Servicii de mentenanță, suport și dezvoltare pentru

Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,

componenta **DRG**

CAIET DE SARCINI

Avizat: Ghenadie Damașcan, șef DCPSM_____,

Cornelia Nistor, șef SPAS_____

Coordonare: Ghenadie Chifac,

Șef adjunct DTI_____

Cuprins

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

Avizat: Ghenadie Damașcan, șef DCPSM_____,

Cornelia Nistor, șef SPAS_____

Coordonare: Ghenadie Chifac,

Șef adjunct DTI_____

Denumire. Cadrul legal. Baza Juridică. Acte normative

Sistemul Informațional de Raportare și Evidența a Serviciilor Medicale, componenta DRG (în continuare – DRG) reprezintă un instrument informatic de colectare și procesare centralizată de date în regim online gestionat de Compania Națională de Asigurări în Medicină. În prezent sistemul este operațional la nivel național și este găzduit în platfoma guvernamentală comună MCloud asupra lui desfășurând-se în mod continuu servicii de întreținere și dezvoltare.

Crearea și funcționarea DRG este reglementată de următoarele acte legislative și normative:

- Legea nr.1069/2000 cu privire la informatică;
- Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea nr. 412/2004 cu privire la Statistica Oficială;
- Legea nr.264/2004 cu privire la documentul electronic și semnătura digitală;
- Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- Legea nr. 142 din 19 iulie 2018 cu privire la schimbul de date și interoperabilitate;
- Hotărîrea Guvernului nr.272/2002 privind măsurile de creare a sistemului informațional automatizat „Registrul de stat al unităților de drept";
- Hotărîrea Guvernului nr. 333/2002 pentru aprobarea Concepției sistemului informațional automatizat Registrul de stat al populației;
- Hotărîrea Guvernului nr.562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
- Hotărîrea Guvernului nr.1032/2006 cu privire la aprobarea Concepției sistemului informațional automatizat „Registrul resurselor și sistemelor informaționale de stat";
- Hotărîrea Guvernului nr. 1123/2010 privind aprobarea cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
- Hotărîrea Guvernului nr. 857/2013 cu privire la Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020";
- Hotărîrea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură digitală (MSign);
- Hotărîrea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- Hotărîrea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
- Ordinul MS și CNAM nr. 397/125A/2013 privind aprobarea Regulamentului cu privire la modalitatea de codificare, colectare, raportare și validare a datelor la nivel de pacient în cadrul finanțării spitalelor în bază de DRG (CASE-MIX);
- Ordinul MS și CNAM nr.1004/670-A „Cu privire la aprobarea Listei programelor de activitate spitalicească, Listei intervențiilor chirurgicale repartizate pe programe speciale, Listei consumabilelor costisitoare achitate suplimentar plății per „caz tratat" în cadrul programelor speciale în sistemul DRG;
- Ordinul Ministerului Dezvoltării Informaționale nr.78/2006 cu privire la aprobarea reglementării tehnice „Procesele ciclului de viață al software-ului" RT 38370656-002:2006 (Monitorul Oficial nr. 95-97/335 din 23 iunie 2006);

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

- Ordinul CNAM nr. 204/2020 cu privire la aprobarea Politicii de securitate informațională în cadrul Companiei Naționale de Asigurări în Medicină.

Obiectul achiziției

Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță, suport și formulează condițiile pentru dezvoltarea funcționalităților sistemului în scopul extinderii acestuia în zonele de interes business al Autorității Contractante. În mod concret, prezentul proiect are **următoarele componente:**

OBIECTUL ACHIZIȚIEI	DURATA / TERMEN
A. Mentenanța și suportul DRG	Servicii asigurate timp de **6 luni** de la semnarea contractului. Serviciile se refera inclusiv la artefactele dezvoltate pe parcursul contractului asupra funcționalităților existente
B. Dezvoltări necesare funcționalităților DRG, transfer de cunoștințe și consultanță	Furnizorul va livra servicii de dezvoltare, transfer de cunoștințe și consultanță la cerere, în condițiile prezentei proceduri.

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra DRG pentru o perioadă de **minim 12 luni** după semnarea actului de predare primire pentru eventualele modificări software (cod sursă) realizate pe perioada contractului.

De asemenea, prestatorul serviciilor va documenta toate operațiunile de modificare a sistemului și le va prezenta Beneficiarului împreună cu codul sursă DRG (cu includerea comentariilor pentru acesta), 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.

În capitolele inițiale „Descriere generală a DRG" și „Specificații tehnice DRG" sunt prezentate în toate detaliile necesare potențialilor ofertanți pentru a evalua corect efortul, cunoștințele necesare și răspunderea pe care o asumă în prezenta procedura de achiziție.

Descriere generală a DRG

În scopul înțelegerii cât mai corecte a cerințelor Caietului de Sarcini, Autoritatea Contractantă aduce la cunoștința participanților la procedura de achiziție detaliile tehnice funcționale ale

Avizat: Ghenadie Damaşcan, şef DCPSM_____,

Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____

Şef adjunct DTI_____

sistemului. Sistemul informațional 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 Companiei Naționale de Asigurări în Medicina și Ministerului Sănătății, Muncii și Protecției Sociale 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).

Definiții și abrevieri

Abreviere/Acronim	Descriere
CNAM	Compania Națională de Asigurări în Medicină
MSMPS	Ministerul Sănătății, Muncii și Protecției Sociale
DRG	Sistemul Informațional de Raportare și evidență a Serviciilor Medicale, componenta DRG
Dezvoltare	Crearea și implementarea unor noi module funcționale și/sau modificarea modulelor existente ale unui sistem informațional, precum și reigineria sistemului informațional.
Mentenanță	Reprezintă un ansamblu de activități care includ: asigurarea

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

Abreviere/Acronim	Descriere
	funcționalității și a securității complexului de mijloace tehnice și de program; actualizarea versiunii sistemului informațional; întreținerea sistemului informațional și resursei informaționale; restabilirea funcționalităților sistemului informațional, în cazul apariției defecțiunilor; asigurarea suportului metodologic și practic pentru utilizatori.
IDNP	(Număr de Identificare Personal) – numărul de identificare a unei persoane, utilizat in practica internațională sub forma de prescurtare.
CCAP	Programul de Audit al Codificării Clinice
MCloud	Cloud-ul guvernamental al Republicii Moldova
Proces	Secvența fixa de evenimente realizate de către un grup de activități conectate la nivel logic ce utilizează resursele organizaționale pentru obținerea celor mai bune rezultate spre îndeplinirea obiectivelor organizaționale.
Rol	Comportamentul si obligațiile specifice ale unei persoane sau ale unor persoane care lucrează in echipa (grup de lucru).
Arhitectură	Toate soluțiile esențiale legate de organizarea sistemului software precum si setul de elemente si interfețe structurale, împreună cu cooperarea descrisa in termenii acestor elemente.
Bază de date	Toate datele combinate organizate in conformitate cu anumite reguli, care oferă principiile generale de descriere, stocare si procesare a datelor.
SSL	Protocol criptografic care asigură comunicarea sigură între 2 noduri ale rețelei de calculatoare pentru acțiuni cum ar fi vizitarea paginilor Web, e-mail, internet-fax, schimb de mesaje instantanee și alte transferuri de date.
TIC	Tehnologie Informatică și de Comunicație
KP	coeficientul provizoriu de ajustare a valorilor relative

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;

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

Coordonat șef adjunct DEM

- 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 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 în sistemul MCloud:
  - Servere protejate redundant pentru hosting al bazelor de date, softului de sistem si softului funcțional (aplicatii si subsisteme);
  - Echipamente de comunicații pentru formarea rețelelor locale LAN si organizarea comunicațiilor teritoriale WAN;
  - Serverele puse la dispoziție au procesoare din familia Intel x86/x64

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

- Platforma hardware pusa la dispoziție de către beneficiar este dimensionata corespunzător pentru a permite funcționarea in bune condiții a sistemului.
- Performanta optima, in limita normelor obiective de uzura, pentru realizarea structurii funcționale si asigurarea extinderii ulterioare a sistemului;
- este flexibila in utilizarea mijloacelor disponibile destinate recepționarii informației din surse externe (alte instituții publice);
- asigura un nivel înalt de securitate in privința aplicațiilor si transportului de date;
- asigura normele de funcționare ale platformelor informatice guvernamentale.

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

Integritatea informației și fiabilitatea sistemului

Complexul tehnic de prelucrare și transportare a datelor

Asigurarea tehnică a sistemului se constituie din calculatoare personale, servere, mijloacele de imprimare, 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;

Avizat: Ghenadie Damașcan, șef DCPSM

Cornelia Nistor, șef SPAS

Coordonare: Ghenadie Chifac,

Șef adjunct DTI

- 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 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 stații și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;
- Nivelul de securitate la nivel business: reprezentat prin modulul de acces la sistem: autentificare unică cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date.
- Nivelul de securitate al bazei de date: baza de date MS SQL server are propriul mecanism de securitate; accesul la informații se face cu user/parola criptate în mod implicit pe canalul de comunicație. Integritatea bazei de date este 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.

