

Servicii de mentenanță și suport pentru
Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale,
componenta **DRG**

OFERTA TEHNICA

CERINTA / Informare a Autoritatii Contractante		RASPUNS OFERTANT / luare la cunoștință	
<p>Obiectul achiziției</p> <p>Sistemul descris în continuare face obiectul achiziției serviciilor de mentenanță și suport. În mod concret, prezentul proiect are următoarele componente:</p>		<p>Obiectul ofertei</p> <p>Sistemul descris în continuare face obiectul ofertei serviciilor de mentenanță și suport. În mod concret, prezentul proiect are următoarele componente:</p>	
OBIECTUL ACHIZIȚIEI	Descriere	OBIECTUL ACHIZIȚIEI	Descriere
<p>Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG:</p> <ul style="list-style-type: none"> • Servicii de mentenanță preventivă și Suport – în bază de abonament; • Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing. 	<p><i>Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.</i></p>	<p>Servicii de mentenanță (preventivă, corectivă, adaptivă) și suport pentru Sistemul Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG:</p> <ul style="list-style-type: none"> • Servicii de mentenanță preventivă și Suport – în bază de abonament; • Servicii de mentenanță corectivă și adaptivă – în bază de trouble ticket/ticketing. 	<p><i>Servicii asigurate timp de 12 luni. Serviciile se referă la SI, serviciile web aferente acestuia, inclusiv la artefactele modificate sau elaborate pe parcursul perioadei de desfășurare a activităților de mentenanță.</i></p>
<p>În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul (Furnizorul/Ofertantul) va avea acces la sistemul informațional și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra Sistemului Informațional de Raportare și Evidență a Serviciilor Medicale, componenta DRG (în continuare – DRG) pentru o perioadă de minim 12 luni după încetarea contractului.</p>		<p>Am luat la cunoștință informațiile privind tehnologia folosită și modul în care sunt prelucrate datele.</p> <p>Asumam ca, în calitate de prestator, vom avea acces la sistemul informațional și asumam 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.</p>	

<p>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.</p>	<p>Asumam ca vom 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.</p>
<p>Descriere generală a DRG</p> <p>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.</p> <p>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.</p> <p>Funcționarea continuă și operarea în sistemul DRG are următoarele obiective:</p>	<p>Descriere generală a DRG</p> <p>Asumam înțelegerea ca 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.</p> <p>Întelegem 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. Întelegem ca 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.</p> <p>Asumam înțelegerea faptului ca funcționarea continuă și operarea în sistemul DRG are următoarele obiective:</p>
<p><i>Creșterea eficienței serviciilor spitalicești</i></p> <p>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.</p>	<p><i>Creșterea eficienței serviciilor spitalicești</i></p> <p>Am luat cunoștința ca 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.</p>

<p>Creșterea eficienței tehnice la nivelul furnizorului de serviciilor spitalicești</p> <p>DRG permite spitalelor să-și evidențieze cu claritate tipurile de pacienți și resursele atrase pentru aceștia, iar prin compararea cu costurile necesare se generează cadrul de funcționare pentru o eficiență cât mai mare (economiiile făcute fiind păstrate la nivelul spitalului).</p> <p>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).</p>	<p>Creșterea eficienței tehnice la nivelul furnizorului de serviciilor spitalicești</p> <p>DRG permite spitalelor să-și evidențieze cu claritate tipurile de pacienți și resursele atrase pentru aceștia, iar prin compararea cu costurile necesare se generează cadrul de funcționare pentru o eficiență cât mai mare (economiiile făcute fiind păstrate la nivelul spitalului).</p> <p>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).</p>
<p>Specificații tehnice DRG</p> <p>Caracteristici generale de funcționare</p> <p>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:</p>	<p>Asumam înțelegerea specificațiilor tehnice DRG:</p> <p>Caracteristici generale de funcționare</p> <p>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:</p>
<ul style="list-style-type: none"> ➤ 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 	<ul style="list-style-type: none"> ➤ 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.

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.

<p>Interfața Utilizator</p> <p>Această interfață este accesibilă pentru toți utilizatorii autorizați în DRG:</p> <ul style="list-style-type: none"> ✓ 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. 	<p>Asumam intelegerea modului de operare al interfaței Utilizator</p> <p>Această interfață este accesibilă pentru toți utilizatorii autorizați în DRG:</p> <ul style="list-style-type: none"> ✓ 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.
<p>Hardware și canale de comunicație</p> <p>Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:</p>	<p>Asumam intelegerea hardware-ului și canalelor de comunicație</p> <p>Arhitectura sistemului este ierarhică, client-server și conține următoarele componente:</p>
<ul style="list-style-type: none"> • Platforma hardware, formata din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat pe platforma guvernamentală comună MCloud: <ul style="list-style-type: none"> ○ 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 	<ul style="list-style-type: none"> • Platforma hardware, formata din Complexul tehnic de prelucrare și transportare a datelor, acesta fiind asigurat pe platforma guvernamentală comună MCloud: <ul style="list-style-type: none"> ○ 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

<p>recepționarii informației din surse externe (alte instituții publice);</p> <ul style="list-style-type: none"> ○ asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date; ○ asigura normele de funcționare ale platformelor informatice guvernamentale. 	<p>recepționarii informației din surse externe (alte instituții publice);</p> <ul style="list-style-type: none"> ○ asigura un nivel înalt de securitate în privința aplicațiilor și transportului de date; ○ asigura normele de funcționare ale platformelor informatice guvernamentale.
<ul style="list-style-type: none"> ● Platforma software. Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici: <ul style="list-style-type: none"> ▪ Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise; ▪ Sistemul de gestiune al bazelor de date este marca aceluiși 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. 	<ul style="list-style-type: none"> ● Platforma software. Din considerente de costuri, suport tehnic și omogenitate, infrastructura software are următoarele caracteristici: <ul style="list-style-type: none"> ▪ Sistemele de operare ale serverelor sunt Microsoft Windows/Linux, din gama Enterprise; ▪ Sistemul de gestiune al bazelor de date este marca aceluiși 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.

<p><i>Integritatea informației și fiabilitatea sistemului</i></p> <p><u>Complexul tehnic de prelucrare și transportare a datelor</u></p> <p>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.</p>	<p>Asumam intelegerea modalitatii in care se asigura integritatea informației și fiabilitatea sistemului:</p> <p><u>Complexul tehnic de prelucrare și transportare a datelor</u></p> <p>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.</p>
<p><i>Sistemul de securitate</i></p> <p>DRG funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.</p>	<p>Asumam intelegerea sistemului de securitate</p> <p>DRG funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor.</p>
<p><u>Caracteristici:</u></p> <ul style="list-style-type: none"> • asigură accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator; • este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscrisoare, redactare, ștergere, consultare etc.); • este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor; • toate conturile de utilizator sunt create de administratorul de system; 	<p><u>Caracteristici:</u></p> <ul style="list-style-type: none"> • asigură accesul controlat al utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile și obligațiunile fiecărui utilizator; • este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscrisoare, redactare, ștergere, consultare etc.); • este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structura ale bazei de date accesibile lor; • toate conturile de utilizator sunt create de administratorul de system;

<ul style="list-style-type: none"> • 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; 	<ul style="list-style-type: none"> • 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;
<p>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.</p>	<p>Intelegem natura specială a informațiilor gestionate în cadrul DRG și motivele pentru care acesta are implementat un mecanism de securitate care permite numai accesul autorizat asupra componentelor sale.</p>
<p>Sistemul are următoarele nivele de securitate care asigură confidențialitatea datelor:</p> <ul style="list-style-type: none"> - <u>Nivelul de securitate la nivel de aplicație:</u> reprezentat prin protocolul de comunicație între stațiile clientului și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL; - <u>Nivelul de securitate la nivel business:</u> reprezentat prin modulul de acces la sistem: autentificare unică cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date. - <u>Nivelul de securitate al bazei de date:</u> 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). 	<p>Asumăm înțelegerea nivele de securitate care asigură confidențialitatea datelor:</p> <ul style="list-style-type: none"> - <u>Nivelul de securitate la nivel de aplicație:</u> reprezentat prin protocolul de comunicație între stațiile clientului și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL; - <u>Nivelul de securitate la nivel business:</u> reprezentat prin modulul de acces la sistem: autentificare unică cu user/parola și asigurarea în baza acestora a accesului corespunzător la nivelul de date. - <u>Nivelul de securitate al bazei de date:</u> 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).
<p>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</p>	<p>Intelegem și asumăm că sistemul asigură dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grupă de utilizatori</p>

<p>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.</p>	<p>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.</p>
<p>În sistem există următoarele tipuri majore de utilizatori:</p> <ul style="list-style-type: none"> - 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. <p>La nivel aplicativ, sistemul generează o listă de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.</p>	<p>Am luat la cunostinta ca in sistem există următoarele tipuri majore de utilizatori:</p> <ul style="list-style-type: none"> - 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. <p>La nivel aplicativ, sistemul generează o listă de utilizatori cu diferite drepturi de acces, care dețin un set combinat de drepturi.</p>

Dirijarea cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

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

Am luat la cunostinta modalitatea de dirijare cu drepturile de acces, instrumente de autentificare și autorizare

Funcțiile principale de administrare realizate în sistem sunt:

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

Retenția datelor, acces securizat și audit

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

Am luat la cunostinta si asumam modalitatea de realizare a retenției datelor, accesului securizat și auditului

- **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 competența. 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.

