Prestatorul este responsabil pentru securitatea tehnologică și funcțională a softului aplicativ în limitele sarcinilor de mentenanță îndeplinite.

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

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

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

➤ Colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea;

➤ Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiții ce asigură integritatea copiilor de rezervă efectuate;

➤ Menținerea formalizată a Registrului privind deținerea probelor conservate (chain of custody).

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

Livrabile

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

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

Lunar, odată cu actul de primire-predare serviciilor se va expedia Beneficiarului ultima versiune a codului sursă (compilabil).

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 finalizate în domeniul TIC sau domenii conexe.
- 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 domeniul managementului proiectelor TIC.
- Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru 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).

Business Analist (minim 1 persoană)

- Studii superioare finalizate în domeniul TIC sau domenii conexe.
- Deținerea certificatului și/sau documentului analogic, ce confirmă dobândirea cunoștințelor în modelarea business-proceselor a conținutului sistemelor IT.
- Minim 3 ani de experiență în domeniul analizei de business și modelarea proceselor pentru proiecte TIC.
- Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru 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 finalizate în domeniul TIC sau domenii conexe.
- 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 dobândită prin participarea, în calitate de consultant, auditor, expert sau în alte roluri similare, în analiza vulnerabilităților și interpretarea rezultatelor obținute în urma proceselor de testare a securității.
- Minim 3 ani de experiență în domeniul securității informaționale pentru proiecte TIC.
- Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru 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 infrastructură sistem (minim 1 persoană)

- Studii superioare finalizate în domeniul TIC sau domenii conexe.
- Cunoașterea limbii de stat;
- Minim 3 ani de experiență în domeniul de specialitate.
- 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 front-end (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Certificate ce confirmă nivelul de pregătire în domeniul de specializare (dacă deține);
- Cunoaște limba de stat;
- Are experiență de minim 3 ani în domeniul TIC, dezvoltare software;
- Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru domeniul medical;
- Cunoaște și are experiență în tehnologiile și componentele back-end și front-end ale sistemului informațional descrise în prezentul caiet de sarcini, precum și alte tehnologii înrudite;
(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 back-end (minim 1 persoană)

- Studii superioare finalizate cu diplomă de licență în domeniul TIC sau domenii conexe;
- Certificate ce confirmă nivelul de pregătire în domeniul de specializare (dacă deține);
- Cunoaște limba de stat;
- Are experiență de minim 3 ani în domeniul TIC, dezvoltare software;
- Cunoaște și are experiență în tehnologiile și componentele back-end și front-end ale sistemului informațional descrise în prezentul caiet de sarcini, precum și alte tehnologii înrudite;
- Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru 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 baze de date (minim 1 persoană)

- Studii superioare finalizate în domeniul TIC sau domenii conexe.
- Cunoașterea limbii de stat;
- Are experiență de minim 3 ani în domeniul TIC, baze de date;

– Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru 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).

Software Tester (minim 1 persoană)

– Studii superioare finalizate în domeniul TIC sau domenii conexe;
– Experiență demonstrată în testarea funcțională a sistemelor informaționale;
– Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale;
– Experiență în 1-2 proiecte relevante pentru sisteme integrate sau pentru 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).

RECHIZITELE JURIDICE, POȘTALE ȘI DE PLĂȚI ALE PĂRȚILOR

Prestatorul

Adresa poștală: mun. Chișinău, str. Lev Tolstoi, 74, ap. 78

Telefon: 069393169

Cod fiscal: 1019600011052

Banca: B.C. Victoriabank S.A. suc. 14 Chișinău

Cod: VICBMD2X446

Cod TVA: 0210173

IBAN: MD33VI022241400000287MDL

Beneficiarul

Adresa poștală: mun. Chișinău, bd. Vlaicu Pîrcălab, 46

Telefon/fax: 022 780-295, 022 780-240

IBAN: MD58TRPEAD518720A01857AA

Banca: Ministerul Finanțelor – Trezoreria de Stat

Cod: TREZMD2X

Cod fiscal: 1007601007778

Adresa poștală: mun. Chișinău, bd. Vlaicu Pîrcălab, 46

SEMNĂTURILE PĂRȚILOR

Prestatorul
Administrator
Atanasie BUTUCEA



Beneficiarul
Director general
Ion DODON



SPECIFICAȚII TEHNICE

Denumirea serviciilor	Țara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6
Lotul 1 - Servicii de mentenanță și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG					
Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – în bază de abonament	MD	Das Soft Plus SRL	Conform Caietului de sarcini inclus la Capitolul II Condiții speciale ale Contractului	Conform Caietului de sarcini inclus la 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) – la cerere	MD	Das Soft Plus SRL	Conform Caietului de sarcini inclus la Capitolul II Condiții speciale ale Contractului	Conform Caietului de sarcini inclus la Capitolul II Condiții speciale ale Contractului	Moldova Standard
Lotul 2 - Servicii de mentenanță și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta SIP					
Servicii de mentenanță preventivă și suport a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – în bază de abonament.	MD	Das Soft Plus SRL	Conform Caietului de sarcini inclus la Capitolul II Condiții speciale ale Contractului	Conform Caietului de sarcini inclus la 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) – la cerere	MD	Das Soft Plus SRL	Conform Caietului de sarcini inclus la Capitolul II Condiții speciale ale Contractului	Conform Caietului de sarcini inclus la Capitolul II Condiții speciale ale Contractului	Moldova Standard



Prestatorul
Administrator
Afanasie BUTUCEA

SEMNĂTURILE PĂRȚILOR



Beneficiarul
Director general
Ion DODON

Anexa nr. 2
la contractul nr. 33/CP
din "31" 12 2025

SPECIFICAȚII DE PREȚ

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 - Servicii de mentenanță și suport 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	61 850,25	74 220,30	742 203,00	890 643,60	01.01.2026- 31.12.2026	MD58TRPEAD518720 A01857AA
72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta DRG) – la cerere	Om/ore	900	210,38	252,456	189 342,00	227 210,40	01.01.2026- 31.12.2026	MD58TRPEAD518720 A01857AA
Lotul 2 - Servicii de mentenanță și suport 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	61 850,25	74 220,30	742 203,00	890 643,60	01.01.2026- 31.12.2026	MD58TRPEAD518720 A01857AA

72200000-7	Servicii de mentenanță corectivă și adaptivă a Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, (componenta SIP) – la cerere	Om/ore	900	210,38	252,456	189 342,00	227 210,40	01.01.2026-31.12.2026	MD58TRPEAD518720 A01857AA	
Suuma totală, fără TVA							1 863 090.00			
Suma totală, inclusiv TVA							2 235 708.00			

SEMĂTURILE PĂRȚILOR

**Prestatorul
Administrator
Afanasie BUTUCEA**



**Beneficiarul
Director general
Ion DODON**



Anexa nr. 3
la contractul nr. 33/CP
din "31" 12 2025

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 _____
Semnătura, F.N.P.

Beneficiarul _____
Semnătura, F.N.P.

Contrasemnat:

" _____ " _____ 202__
Semnătura F.N.P. și funcția persoanei care
a recepționat bunuri

SEMNĂTURILE PĂRȚILOR



**Prestatorul
Administrator
Afanasie BUTUCEA**

**Beneficiarul
Director general
Ion DODON**