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

Dirijarea cu drepturile de acces, instrumente de autentificare şi autorizare

Funcţiile principale de administrare realizate în sistem sunt:

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

Retenţia datelor, acces securizat şi audit

- **Retenţia datelor şi controlul versiunilor.** Sistemul permite stocarea informaţiilor medicale (fise medicale) în conformitate cu cerinţele legale cu toate versiunile acestora prin operaţii programabile de backup.
- **Securitate.** Pentru asigurarea securităţii, toate accesările sistemului respecta regulile de control a accesului în vederea protejării vieţii private. Masurile de securitate ajuta la prevenirea utilizării neautorizate a datelor şi protejează împotriva pierderii, modificării neautorizate şi distrugerii datelor din sistem.
- **Autentificare.** Toţi utilizatorii care accesează sistemul sunt supuşi procesului de autentificare.
- **Autorizare la funcţionalităţi.** Utilizatorii care folosesc sistemul sunt autorizaţi să acceseze funcţionalităţile sistemului pe baza identităţii, rolurilor pe care le au în sistem şi pe baza permisiunilor asociate rolului sau rolurilor din care fac parte utilizatorii.
- **Autorizare la date.** Utilizatorii care folosesc sistemul sunt autorizaţi să acceseze funcţionalităţile sistemului pe baza identităţii, rolurilor din sistem şi 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 fişele electronice ale pacienţilor săi.
- **Nerepudierea.** Nerepudierea este o modalitate de a garanta faptul ca utilizatorul nu poate nega mai târziu ca a efectuat o operaţiune. Nerepudierea este implementata prin următoarele mecanisme:
  - Unicitatea utilizatorilor în sistem
  - Auditarea tuturor operaţiunilor efectuate de 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 comunicaţie cât şi la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit.** Toate operaţiunile efectuate de utilizatori sau de către alte sisteme care accesează sistemul păstrează o urma în componenta de auditare. Este permisa astfel investigarea incidentelor de către un administrator.

Avizat: Ghenadie Damaşcan, şef DCPSM_____,

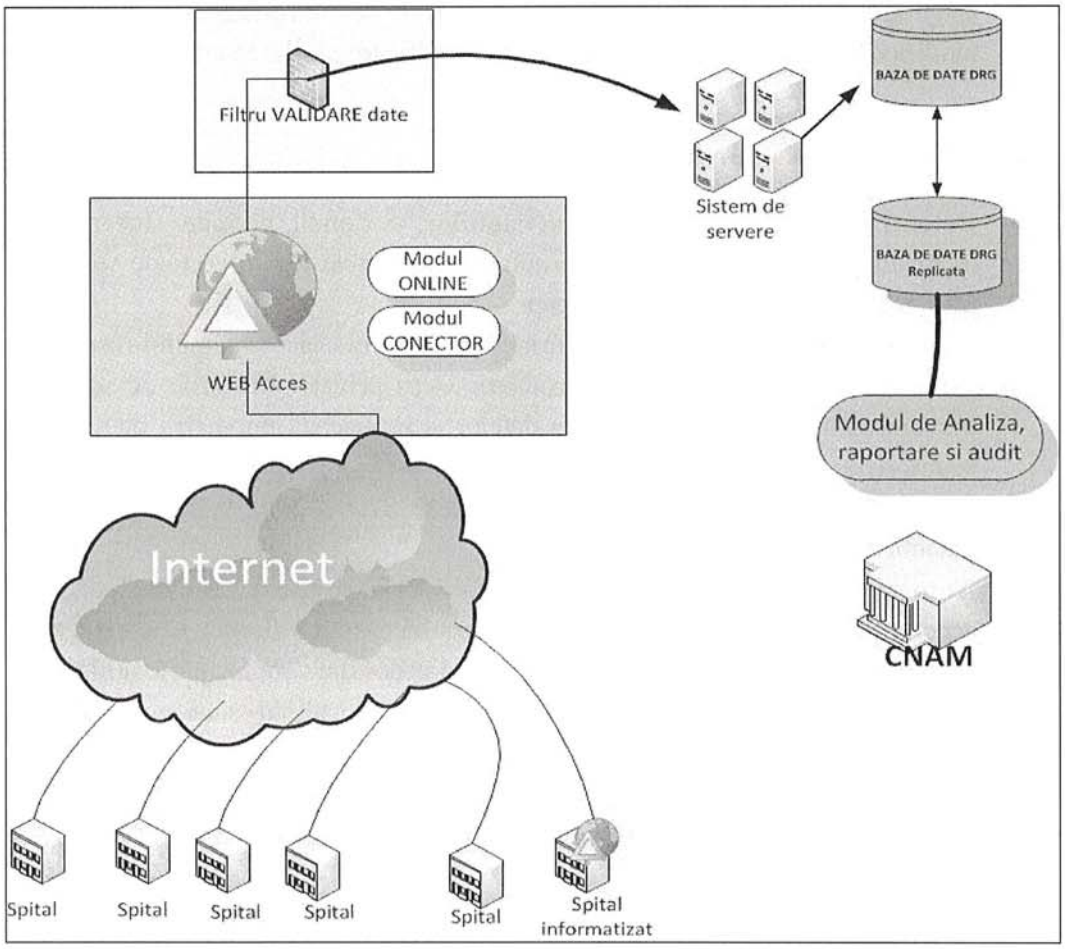
Cornelia Nistor, şef SPAS_____

Coordonare: Ghenadie Chifac,

Şef adjunct DTI_____

Arhitectura DRG

Sistemul are o arhitectura client-server, 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:



Schema arhitecturală DRG

Componente operaționale ale DRG sunt operaționale în următoarea structură modulară:

- ✓ Modulul de administrare sistem colector
- ✓ Modulul de autentificare
- ✓ Modulul colectare date Real Time
- ✓ Modulul de nerepudiere
- ✓ Modulul de validare
- ✓ Modulul de înregistrare raportări

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

- ✓ 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:

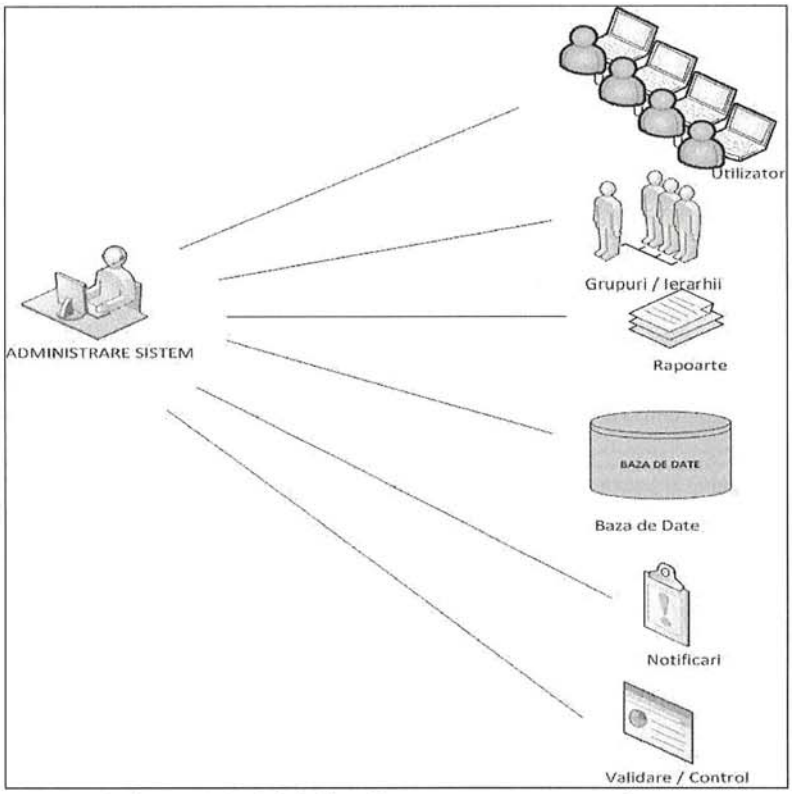
- Managementul utilizatorilor (creare, ștergere, modificare date utilizatori). Fiecare instituție care execută raportare în DRG are desemnat cel puțin un utilizator al sistemului care transmite raportările; modalitatea de alocare a acestei resurse umane este răspunderea instituției.
- Administrarea sistemului. Administratorii sistemului pot efectua setări la nivelul celorlalte module si pot verifica funcționarea corecta a fiecărui modul. Nivelul de acces al administratorilor este corespunzător cerințelor la care aceștia răspund:
  - administratorii pot modifica informațiile de referința ale operatorilor sistemului (nume, prenume, locație, instituție, etc.)
  - administratorii pot modifica intervalele temporale 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.

