ANUNȚ DE PARTICIPARE

privind achiziționarea serviciilor de mentenanță și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG și SIP

prin procedura de achiziție *Licitație deschisă*

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

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

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

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

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

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

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

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

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

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

Nr. d/o	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1.	Vor fi excluși operatorii economici care nu şi-au îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în ţara în care este stabilit.	Certificat de efectuare regulată a plăţii impozitelor, contribuţiilor (valabil la data deschiderii ofertei) - eliberat de Inspectoratul Fiscal Principal de Stat, confirmat prin semnătura electronică, ori link-ul la accesarea unei baze de date naționale disponibile gratuit	***Obligatoriu***

		pentru autoritatea contractantă care deține informațiile privind lipsa/existența restanțelor. confirmată prin aplicarea semnăturii electronice a participantului	
2.	Declaraţii privind cifra de afaceri în domeniul de activitate aferent obiectului contractului (prestarea serviciilor similare) într-o perioadă anterioară care vizează activitatea pentru ultimii 3 ani - a cîte min 1 000 000,00 lei pentru fiecare din ultimii 3 ani original confirmat prin semnătura electronică a participantului: (la solicitare se va prezenta documente primare de confirmare copiile contractelor, raport financiar etc.)	Declarație privind lista principalelor prestări de serviciul efectuate în ultimii 3 ani de activitate similare obiectului de achiziție conform ***Anexei nr. 12*** din Ordinul MF 115/2021 - confirmată prin semnătura electronică	***Obligatoriu***
3.	Demonstrarea accesului la personalul necesar pentru îndeplinirea corespunzătoare a obiectului contractului ce urmează a fi atribuit	Conform Caietului de sarcini (Anexa nr. 1 / Anexa nr.2)	***Obligatoriu***
4.	Declarație de garanție	Autoritatea Contractantă solicită o garanție a aplicației acordată de către ofertanți pentru o perioada de 12 luni de la încetarea contractului. Confirmată prin aplicarea semnăturii electronice a persoanei responsabile a ofertantului. Pe perioada desfășurării contractului, codul sursă al aplicației va fi supus modificărilor efectuate de către specialiștii prestatorului. Orice modificare în codul sursă are ca efect o nouă versiune a aplicației care este supusă garanției contractuale a ofertantului în baza cerințelor minime și obligatorii ale Caietului de Sarcini.	***Obligatoriu***
5.	Va fi exclus din procedura de atribuire a contractului de achiziţii publice orice ofertant sau candidat despre care are cunoştinţă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanţe judecătoreşti, pentru participare la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, pentru fraudă şi/sau pentru spălare de bani, pentru infracţiuni de terorism sau infracţiuni legate de activităţi teroriste, finanţarea terorismului, exploatarea prin muncă a copiilor şi alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	***Obligatoriu*** *Lipsa condamnării pe parcursul a ultimilor 5 ani.*
6.	Va fi exclus orice operator economic care se află în proces de insolvabilitate ca urmare a hotărârii judecătoreşti.	La depunerea ofertei prin declararea în DUAE	***Obligatoriu*** *Nu se află în proces de insolvabilitate*
7.	Garanția pentru ofertă în **valoare de 1%**	**Garanţia pentru ofertă emisă de către o bancă comercială *sau* prin transfer la contul autorității contractante, conform următoarelor date bancare:** Beneficiarul plății: **Compania Națională de Asigurări în Medicină** Denumirea Băncii: **Ministerul Finanțelor –**	***Obligatoriu***

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

Anexa nr.1

CAIET DE SARCINI

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **DRG**

Obiectul achiziției

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

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

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

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

Descriere generală a DRG

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

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

Funcționarea continuă și operarea în sistemul DRG are următoarele obiective:

A. Creșterea eficienței serviciilor spitalicești

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

B. Creșterea eficienței tehnice la nivelul furnizorului de serviciilor spitalicești

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

Specificații tehnice DRG

Caracteristici generale de funcționare

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

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

Interfața Utilizator

Această interfață este accesibilă pentru toți utilizatorii autorizați în DRG:

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

Hardware și canale de comunicație

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

- **Platforma hardware**, formata din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat pe platforma guvernamentală comună MCloud:

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

- **Platforma software.** Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici:

    - Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise;
    - Sistemul de gestiune al bazelor de date este marca aceluiași producător ca și sistemul de operare, respectiv Microsoft SQL Server 2017, vers. 14.
    - Pe stațiile utilizatorilor există în mod implicit .NET Framework 3.5 SP1 sau mai nou și navigator web implicit al producătorului sistemului de operare sau browser web modern.

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare și transportare a datelor

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

Sistemul de securitate

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

Caracteristici:

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

- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor;

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

Sistemul are următoarele nivele de securitate care asigură confidențialitatea datelor:

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

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

În sistem există următoarele tipuri majore de utilizatori:

- nivelul **Operator**: permite introducerea și modificarea datelor specifice activității sale;

- nivelul **Administrator**: permite arhivarea datelor, verificarea datelor, elaborarea rapoartelor, asigurarea securității informaționale și alte configurări.

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

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

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

Retenția datelor, acces securizat și audit

- **Retenția datelor și controlul versiunilor.** Sistemul permite stocarea informațiilor medicale (consultații, fișe medicale și bilete de trimitere) în conformitate cu cerințele legale cu toate versiunile acestora prin operații programabile de backup.
- **Securitate.** Pentru asigurarea securității, toate accesările sistemului respectă regulile de control a accesului în vederea protejării vieții private. Masurile de securitate ajuta la

prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.

- **Autentificare.** Toți utilizatorii care accesează sistemul sunt supuși procesului de autentificare.
- **Autorizare la funcționalități.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem și pe baza permisiunilor asociate rolului sau rolurilor atribuite utilizatorilor.
- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului sau rolurilor din care face parte utilizatorul doar pe domeniul sau de competenta. Spre exemplu, un medic are acces doar la fișele electronice ale pacienților săi.
- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai târziu că a efectuat o operațiune. Nerepudierea este implementată prin următoarele mecanisme:
  - unicitatea utilizatorilor în sistem;
  - jurnalizarea tuturor operațiunilor efectuate de sistem;
  - mecanism de control al versiunilor pentru înregistrările medicale.
- **Securitatea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit.** Toate operațiunile efectuate de utilizatori sau de către alte sisteme care accesează sistemul păstrează o înregistrare în componența auditului. Astfel, este permisă investigarea incidentelor de către un administrator.

