Servicii de actualizare, modernizare și dezvoltare pentru

Sistemul Informațional de Evidență a pacientului CSPT (SIYK)

CAIET DE SARCINI

CUPRINS

Denumire

Sistemul Informațional de Evidență a pacientului (în continuare SIYK), este un sistem informatic care permite informatizarea proceselor de business cheie ale *Centrelor de Sănătate Prietenoase Tinerilor (*în continuare CSPT*).* Dezvoltarea sistemului a presupus activități de analiza in care au fost implicați Prestatori externi de soluții software cat si specialiști CSPT. În prezent sistemul este operațional la nivel CSPT si este considerat un succes pentru scopul adresat. Sistemul informatic SIYK este găzduit în Cloud-ul Guvernamental.

Referințe. Cadrul legal. Baza Juridica. Acte normative

Baza normativă sub care se desfășoară proiectul include legislația națională în vigoare, convențiile și tratatele internaționale, la care Republica Moldova este parte. Crearea și funcționarea sistemelor informaționale este reglementată de următoarele acte legislative și normative:

Acte legislative

- Constituția Republicii Moldova;
- Legea nr.273/1994 privind actele de identitate din sistemul naţional de paşapoarte;
- Legea nr.411/1995 ocrotirii sănătăţii.
- Legea nr.148/2023 privind accesul la informațiile de interes public.
- Legea nr.1069/2000 cu privire la informatică.
- Legea nr. 467/2003 cu privire la informatizare şi la resursele informaţionale de stat.
- Legea nr.71/2007 cu privire la registre.
- Legea nr.195/2024 privind protecția datelor cu caracter personal.
- Legea nr.48/2023 privind securitatea cibernetică;
- Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;
- Legea nr.93/2017 cu privire la statistica oficială.

Hotărîri ale Guvernului

- HG nr.710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare)
- HG nr. 821/2025 cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030;
- HG nr. 387/2023 cu privire la aprobarea Strategiei naționale de sănătate „Sănătatea 2030”;
- HG nr. 556/2025 cu privire la aprobarea Programului național pentru digitalizare și inovare în sănătate pe anii 2025-2030;

Alte acte normative

- Ordinul MS nr.868/2013 cu privire la organizarea activității Centrelor de Sănătate Prietenoase Tinerilor.
- Ordinul nr.1086/2016 cu privire la aprobarea Regulamentelor-cadru de organizare și funcționare ale prestatorilor de servicii de sănătate.
- Ordinul MS nr.404/2007 cu privire la delimitarea juridică a asistenței medicale primare la nivel raional.
- Ordinul MS nr.695/2010 Cu privire la Asistența Medicală primară din Republica Moldova.

Standarde Naționale și Reglementări tehnice

- Standardul Naționale SN ISO/CEI 15288:2005 "Ingineria sistemelor. Procesele ciclului de viață al sistemului”;
- Reglementarea tehnică "Procesele ciclului de viață al software-ului" (RT 38370656-002:2006) aprobată prin Ordinul Ministrului Dezvoltării Informaționale №.78 din 01.06.2006;
- Prestandarde naționale CEN, EN și ISO în domeniul informaticii medicale, aprobate de Institutul de Standardizare și Metrologie al Republicii Moldova;

Obiectivul proiectului

Sistemul descris in continuare face obiectul achizitiei serviciilor si formuleaza conditiile pentru dezvoltarea functionalitatilor noi a sistemului in scopul extinderii acestuia in zonele de interes business al Autoritatii Contractante. In mod concret, prezentul proiect are ca scop dezvoltari necesare functionalitatilor noi *SIYK*, care ca urmare acestora Prestatorul va livra servicii de dezvoltare noi, transfer de cunoștințe și consultanță la cerere, in conditiile prezentei proceduri .

Sistemul este descris atat la nivel arhitectural cat si functional, iar in prezenta documentatie sunt prezente informatii privind tehnologia folosita si modul in care sunt prelucrate datele. Prestatorul isi va asuma toate riscurile ce decurg din modificarea acestuia. Asumarea serviciilor din acest proiect implica acordarea garanției asupra *SIYK* pentru o perioada de minim 6 luni de la încetarea contractului pentru functionalitatile dezvoltate. De asemenea **Prestatorul serviciilor va documenta toate operatiunile de modificare a sistemului si le va prezenta Beneficiarului împreuna cu codul sursa care a suportat modificări**, acordand garantie pentru funcționarea dezvoltarilor operate in cadrul sistemului de la intrarea in regim de productie si ori de cate ori intervine asupra lui.

In capitolele initiale „Descriere generala a sistemului *SIYK*" si „Specificatii tehnice *SIYK*" sunt prezentate in totalitate detaliile necesare potentialilor ofertanti pentru a evalua corect efortul, cunostintele necesare si raspunderea pe care o asuma in prezenta procedura de achizitie a serviciilor de ajustare/dezvoltare a *SIYK*.