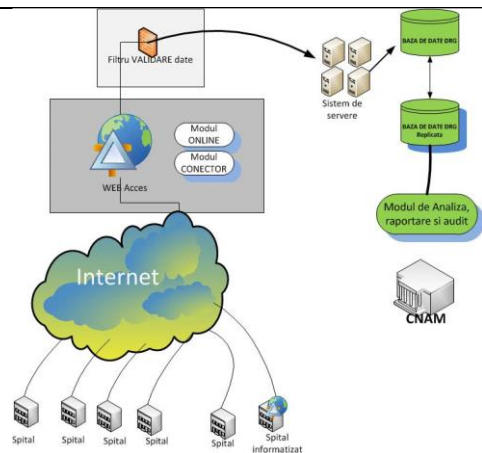
- **Securitatea schimbului de date.** Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atât la nivelul canalului de comunicație cât și la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit.** Toate operațiunile efectuate de utilizatori sau de către alte sisteme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

- 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:

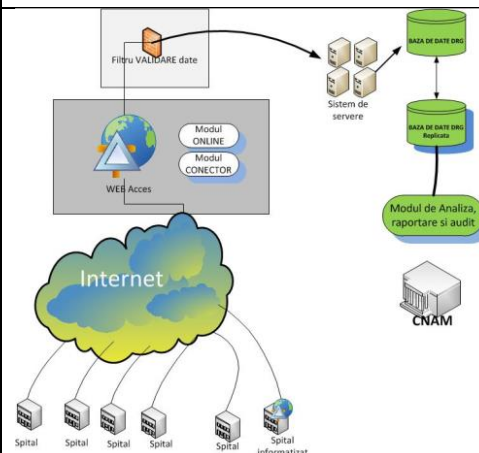


Componentele DRG sunt operaționale și sunt prezente conform modulelor:

- ✓ 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);

Asumam intelegerea arhitecturii 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:



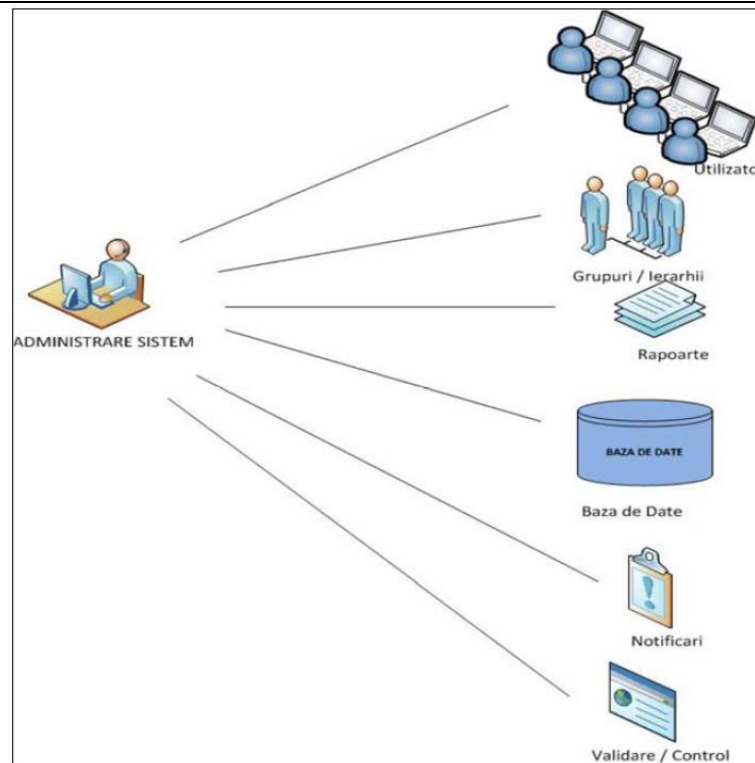
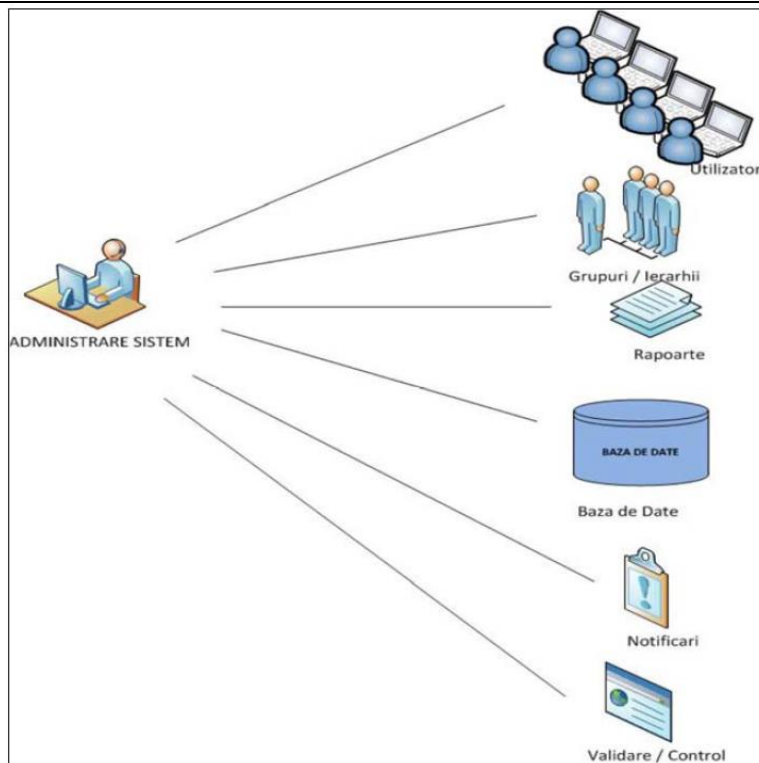
Am luat la cunostinanta cu lista de componentele DRG sunt operaționale și sunt prezente conform modulelor:

- ✓ 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);

<ul style="list-style-type: none"> ✓ Modulul de Analiză la nivel de Baza de Date; ✓ Modul conector pentru Auditul Codificării. 	<ul style="list-style-type: none"> ✓ Modulul de Analiză la nivel de Baza de Date; ✓ Modul conector pentru Auditul Codificării.
<p>Modulul de administrare sistem colector</p> <p>În cadrul acestui modul se execută:</p>	<p>Am luat la cunostinta si asumam intelegerea pentru modulul de administrare system colector</p> <p>În cadrul acestui modul se execută:</p>
<ul style="list-style-type: none"> ➤ 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. 	<ul style="list-style-type: none"> ➤ 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.
<ul style="list-style-type: none"> ➤ 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: <ul style="list-style-type: none"> ➤ 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; 	<ul style="list-style-type: none"> ➤ 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: <ul style="list-style-type: none"> ➤ 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.

- 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.