Arhitectura DRG

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

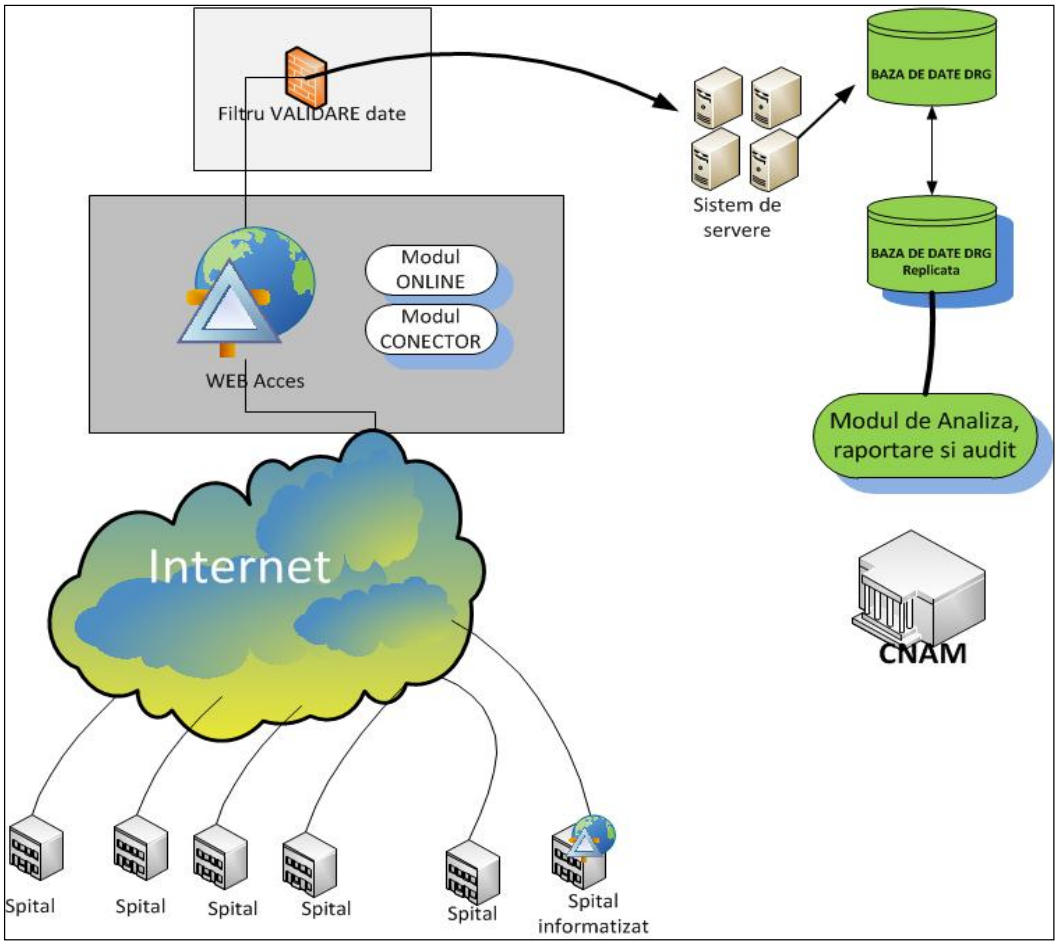


Figura 1. Schema arhitecturală DRG

Componentele DRG sunt operaționale și sunt prezente conform modulelor:

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

Modulul de administrare sistem colector

În cadrul acestui modul se execută:

- ➢ **Managementul utilizatorilor** (creare, ștergere, modificare date utilizatori). Fiecare instituție care execută raportare în DRG are desemnat cel puțin un utilizator al sistemului care transmite raportările; modalitatea de alocare a acestei resurse umane este răspunderea instituției.

- **Administrarea sistemului.** Administratorii sistemului pot efectua setări la nivelul celorlalte module și pot verifica funcționarea corectă a fiecărui modul. Nivelul de acces al administratorilor este corespunzător cerințelor de care aceștia răspund:
  - administratorii pot modifica informațiile de referință ale operatorilor sistemului (nume, prenume, locație, instituție, etc.);
  - administratorii pot modifica intervalele temporare în care transmiterea raportărilor este permisă;
  - administratorii pot vizualiza informații existente în modulul de nerepudiere (fișierele care conțin informațiile raportate trec prin modulul de nerepudiere);
  - administratorii pot vizualiza informațiile existente în modulul de înregistrare și să confirme funcționarea normală a acestuia;
  - administratorii pot vizualiza existenta rapoartelor transmise și stadiul în care se afla acestea față de modulul de validare;
  - administratorii pot face modificări asupra Modulului de Notificare și Raportare.
  - administratorii pot verifica transmiterea corectă a rapoartelor către Modulul Warehouse, unde sunt depozitate informațiile în vederea prelucrării.