Definiții și abrevieri

Abreviere/Acronim	Descriere
CIM	Clasificarea Statistica Internațională a Bolilor si Problemelor de Sănătate Asociate;
Bază de date	Toate datele combinate organizate in conformitate cu anumite reguli, care oferă principiile generale de descriere, stocare si procesare a datelor;
DSM	Diagnoza Sănătății Mintale;
AEV	Adolescenți extrem de vulnerabili;
TRS	Tineri cu Risc Sporit de infectare;
IDNO	Codul Unic de Identificare a Persoanei Juridice din Republica Moldova (codul fiscal);

Abreviere/Acronim	Descriere
SI	Sistemul Informațional;
SIYK	Sistemul Informațional de Evidență a pacientului în cadrul Centrelor de Sănătate Prietenoase Tinerilor;
CSPT	Centrele de Sănătate Prietenoase Tinerilor;
Scorul Ferriman Gallwey	evaluare numerică utilizată pentru a evalua severitatea hirsutismului la femei;
Tanner Stages	sistem de clasificare obiectiv pe care Prestatorii îl folosesc pentru a documenta și urmări dezvoltarea și succesiunea caracteristicilor sexuale secundare ale copiilor în timpul pubertății;

Destinația sistemului

SIYK este destinat colectării, stocării și analizei datelor: despre participanții la sistemul CSPT, despre serviciile prestate de către CSPT, cu prezentarea informației respective autorităților publice de profil, în modul stabilit de legislație. Prezentarea și analiza datelor este efectuată atît la nivel de specialist din subdiviziune, cît și la nivel central.

Scopul și principiile SIYK

Sistemul Informațional de Evidență a pacientului (în continuare - SIYK) în cadrul Centrelor de Sănătate Prietenoase Tinerilor (în continuare CSPT) este destinat informatizării funcțiilor și fluxurilor principale ale specialiștilor din cadrul CSPT. De asemenea, SIYK asigură înregistrarea și evidenței consultațiilor prestate, gestiunea personalului și infrastructurii CSPT, generarea automatizată a documentelor și rapoartelor de activitate, controlul și coordonarea automatizată a activității subdiviziunilor de bază ale CSPT precum și acumularea informației necesare pentru luarea deciziilor inclusiv a celor referitoare la starea beneficiarilor deserviți.

Setul de date folosit in functionalitatea a sistemului cuprinde:

- IDNP beneficiar (neobligatoriu);
- Sex beneficiar ;
- Numele şi Prenumele beneficiar;
- Data naşterii;

- Subdiviziunea prestatoare;
- Locul de munca/studii beneficiar (neobligatoriu);
- Localitatea;
- Adresa la domiciliu (neobligatoriu);
- Telefon (neobligatoriu);
- E-mail (neobligatoriu);
- Mediul ;
- Data activitatii;
- Ora activitatii;
- Perioada activitatii;
- Tipul activitate prestat;
- Categoria beneficiar;
- Consumabil distribuit;
- Subiectul acordat in cadrul activitatii;
- Voluntari;

Astfel, SIYK este destinat automatizării fluxului informațional în cadrul subdiviziunilor din CSPT și are următoarele obiective:

1) formarea bazei de date la nivel de CSPT cu informații ce permit crearea unui tablou general în asistență integrată a sănătății adolescenților și tinerilor conform principiilor de servicii de sănătate prietenoase;
2) extinderea, sporirea numărului și calității serviciilor de sănătate prietenoase acordate tinerilor;
3) constituirea resurselor informaționale de stat privind sănătatea populației;
4) sporirea semnificativa a eficienței dirijării și circulației documentelor medicale;
5) obținerii operative a informațiilor actualizate cu prezentarea lor organelor de profil.

Principiile de bază ale SIYK sunt următoarele:

1) *principiul legitimității*, potrivit căruia funcțiile și operațiile efectuate de specialiști sunt legale și conforme cu drepturile omului și legislația națională în vigoare;

2) *principiul autenticității datelor*, care presupune că informațiile păstrate pe dispozitive de stocare a datelor sau pe suport de hîrtie corespund stării reale a obiectelor din SIYK;

3) *principiul identificării*, conform căruia pachetelor informaționale li se atribuie un cod de clasificare la nivel de sistem, prin care este posibilă identificarea univocă și raportarea la acestea;

4) *principiul auditului sistemului*, care presupune înregistrarea informației despre schimbările care au loc, pentru a face posibilă reconstituirea istoriei unui document sau starea lui la o etapă anterioară;

5) *principiul independenței de platforma software*, conform căruia SIYK poate fi construit pe baza modulelor elaborate la comandă sau a produselor software existente. Conceptul nu limitează în nici un fel abordarea dezvoltării sistemului atît timp cît sunt satisfăcute nevoile identificate.