Avizat: Ghenadie Damașcan, șef DCPSM_____,

Cornelia Nistor, șef SPAS_____

Coordonare: Ghenadie Chifac,

Șef adjunct DTI_____



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

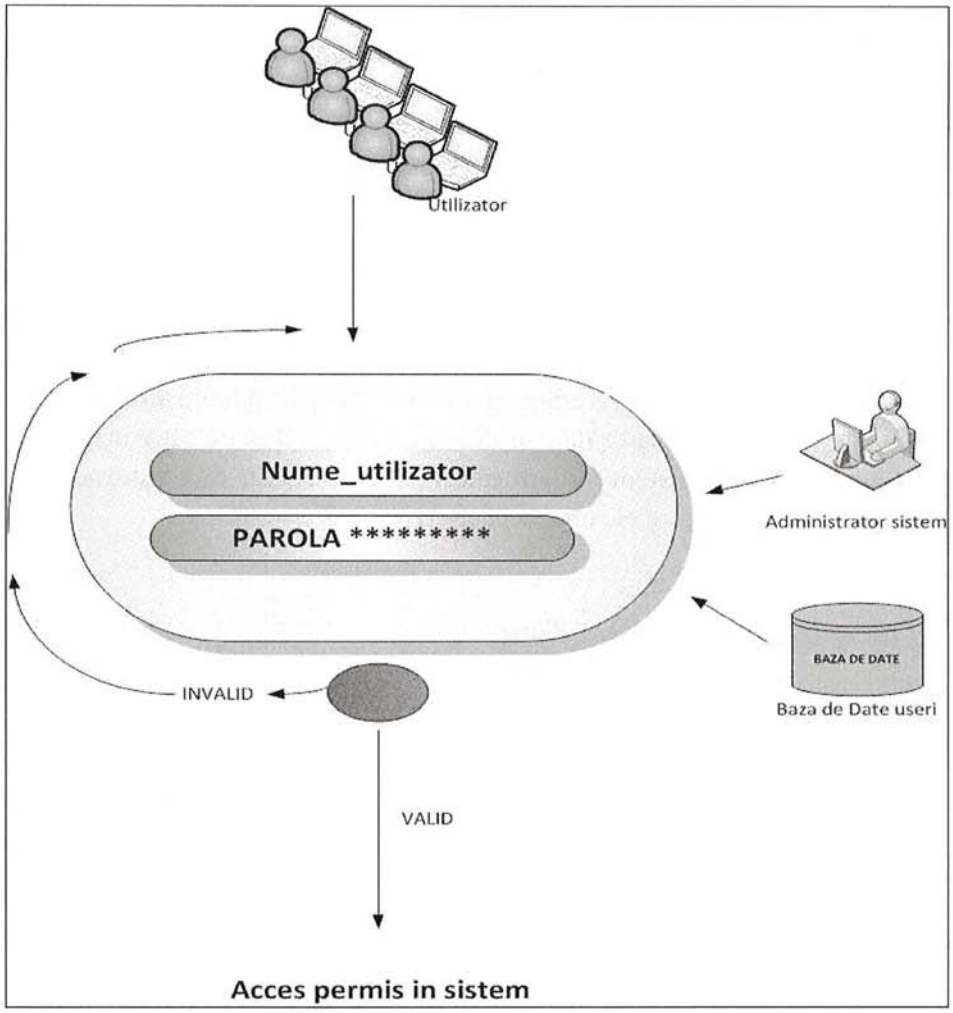
Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

transmise rămâne exclusiv responsabilitatea instituțiilor medicale / operatorilor care folosesc sistemul.

Modulul de autentificare

Modulul de autentificare garantează accesul securizat al utilizatorilor în sistem. Pentru a se loga, utilizatorii au un username şi o parola pe care le utilizează la accesarea sistemului. Modelul de autentificare garantează unicitatea utilizatorului în sistem.



Schema Modul de Autentificare

Avizat: Ghenadie Damaşcan, şef DCPSM_____,

Cornelia Nistor, şef SPAS_____

Coordonare: Ghenadie Chifac,

Şef adjunct DTI_____

Transmiterea "pachetului" de autentificare, format din username şi parolă / semnătură, se face în mod securizat, prin utilizarea protocolului de comunicaţie https.

- Sistemul asigura funcţionarea permanentă a modulului de autentificare şi oferă mesaje ajutătoare în cazul introducerii incorecte a datelor de autentificare (utilizator / parola incorecte). Mesajele sunt explicite, scurte şi coerente, în limba româna, astfel încât nu creează confuzii la nivelul utilizatorilor.
- Interfaţa de logare conţine de asemenea informaţii privind condiţiile de acces ale utilizatorilor în sistem şi un mesaj prin care utilizatorilor le este adus la cunoştinţa că nerespectarea condiţiilor de acces se sancţionează conform legii.
- Odată intraţi în sistem, utilizatorii deţin exclusiv acele drepturi de care au nevoie pentru a-şi desfăşura activitatea; sistemul dispune de un mecanism de control acces care să permită utilizatorilor, în mod implicit un număr minim de acţiuni permise şi nu este necesară intervenţia administratorilor decât pentru acordarea de drepturi speciale atunci când este necesar acest lucru. Acţiunile minimale pe care le desfăşoară utilizatorii sunt cele aferente transferului de date în intervalul de timp permis, de rescriere a rapoartelor trimise în cazul în care sunt necesare modificări sau cele de introducere informaţii despre pacienţi. Conţinutul rapoartelor este exclusiv responsabilitatea utilizatorilor şi, în nici un caz administratorii sistemului nu vor interveni în modificarea datelor din rapoartele trimise de către instituţiile medicale.
- Administratorii sistemului pot interveni în cazul în care este necesară modificarea datelor de conectare ale unui utilizator.

Modulul de colectare date Real Time

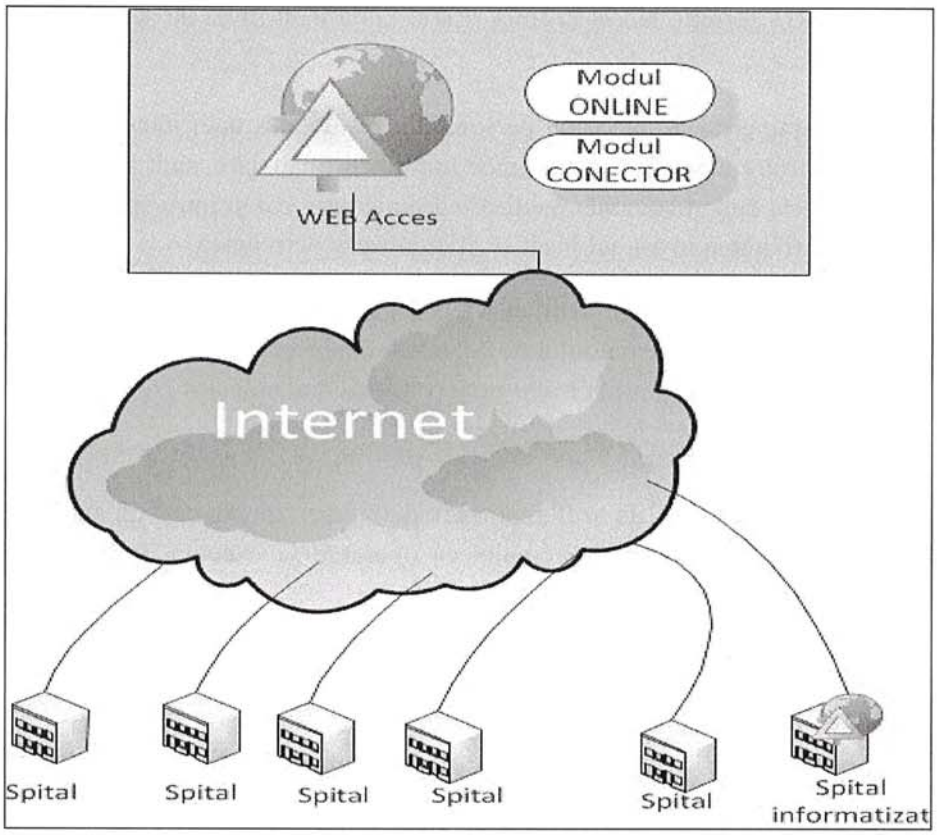
Acest modul este cel care transformă operarea DRG într-o activitate aflată la dispoziţia permanentă a oricărui spital: este un modul destinat acelor instituţii care nu au un sistem informatic integrat al activităţii medicale, şi care, în prezent lucrează cu diferite programe informatice în vederea generării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

Acest modul are o interfaţă de lucru universală cu un aspect operaţional intuitiv şi uşor de urmărit, care nu necesită cunoştinţe tehnice informatice avansate; orice medic sau asistent îl poate utiliza în activitatea curentă în vederea introducerii în sistemul naţional a informaţiilor despre pacienţii pe care îi tratează.