Nivelul de acces al acestui modul:

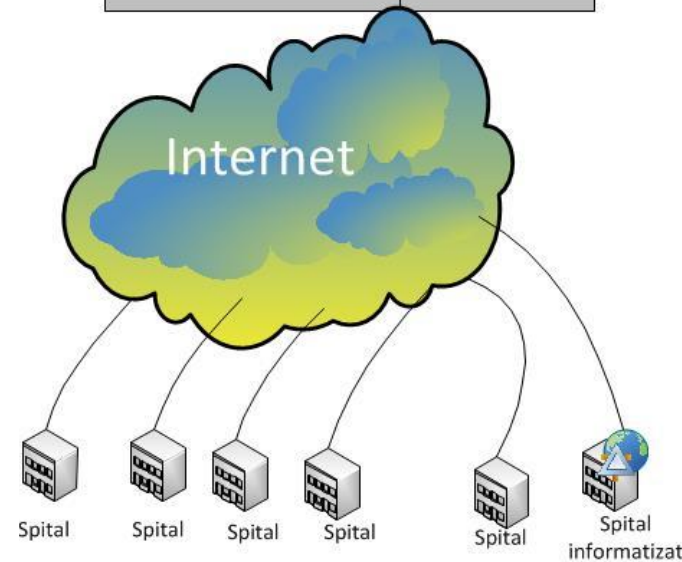
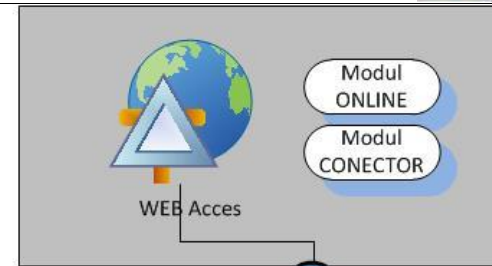
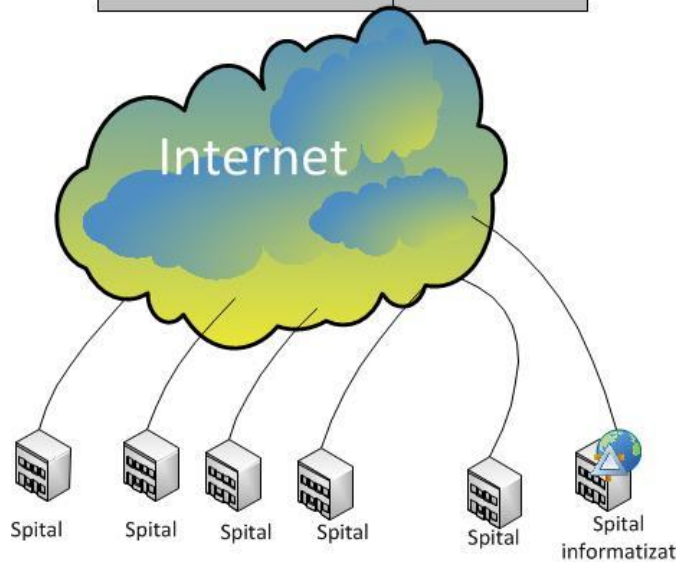
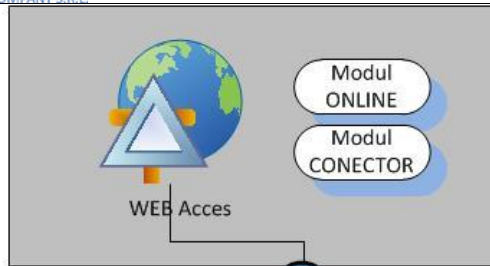
- modulul care are acces la toate nivelurile sistemului;
- doar administratorii sistemului au acces la acest modul, în vederea efectuării operațiilor necesare funcționării normale a sistemului.

Asumam înțelegerea că nivelul de acces al acestui modul este caracterizat de:

- 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.

<p>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.</p>	<p>Am luat cunostinta ca 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.</p>
<p>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.</p>	<p>Intelegem si asumam ca 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.</p>
<p>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.</p>	<p>Asumam intelegerea ca 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.</p>

<p>Modulul de colectare date Real Time</p> <p>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.</p>	<p>Asumam intelegerea functionarii pentru modulul de colectare date Real Time:</p> <p>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.</p>
<p>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.</p>	<p>Am luat cunostinta si intelegem ca 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.</p>
<p>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.</p>	<p>Confirmam intelegerea modalitatii de prelucrare a datelor prin care 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.</p>



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.

Intelegem ca 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. De asemenea ca 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

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

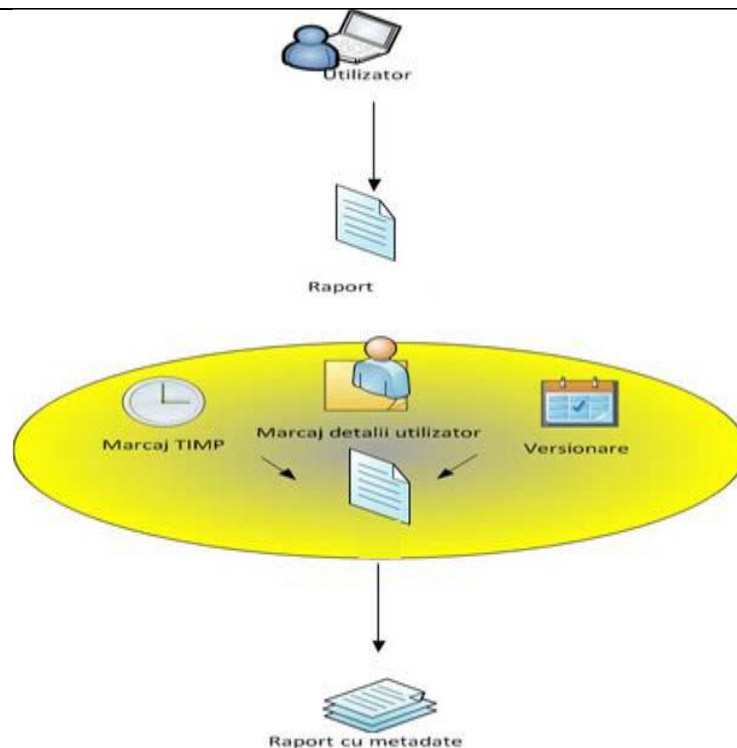
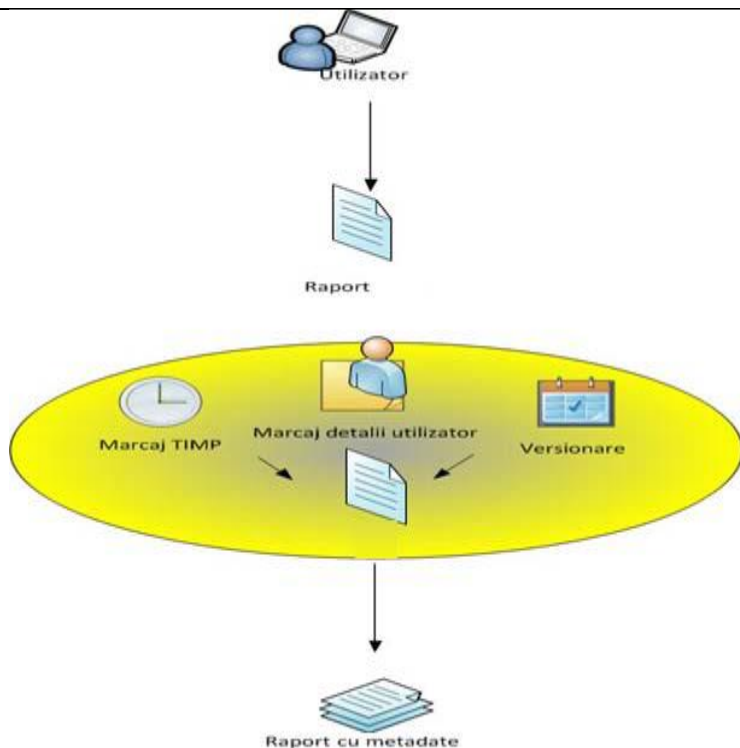
<p>tratat. Modul prenotat are capacitatea de a trece în analiza sau chiar să elimine activitățile suspecte sau lipsite de fond.</p>	<p>tratat. Modul prenotat are capacitatea de a trece în analiza sau chiar să elimine activitățile suspecte sau lipsite de fond.</p>
<p>Modulul are și rolul de a elimina 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.</p>	<p>Asumam intelegerea faptului ca 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 si ca 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.</p>
<p>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.</p>	<p>Intelegem modalitatea prin care se elimină 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.</p>
<p>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.</p>	<p>Asumam intelegerea faptului ca, 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.</p>
<p>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.</p>	<p>Intelegem ca 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.</p>

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.

Asumam intelegerea functionarii pentru 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.