6) *principiul accesibilității și integrabilității*, care presupune că SIYK, chiar dacă oferă funcționalități multiple, este construit ca un element integral și folosit de utilizatori prin intermediul unei interfețe unice. Mai mult decît atît, acest principiu prevede că expansiunea și dezvoltarea sistemului se vor face prin protocoale și puncte de conexiune proiectate din start;

7) *principiul confidențialității informației*, care prevede răspunderea personală, în conformitate cu legislația în vigoare, a specialiștilor responsabili de prelucrarea informației în sistem pentru utilizarea și difuzarea neautorizată a informației;

8) *principiul orientării spre utilizator*, potrivit căruia structura, conținutul, mijloacele de acces și navigarea sunt focalizate spre utilizatori;

9) *principiul dezvoltării progresive*, potrivit căruia elaborarea sistemului și modificarea permanentă a componentelor sale se efectuează în conformitate cu tehnologiile informaționale avansate;

10) *principiul consecutivității*, care presupune elaborarea și implementarea proiectului pe etape;

11) *principiul eficienței funcționării*, care presupune optimizarea raportului dintre calitate și cost;

12) *principiul securității informaționale*, care presupune asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirii pentru lucru atît a SIYK, cit și a datelor acestuia.

Caracteristici de funcționare

Arhitectura. Modelul operațional

SIYK este dezvoltat în baza unei arhitecturi client-server de tip *MVC (Laravel)* fiind asigurată independența de platformă a nivelului client. În organizarea *MVC*,

modelul reprezintă informația (datele) de care are nevoie aplicația, viewerul corespunde cu elementele de interfață iar controller-ul reprezintă sistemul comunicativ și decizional ce procesează datele informaționale, făcînd legătura intre *model* și *view*. În consecință:

- **Modelul** reprezintă partea de hard-programming, partea logica a aplicației. El are în responsabilitate acțiunile și operațiile asupra datelor, autentificarea utilizatorilor, integrarea diverselor clase ce permit procesarea informațiilor din diverse baze de date.
- **View-ul** se ocupă de afișarea datelor, practic aceasta parte a programului va avea grija de cum vede utilizatorul final informația procesată de controller. O data ce funcțiile sunt executate de model, view-ului îi sunt oferite rezultatele, iar acesta le va trimite către browser. În general viewul este o mini-aplicație care ajută la organizarea unor informații, avînd la baza diverse template-uri.
- **Controller-ul** reprezintă creierul aplicației. Aceasta face legătura intre model și view, între acțiunile utilizatorului și partea decizională a aplicației. În funcție de nevoile utilizatorului, controllerul apelează diverse funcții definite special pentru secțiunea funcțională exploatată de utilizator. Funcția se va folosi de model pentru a prelucra (extrage, actualiza) datele, după care informațiile noi vor fi trimise către view, ce le va afișa apoi prin template-uri.

Datorită arhitecturii alese, în perspectivă va fi facilă dezvoltarea continuă a *SIYK* ca urmare a divizării sistemului informatic pe diferite nivele relativ independente din punct de vedere funcțional.

Astfel nivelul prezentare (ce corespunde părții de view a aplicației) nu trebuie să cunoască mecanismele de implementare a conexiunilor la baza de date și algoritmii de prelucrarea a datelor ci expune un șir de template-uri pe care celelalte nivele trebuie să le utilizeze pentru a prezenta corect interfața și datele.

Astfel, SIYK are o arhitectură pe 3 nivele, si funcționează centralizat pe infrastructura hardware concepută pentru disponibilitate 99.9% și are următoarele caracteristici generale:

- acoperă procesele din cadrul CSPT;
- 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 ușurința noi modificări cu intervenții exclusiv asupra componentei de actualizat, minimizînd costurile și timpul necesar realizării modificărilor;
- are o arhitectura moderna cu un grad înalt de performanta, structurată pe 3 nivele (nivelul pentru baze de date, nivelul pentru aplicație și nivelul acces/utilizator);
- SIYK este orientat către deservirea unui număr sporit de accesări din partea utilizatorilor, inclusiv simultan și în intervale reduse de timp;
- recunoaște corect sursele informaționale, le acceptă si le integrează in sistem;
- întreține în limba romînă interfața utilizator, conținutul registrelor, nomenclatoarelor, bazelor de date, rapoartelor și documentelor generate;
- permite ca utilizatorul să se autentifice o singură dată pentru a accesa toate modulele aplicației în limita rolului de acces;
- corespunde cerințelor standardelor securității și confidențialității informației și prelucrării datelor cu caracter personal;
- asigură o siguranță sporită în exploatare.

Interfața Utilizator

Interfața este accesibilă permanent la toți specialiștii din subdiviziuni.