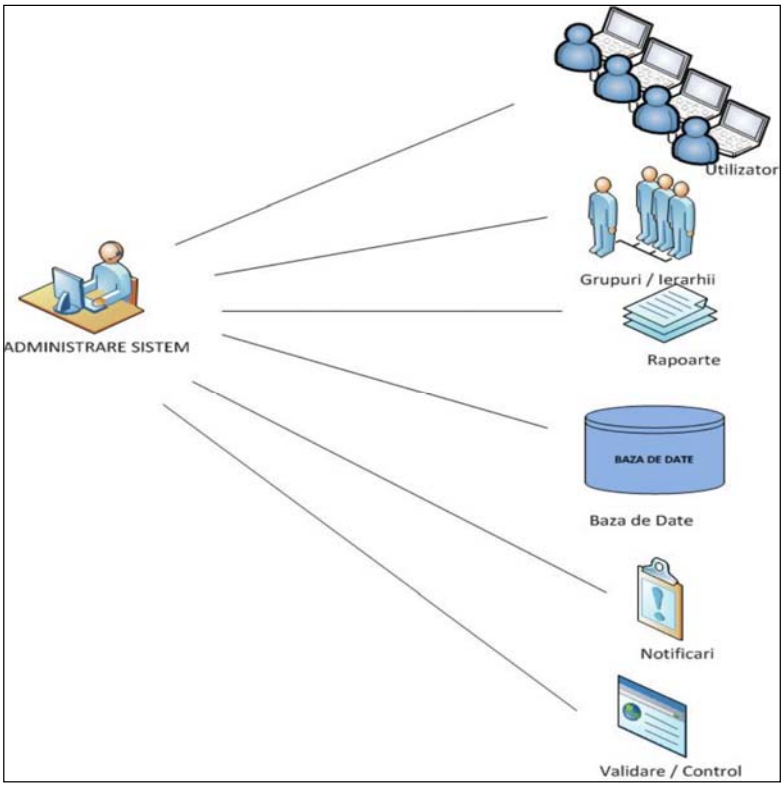


Figura 2. Schema Modulul de administrare sistem colector

Nivelul de acces al acestui modul:

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

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

Administratorii sistemului au rolul de a verifica fluxul normal al prelucrării datelor de către sistem și de a ajusta situațiile de excepție atunci când este cazul. Prin situații de excepție se înțeleg

acele cazuri în care sistemul răspunde corect din punct de vedere al fluxului, dar cerințele unui utilizator sunt diferite și justificate.

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

Modulul de colectare date Real Time

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

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

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

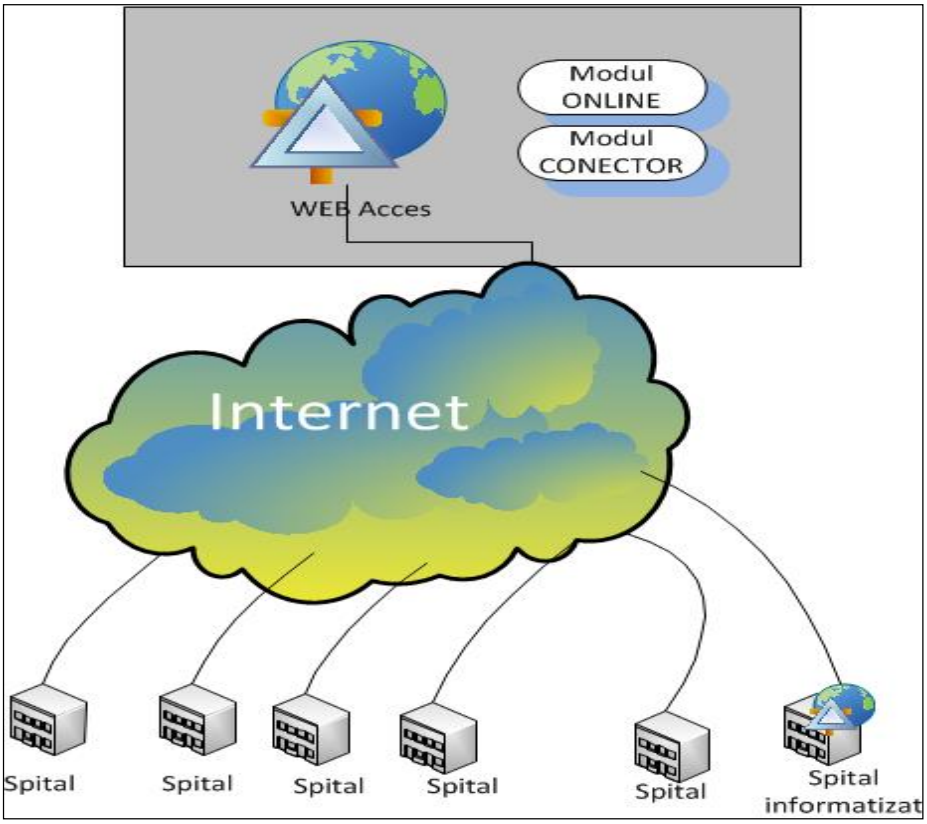


Figura 4. Modulul de colectare date Real Time

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

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

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

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

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

Modulul de nerepudiere

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

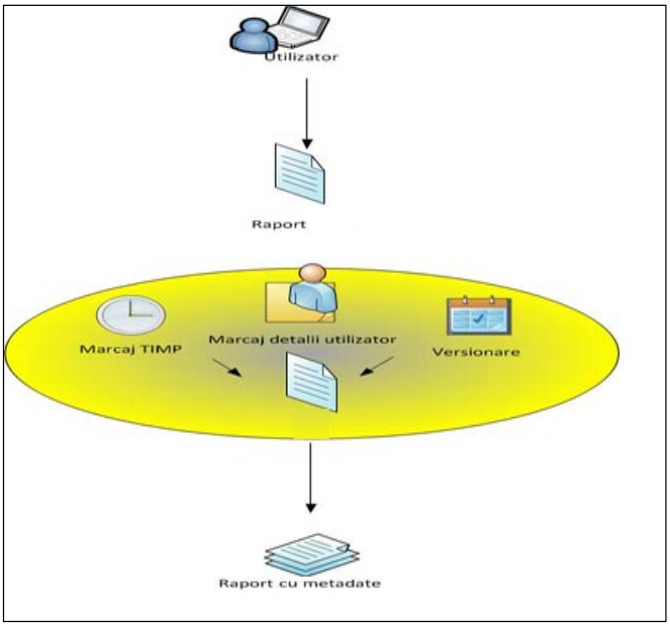


Figura 5. Modulul de nerepudiere

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

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

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

Modulul de validare

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

- ➢ Modulul de validare operează în mod minimal fișierele transmise (setul minim de date la nivel de pacient) și le acceptă doar pe cele care se încadrează în formatul dorit de către CNAM;

- ➢ Modulul de validare verifică, de asemenea, existența metadatelor de corespondența între utilizator și fișier înainte de trecerea în sistem a fișierelor al căror conținut îl constituie rapoartele. În cazul în care apar neconcordanțe între ceea ce așteaptă sistemul și ceea ce livrează utilizatorii, se trimit alerte către „Modulul de notificare, raportare și audit” care prelucrează situațiile în mod corespunzător, în sensul aducerii la forma standard a raportărilor.