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

Confirmam intelegerea faptului ca 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

<p>utilizator primește prin intermediul acestui modul un pachet de metadata care conține:</p>	<p>transferat de către un utilizator primește prin intermediul acestui modul un pachet de metadata care conține:</p>
<ul style="list-style-type: none"> ✓ Data și ora la care au fost transmise fișierele către sistem; ✓ Numele utilizatorului care a transmis fișierul; pentru fiecare fișier în parte se atașează metadatale corespunzătoare. Sistemul face automat asocierea între utilizator și fișierul transmis. ✓ Numele utilizatorului care a rescris ultima versiune a fișierului – va fi stabilit în faza de analiză, în funcție de particularitățile observate; 	<ul style="list-style-type: none"> ✓ Data și ora la care au fost transmise fișierele către sistem; ✓ Numele utilizatorului care a transmis fișierul; pentru fiecare fișier în parte se atașează metadatale corespunzătoare. Sistemul face automat asocierea între utilizator și fișierul transmis. ✓ Numele utilizatorului care a rescris ultima versiune a fișierului – va fi stabilit în faza de analiză, în funcție de particularitățile observate;
<p>Aceste informații sunt disponibile atât administratorilor și, parțial, utilizatorilor. Adăugarea metadatelor la fișiere este o operațiune pe care modulul de nerepudiare 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.</p>	<p>Intelegm modul de prelucrare a datelor precum ca aceste informații sunt disponibile atât administratorilor și, parțial, utilizatorilor. Adăugarea metadatelor la fișiere este o operațiune pe care modulul de nerepudiare 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.</p>

Modulul de validare

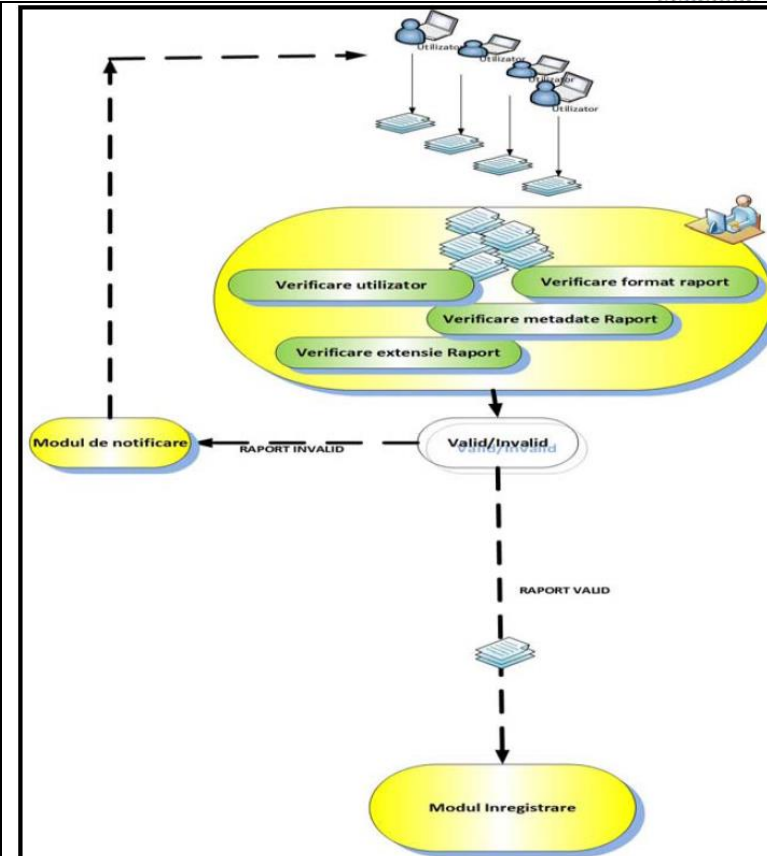
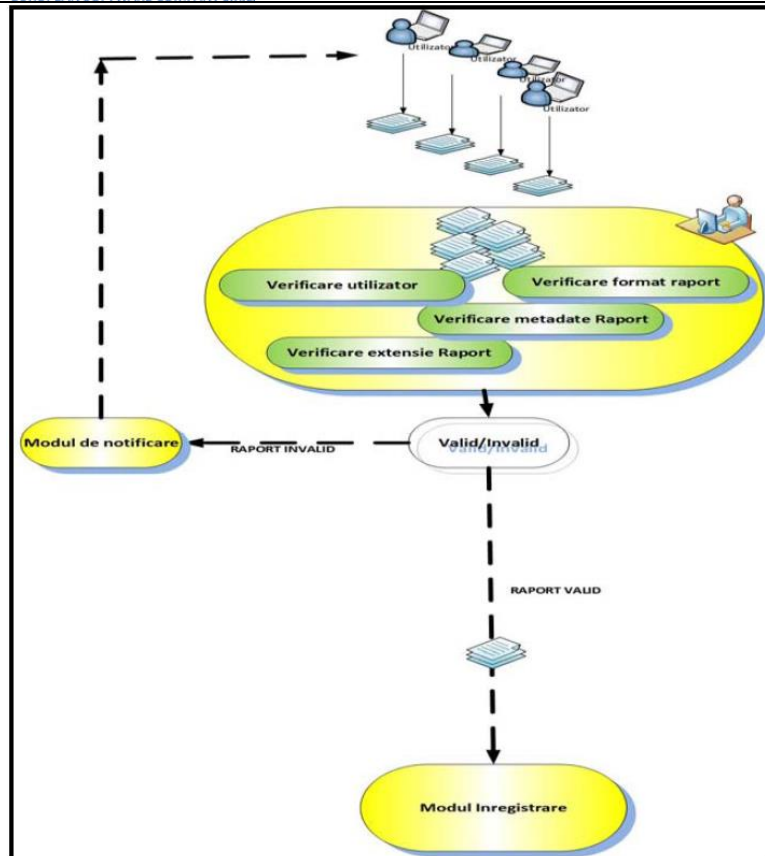
DRG reduce situațiile în care utilizatorii trimit setul minim de date la nivel de pacient al căror format este necorespunzător.

- 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 elimină la timp cât mai multe cazuri în care apare eroarea umană.

Asumam înțelegerea funcționării pentru 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 elimină la timp cât mai multe cazuri în care apare eroarea umană.



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

Asumam intelegerea functionarii pentru 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:

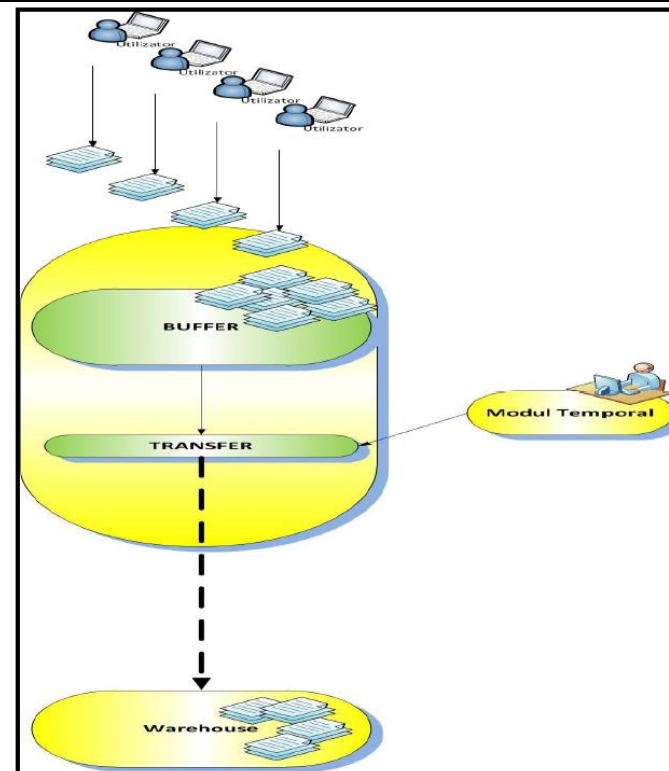
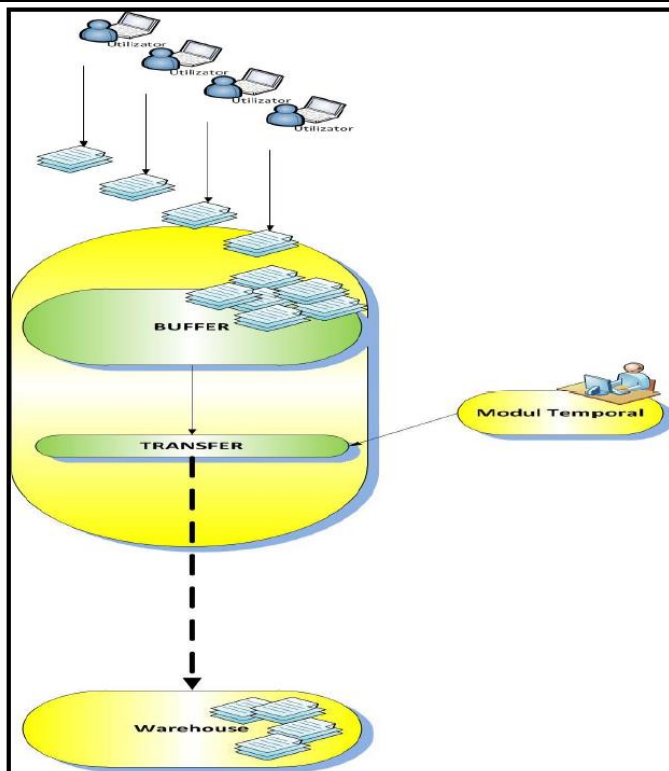
1. Componenta „buffer”, temporară, care colectează toate raportările utilizatorilor în toate versiunile pe care

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.