- interfața de lucru este accesată din browserul web și nu necesită instalarea de componente software suplimentare;
- interfața utilizatorului este în limba romană;
- interfața permite moduri alternative de introducere a datelor, atît prin utilizarea tastaturii, cît și a mouse-ului;

Infrastructura hardware-software și canale de comunicație

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

- **Platforma hardware**, formată din complexul tehnic de prelucrare și transportare a datelor, care asigură:
  - ✓ Servere protejate redundant pentru hosting al bazelor de date, softului de sistem și softului funcțional (aplicații);
  - ✓ Echipamente de comunicații pentru formarea rețelelor locale LAN și organizarea comunicațiilor teritoriale WAN;
  - ✓ Serverele puse la dispoziție au procesoare din familia Intel x86/x64
  - ✓ Performanță optimă, pentru realizarea obiectivelor și asigurarea extinderii ulterioare a sistemului;
  - ✓ Nivel înalt de securitate în privința aplicațiilor și transportului de date.

- **Platforma software**, are următoarele caracteristici:

- ✓ Sistemele de operare ale serverelor de baze de date și aplicații sunt din gama Linux (*Ubuntu 18.04*);
- ✓ Sistemul de gestiune al bazelor de date este PostgreSQL (*v 9.6*).
- ✓ Mediul de executie a aplicatiei este dezvoltată utilizînd limbajul de programare PHP (*v 7.1.33*)
- ✓ Pe stațiile utilizatorilor exista in mod implicit navigator web (MS Internet Explorer/MS Edge, Mozilla FireFox, Google Chrome, Safari, Opera).
- ✓ Pentru generarea rapoartelor și a documentelor statistice este utilizat o platformă bine cunoscută: JasperReports Server (*v 6.4*)

Sistemul de securitate

Sistemul SIYK funcționează în conformitate cu standardele de securitate în vigoare în ceea ce privește confidențialitatea informațiilor și prelucrarea datelor cu caracter personal. Mecanismele principale de securitate informațională ale SIYK utilizate sunt următoarele:

- asigură autentificarea și autorizarea utilizatorilor la baza de date cu diversificarea procedurilor de prelucrare și consultare a datelor în funcție de atribuțiile si obligațiunile fiecărui utilizator;
- este receptiv la eventualele modificări în lista utilizatorilor și/sau drepturilor acordate lor referitor la executarea procedurilor de prelucrare a datelor (înscriere, redactare, ștergere, vizualizare etc.);
- este receptiv la eventualele modificări ale drepturilor utilizatorilor referitoare la elementele de structură ale bazei de date accesibile lor;
- toate conturile de utilizator sunt create de administratorul de sistem.
- include mijloace de protecție a datelor în cazuri de dereglări de sistem, acces neautorizat, accidente tehnice;
- include mijloace de securitate a datelor la transportarea acestora prin intermediul rețelelor.
- înregistrarea acțiunilor utilizatorilor sistemului informatic ;
- criptarea informației;
- auditul informatic;
- procedurile de restabilire în caz de dezastru.

Avînd in vedere natura specială a informațiilor gestionate în cadrul SIYK, acesta are implementat un mecanism de securitate care permite doar accesul autorizat asupra componentelor sale. Asigurarea securității informaționale include totalitatea măsurilor juridice, organizatorice, economice și tehnologice, orientate

spre prevenirea pericolelor securității resurselor și infrastructurii informaționale. Totalitatea măsurilor de asigurare a securității informației SIYK sunt realizate în conformitate cu standardul ISO 27001.
Sistemul are următoarele nivele de securitate care asigura confidențialitatea datelor:

- Nivelul de securitate la nivel de aplicație: reprezentat prin protocolul de comunicație între stații și server; acesta este securizat, tip HTTPS cu certificate de criptare SSL;

Sistemul asigură dirijarea și controlul nivelului de acces și a drepturilor de identificare și autentificare pentru totalitatea obiectelor. Pentru fiecare grup de utilizatori sunt create drepturi 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 anumite grupuri de utilizatori. Sistemul asigură verificarea automată a drepturilor în momentul autentificării în sistem. În ulterioarele accesări a sistemului creează un jurnal al accesărilor – jurnalul de audit.

Pot fi delimitate următoarele probleme de asigurare a securității informaționale cu care s-ar putea confrunta sistemul informatic:

- asigurarea confidențialității informației (prevenirea obținerii informațiilor de către persoanele care nu au drepturile și competențele respective);
- asigurarea integrității logice a datelor (prevenirea introducerii, actualizării și ștergerii nesancționate a informației sau introducere a datelor denaturate);
- asigurarea securității infrastructurii informaționale de tentative de a defecta sau de a modifica funcționarea acesteia.

Veriga cea mai sensibilă la risc în sistemul de securitate este factorul uman. Din aceste considerente, instruirea personalului la capitolul însușirii metodicii rezistenței la amenințări informatice este un element foarte important.