- ➢ Modulul de validare este ultima componentă a sistemului care decide automat dacă un raport este valid sau nu; atenția acordată acestui modul este ridicată iar analiza situațiilor neconforme și alinierea acestora sunt urmărite permanent.

- ➢ Modulul de validare are capacitatea de a trata cât mai multe situații comune și elimina la timp cât mai multe cazuri în care apare eroarea umană.

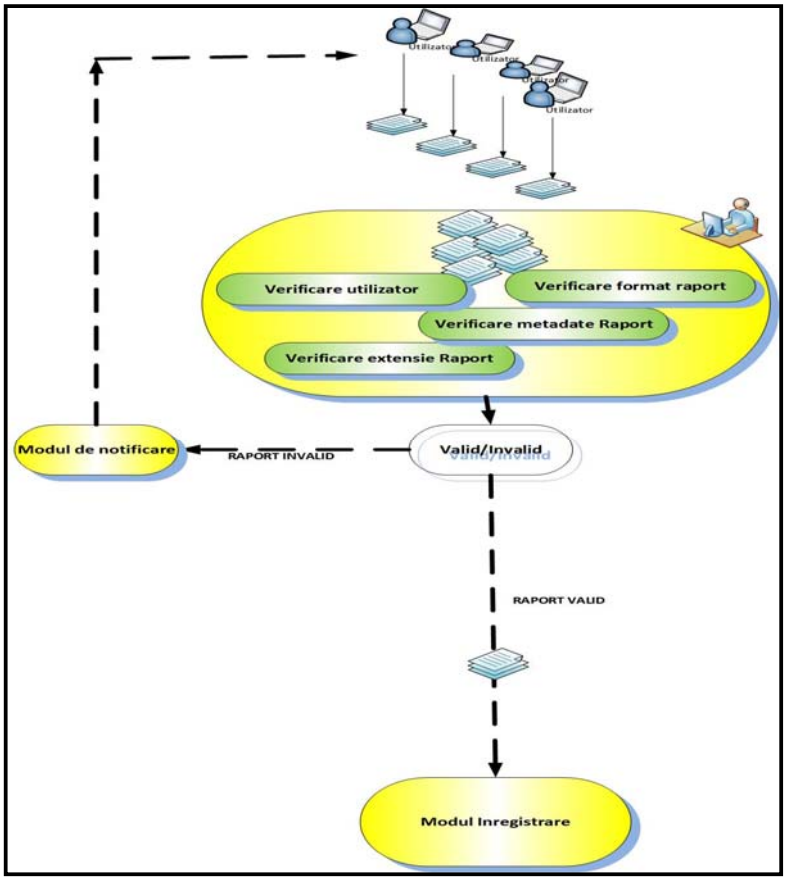


Figura 6. Schema Modulului de Validare

Modulul de înregistrare raportări

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

Modulul de înregistrare a raportări conține două componente:

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

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

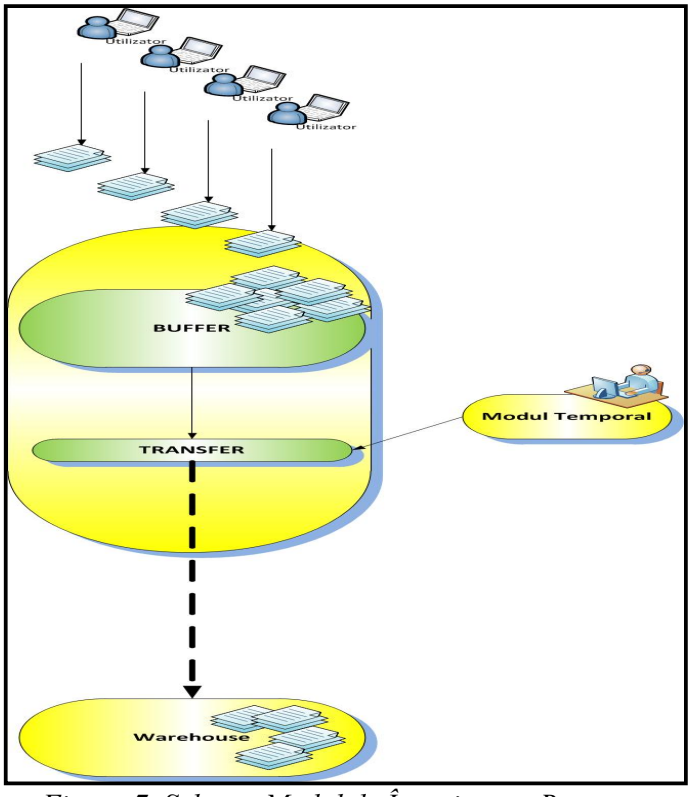


Figura 7. Schema Modul de Înregistrare Rapoarte

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

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

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

Modulul de setări, raportare și audit

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

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

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

✓ **Audit:** aceasta funcție a modulului identifică acțiunile desfășurate de către un utilizator, în mod cronologic; în cazul apariției unei probleme, la nivel de administrator de sistem, se poate vedea istoricul operațiilor desfășurate de orice utilizator în vederea identificării și corectării problemei. Sunt vizibile atât informațiile referitoare la logarile în sistem cât și cele referitoare la fișierele cu care utilizatorul a operat. Funcția de audit folosește în mod implicit modulul de nerepudiere care asigura

orice investigație ca datele existente în sistem sunt cele corecte și ca asocierea între conținutul informatic și activitatea umană este incontestabilă.