Informaţiile pot fi introduse de către utilizatorii autorizaţi direct în sistem non-stop, la nivel naţional, într-o interfaţă accesibilă de pe orice calculator care dispune de un browser şi de o legătura la serverul sistemului DRG: vârsta, sex, durata de spitalizare, diagnostice principale şi secundare, proceduri, starea la externare şi greutatea la naştere (în cazul nou-născuţilor), iar în funcţie de acestea pacienţii sunt clasificaţi într-o categorie distinctă (o grupă de diagnostice), în conformitate cu nomenclatoarele din domeniu.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____



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

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

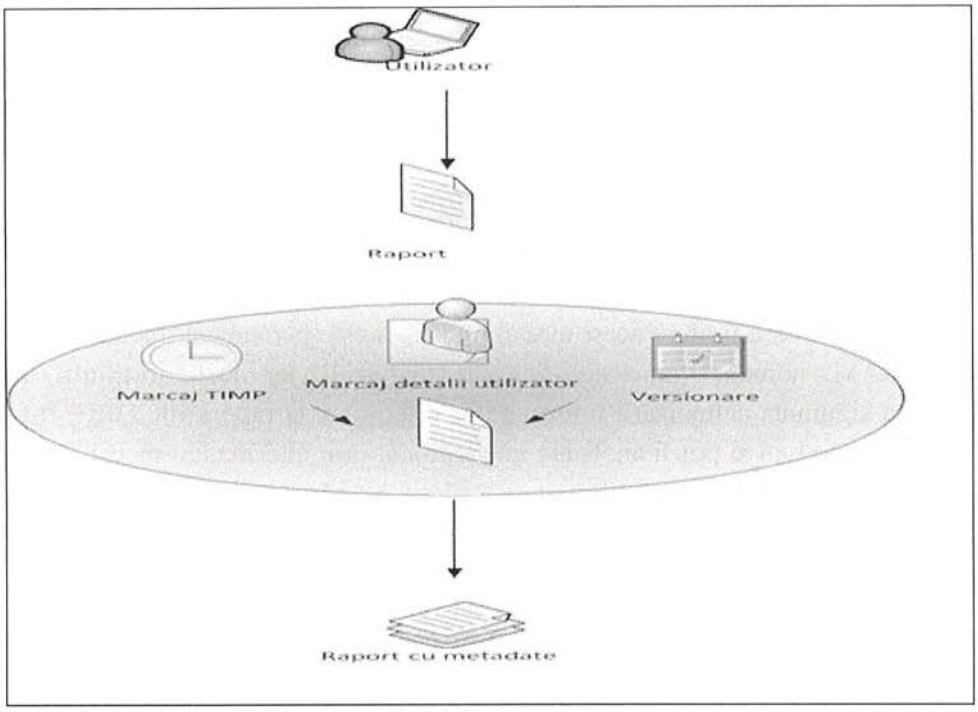
oricărui spital, DRG permite lucrul în timp real şi la un înalt nivel de securitate, direct spre baza de date a CNAM.

Operaţional, prin punerea la dispoziţia personalului medical a unei interfeţe de lucru în vederea acestui tip de raportare medicală cu puternice implicaţii financiare, sunt premisele unei colaborări eficiente inter / intra departamentale medical-administrativ cât şi între spitale care sunt interesate să îşi modeleze activitatea în aşa fel încât să eficientizeze activitatea.

Alegerea modului în care sunt efectuate raportările către CNAM este opţiunea instituţiilor medicale: acestea pot folosi fie modulul de colectare date Real Time sau software-ul intern şi 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 toţi utilizatorii sistemului ca operarea se execută în mod unic şi că nici un utilizator nu poate nega acţiunile legate de sistem.



Modulul de nerepudiere

Fiecare utilizator este unic în sistem, lucru verificabil prin intermediul modulului de autentificare. Modulul de nerepudiere se referă la faptul că acţiunile pe care le efectuează un utilizator nu pot fi negate de acesta, deoarece fiecare acţiune are directă corespondenţă cu un utilizator. Orice fişier transferat de către un utilizator primeşte prin intermediul acestui modul un pachet de metadate care conţine:

- ✓ Data şi ora la care au fost transmise fişierele către sistem;

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

- ✓ Numele utilizatorului care a transmis fişierul; pentru fiecare fişier în parte se ataşează metadatele corespunzătoare. Sistemul face automat asocierea între utilizator şi fişierul transmis.
- ✓ Numele utilizatorului care a rescris ultima versiune a fişierului – va fi stabilit în faza de analiză, în funcţie de particularităţile observate;

Aceste informaţii sunt disponibile atât administratorilor şi, parţial, utilizatorilor. Adăugarea metadatelor la fişiere este o operaţiune pe care modulul de nerepudiere o execută în mod automat şi independent de opţiunile utilizatorilor. Orice raport transmis către sistem este însoţit de elemente de identificare unice: data, ora, nume utilizator etc. În cazul auditării sistemului, sunt disponibile date referitoare la acţiunile fiecărui utilizator, corelate integral cu informaţiile introduse în sistem.

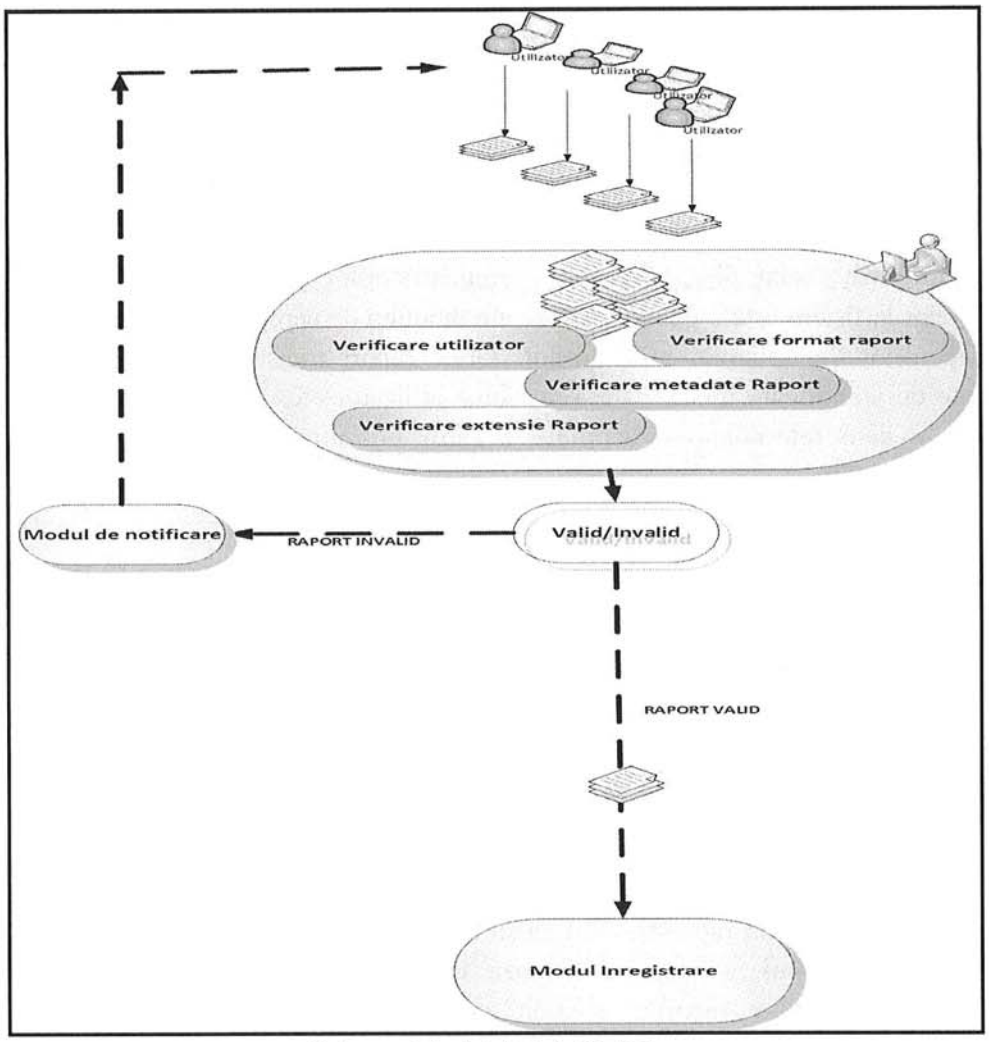
Modulul de validare

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

- ➢ Modulul de validare operează în mod minimal fişierele transmise (setul minim de date la nivel de pacient) şi le acceptă doar pe cele care se încadrează în formatul dorit de către CNAM;
- ➢ Modulul de validare verifică, de asemenea, existenţa metadatelor de corespondenţa între utilizator şi fişier înainte de trecerea în sistem a fişierelor al căror conţinut îl constituie rapoartele. În cazul în care apar neconcordanţe între ceea ce aşteaptă sistemul şi ceea ce livrează utilizatorii, se trimit alerte către „Modulul de notificare, raportare şi audit" care prelucrează situaţiile 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; atenţia acordată acestui modul este ridicată iar analiza situaţiilor neconforme şi alinierea acestora sunt urmărite permanent.
- ➢ Modulul de validare are capacitatea de a trata cât mai multe situaţii comune şi elimina la timp cât mai multe cazuri în care apare eroarea umană.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____



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).