Orice modificare potențial periculoasă: modificarea informației unei înregistrări, marcarea la ștergere, adăugarea unor înregistrări noi, etc. sunt jurnalizate în registre electronice speciale (fișiere log) arătînd momentul de timp și utilizatorul care a efectuat modificarea potențial periculoasă.
În caz că modificările potențial periculoase nu implică suprimarea fizică a datelor pentru fiecare înregistrare este posibilă accesarea informației privind utilizatorul care a efectuat ultima modificare. În consecință, sistemul informatic dispune de un instrument eficient care va da posibilitatea de a efectua o analiză a comportamentului utilizatorilor (sau a productivității lor).

SIYK are implementate normele generale de securitate a datelor publicate în Internet. Sistemul informatic poate bloca automat anumite adrese IP de pe care se

încearcă obținerea accesului nesancționat. Sistemul informatic posedă un instrumentar de monitorizare a accesărilor și a metodelor cu care au încercat accesul nesancționat la baza de date.

La nivel fizic politica de asigurare a securității informaționale se realizează prin intermediul unor module automate de generare a copiilor de rezervă a fișierelor și bazelor de date aflate în producție.

Politica de securitate este adusă la cunoștința fiecărui utilizator. Fiecare utilizator cunoaște obligațiunile de serviciu în materie de respectare a securității informaționale și totalitatea procedurilor formale pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

In sistem exista următoarele tipuri majore de utilizatori:

- Beneficiar
- Administrator *SIYK*
- Manager
- Specialist
- Receptie

Beneficiar - persoana care poate beneficia de serviciile de consultanta, avînd dreptul de ași păstra anonimatul pe tot parcursul activității prestat de către *CSPT* la libera alegere a specialistului.

Administrator *SIYK* – persoana care are acces deplin la toate funcționalitățile sistemului informațional; configurează conturile de acces, monitorizează în sistem informațiile despre acțiunile întreprinse de către prescriptor, prestator în domeniul de competență.

Manager - persoana care are acces deplin la sistemului informațional, monitorizează în sistem informațiile despre acțiunile întreprinse de către specialiști, precum și activitățile prestate pe domeniul de competență.

Subdiviziune – instituția care stabilește programul de prestare a serviciilor medicale prin planificarea unei activități (interval de timp în care un anumit serviciu este prestat de către un specialist), prestează serviciile de consultanță, înregistrează serviciile medicale prestate în SIYK.

Specialist – persoana responsabilă pentru introducerea serviciului/activității prestat/e în acordarea asistenței beneficiarului.

Recepție - persoana responsabilă programarea unei consultații si gestiune a programărilor

Sistemul dispune de mecanisme de retenție a datelor, asigurare acces securizat si audit (jurnalizare) al acțiunilor:

- **Retenția datelor**. Sistemul permite stocarea informațiilor cu privire la beneficiari (consultații, testări, instruiri, etc) 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 datelor cu caracter personal. Măsurile de securitate asigură prevenirea utilizării neautorizate a datelor și protejează împotriva pierderii, modificării neautorizate și distrugerii datelor din sistem.
- **Autorizare la funcționalități**. Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor pe care le au în sistem și pe baza permisiunilor asociate rolului sau rolurilor din care fac parte utilizatorii.
- **Autorizare la date**. Utilizatorii care folosesc sistemul sunt autorizați să acceseze funcționalitățile sistemului pe baza identității, rolurilor din sistem și pe baza permisiunilor asociate rolului, sau rolurilor, din care face parte utilizatorul doar pe domeniul său de competență.
- **Ne repudierea**. Ne repudierea este o modalitate de a garanta faptul că utilizatorul nu poate nega mai tîrziu că a efectuat o operațiune. Ne repudierea este implementată prin următoarele mecanisme:
  - ✓ Unicitatea utilizatorilor in sistem
  - ✓ Auditarea tuturor operațiunilor efectuate de sistem;
  - ✓ Mecanism de control al versiunilor pentru înregistrările serviciilor prestate.
- **Securizarea schimbului de date**. Orice comunicare din cadrul sistemului cu exteriorul utilizează metode de criptografie atît la nivelul canalului de comunicație cît și la nivelul mesajelor (mesaje SOAP) transmise.
- **Audit**. Toate operațiunile efectuate de utilizatori păstrează o urma in componenta de loguri. Este permisă astfel investigarea incidentelor de către un administrator.