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.



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

- i. „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.
- ii. „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.

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

- i. „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.
- ii. „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 permanentă între utilizatori, beneficiari și entitatea informatică:

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

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

✓ **Audit:** aceasta funcție a modulului identifică acțiunile desfășurate de către un utilizator, în mod cronologic; în cazul apariției unei probleme, la nivel de administrator de sistem, se poate vedea istoricul operațiilor desfășurate de orice utilizator în vederea identificării și corectării problemei. Sunt vizibile atât informațiile referitoare la logarile în sistem cât și cele referitoare la fișierele cu care utilizatorul a operat. Funcția de audit folosește în mod implicit modulul de nerepudiare care asigură orice investigație ca datele existente în sistem sunt cele corecte și ca asocierea între conținutul informatic și activitatea umană este incontestabilă.

Asumăm înțelegerea funcționării pentru modulul de setări, raportare și audit

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

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

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

✓ **Audit:** aceasta funcție a modulului identifică acțiunile desfășurate de către un utilizator, în mod cronologic; în cazul apariției unei probleme, la nivel de administrator de sistem, se poate vedea istoricul operațiilor desfășurate de orice utilizator în vederea identificării și corectării problemei. Sunt vizibile atât informațiile referitoare la logarile în sistem cât și cele referitoare la fișierele cu care utilizatorul a operat. Funcția de audit folosește în mod implicit modulul de nerepudiare care asigură orice investigație ca datele existente în sistem sunt cele corecte și ca asocierea între conținutul informatic și activitatea umană este incontestabilă.

Modulul Depozit (Warehouse)

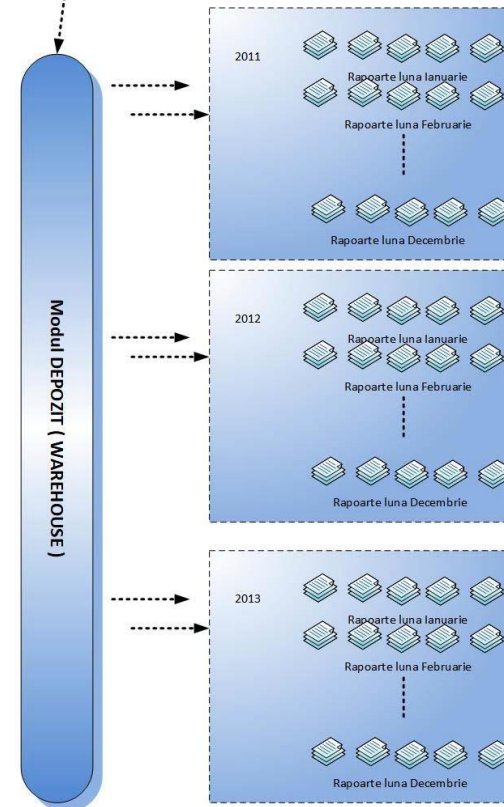
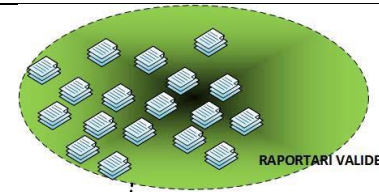
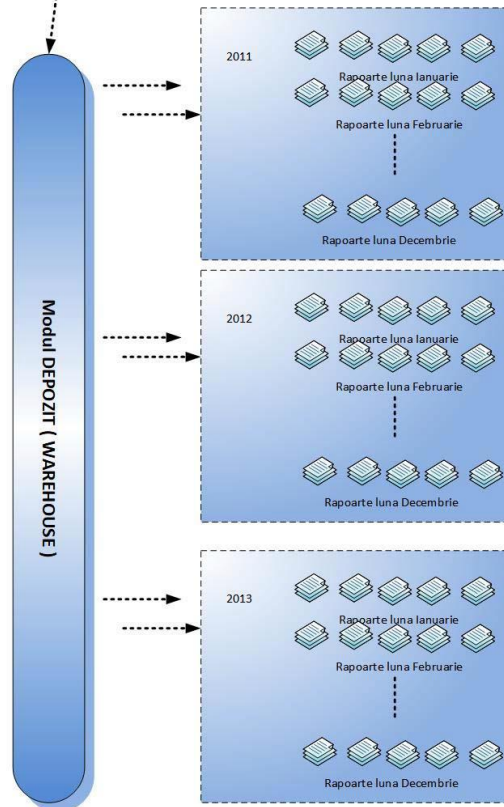
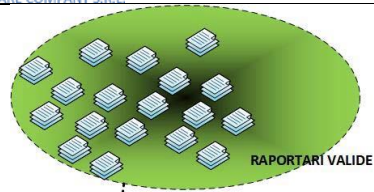
În cadrul fluxului de colectare de către sistem a raportărilor de la instituțiile medicale, Modulul Depozit (warehouse) este componenta finală, cea care deține datele necesare prelucrării. Aici se găsesc informațiile utile Beneficiarului, motiv pentru care acestea:

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

Asumam înțelegerea funcționării pentru modulul Depozit (Warehouse)

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

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



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

Asumam intelegerea detaliilor privind zona de stocare a Modulului Depozit (warehouse) poate fi controlată atât de administratorii sistemului DRG cât și de inginerii de sistem informatic MCloud.

<i>Modulul de Analiză la nivel de Baza de Date</i>	Asumam intelegerea functionarii pentru modulul de Analiză la nivel de Baza de Date
<p>Sistemul DRG creează în mod dinamic o bază de date actualizată 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 neconcordanțe ulterioare în diagnosticarea pacientului.</p>	<p>Sistemul DRG creează în mod dinamic o bază de date actualizată 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 neconcordanțe ulterioare în diagnosticarea pacientului.</p>
<p>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.</p>	<p>Întelegem că 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.</p>
<p>Modulul de analiză, raportare și audit poate fi utilizat de departamentele autorizate ale CNAM în vederea generării de rapoarte bazate pe template-uri, dar și ad-hoc, utile în activitatea curentă. Sistemul răspunde următoarelor solicitări:</p>	
<p>1) Evitarea fraudării. Sistemul SI DRG este un sistem operațional la nivel național, iar CNAM dispune de o bază de date unică, cu informații reale; veridicitatea informațiilor se verifică în două feluri:</p> <ul style="list-style-type: none"> - <u>în timp real:</u> respingerea informațiilor eronate cu atenționarea celui care introduce datele; sistemul nu permite introducerea de date necorespunzătoare. - <u>în urma auditării:</u> 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 personalizate în așa fel încât echipele care execută auditarea și evaluarea să obțină o listă consistentă și reală pe care să o verifice și în teren. Prin utilizarea sistemului informatic pot fi identificate cazurile de fraudare. 	<p>1) Evitarea fraudării. Sistemul SI DRG este un sistem operațional la nivel național, iar CNAM dispune de o bază de date unică, cu informații reale; veridicitatea informațiilor se verifică în două feluri:</p> <ul style="list-style-type: none"> - <u>în timp real:</u> respingerea informațiilor eronate cu atenționarea celui care introduce datele; sistemul nu permite introducerea de date necorespunzătoare. - <u>în urma auditării:</u> 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 personalizate în așa fel încât echipele care execută auditarea și evaluarea să obțină o listă consistentă și reală pe care să o verifice și în teren. Prin utilizarea sistemului informatic pot fi identificate cazurile de fraudare.