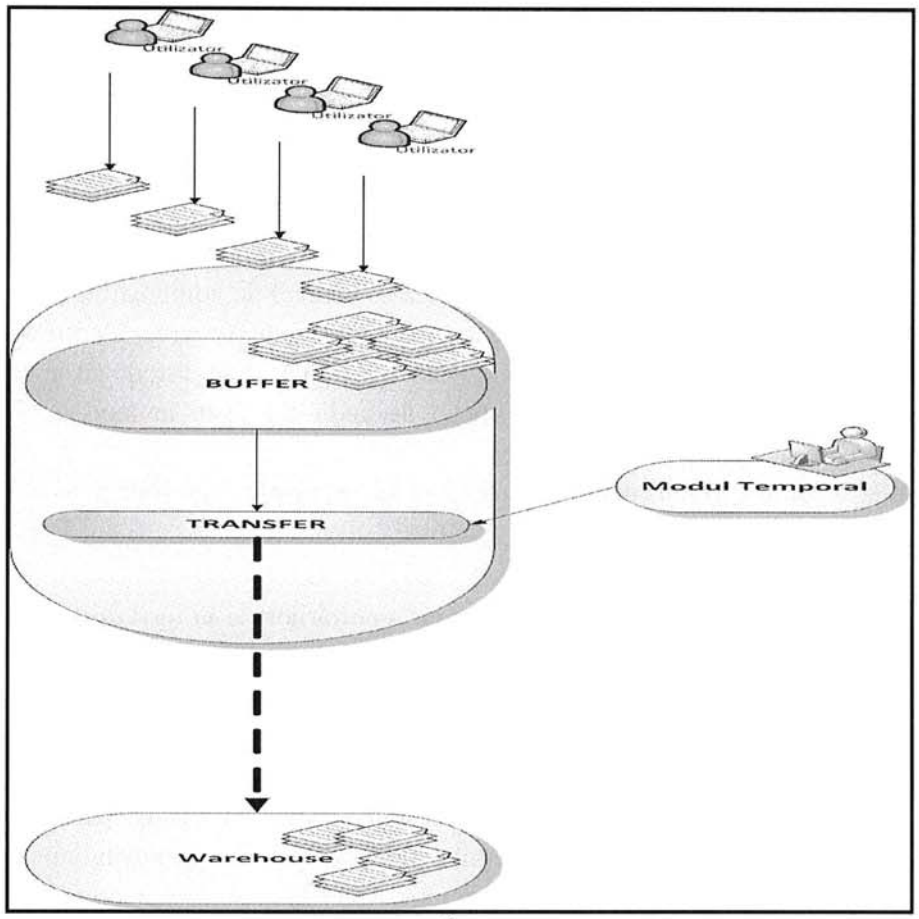
Modulul de înregistrare a raportări conține două componente:

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.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

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.



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

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

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.

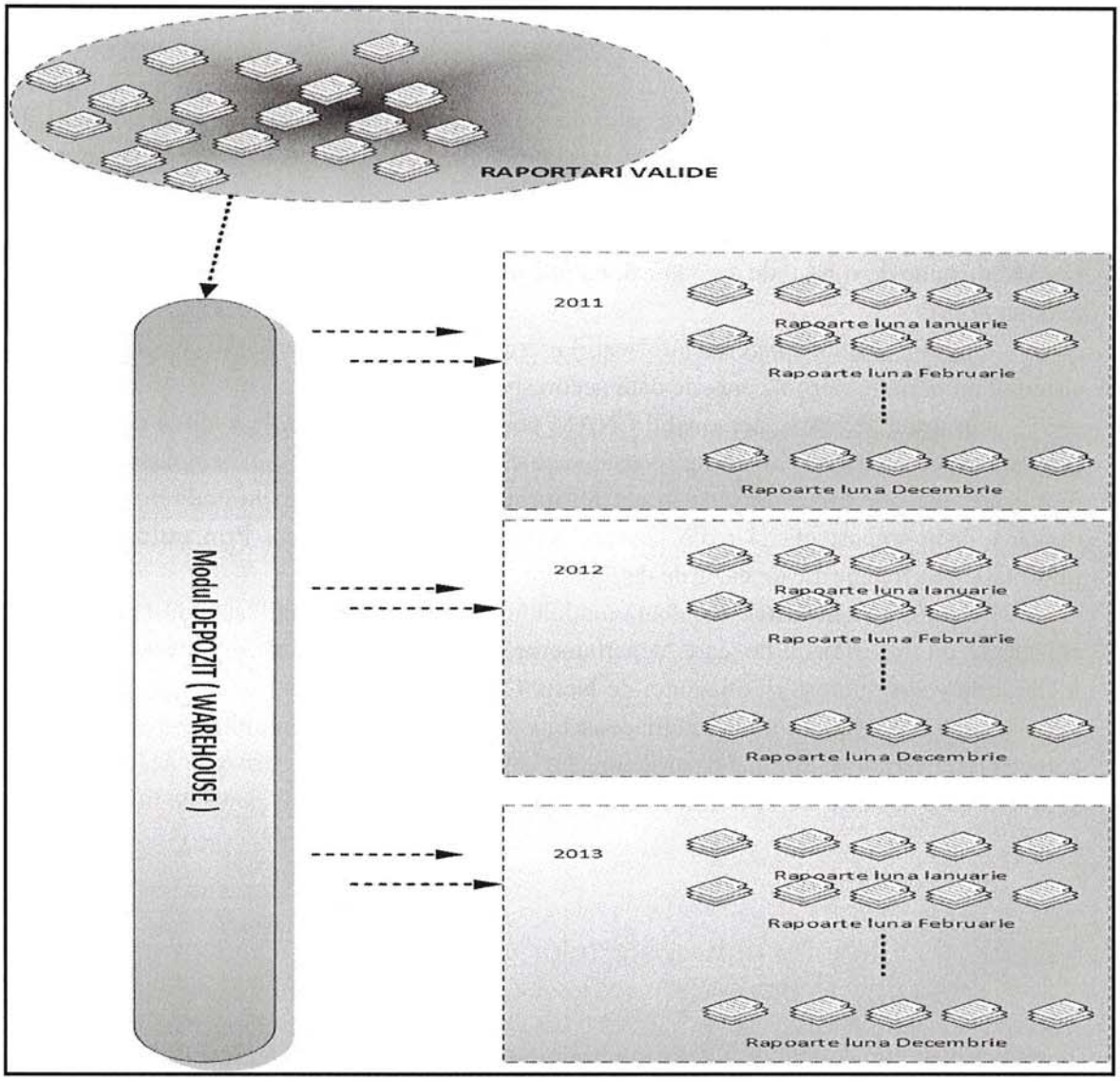
Modulul Depozit (Warehouse)

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.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____



Schema Modul Depozit Rapoarte DRG (Warehouse)

Zona de stocare a Modulului Depozit (warehouse) poate fi controlată atât de administratorii sistemului DRG cât şi de inginerii de sistem informatic M-Cloud, protecţia fiind în bucla închisa [fiecare controlează pe cel de care este controlat

Modulul de Analiză la nivel de Baza de Date

Sistemul DRG creează în mod dinamic o bază de date updatată permanent, cu informaţii consistente; sistemul este un instrument performant de interogare care permite extragerea de rapoarte necesare CNAM şi MSMPS, oferind o imagine clară a istoricului diagnosticelor pacienţilor; 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 şi închiderii, se pot obţine statistici în timp real. Odată ce perioada de raportare este

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

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.