Modulele SIYK

SIYK este constituit dintr-un set de module care acoperă diverse funcționalități și au acces restricționat în dependență de rol și drepturi de acces al

fiecărui utilizator. În baza unei analize a SIYK, se poate conchide că conține următoarele module de bază:

1. **MODULUL DESTINAT MONITORIZĂRII CALITĂȚII SERVICIILOR PRESTATE** care cuprinde următoarele componente de bază:
    - **Componenta de configurare a infrastructurii CSPT** care furnizează funcționalitățile necesare gestiunii profilurilor *Centrelor de Sănătate Prietenoase Tinerilor*.
    - **Componenta de gestiune a specialiștilor CSPT** care conține formularele electronice necesare gestiunii profilurilor specialiștilor CSPT.
    - **Componenta de configurare a obiectivelor de activitate a CSPT și monitorizare a îndeplinirii lor** care furnizează funcționalitățile destinate configurării indicatorilor de performanță planificați anual ale *CSPT* și monitorizare a procesului de atingere a acestor obiective.
2. **MODULUL DESTINAT ÎNREGISTRĂRII ACTIVITĂȚILOR DE CONSULTANȚĂ** care cuprinde următoarele componente de bază:
    - **Componenta de gestiune a profilurilor beneficiarilor (**pacienților**)** care furnizează funcționalitățile necesare creării și gestiunii profilurilor tinerilor care se adresează pentru consultații la *CSPT*.
    - **Componenta de gestiune a activităților instructiv-metodice** care furnizează funcționalitățile necesare evidenței activității instructiv-metodice efectuate în cadrul *CSPT*.
    - **Componenta de gestiune a activităților de consultanță medicală** care furnizează funcționalitățile necesare evidenței activității de acordare a asistenței medicale pacienților *CSPT*.
    - **Componenta de gestiune a activităților de consultanță socială** care furnizează funcționalitățile necesare evidenței activității de acordare a asistenței sociale pacienților *CSPT*.
    - **Componenta de gestiune a activităților de consultanță psihologică** care furnizează funcționalitățile necesare evidenței activității de acordare a asistenței psihologice pacienților *CSPT*.
    - **Dashboard-ul utilizatorului autorizat** care furnizează funcționalitățile de calculare și afișare în timp real a indicatorilor de performanță cheie a *SIYK* și asigurare a accesului rapid la

înregistrările critice aferente atribuțiilor de serviciu ale utilizatorilor autorizați

3. **MODULUL DESTINAT GENERĂRII RAPOARTELOR ȘI STATISTICILOR** furnizează funcționalitățile necesare generării și salvării în format DOCX, XLSX și PDF a rapoartelor și statisticilor în baza stocului de date al sistemului informatic. Un caz particular al rapoartelor și statisticilor reprezintă documentele tipizate extrase prin intermediul *SIYK (exemplu: raportul 49-san Activități instructiv-metodice, 49-san Activități consultative, Volumul acordat de asistență specializată, etc.)*.
4. **MODULUL DE GESTIUNE A SISTEMULUI INFORMATIC** care cuprinde următoarele componente de bază:
    - **Componenta de configurare globală a sistemului informatic** prin intermediul căreia sunt configurați parametrii generali de funcționare a sistemului informatic.
    - **Componenta de gestiune a resurselor sistemului informatic** prin intermediul căreia sunt gestionate componentele funcționale ale aplicației, definirea statutelor, tranzițiilor prin care pot trece resursele, definirea regulilor de acces în funcție de grupurile de utilizatori precum și formularea strategiei de jurnalizare a evenimentelor de business.
    - **Componenta de gestiune a utilizatorilor** care permite gestiunea profilurilor tuturor utilizatorilor cu drept autorizat la resursele sistemului informatic (utilizatorii aferenți *CSPT*). *SIYK* permite diferențierea dinamică a accesului utilizatorilor la resursele sistemului informatic prin intermediul unui mecanism de definire a drepturilor și rolurilor.
    - **Componenta de gestiune a grupurilor utilizatorilor** care permite configurarea grupurilor utilizatorilor în funcție de funcționalitățile specifice disponibile lor și a rolurilor în cadrul fluxurilor de lucru implementate în cadrul *CSPT*.
    - **Componenta de gestiune a nomenclatoarelor și clasificatoarelor (metadatelot)** care permite administrarea structurii și conținutului sistemului complex de nomenclatoare (naționale și interne ale *CSPT*) ale *SIYK* prin intermediul cărora este efectuată preferențierea informației conținute în baza de date și adaptarea conținutului bazei de date și rapoartelor modificărilor legislative sau procedurale în activitatea *CSPT*.

- **Componenta de gestiune a notificărilor** furnizează funcționalități de notificare automatizată prin Email sau mecanismele interne *CSPT* a utilizatorilor autorizați sau a entităților ce fac obiectul proceselor de business implementate în *CSPT*.
- **Componenta de monitorizare a activității utilizatorilor** permite jurnalizarea totalității evenimentelor activității utilizatorilor. Acest lucru este necesar pentru asigurarea unor măsuri elementare de securitate și anticiparea unor eventuale probleme în acest domeniu. Mecanismul de jurnalizare a activității utilizatorilor înregistrează următoarele evenimente:
    i. conectarea la sistem;
    ii. deconectarea de la sistem;
    iii. adăugare / modificare informație;
    iv. suprimare informație.
- **Componenta de generare a copiei de rezervă a Bazei de Date a sistemului informatic**, care permite crearea copiilor de rezervă a bazei de date *SIYK*, în scopul asigurării securității fizice a datelor.