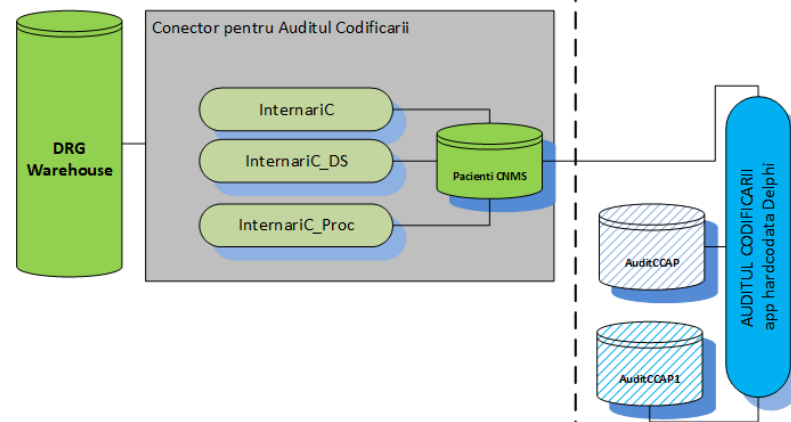
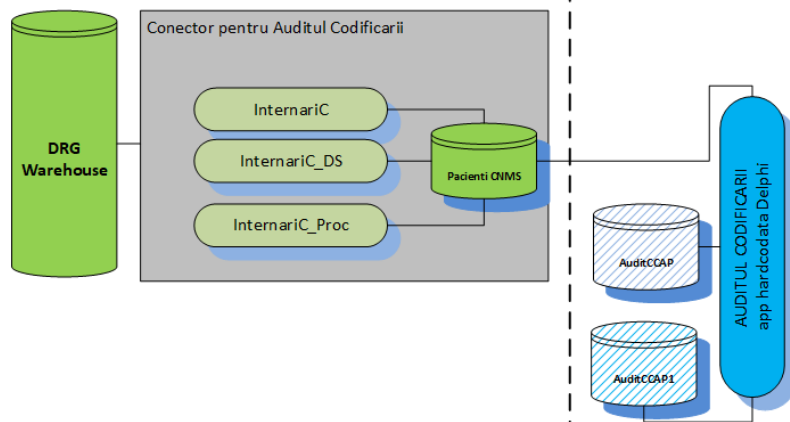
<p>2) Creșterea eficienței. Existența modulului de analiză, raportare și audit la nivelul CNAM constituie un instrument pe care departamentele autorizate CNAM implicate în raportare îl folosesc în vederea creșterii eficienței de lucru. Căutările sunt rapide, rapoartele sunt generate cu mare ușurință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

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 execută auditul codificării prin operațiuni care nu afectează aplicația ci doar baza de date. Astfel operatorii Autorității Contractante care efectuează auditul codificării continuă să folosească vechea aplicație hardcodată care folosește date din warehouse-ul DRG.

Asumam si confirmam functionarea pentru modulul conector pentru Audit al codificarii

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 execută auditul codificării prin operațiuni care nu afectează aplicația ci doar baza de date. Astfel operatorii Autorității Contractante care efectuează auditul codificării continuă să folosească vechea aplicație hardcodată care folosește date din warehouse-ul DRG.



CNAM va continua să emită fie solicitări de dezvoltare a sistemului CCAP, fie de execuție a unor proceduri la nivelul bazelor de date și conectorilor în scopul obținerii rezultatelor dorite până la momentul includerii definitive în CCAP a funcționalităților de audit al codificării. În prezenta procedura de achiziție CNAM solicită operațiuni de mentenanță care se referă exclusiv la

Am luat la cunostinta ca 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 si ca in prezenta procedura de achiziție CNAM solicită operațiuni de mentenanță care se

<p>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.</p>	<p>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.</p>
<p>Codul dezvoltat în sensul susținerii modului de conectare pentru auditul codificării permite operatorilor de audit să desfășoare în cadrul vechii aplicații două operațiuni:</p> <ul style="list-style-type: none"> ➤ Selectarea fișelor medicale a bolnavului spitalizat pentru audit (Database DRG). ➤ Importul fișelor medicale din "Database DRG" în aplicație și efectuarea auditului. 	<p>Am luat la cunostinta ca codul dezvoltat în sensul susținerii modului de conectare pentru auditul codificării permite operatorilor de audit să desfășoare în cadrul vechii aplicații două operațiuni:</p> <ul style="list-style-type: none"> ➤ Selectarea fișelor medicale a bolnavului spitalizat pentru audit (Database DRG). ➤ Importul fișelor medicale din "Database DRG" în aplicație și efectuarea auditului.
<p>CNAM deține codul sursa necesar pentru prelucrarea noii baze de date Pacienți CNMS și asupra view-urilor de internări [InternariC, InternariC_DS, InternariC_Proc] și ListaSpitale, care colectează și interpretează informațiile din baza de date Wodehouse a DRG, acestea intrând în obiectul operațiunilor de mentenanță pe care urmează să le desfășoare furnizorul serviciilor.</p>	<p>Am luat la cunostinta ca CNAM deține codul sursa necesar pentru prelucrarea noii baze de date Pacienți CNMS și asupra view-urilor de internări [InternariC, InternariC_DS, InternariC_Proc] și ListaSpitale, care colectează și interpretează informațiile din baza de date Wodehouse a DRG, acestea intrând în obiectul operațiunilor de mentenanță pe care urmează să le desfășoare furnizorul serviciilor.</p>
<p>În prezent, la procedura de audit al codificarii prin intermediul aplicatiei CCAP nu este posibilă logarea/autentificarea concomitentă a Auditorilor I/II în aplicație și ca urmare nu este posibilă analiza concomitentă/independentă de către Auditor I și Auditor II a fișelor supuse auditului. În acest context, CNAM solicită analiza subiectului prenotat, și ajustarea compartimentului conform solicitării. Totodată, CNAM subliniază faptul ca, în cazul în care nu este posibilă ajustarea propriu-zisă a conexiunii concomitente în CCAP, CNAM solicită reingineria modulului de audit al codificării în SI DRG.</p>	<p>Intelegem si asumam ca in prezent, la procedura de audit al codificarii prin intermediul aplicatiei CCAP nu este posibilă logarea/autentificarea concomitentă a Auditorilor I/II în aplicație și ca urmare nu este posibilă analiza concomitentă/independentă de către Auditor I și Auditor II a fișelor supuse auditului. În acest context, CNAM solicită analiza subiectului prenotat, și ajustarea compartimentului conform solicitării. Totodată, CNAM subliniază faptul ca, în cazul în care nu este posibilă ajustarea propriu-zisă a conexiunii concomitente în CCAP, CNAM solicită reingineria modulului de audit al codificării în SI DRG.</p>
<p>Cerințe de Mentenanță preventivă și Suport</p>	<p>Servicii oferitate de Mentenanță preventivă și Suport</p>

<p>Cerințele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanță elaborat de Prestator și aprobat de Beneficiar.</p>	<p>Am luat la cunostinta ca cerințele CNAM asupra serviciilor de mentenanță preventivă, reflectate în acest capitol sunt orientate spre identificare și înlăturarea defectelor ascunse înainte ca acestea să se manifeste și organizarea proceselor în așa mod încât să permită înlăturarea incidentelor în cazul apariției acestora, în timp restrâns și cu pierderi minime. Totodată, prestarea serviciilor vor fi realizate în conformitate cu un plan de mentenanță elaborat de Prestator și aprobat de Beneficiar.</p>
<p>De menționat că prin procesul de mentenanță se controlează funcționarea produsului software, se înregistrează problemele pentru analiză, se întreprind acțiuni de avertizare și de corecție, precum și acțiuni de adaptare și de perfecționare a produsului software. Scopul procesului de mentenanță constă în menținerea capacității sistemului software de a presta servicii, precum și în modificarea produsului software, păstrînd integritatea lui.</p> <p>Pentru mentenanță sistemului DRG, CNAM formulează următoarele cerințe:</p>	<p>Confirmam că prin procesul de mentenanță se controlează funcționarea produsului software, se înregistrează problemele pentru analiză, se întreprind acțiuni de avertizare și de corecție, precum și acțiuni de adaptare și de perfecționare a produsului software. Scopul procesului de mentenanță constă în menținerea capacității sistemului software de a presta servicii, precum și în modificarea produsului software, păstrînd integritatea lui.</p> <p>Pentru mentenanță sistemului DRG, CNAM formulează următoarele cerințe:</p>
<ul style="list-style-type: none"> ➤ 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 și soluționarea incidentelor; ➤ Analiza parametrilor de funcționare a sistemului; ➤ Identificarea și raportarea riscurilor potențiale; ➤ Actualizarea parametrilor existenți în partea utilizatorilor, conform cerințelor legislației în vigoare (spre exemplu: actualizarea/completarea nomenclatoarelor programelor special, diagnosticelor, procedurilor, spitalelor, rapoartelor, modificarea valorilor relative, aplicarea/anularea aplicării KP, 	<ul style="list-style-type: none"> ➤ 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 și soluționarea incidentelor; ➤ Analiza parametrilor de funcționare a sistemului; ➤ Identificarea și raportarea riscurilor potențiale; ➤ Actualizarea parametrilor existenți în partea utilizatorilor, conform cerințelor legislației în vigoare (spre exemplu: actualizarea/completarea nomenclatoarelor programelor special, diagnosticelor, procedurilor, spitalelor, rapoartelor, modificarea valorilor relative, aplicarea/anularea aplicării KP,

completarea/modificarea algoritmilor de validare și excepțiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora, conform formatului solicitat și menținerea posibilităților de extragere a datelor de către utilizator.