Modalitatea de întocmire a ofertelor

Toate cerințele din caietul de sarcini sunt minime și obligatorii, iar nerespectarea sau respectarea parțiala 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. Pentru toate cerințele ofertanții vor răspunde punct cu punct într-un tabel cu minim 2 coloane „Cerința" „Răspuns"

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Cerințe de Mentenanță și Suport

Cerințele față de serviciile de mentenanță

Cerinţele CNAM asupra serviciilor de mentenanţă reflectate în acest capitol sunt orientate spre identificare şi înlăturarea defectelor ascunse înainte ca acestea să se manifeste şi organizarea proceselor în aşa mod încât să permită înlăturarea incidentelor în cazul apariţiei acestora, în timp restrâns şi 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 mentenanţă sistemului DRG, CNAM formulează următoarele cerinţe:

- Analiza/diagnosticarea, izolarea şi remedierea problemelor semnalate de către Beneficiar privind funcţionalităţile sistemului (metode: remote, telefonic sau la sediul Beneficiarului);
- Asistenţa tehnică pentru probleme critice semnalate de către beneficiar privind funcţionalităţile sistemului prin intermediul platformei Service Desk;
- Identificarea, investigarea, analiza şi soluţionarea incidentelor;
- Analiza parametrilor de funcţionare a sistemului, identificarea şi raportarea riscurilor potenţiale;
- Actualizarea parametrilor existenţi în partea utilizatorilor-CNAM şi utilizatorilor-spital, conform cerinţelor legislaţiei 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 şi excepţiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora, conform formatului solicitat şi menţinerea posibilităţilor de extragere a datelor de către utilizator-CNA şi utilizator-spital.
- Depanarea erorilor, formarea raportului de analiză şi a recomandărilor; gestiunea jurnalului de incidente şi raportare statistică privind incidentele;
- Ajustarea compartimentului DRG ->„URGENTA” din baza de date spital/CNAM conform Anexei nr.4 (Fişa medicală UPU) la Standard de organizare, funcţionare şi practică în cadrul UPU din cadrul IMS, aprobate prin Ordinul Ministerului Sănătăţii nr.424 din 02.06.2017 „Cu privire la aprobarea Standardului de organizare, funcţionare şi practică în cadrul Unităţilor de Primiri Urgenţe”;
- Ajustarea compartimentului Rapoarte - Rapoarte urgenta din DRG;
- Actualizarea/modificarea după formă şi conţinut a rapoartelor existente în aplicaţie pe partea utilizatorilor-CNAM şi utilizatorilor-spital;
- Menţinerea funcţionării serviciilor web aferente.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Suport Utilizatori

Utilizatorii DRG sunt cei care interpretează datele colectate de sistem. Prin oferta, furnizorul serviciilor achiziționate de către Beneficiar asuma următoarele condiții minime de suport tehnic pe aplicație pentru utilizatorii:

- Verificarea funcționalităților sistemului și a eventualelor probleme semnalate de către utilizatorii CNAM; in situații de funcționare defectuoasa, deschid tichete de intervenție pentru remedierea defecțiunilor.
- Suport tehnic pentru toate funcționalitățile aplicației: existente sau dezvoltate și implementate în timpul contractului;
- Asistenta tehnica pentru utilizatorii CNAM prin email, Service Desk;
- Modalități de asigurare a suportului; email, telefon, remote acces (detaliile se vor preciza în mod explicit în Oferta tehnică);
- Timp de intervenție la utilizator (rezolvare tichet): 1 zi lucrătoare.

Suport platforma software

1. Servicii dedicate Sistemelor de Operare

În această categorie întră următoarele servicii minime relative de administrare și mentenanță a Sistemelor de operare Microsoft Windows Server 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;
- verificare politici de securitate și depistare intruziuni/vulnerabilități;
- optimizarea configuratei 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.

2. 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:

- updatarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către Autoritatea Contractanta;

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

- recomandări privind alocarea corecta a tipului și spațiului de disk;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- răspunderea asupra backup-ului și restaurării bazei de date, configurarea programării secvențelor de backup;
- orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.

3. Servicii dedicate componentelor, inclusiv a celor de interoperabilitate

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

- verifică și optimizează secvențele de cod (în principal cod Java);
- 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.

Autoritatea Contractanta 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. Autoritatea Contractanta consideră că eventualele incidente de securitate sau pierderi de date sunt inacceptabile pe perioada desfășurării contractului, iar situațiile de acest tip vor fi tratate pe linie tehnică cât și juridică, în conformitate cu legislația Republicii Moldova.

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

Avizat: Ghenadie Damașcan, șef DCPSM_____,

Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____

Șef adjunct DTI_____

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

- ✓ Interfața aplicativa 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

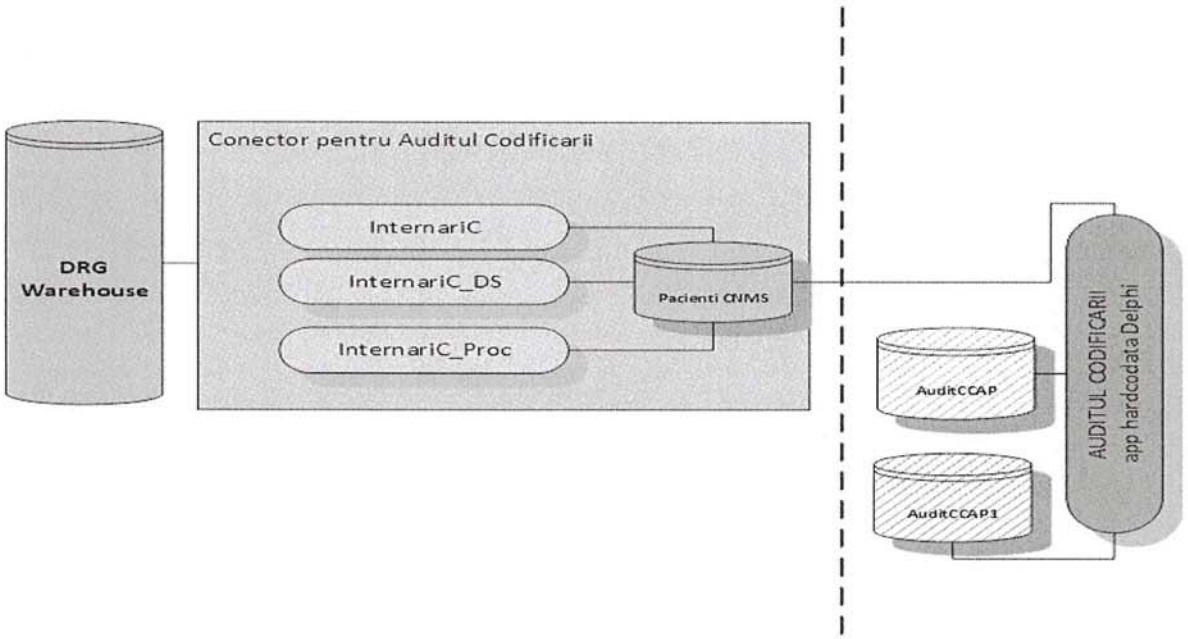
- Generarea programată a rapoartelor.
- Îmbunătățirea, ajustarea și completarea rapoartelor CNAM. Raport complex, intern, etc.
- Implementarea restricțiilor CNAM: obligativitate câmpuri în dependența cu datele completate, eliminare cazuri medicale dublate, diagnostice secundare, proceduri secundare,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

Avizat: Ghenadie Damașcan, șef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____ Șef adjunct DTI_____

Modulul conector pentru Audit al codificarii

Funcţionalitatea de audit a codificării este acoperita de o aplicaţie pentru care Autoritatea Contractanta nu deţine codul sursa. Cea mai mare parte din informaţiile prelucrate de către aplicaţia de Audit a codificării se găsesc actualizate in timp real in CCAP. In lipsa codului sursa, dezvoltatorii CCAP au reuşit sa atingă o parte din obiectivele funcţionale ale operatorilor care executa auditul codificării prin operaţiuni care nu afectează aplicaţia ci doar baza de date. Astfel operatorii Autorităţii Contractante care efectuează auditul codificării continua sa folosească vechea aplicaţie hardcodata care foloseşte date din warehouse-ul DRG.



Autoritatea Contractanta va continua sa emită fie solicitări de dezvoltare a sistemului CCAP, fie de execuţie a unor proceduri la nivelul bazelor de date si conectorilor in scopul obţinerii rezultatelor dorite pana la momentul includerii definitive in CCAP a funcţionalităţilor de audit al codificării. In prezenta procedura de achiziţie Autoritatea Contractantă solicita operaţiuni de mentenanţa care se refera exclusiv la funcţionalităţile asupra cărora deţine codul sursa, urmand ca pe parcursul dezvoltării funcţionalităţilor in cadrul CCAP, aria de mentenanţa sa se extindă corespunzător.

Codul dezvoltat in sensul susţinerii modului de conectare pentru auditul codificării permite operatorilor de audit sa desfăşoare in cadrul vechii aplicaţii doua operaţiuni:

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

Autoritatea Contractantă deţine codul sursa necesar pentru prelucrarea noii baze de date **Pacienţi CNMS** si asupra **view-rilor de internari** [InternariC, InternariC_DS, InternariC_Proc] si **ListaSpitale**, care colectează si interpretează informaţiile din baza de date Wodehouse a DRG, acestea intrând in obiectul operaţiunilor de mentenanţa pe care urmează sa le desfăşoare

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Coordonat şef adjunct DEM

furnizorul serviciilor. Autoritatea Contractantă subliniază faptul ca unul dintre obiectivele de viitor pentru dezvoltarea CCAP este introducerea –totala sau parțială – a funcționalităților modulului de audit al codificării in SI DRG.