Modulul Depozit (Warehouse)

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

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

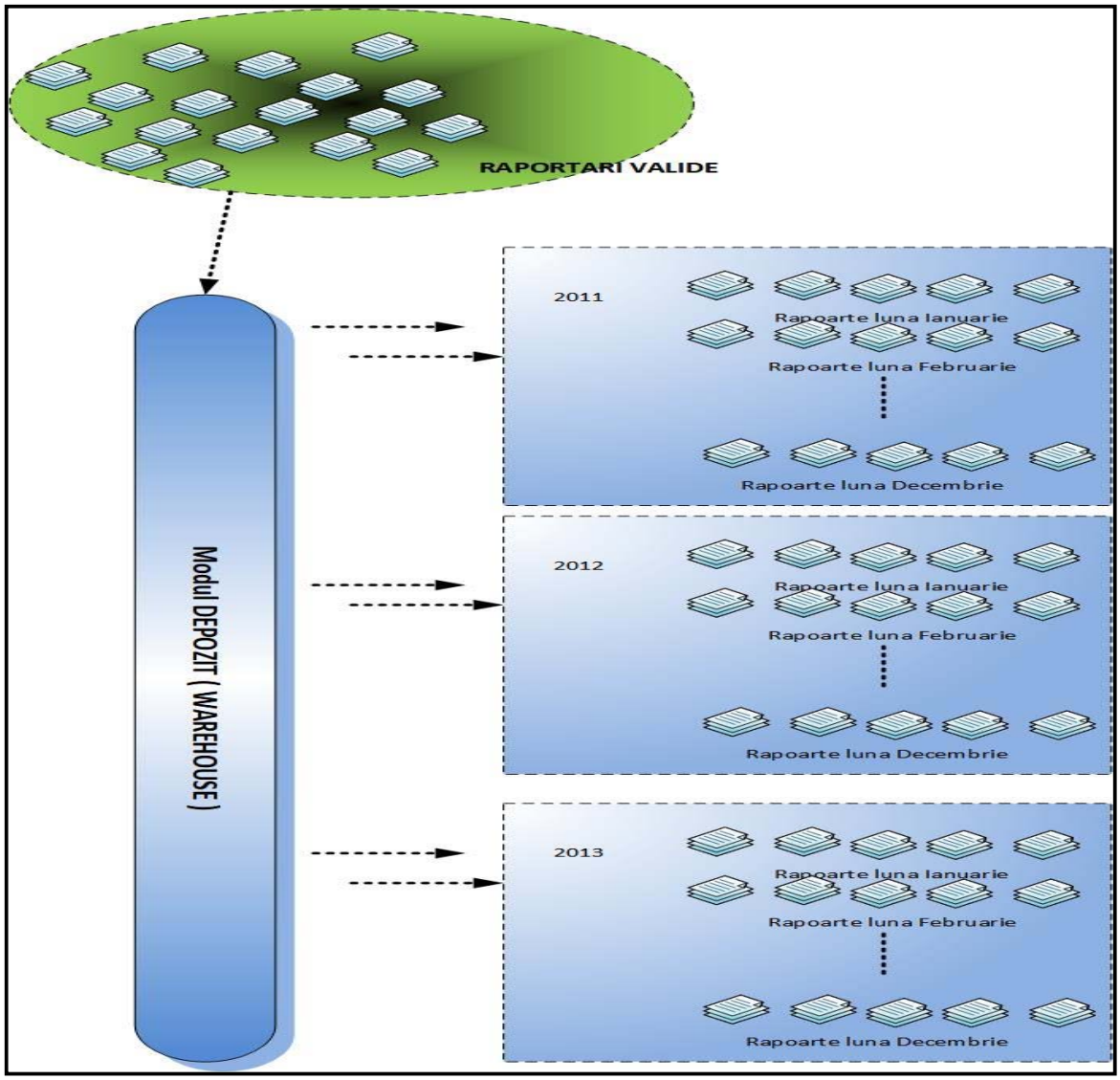


Figura 8. Schema Modul Depozit Rapoarte DRG (Warehouse)

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

Modulul de Analiză la nivel de Baza de Date

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

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

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

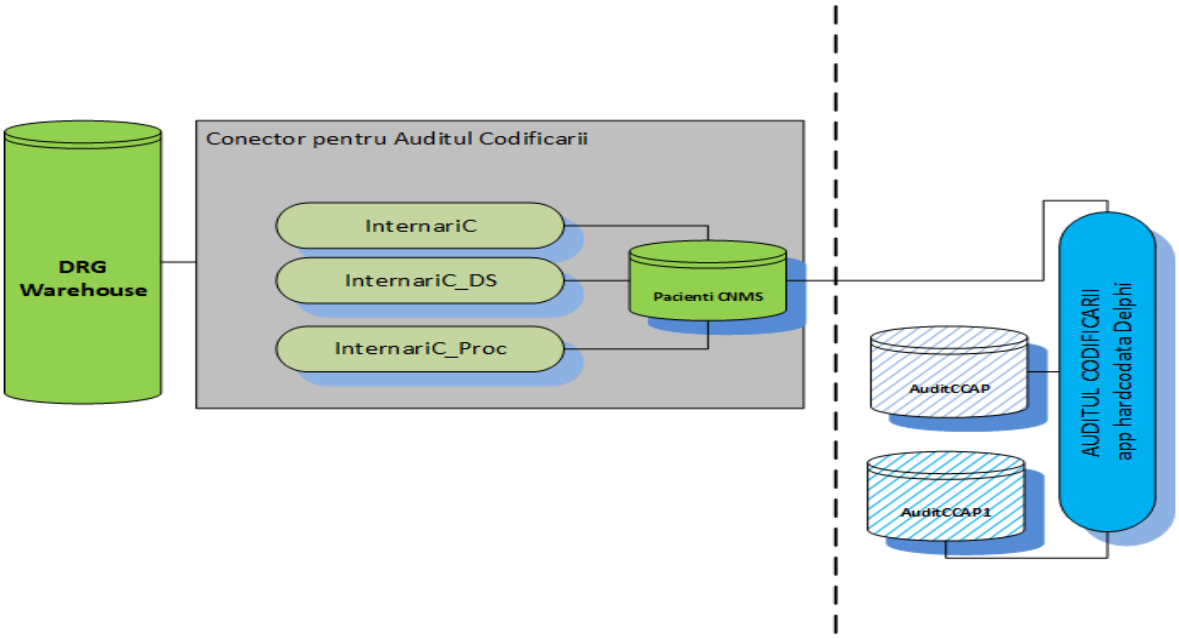
1) Evitarea fraudării. Sistemul SI DRG este un sistem operațional la nivel național, iar CNAM dispune de o baza de date unică, cu informații reale; veridicitatea informațiilor se verifica in doua feluri:

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

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

Modulul conector pentru Audit al codificării

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



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

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

- **Selectarea fișelor medicale a bolnavului spitalizat pentru audit (Database DRG).**

- **Importul fișelor medicale din "Database DRG" în aplicație şi efectuarea auditului.**

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

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

A. Cerințe de Mentenanță preventivă și Suport

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

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă

constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanță sistemului DRG, CNAM formulează următoarele cerințe:

- Analiza/diagnosticarea, izolarea și remedierea problemelor semnalate de către Beneficiar privind funcționalitățile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistența tehnică pentru probleme critice semnalate de către beneficiar privind funcționalitățile sistemului prin intermediul intermediul unei ***platforme Service Desk (ticketing) gestionată și deținută de Furnizor***;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcționare a sistemului;
- Identificarea și raportarea riscurilor potențiale;
- Actualizarea parametrilor existenți în partea utilizatorilor, conform cerințelor legislației în vigoare (spre exemplu: actualizarea/completarea nomenclatoarelor programelor special, diagnosticelor, procedurilor, spitalelor, rapoartelor, modificarea valorilor relative, aplicarea/anularea aplicării KP, completarea/modificarea algoritmelor de validare și excepțiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora, conform formatului solicitat și menținerea posibilităților de extragere a datelor de către utilizator.
- Depanarea erorilor, formarea raportului de analiză și a recomandărilor;
- Gestiunea jurnalului de incidente și raportare statistică privind incidentele;
- Actualizarea/modificarea după formă și conținut a rapoartelor existente;
- Menținerea funcționării serviciilor web aferente.

Suport Utilizatori

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

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

Suport platforma software

Servicii dedicate Sistemelor de Operare

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

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifestă transparent și înlăturarea cauzelor care le-au produs sau recomandarea măsurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;

- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- optimizarea configuratiei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanta și disponibilitate a sistemului;
- asigurarea funcționării continue a conectorilor;
- migrarea cazurilor medicale pe perioade definite de timp prin web-servicii pentru instituții medicale cu sisteme informatice proprii;
- mapare câmpuri, import cazuri medicale pe perioade definite de timp prin web-servicii instituții medicale cu sisteme informatice proprii.

Servicii dedicate sistemelor de gestiune a bazelor de date

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

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

Servicii dedicate componentelor, inclusiv a celor de interoperabilitate

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

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

Efectuarea testelor de penetrare

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

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

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

Operațiuni specifice DRG

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

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

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

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

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

Reguli de Validare

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

Întreținerea bazei de date a sistemului

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

Rapoarte CNAM

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

B. Cerințe de mentenanță adaptivă şi corectivă a DRG

Asumarea contextului adaptării şi corecţiei software

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

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

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

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

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

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

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

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

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

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

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

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

Prestarea serviciilor de mentenanță adaptivă şi corectivă

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

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

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

➢ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condiţiile 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 agreate de Beneficiar, ținînd cont și de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părți.

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

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

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

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

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

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

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

Serviciul de Suport Client "Hot-Line"

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

➢ pentru soluționarea defectelor;

➢ pentru solicitarea modificărilor funcționalităților existente;

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

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

➢ pentru solicitarea analizei unei solicitări de modificare.

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

➢ expedierea unui e-mail la adresa SSC;

➢ efectuarea unui apel telefonic;

➢ crearea unui ticket în platforma de Service Desk.

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

Reguli față de procesul de aplicare a modificărilor

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

Reguli privind prestare a serviciilor de suport

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

Clasificarea incidentelor

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

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

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

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

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

Tabelul 2. Matricea de estimare a urgenţei incidentului

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

Tabelul 3. Matricea de evaluare a impactului incidentului

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

Raportarea şi soluţionarea incidentelor

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

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

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

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

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

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

Securitatea informației

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

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

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

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

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;

➢ Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

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

Livrabile

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

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

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

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

Modalitatea de întocmire a ofertelor

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

Cerințe privind experiența personalului

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

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

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

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

Manager de proiect (minim 1 persoană)

- Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.

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

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

Business Analist *(minim 1 persoană)*

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

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

Specialist securitatea informațională (minim 1 persoană)

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

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

Specialist infrastructură sistem (minim 1 persoană)

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

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

Specialist programator (minim 1 persoană)

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

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

Specialist baze de date (minim 1 persoană)

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

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

Software Tester (minim 1 persoană)

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

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

Anexa nr.2

CAIET DE SARCINI

Servicii de mentenanță și suport pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **SIP**

Obiectul achiziției

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

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

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

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

Descriere generală a SIP

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

Setul de date folosit în funcționalitatea sistemului cuprinde:

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

- Data și ora efectuării programării serviciilor medicale;
- Data și ora prestării serviciilor medicale;
- Statutul/categoria serviciilor medicale
- Diagnosticul la trimitere (prin selectare din Lista Diagnosticelor);
- Numele și Prenumele Pacientului;
- Data nașterii;
- Adresa la domiciliu.

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

Specificații tehnice SIP

Caracteristici generale de funcționare

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

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

Interfața Utilizator

Aceasta interfața este accesibilă pentru toți utilizatorii autorizați în SIP:

- ✓ SIP dispune de o interfață inteligenta, intuitiva și prietenoasă cu utilizatorul;
- ✓ interfața de lucru este integral în browser-ul web și nu necesită instalarea de componente software suplimentare;
- ✓ interfața utilizatorului este în limba de stat;
- ✓ interfața permite moduri alternative de introducere a datelor medicale, atât prin utilizarea tastaturii, cât și a mouse-ului

- ✓ mesajele de informare / avertizare sunt simple și nu necesită cunoștințe tehnice avansate.