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

completarea/modificarea algoritmilor de validare și excepțiilor de aplicare regulilor de validare, etc), inclusiv asigurarea generării acestora, conform formatului solicitat și menținerea posibilităților de extragere a datelor de către utilizator.

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

Support 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.

Servicii oferite pentru suportul Utilizatorilor

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

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

Suport platforma software

Servicii dedicate Sistemelor de Operare

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

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

Oferta servicii de suport platforma software

Servicii oferite, dedicate Sistemelor de Operare

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

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

informatice proprii.

Servicii dedicate sistemelor de gestiune a bazelor de date

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

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corectă a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidențialității și securității datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerințelor de securitate informațională de către utilizatori, să documenteze și să raporteze cazurile și tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea și lichidarea consecințelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securității privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale DRG și mijloacelor software folosite pentru

informatice proprii.

Servicii oferite, dedicate sistemelor de gestiune a bazelor de date

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

- actualizarea sistemului de gestiune al bazelor de date și a tool-urilor sale conform licenței deținute de către CNAM;
- recomandări privind alocarea corectă a tipului și spațiului de disk;
- asigurarea implementării măsurilor tehnice necesare pentru asigurarea confidențialității și securității datelor cu caracter personal;
- modificarea structurii bazei de date în funcție de cerințele aplicației;
- activarea utilizatorilor și menținerea securității sistemului de gestiune a bazei de date;
- supravegherea respectării cerințelor de securitate informațională de către utilizatori, să documenteze și să raporteze cazurile și tentativele de încălcare a acestora, să întreprindă măsurile necesare pentru prevenirea, limitarea și lichidarea consecințelor cu informarea ulterioară a Beneficiarului.
- verificarea continuă și asigurarea condițiilor impuse de tipul de licențiere;
- controlarea și monitorizarea accesului utilizatorilor la baze de date;
- efectuarea auditului securității privind gestiunea datelor cu caracter personal;
- monitorizarea și optimizarea performanței bazei de date;
- planificarea conform procedurii elaborate a backup-ului și restaurării datelor și aplicației;
- Planificarea backup-ului, generearea copii de rezervă ale DRG și mijloacelor software folosite pentru

<p>prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum și restaurarea acestora.</p> <ul style="list-style-type: none"> ➤ orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date. 	<p>prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate) precum și restaurarea acestora.</p> <ul style="list-style-type: none"> ➤ orice alte activități care au drept scop funcționarea corectă și în condiții de securitate a bazei de date.
<p><i>Servicii dedicate componentelor, inclusiv a celor de interoperabilitate</i></p> <p>În această categorie intră următoarele servicii minime relative la codul aplicației DRG care vor fi desfășurate de către Furnizor:</p> <ul style="list-style-type: none"> ➤ verifică și optimizează secvențele de cod; ➤ identifică și analizează problemele și potențialele probleme de la nivelul codului; ➤ rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației; ➤ soluționează incidentele apărute la nivelul codului; ➤ modifică rapoartele, șabloanele, serviciile aplicative; ➤ comunică cu echipele de suport în scopul funcționării corecte și permanente a sistemului. 	<p><i>Servicii oferite, dedicate componentelor, inclusiv a celor de interoperabilitate</i></p> <p>În această categorie intră următoarele servicii minime relative la codul aplicației DRG care vor fi desfășurate de către Furnizor:</p> <ul style="list-style-type: none"> ➤ verifică și optimizează secvențele de cod; ➤ identifică și analizează problemele și potențialele probleme de la nivelul codului; ➤ rezolvă și/sau face recomandări privind cerințele de utilizare și interfața a aplicației; ➤ soluționează incidentele apărute la nivelul codului; ➤ modifică rapoartele, șabloanele, serviciile aplicative; ➤ comunică cu echipele de suport în scopul funcționării corecte și permanente a sistemului.

Efectuarea testelor de penetrare

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

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

Efectuarea testelor de penetrare

Intelegem si asumam teste de penetrare ce 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.

Am luat la cunostinta si asumam ca toate operațiunile se vor desfășura în condițiile unei strânse comunicări cu specialiștii Cloud-ului guvernamental și a menținerii calității și securității sistemului. Confirmam si justificam ca specialiștii nostri dețin 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.

Prin oferta asumam desfasurarea urmatoarelor 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. Am luat la cunostinta ca 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

Intelegem si asumam ca orice modificare asupra codului

<p>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.</p>	<p>sursa are ca efect o nouă versiune operațională a aplicației, conforma legislației. Confirmam că deținem cunoștințele necesare bunei desfășurări a acestor operațiuni și întreținerea noilor versiuni ale aplicației pe toată perioada desfășurării contractului.</p>
<p>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:</p> <ul style="list-style-type: none"> ✓ 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. <p>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:</p>	<p>Asumam ca 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:</p> <ul style="list-style-type: none"> ✓ 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. <p>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:</p>
<p>Reguli de Validare</p> <ul style="list-style-type: none"> ➤ 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 	<p>Reguli de Validare</p> <ul style="list-style-type: none"> ➤ 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

<p>ID-urilor unice.</p>	<p>ID-urilor unice.</p>
<p>Întreținerea bazei de date a sistemului</p> <ul style="list-style-type: none"> ➤ 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. 	<p>Întreținerea bazei de date a sistemului</p> <ul style="list-style-type: none"> ➤ 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.
<p>Rapoarte CNAM</p> <ul style="list-style-type: none"> ➤ 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. 	<p>Rapoarte CNAM</p> <ul style="list-style-type: none"> ➤ 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.
<p>Cerințe de mentenanță adaptivă și corectivă a DRG</p> <p>Asumarea contextului adaptării și corecției software</p>	<p>Oferta de mentenanță adaptivă și corectivă a DRG</p> <p>Asumarea contextului adaptării și corecției software</p>
<p>În categoria serviciilor de mentenanță adaptivă și corectivă a DRG intră acele servicii necesare pentru adaptarea și corecția sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul "A. Cerințe de Mentenanță preventivă și Suport".</p>	<p>În categoria serviciilor de mentenanță adaptivă și corectivă a DRG intră acele servicii necesare pentru adaptarea și corecția sistemului sau a parametrilor acestuia cu excepția celor indicate în capitolul "A. Cerințe de Mentenanță preventivă și Suport".</p>
<p>Contextul în care Furnizorul va desfășura serviciile contractate este următorul:</p> <ul style="list-style-type: none"> ➤ 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 	<p>Am luat la cunostinta si asumam contextul în care vom desfășura serviciile contractate este următorul:</p> <ul style="list-style-type: none"> ➤ 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

<p>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.</p>	<p>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.</p>
<p>➤ 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.</p>	<p>➤ Confirmam ca 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.</p>
<p>➤ 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.</p>	<p>➤ 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.</p>
<p>➤ 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.</p>	<p>➤ 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.</p>
<p>➤ 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.</p>	<p>➤ 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.</p>
<p>➤ 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 defectiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în</p>	<p>➤ 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 defectiunile aplicației în perioada de garanție vor fi suportate de către Furnizor în</p>

condițiile legii.	condițiile legii.
<p>➤ În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatearea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.</p>	<p>➤ În cazul eventualelor incidente generate de operațiuni executate de Furnizor sau de lipsa de execuție a unor operațiuni obligatorii (updatearea configurației, patch-uri, etc) care conduc la alterarea configurației operaționale a sistemului, Furnizorul asumă cheltuielile de repunere în producție.</p>
<p>➤ Ofertanții trebuie să demonstreze experiența acumulată și a performanțelor în ajustarea și prestarea ulterioară a serviciilor de suport și menținere SIA integrate de complexitate asemănătoare prin descrierea proiectelor de mentenanță SI complexe bazate pe tehnologiile similare.</p>	<p>➤ A se vedea documentele justificative.</p>
<p>➤ 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.</p>	<p>➤ Intelegem și asumăm ca 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 este pregătită în sensul cunoașterii amănunțite a modului în care funcționează întregul sistem și deține resursele necesare unor solicitări cu termene de realizare foarte scurte. Totodată, avem 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.</p>
CNAM solicită în prezenta procedura disponibilitatea specialiștilor și cere Ofertanților specificarea în Oferta financiară a prețului pentru minim 900 de ore pentru cererile suplimentare de ordin tehnic dedicate ajustării și consultanței software a	A se vedea oferta financiară.