Avizat: Ghenadie Damaşcan, şef DCPSM_____,

Cornelia Nistor, şef SPAS_____

Coordonare: Ghenadie Chifac,

Şef adjunct DTI_____

B. Cerințe de dezvoltare a DRG, transfer de cunoștințe și consultanță

Asumarea contextului dezvoltărilor software

În categoria serviciilor de dezvoltare intră acele servicii necesare pentru modificarea sistemului sau a parametrilor acestuia ca urmare a modificării logicii de business, de modificare sau de introducere a funcționalităților noi în sistem. Efectul execuției de servicii suplimentare îl constituie o nouă versiune a aplicației, adaptată cerințelor Autorității Contractante și implică activitatea analiștilor și dezvoltatorilor, cu excepția celor indicate în capitolul A.Cerințe de Mentenanță 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. Beneficiarul își păstrează în continuare dreptul de proprietate asupra aplicației. Pentru o înțelegere clară, modificările funcționalităților existente sau noile dezvoltări 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 modificărilor de cod aparține dezvoltatorului. Orice modificare asupra aplicației implică din partea dezvoltatorului obligația acordării garanției pentru întreg sistemul și nu doar pe modificările efectuate.
- In același context este important de reținut faptul ca eventualele incidente, disfuncționalități sau alterări de configurație care privesc buna funcționare a DRG se vor trata exclusiv cu furnizorul serviciilor și nu cu terțe persoane. Asumarea serviciilor din acest proiect implica acordarea garanției asupra DRG pentru o perioada de minim 12 luni de la 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 sau funcționalități noi, iar Furnizorul trebuie sa fie pregătit în permanenta 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 executa operațiunile tehnice asupra acestora pana la finalizarea contractului și acorda garanție asupra lor, în forma în care au fost predate, de **minim 12 luni** de la

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

încetarea contractului. Cheltuielile generate de defecțiunile aplicației în perioada de garanție vor fi suportate de către Furnizor.

- 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 cât și daunele provocate de incident.
- Cererile de dezvoltare au termene relativ scurte și survin în general în urma unor modificări legislative sau în urma îmbunătățirilor funcționării business-proceselor. Autoritatea Contractanta a constatat ca, de obicei, modificările efectuate au un impact imediat în utilizare și asupra altor componente. Atunci când este efectuată o modificare în sistem, rezultatul acesteia este doar o parte a ceea ce trebuie urmărit, fiind necesare operațiuni regulate de întreținere și verificare a corectitudinii datelor din întregul sistem. Pentru buna desfășurare a operațiunilor de dezvoltare software, dar și de consultanța în menținerea caracterului consolidat al informațiilor din sistem, echipa tehnica a Furnizorului trebuie să fie pregătita în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și sa dețină resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, trebuie să aibă capacitatea de înțelegere și viziune a impactului oricăror modificări sunt propuse de beneficiar sau care sunt necesare în așa fel încât sa asigure funcționarea continuă a sistemului și să intervină corect ori de câte ori este nevoie.
- Pentru a se asigura ca aceste condiții sunt îndeplinite, Autoritatea Contractanta a solicitat în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților **specificarea în Oferta financiară a prețului pentru minim 80 de zile/om pentru cererile suplimentare de ordin tehnic dedicate dezvoltării și consultanței software a DRG cum ar fi dezvoltarea unor interfețe automatizate pentru schimbul de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate MConnect, integrarea DRG cu serviciul electronic guvernamental Mpass, MNotify, MLog, precum și dezvoltarea Fișei medicale pentru Unități Primiri Urgente (UPU) aprobată prin Ordinul Ministerului Sănătății nr.424/2017 „ Cu privire la aprobarea Standardului de organizare, funcționare și practică în cadrul Unităților de Primiri Urgențe". Cererile Autoritarii Contractante se vor face conform formularului de comandă servicii suplimentare de mai jos** *[Change Request].* **Rezervarea a 80 de zile/om la un preț prestabilit [și punctat] creează Autorității Contractante avantajul implementării rapide a necesităților tehnice și de consultanță imediate ale SI DRG și asigura continuitatea serviciului în situațiile urgente.**

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Cererea cu privire la propunerea de dezvoltare

FORMULAR DE ÎNREGISTRARE			
SUBSISTEMUL			
		Autor:	
		Data:	
Categoria problemei	Software ☐	Procese ☐	Date ☐
Prioritate	Înaltă ☐	Medie ☐	Joasă ☐
Descrierea:			
Elemente anexate:			
Semnătura autorului:			
Soluţionat de către:		**Data:**	
Descrierea soluţiei:			

Prestator:

L.Ş.

Beneficiar:

L.Ş.

Avizat: Ghenadie Damaşcan, şef DCPSM_____,

Cornelia Nistor, şef SPAS_____

Coordonare: Ghenadie Chifac,

Şef adjunct DTI_____

Mod de lucru. Modalități de intervenție

Sistemul este găzduit în MCloud-ul guvernamental și operează în regim profesional. În timpul desfășurării operațiunilor de întreținere este important de păstrat o comunicare corectă între echipa Furnizorului și cea a beneficiarului. Experții beneficiarului trebuie să înțeleagă terminologia tehnică specifică sistemelor informatice, nu doar pe cea specifică aplicației. Experiențele anterioare ale beneficiarului au demonstrat ca unele situații pot fi tratate doar în condițiile implicării echipelor tehnice de la toate nivelurile sistemului în condițiile de menținere permanentă a calității și securității sistemului. Buna comunicare între echipele de suport este esențială în procesul de întreținere al sistemului și al asigurării unei bune experiențe a utilizatorilor sistemului. Toate operațiunile de acest fel se desfășoară în condiții maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Operațiunile de întreținere la nivelul aplicativ și de platformă software se desfășoară în mod securizat prin accesul experților din afară centrului de date. Situațiile mai simple – în special recomandări – pot fi tratate telefonic sau prin mail. Pot apărea însă și situații cu nivel ridicat de complexitate sau risc, în care este necesară prezența on-site a echipelor de suport tehnic și comunicarea între managerii acestora devine obligatorie pentru succesul operațiunilor. Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

- Intervenție de la distanță [remote acces], securizată. Se vor respecta recomandările specialiștilor Centrului de Date al cloud-ului guvernamental
- Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.
- Intervenții on-site, în situațiile în care specialiștii centrului de date guvernamental apreciază că este necesară o astfel de abordare a situației.

Cerințe pentru Service Desk

Prin oferta, furnizorul serviciilor achiziționate de către Beneficiar își asumă următoarele condiții minime de suport tehnic pe aplicație, la nivelul Service Desk -ului:

- Disponibilitate Service Desk prin email, telefon acordat la programul de lucru al beneficiarului
- Modalități de asigurare a suportului; email, telefon, remote acces.

Obligații solicitate pentru Service Desk **în cazul unui incident la nivelul centrului de date:**

- Personalul Service Desk -ului va trebui să aibă permanent actualizată lista specialiștilor disponibili pentru intervenție;

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

- Personalul Service Desk -ului trebuie să mențină legătura cu specialiștii (telefonica, mail, sms) pe parcursul intervențiilor astfel încât utilizatorii să poată primi informații corecte privind starea de funcționare a sistemului
- Service Desk -ul nu va dirija utilizatorii către echipele de intervenție și va acționa ca punct unic de contact pe toată durata incidentului pană la reintrarea sistemului în regim normal de operare.

Nivelul serviciilor

1. Nivelul serviciilor stabilește cerințele privind parametrii la care trebuie să fie prestate aceste *servicii* de către Prestator. Reprezintă nivelul agreat de Beneficiar al indicatorilor cantitativi care caracterizează calitatea funcționării serviciului (conform terminologiei internaționale Service Level Agrement).

Parametrii ce caracterizează nivelul *serviciilor de suport* sunt următorii:

Timp de Răspuns/Reacție (TR) - este timpul în care furnizorul va reacționa la o solicitare de suport/incident, va diagnostica situația și va stabili acțiunile necesar a fi întreprinse pentru soluționare.

Timp de Soluționare (TS) – este timpul obiectiv în care se așteaptă ca furnizorul va întreprinde acțiunile în zona să de responsabilitate pentru a soluționa complet solicitarea Beneficiarul.

Solicitările Beneficiarul pentru servicii sunt clasificate din punct de vedere al importanței acestora pentru Beneficiarul. Importanța pentru Beneficiarul este apreciată în funcție de impactul (produs sau probabil) al evenimentului ce a generat necesitatea plasării solicitării asupra parametrilor de calitate pentru funcționarea sistemului.

Reguli privind Managementul incidentelor

Clasificarea incidentelor

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

Impactul incidentului caracterizează consecințele acestuia asupra disponibilității și performanței sistemului informatic deservit. Urgența incidentului caracterizează operativitatea cu care acesta trebuie soluționat, pentru a minimiza impactul incidentului asupra Beneficiarului.