5. **MODULUL DE DOCUMENTARE SIYK** care furnizează funcționalități de afișare a documentației de utilizare a sistemului informatic într-un format accesibil și comod. Acesta nu se va deosebi după principiile sale de mecanismele de Help integrate în soluțiile desktop consacrate.

Cerinte de dezvoltare a SIYK, transfer de cunoștințe și consultanță

Asumarea contextului dezvoltărilor software

Contextul în care Prestatorul va desfășura serviciile contractate este următorul:

- Beneficiarul deține dreptul de proprietate asupra codului aplicației. Orice operațiune de modificare a codului generează o noua versiune a aplicației pentru care dezvoltatorul [cel care efectuează modificarea] va oferi garanție completa. Beneficiarul își păstrează in continuare dreptul de proprietate asupra aplicației. Beneficiarul nu intervine asupra codului aplicației, motiv pentru care răspunderea funcționării corecte a aplicației in timpul si după executarea modificărilor de cod aparține dezvoltatorului. Orice modificare asupra aplicației

implica din partea dezvoltatorului obligația acordării garanției pentru întreg sistemul si nu doar pe modificările efectuate.

- Beneficiarul își păstrează dreptul de proprietate asupra aplicației indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului.
- Serviciile vor fi realizate prin modernizarea componentelor software și a infrastructurii existente, fără afectarea funcționalităților operaționale ale sistemului, cu excepția situațiilor în care modificările sunt necesare pentru compatibilitatea cu tehnologiile actuale sau pentru eliminarea unor vulnerabilități ori limitări tehnice.
- Procesul de modernizare va include analiza aplicației, actualizarea tehnologiilor utilizate, optimizarea codului sursă, migrarea infrastructurii software, testarea funcțională și tehnică, precum și asigurarea mentenanței și suportului tehnic după implementare.

Analiza tehnică și proiectarea soluției

Durata maximă de realizare a acestei etape va fi de o lună de la data intrării în vigoare a contractului precum si accesul la sistemele informatice, bazele de date, documentația și celelalte informații necesare prestării serviciilor. În cadrul acestei etape, Prestatorul va efectua analiza tehnică a sistemului existent, a infrastructurii hardware și software, a bazelor de date și a componentelor aplicației, va identifica incompatibilitățile tehnologice și riscurile existente. La finalizarea etapei, Prestatorul va prezenta Beneficiarului planul de implementare / documentația tehnică aferentă.

Modernizarea infrastructurii tehnologice

În cadrul acestei etape, prestatorul va moderniza infrastructura tehnologică necesară funcționării aplicației, astfel încît aceasta să utilizeze componente **software aflate în perioada oficială de suport și compatibile cu arhitectura existentă**. Nu vor fi utilizate versiuni software ieșite din ciclul de mentenanță, cu excepția situațiilor justificate tehnic și aprobate de beneficiar. Toate modificările realizate asupra infrastructurii vor fi documentate la finalul implementării. Durata maximă de realizare a acestei etape este de 2 luni. Prestatorul va analiza infrastructura hardware și software existentă și va implementa măsurile necesare pentru creșterea nivelului de securitate, disponibilitate și performanță. În funcție de rezultatele analizei, vor fi realizate, după caz, următoarele activități:

- actualizarea sistemului de operare la o versiune aflată în suport pe termen lung (LTS) sau echivalent;
- actualizarea serverului web și a componentelor software aferente;
- modernizarea mediului de execuție al aplicației și actualizarea bibliotecilor necesare funcționării acesteia;
- actualizarea sistemului de gestiune a bazelor de date la o versiune compatibilă și aflată în suport;
- configurarea și optimizarea serviciilor necesare funcționării aplicației;
- implementarea măsurilor de securitate recomandate pentru infrastructură și servicii;
- configurarea și testarea mecanismelor de backup și restaurare;
- optimizarea parametrilor de funcționare ai serverelor, în vederea asigurării unei performanțe și stabilități corespunzătoare.

Separarea componentelor infrastructurii

Prestatorul va evalua oportunitatea separării aplicației și a bazei de date dupa caz pe servere sau mașini virtuale distincte, în funcție de configurația infrastructurii existente și de rezultatele analizei tehnice. Dacă această abordare este justificată din punct de vedere tehnic și poate fi implementată în infrastructura disponibilă, prestatorul va propune o arhitectură care să contribuie la:

- reducerea riscului generat de existența unui punct unic de defectare;
- creșterea performanței generale a sistemului;
- îmbunătățirea posibilităților de extindere și scalare;
- simplificarea activităților de administrare și mentenanță;
- creșterea nivelului de securitate prin separarea serviciilor critice.