<p>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.</p>	
<p>Reguli privind prestare a serviciilor de mentenanță adaptivă și corectivă</p> <p>Serviciile de mentenanță adaptivă și corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.</p>	<p>Reguli privind prestare a serviciilor de mentenanță adaptivă și corectivă</p> <p>Serviciile de mentenanță adaptivă și corectivă sunt orientate spre asigurarea efectuării modificărilor/adăugărilor funcționalităților ca urmare al modificării cadrului legal sau îmbunătățirii esențiale a business proceselor.</p>
<p>Solicitarea serviciilor de mentenanță adaptivă și corectivă</p> <p>Solicitarea serviciilor de mentenanță adaptivă și corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.</p> <p>În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului și a costului estimativ conform tarifelor.</p>	<p>Oferta privind solicitarea serviciilor de mentenanță adaptivă și corectivă</p> <p>Solicitarea serviciilor de mentenanță adaptivă și corectivă se efectuează de Beneficiar în baza unei Cereri cu privire la propunerea de modificare.</p> <p>În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului și a costului estimativ conform tarifelor.</p>
<p>Prestarea serviciilor de mentenanță adaptivă și corectivă</p> <p>Prestarea serviciilor de mentenanță adaptivă și corectivă se va efectua cu aplicarea următoarelor reguli:</p>	<p>Oferta privind prestarea serviciilor de mentenanță adaptivă și corectivă</p> <p>Prestarea serviciilor de mentenanță adaptivă și corectivă se va efectua cu aplicarea următoarelor reguli:</p>
<p>➤ Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului și acceptării rezultatului de către Beneficiar.</p>	<p>➤ Termenul de prestare a serviciului include timpul necesar Prestatorului colectării informației, documentării, analizei, prestării nemijlocite a serviciului și acceptării rezultatului de către Beneficiar.</p>

<ul style="list-style-type: none"> ➤ Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar. 	<ul style="list-style-type: none"> ➤ Serviciul se consideră prestat în momentul confirmării acceptării soluției de către Beneficiar.
<ul style="list-style-type: none"> ➤ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarificare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei și rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare. 	<ul style="list-style-type: none"> ➤ Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarificare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei și rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.
<ul style="list-style-type: none"> ➤ Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute și acceptate, și a standardelor agreeate de Beneficiar, ținând cont și de ultimele cerințe în materie de elaborare, și calculate în baza tarifelor convenite de părți. 	<ul style="list-style-type: none"> ➤ Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare, în baza unor proceduri general recunoscute și acceptate, și a standardelor agreeate de Beneficiar, ținând cont și de ultimele cerințe în materie de elaborare, și calculate în baza tarifelor convenite de părți.
<ul style="list-style-type: none"> ➤ Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor și condițiilor înaintate de Beneficiar. 	<ul style="list-style-type: none"> ➤ Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare, conform cerințelor și condițiilor înaintate de Beneficiar.
<p>Cerințe privind calitatea serviciilor</p> <p>Mod de lucru. Modalități de intervenție</p>	<p>Oferta privind calitatea serviciilor</p> <p>Oferta privind mod de lucru. Modalități de intervenție</p>
<p>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.</p>	<p>Asumam intelegerea faptului ca 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.</p>
<p>Pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul</p>	<p>Confirmam ca pe perioada contractului vor fi disponibile din partea Furnizorului următoarele modalități de intervenție în cazul</p>

<p>incidentelor dar și pentru operațiuni normale de întreținere:</p>	<p>incidentelor dar și pentru operațiuni normale de întreținere:</p>
<ul style="list-style-type: none"> ➤ Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental 	<ul style="list-style-type: none"> ➤ Intervenții de la distanță securizată. Se vor respecta recomandările specialiștilor cloud-ului guvernamental
<ul style="list-style-type: none"> ➤ Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință. 	<ul style="list-style-type: none"> ➤ Intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință.
<ul style="list-style-type: none"> ➤ Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației. 	<ul style="list-style-type: none"> ➤ Intervenții on-site la sediul central sau în teritoriu, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Serviciul de Suport Client “Hot-Line”

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

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

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

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

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

Reguli față de procesul de aplicare a modificărilor

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

Serviciul de Suport Client “Hot-Line”

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

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

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

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

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

Reguli față de procesul de aplicare a modificărilor

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

Reguli privind prestare a serviciilor de suport

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

Reguli privind prestare a serviciilor de suport

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

Clasificarea incidentelor

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

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

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

Clasificarea incidentelor

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

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

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

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

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

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

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

Tabelul 2. Matricea de estimare a urgenței incidentului

URGENȚĂ	Descriere

Tabelul 2. Matricea de estimare a urgenței incidentului

URGENȚĂ	Descriere

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

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere
--------	-----------

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

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere
--------	-----------

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

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

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

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

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

Alte cerințe și reguli privind prestarea serviciilor

Soluționarea divergențelor

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

- Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv experți independenți.
- La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.
- Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Alte cerințe și reguli privind prestarea serviciilor

Soluționarea divergențelor

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

- Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv experți independenți.
- La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.
- Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite.
- Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informației

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

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

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

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

- Colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiții ce asigură integritatea copiilor de rezervă efectuate;
- Menținerea formalizată a Registrului privind deținerea probelor conservate (chain of custody).

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

Securitatea informației

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

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

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

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

- Colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea;
- Efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiții ce asigură integritatea copiilor de rezervă efectuate;
- Menținerea formalizată a Registrului privind deținerea probelor conservate (chain of custody).

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

<p>Livrabile</p> <p>Prestatorul menține în stare actuală documentația tehnică. Documentația conține suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.</p> <p>Prestatorul va notifica Beneficiarul despre noile versiuni și modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.</p> <p>La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:</p> <ul style="list-style-type: none"> ➤ 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. 	<p>Livrabile</p> <p>Prestatorul menține în stare actuală documentația tehnică. Documentația conține suficientă informație pentru ca orice echipă de dezvoltatori soft terți să poată prelua serviciile de mentenanță.</p> <p>Prestatorul va notifica Beneficiarul despre noile versiuni și modificările importante, la documentația tehnică aferentă softului aplicativ destinată Beneficiarului.</p> <p>La finalizarea Contractului Prestatorul va asigura predarea și înnoirea următoarelor livrabile:</p> <ul style="list-style-type: none"> ➤ 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.
<p>Modalitatea de întocmire a ofertelor</p> <p>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.</p>	<p>Oferta a fost întocmită în conformitate cu cerințele specificate de către Autoritatea Contractantă în documentația publicată.</p>
<p>Cerințe privind experiența personalului</p>	<p>Experiența personalului implicat în realizarea serviciilor</p>
<p>Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective.</p> <p>În cazul concediilor (ex: de odihnă, concedii medicale,</p>	<p>Am luat cunoștința</p>

<p>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.</p>	
<p>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.</p>	<p>Am luat cunostinta</p>
<p>CNAM a identificat următoarele cerințe minime privind experiența pe care trebuie să o dețină echipa de mentenanță a ofertantului:</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Manager de proiect (minim 1 persoană)</p> <ul style="list-style-type: none"> – 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. </div>	<p>A se vedea documentele justificative.</p>

- 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 BusinessAnalitic.
- 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 similar

(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;

<ul style="list-style-type: none"> – Experiență demonstrată în testarea performanței și încărcării sistemelor informaționale; – Experiență dobândită de minim 2 ani în testarea produselor software de complexitate similară <i>(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).</i> 	
<p>2. Documente obligatorii la depunerea ofertei</p>	<p>A se vedea documentele justificative</p>
<p>3. Documente obligatorii la evaluarea ofertelor</p>	<p>A se vedea documentele justificative.</p>