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

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

		Impact		
		Înalt	*Mediu*	*Jos*
Urgență	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Avizat: Ghenadie Damașcan, șef DCPSM_____,

Coordonare: Ghenadie Chifac,

Cornelia Nistor, șef SPAS_____

Șef adjunct DTI_____

Tabelul 2. Matricea de estimare a urgenței incidentului

URGENȚĂ	Descriere
Înaltă	Un incident este estimat ca având nivelul urgenței "Înalt" în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activități și operațiuni critice pentru afacerea Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea imediată poate preveni riscuri legale majore și de securitate (protecție) a informației.
Medie	Un incident este estimat ca având nivelul urgenței „Mediu" în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc considerabil în timp; - există activități și operațiuni importante pentru afacerea Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea operativă poate preveni riscuri legale moderate și de securitate a informației.
Joasă	Un incident este estimat ca având nivelul urgenței "Jos" în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puțin în timp; - activitățile și operațiunile afectate nu trebuie continuate imediat; - nu există riscuri legale și de securitate a informației semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

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

Raportarea și soluționarea incidentelor

Orice incident aferent Serviciilor este raportat de Beneficiar către SSC, conform procedurilor stabilite la capitolul „Reguli de înregistrare a solicitărilor".

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Prestatorul va reacționa și soluționa incidentele raportate de Beneficiar, conform nivelului serviciilor agreate pentru soluționarea incidentelor. În acest scop, se vor specifica următorii indicatori:

Serviciile de gestiune a incidentelor vor fi asigurate pentru următorul nivel de servicii:

Tabel. Nivelul serviciului pentru soluționarea incidentelor

Prioritate incident	**Timpul de reacție**	**Timpul de soluționare**	**Timp max. pentru corectare a cauzei***	**Raportare primară**
Critică	Timpul de reacție al Prestatorului – imediat	până la 8 ore	12 ore	Telefon
Înaltă	Timpul de reacție al Prestatorului – 1 oră **	12 ore**	24 ore	Telefon; Sistem Service Desk
Medie	Timpul de reacție al Prestatorului – 4 ore**	24 ore	5 zile	Sistem Service Desk
Joasă	Timpul de reacție al Prestatorului – 24 ore	3 zile	zile	Sistem Service Desk
Neglijabilă	Timpul de reacție al Prestatorului – 72 ore	Cel mai bun efort.		Sistem Service Desk

Notă:

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

** Regulile se aplică pentru perioada orelor de lucru. În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort".

Prestatorului poate contacta persoana ce a raportat incidentul, pentru a preciza informația oferită de Beneficiar. De comun acord cu aceasta, Prestatorul poate revizui nivelul impactului și nivelul urgenței soluționării incidentului. Beneficiarul are de asemenea posibilitatea ca ulterior să revizuiască clasificarea stabilită inițial. Revizuirea poate fi necesară în funcție de progresele soluționării incidentului.

Prestatorul va diagnostica cauza incidentului și va identifica măsurile necesare a fi întreprinse pentru soluționarea incidentului. Pe tot parcursul soluționării incidentului, Prestatorul va oferi informația Beneficiarului privind progresele făcute în vederea soluționării incidentului.

Prestatorul poate solicita implicarea la gestiunea incidentului, a persoanelor responsabile ale Beneficiarului. Conlucrarea este necesară în vederea diminuării impactului incidentului și soluționării operative a acestuia.

Un incident se consideră soluționat atunci când funcționalitatea este restabilită pentru Beneficiar, la nivelul stabilit conform prezentelor Reguli. În cazul în care Beneficiarul nu este de acord cu nivelul de soluționare a incidentului, poate solicita deschiderea repetată a incidentului. În caz contrar, incidentul se consideră închis.

Toate incidentele raportate de Beneficiar sunt înregistrate în cadrul SSC. Prestatorul încurajează Beneficiarul să raporteze orice incident sau suspiciune de incident. Acest fapt va permite îmbunătățirea continuă a nivelului Serviciilor prestate.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Soluționarea divergențelor

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

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

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

3) Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite. În acest scop, pot fi ascultate, sau obținute în scris, opiniile membrilor externi, convocați în grupul de lucru, precum și rezultatele de expertiză ale probelor electronice existente.

4) Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru din partea ambelor părți.

Identificarea unei soluții echitabile pentru ambele Părți, în limite angajamentelor asumate ale Părților, este preferabilă în toate situațiile de divergență. În cazul în care o asemenea soluție nu poate fi identificată, părțile vor aplica prevederile Contractului pentru soluționarea litigiilor.

Raportarea privind nivelul serviciilor

Părțile vor opta pentru prestarea transparentă a Serviciilor. În acest scop, Prestatorul va prezenta cu regularitate Beneficiarului rapoarte privind conținutul și nivelul Serviciilor acordate. Beneficiarul va formula propuneri privind conținutul rapoartelor de monitorizare a serviciilor. Structura rapoartelor respective este stabilită de Prestator.

Rapoartele prezentate, regularitatea și modalitatea de prezentare a acestora, este stabilită în tabelul de mai jos.

Tip raport	Conținut	Destinație	Regularitatea
Raport privind volumul serviciilor	Tipul solicitării, durata soluționării	Raportul este prezentat în scopul asigurării transparenței privind prestarea Serviciilor la nivelul agreat de Prestator.	Lunar, pe suport de hârtie. Suplimentar în formă electronica, la solicitarea Beneficiarului.
Raport privind solicitările de modificare	Propunerile de modificare a Serviciilor	Raportul este prezentat în scopul asigurării transparenței dezvoltării SIF.	Lunar, în formă electronică. La solicitarea Beneficiarului, pe suport de hârtie
Raport privind nivelul serviciilor.	Nivelul de disponibilitate a sistemului, întreruperi planificate, incidente raportate, solicitări de suport.	Raportul este prezentat în scopul asigurării transparenței privind prestarea serviciilor la nivelul agreat de Prestator.	Lunar, în formă electronică, disponibil în Sistemul Service Desk. La solicitarea Beneficiarului, pe suport de hârtie.

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

Cerințe privind experiența personalului

Autoritatea Contractantă a identificat următoarele cerințe minime privind expertiza pe care trebuie să o aibă echipa tehnică a furnizorului (min. 3 persoane):
Expert - Manager de proiect 1 persoană – Minim 5 ani experiență în managementul proiectelor în domeniul Tehnologii Informaționale și Comunicații; – Experiență în cel puțin 3 proiecte de implementare a unor soluții similare, în rolul de manager de proiect pentru toată durata proiectului. - Experiență de lucru de cel puțin 1 an în cadrul companiei Ofertantului sau a grupului din care aceasta face parte. – Experiența dobândită prin participarea în cel puțin 1 proiect la activități IT complexe privind infrastructura software și hardware din cadrul sistemelor informaționale medicale (se justifică prin documente semnate de beneficiari ex: recomandări) – Studii Superioare, deținerea unui Certificat cu vechime de minim 5 ani emis de o instituție recunoscută la nivel internațional în domeniul managementului proiectelor (PMP sau PRINCE2 sau echivalent), MoR sau echivalent. – Cunoașterea limbii române este obligatorie. **Notă:** În cazul în care oferta este depusă de o asociere, managerul de proiect trebuie să dispună de experiență în cadrul companiei lider al asocierii
Specialist asigurarea calității în domeniul securității (1 persoana) – Studii superioare finalizate cu diploma de licență în domeniul informatic; – Experiența profesională generală în domeniul informatic de minim 10 ani; – Competențe privind auditul securității sistemelor informatice, dovedite prin prezentarea unei certificări în domeniu emisă de autoritate publică competentă cu recunoaștere generală sau de către un organism de drept public sau privat autorizat. – Competente privind auditarea sistemelor de management al calității, dovedite prin prezentarea unei certificări în domeniu emisă de autoritate publică competentă cu recunoaștere generală sau de către un organism de drept public sau privat autorizat. – Experiența dobândită prin participarea, în funcția de expert calitate, în cel puțin 3 proiecte informatice în domeniul medical (se justifică prin documente semnate de beneficiari ex: recomandări)
Specialist Java și baze de date (1 persoana) - Studii superioare finalizate cu diploma de licență în domeniul informatic; - Experiența conform CV de minim 10 ani în programarea bazelor de date și Java - Experiență conform CV de minim 5 ani în programarea aplicațiilor web și a bazelor de date: HTML, Javascript, CSS, MS Sql Server - Experiența conform CV prin participarea în cel puțin 3 proiecte la activități

Avizat: Ghenadie Damaşcan, şef DCPSM_____, Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____ Şef adjunct DTI_____

tehnice asupra sistemelor informaționale din domeniul medical.

Criterii de evaluare

Condiții obligatorii ale ofertelor pentru calcularea punctajului

Pentru calcularea punctajului doar ofertele care îndeplinesc simultan condițiile:

- **îndeplinesc integral condițiile solicitate privind experiența ofertantului și pregătirea personalului**
- **răspund corect cerințelor Caietului de Sarcini.**

Avizat: Ghenadie Damaşcan, şef DCPSM_____,

Coordonare: Ghenadie Chifac,

Cornelia Nistor, şef SPAS_____

Şef adjunct DTI_____