Hardware și canale de comunicație

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

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

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

Integritatea informației și fiabilitatea sistemului

<u>Complexul tehnic de prelucrare si transportare a datelor</u>

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

Sistemul de securitate

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

Caracteristici:

- asigura accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare si consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, consultare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de sistem.

- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor.

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

Sistemul are următoarele nivele de securitate care asigura confidențialitatea datelor:

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

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

În sistem există următoarele tipuri majore de utilizatori:

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

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

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

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

Retenția datelor, acces securizat

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

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

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

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

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

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

    - Unicitatea utilizatorilor în sistem;

    - Mecanism de control al versiunilor pentru înregistrările medicale.

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

Arhitectura SIP

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

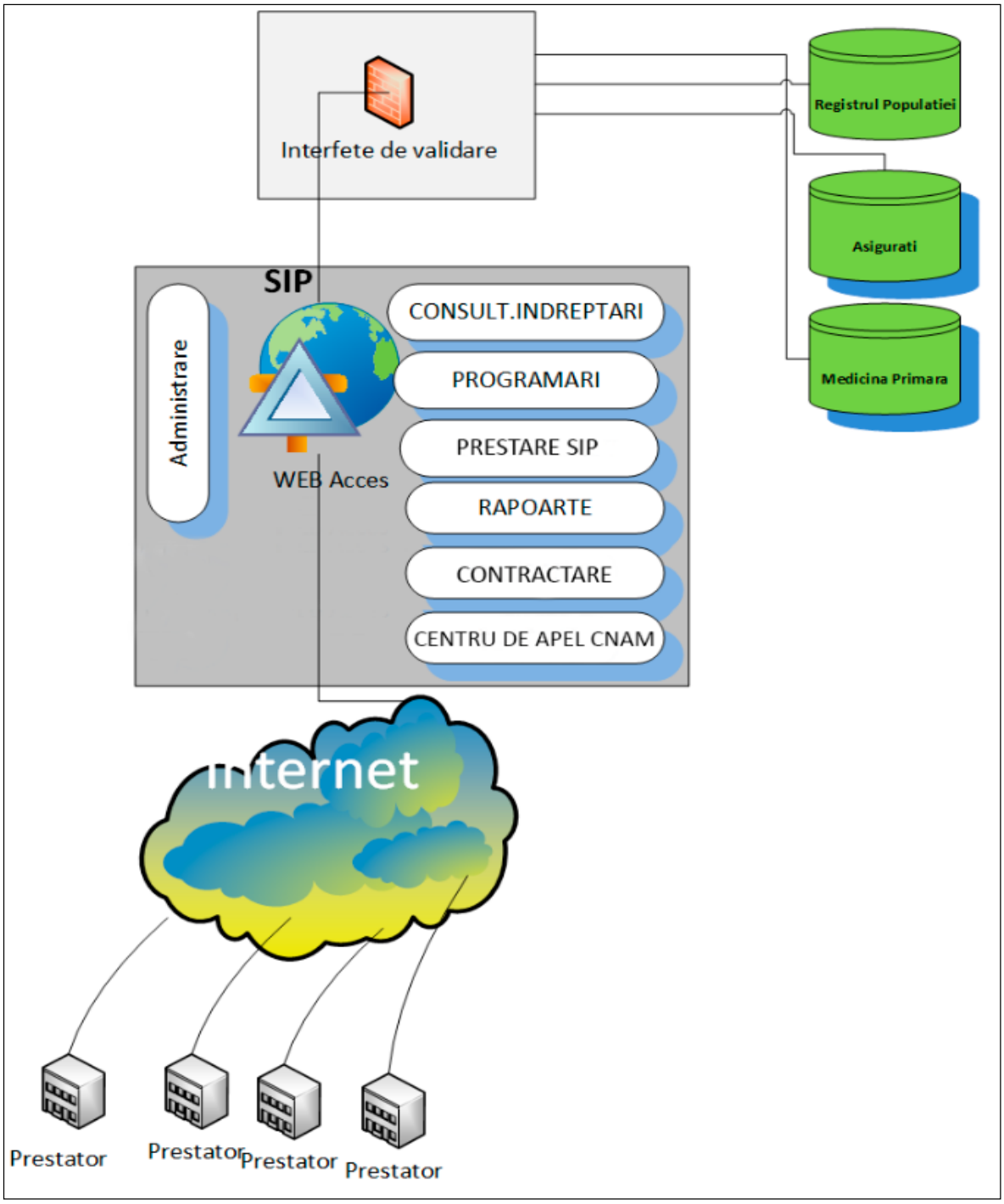


Figura 1. Schema arhitecturală SIP

Componente operaționale ale SIP sunt operaționale în următoarea structură modulară:

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

Modulul de administrare roluri

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

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

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

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

Medicul prescriptor

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

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

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

Prestatorul de servicii medicale

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

- IDNO al instituției prestatoare de servicii medicale;
- Adresa instituției;
- Numărul contractului;
- Lista de servicii medicale asumate pe grupuri și programe, inclusiv sumele contractuale specificate pentru perioadele pe care sunt programate aceste sume.

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

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

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

Modul consult/îndreptări

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

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

Modul programări

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

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

Modulul prestare a serviciilor de înaltă performanță

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

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

Modulul rapoarte

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

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

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

Modulul contractare

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

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

A. Cerințe de Mentenanță preventivă și Suport

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

De menţionat că prin procesul de mentenanţă se controlează funcţionarea produsului software, se înregistrează problemele pentru analiză, se întreprind acţiuni de avertizare şi de corecţie, precum şi acţiuni de adaptare şi de perfecţionare a produsului software. Scopul procesului de mentenanţă

constă în menţinerea capacităţii sistemului software de a presta servicii, precum şi în modificarea produsului software, păstrînd integritatea lui.

Pentru mentenanța SIP, CNAM formulează următoarele cerințe:

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

Suport Utilizatori

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

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

Suport platforma software

Servicii dedicate Sistemelor de Operare

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

- verificare de ansamblu a stării de funcționare a sistemului de operare și a performantelor sale;
- instalare corecții puse la dispoziție de producătorul sistemului de operare (service pack, security patch) conform modelului de licențiere;
- consultarea log-urilor aplicațiilor de securitate și sistem pentru depistarea problemelor ce nu se manifesta transparent și înlăturarea cauzelor care le-au produs sau recomandarea masurilor ce trebuie luate pentru a nu mai apărea astfel de erori;
- verificarea stării de funcționare a driverelor și a componentelor aferente;
- actualizare drivere în cazul apariției de noi versiuni;
- utilizarea spațiului pe disk și alocarea corectă a tipului de disk;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- creare și întreținere conturi de acces locale;
- optimizarea configuratei sistemului de operare;
- comunicare cu specialiștii de infrastructura hardware și de comunicații în sensul menținerii stării operaționale de înaltă performanță și disponibilitate a sistemului.

Servicii dedicate sistemelor de gestiune a bazelor de date

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

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

Servicii dedicate componentelor, inclusiv a celor de interconectare

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

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

Efectuarea testelor de penetrare

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

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

CNAM precizează ofertanților ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului.

Este important ca specialiștii Furnizorului să dețină cunoștințe privind termenii folosiți în comunicare și modul de operare al sistemelor informatice de dimensiuni mari și sa se adapteze cerințelor de securitate impuse de natura datelor prelucrate. CNAM consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului.

Operațiuni specifice SIP

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

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

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

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

B. Cerințe de mentenanță adaptivă şi corectivă a SIP

Asumarea contextului adaptării şi corecţiei software

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

Contextul în care Furnizorul va desfășura serviciile contractate este următorul:

➢ Beneficiarul va deține în continuare dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o nouă versiune a aplicației pentru care dezvoltatorul (cel care efectuează modificarea) va oferi garanție completă. Modificările funcționalităților existente sau noile ajustări ale aplicației se fac la cererea Beneficiarului. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației în timpul și după executarea ajustărilor de cod aparține Furnizorului. Orice ajustare asupra aplicației implică din partea Furnizorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.

➢ Asumarea serviciilor din acest proiect implica acordarea garanției asupra SIP pentru o perioada de minim 12 luni după încetarea contractului. Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.

➢ În baza legislației sau a nevoilor operaționale, Beneficiarul poate solicita Furnizorului modificări noi, iar Furnizorul trebuie sa fie pregătit în permanență să le implementeze rapid, fără a afecta funcționarea normală a sistemului.

➢ În baza nevoilor operaționale, Beneficiarul poate solicita Furnizorului consultanță în formă de răspunsuri scrise la întrebările cu privire la SIP, sau consultanță în formă de prezentări la oficiul CNAM cu privire la întrebări specifice legate de SIP.

➢ Furnizorul este responsabil pentru eventualele incidente asupra SIP generate pe parcursul operațiunilor desfășurate de el sau la recomandarea lui pe durata realizării de noi funcționalități.

➢ Versiunile actualizate și funcționale ale sistemului intră automat în proprietatea Beneficiarului, iar Furnizorul execută operațiunile tehnice asupra acestora pînă la finalizarea contractului și acorda garanție asupra lor de minim 12 luni după încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în condițiile legii.

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

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

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

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

Reguli privind prestare a serviciilor de mentenanță adaptivă şi corectivă

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

Solicitarea serviciilor de mentenanță adaptivă şi corectivă

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

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

Prestarea serviciilor de mentenanță adaptivă şi corectivă

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

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

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

➢ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea

problemei şi rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.

- Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute şi acceptate, şi a standardelor agreate de Beneficiar, ţinînd cont şi de ultimele cerințe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.
- Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor şi condițiilor înaintate de Beneficiar.

Cerințe privind calitatea serviciilor

Mod de lucru. Modalități de intervenție

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

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

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

Serviciul de Suport Client "Hot-Line"

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

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

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

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

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

Reguli față de procesul de aplicare a modificărilor

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

Reguli privind prestare a serviciilor de suport

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

Clasificarea incidentelor

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

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

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

Tabelul 1. Stabilirea priorităţii de soluţionare a incidentelor

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

Tabelul 2. Matricea de estimare a urgenţei incidentului

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

Tabelul 3. Matricea de evaluare a impactului incidentului

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

	- incidentul a afectat doar utilizatori interni ai Beneficiarului.

Raportarea şi soluționarea incidentelor

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

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

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

Alte cerințe şi reguli privind prestarea serviciilor

Soluționarea divergențelor

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

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

Securitatea informației

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

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

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

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

- Colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;

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

➢ Menţinerea formalizată a Registrului privind deţinerea probelor conservate (chain of custody).

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

Livrabile

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

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

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

➢ Codul sursă final compilabil pe suport (DVD-R sau USB);

➢ Documentația tehnică;

➢ Ghidul utilizatorilor;

➢ Ghidul administratorului;

➢ Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

Modalitatea de întocmire a ofertelor

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

Cerințe privind experiența personalului

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

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

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

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

Manager de proiect (minim 1 persoană)

– Studii superioare în domeniul tehnologiilor informaționale sau tehnice, confirmate prin diploma de absolvire/documente confirmative.

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

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

Business Analist *(minim 1 persoană)*

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

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

Specialist securitatea informațională (minim 1 persoană)

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

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

Specialist infrastructură sistem (minim 1 persoană)

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

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

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

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

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

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

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

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

21. Termenul limită de depunere/deschidere a ofertelor:

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

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

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

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

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

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

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

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

(se specifică denumirea proiectului și/sau programului)

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

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

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

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

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

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

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

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

35. **Alte informații relevante:** *nu sunt*

Președintele grupului de lucru: _____ Ion DODON