În situația în care separarea componentelor nu este oportună sau nu poate fi realizată din motive tehnice, prestatorul va prezenta beneficiarului o justificare tehnică și va propune soluții alternative care să asigure un nivel corespunzător de securitate, disponibilitate și performanță.

Adaptarea și optimizarea aplicației

În această etapă, prestatorul va adapta aplicația pentru funcționarea în noua infrastructură tehnologică și va implementa toate modificările necesare pentru

asigurarea compatibilității cu versiunile actualizate ale componentelor software utilizate. Durata maximă de realizare a acestei activitati este de 3 - 4 luni, care vor include actualizarea mediului de execuție al aplicației, actualizarea bibliotecilor și a dependențelor software, eliminarea incompatibilităților tehnologice identificate în etapa de analiză, optimizarea codului sursă și a bazei de date, precum și implementarea măsurilor necesare pentru îmbunătățirea performanței, securității și stabilității sistemului. Prestatorul va actualiza mediul de execuție al aplicației la o versiune aflată în perioada oficială de suport și compatibilă cu infrastructura implementată. În funcție de rezultatele analizei tehnice, activitățile vor include, după caz:

- actualizarea limbajului de programare și a componentelor software utilizate de aplicație la versiuni aflate în suport oficial;
- identificarea și remedierea incompatibilităților dintre aplicația existentă și noile versiuni ale componentelor software;
- actualizarea bibliotecilor, framework-urilor și a celorlalte dependențe utilizate;
- adaptarea codului sursă la cerințele versiunilor actualizate;
- efectuarea testelor de compatibilitate și performanță.

La finalizarea acestei activități, prestatorul va demonstra funcționarea corespunzătoare a aplicației în noul mediu de execuție. Prestatorul va actualiza sistemul de gestiune a bazelor de date la o versiune aflată în perioada oficială de suport, asigurînd păstrarea integrității și consistenței datelor. Procesul de actualizare va include, cel puțin:

- analiza compatibilității bazei de date existente;
- migrarea datelor fără pierderea informațiilor;
- verificarea integrității datelor după migrare;
- optimizarea parametrilor de funcționare ai bazei de date;
- optimizarea interogărilor SQL și a structurilor utilizate;
- validarea funcționalităților aplicației după finalizarea migrării.

Prestatorul va documenta procedurile utilizate pentru realizarea copiilor de siguranță și pentru restaurarea bazei de date, astfel încît recuperarea sistemului să poată fi realizată în condiții de siguranță în cazul apariției unor incidente. În vederea creșterii performanței și reducerii riscurilor tehnice, prestatorul va analiza codul sursă și va implementa măsurile necesare pentru optimizarea aplicației. În funcție de rezultatele analizei, activitățile pot include:

- optimizarea codului sursă;
- optimizarea interogărilor SQL;
- reducerea timpilor de răspuns ai aplicației;

- implementarea mecanismelor de cache, acolo unde acestea sunt justificate;
- eliminarea componentelor software neutilizate sau depășite;
- reorganizarea componentelor aplicației pentru simplificarea administrării și a activităților de mentenanță.

Testarea și validarea sistemului

Înainte de punerea în exploatare a sistemului modernizat, prestatorul va efectua testarea completă a aplicației și a infrastructurii aferente, în scopul verificării funcționării corespunzătoare a tuturor componentelor implementate.

Procesul de testare va avea maxim termen de realizare o lună și va include cel puțin:

- verificarea funcționalităților existente și a modificărilor implementate;
- testarea compatibilității dintre aplicație și componentele infrastructurii modernizate;
- testarea performanței sistemului;
- verificarea mecanismelor de autentificare, autorizare și securitate;
- validarea migrării bazei de date și verificarea integrității informațiilor;
- verificarea mecanismelor de backup și restaurare;
- remedierea neconformităților identificate în procesul de testare.

Punerea în exploatare a sistemului se va realiza numai după remedierea tuturor neconformităților identificate și validarea rezultatelor testării de către beneficiar.

Implementarea în mediul de producție și stabilizarea sistemului

După finalizarea cu succes a etapei de testare, prestatorul va implementa sistemul modernizat în mediul de producție în termen maxim de realizare o lună, cu respectarea măsurilor necesare pentru reducerea riscurilor asociate procesului de migrare și pentru asigurarea continuității serviciilor. În perioada de stabilizare, prestatorul va monitoriza funcționarea sistemului, va acorda suport tehnic beneficiarului și va remedia incidentele sau disfuncționalitățile apărute ca urmare a implementării.

Durata totală estimată pentru executarea serviciilor de modernizare nu va depăși 8 luni de la data semnării contractului, cu excepția situațiilor justificate și aprobate de comun acord de către părți.

Documentație și transfer de cunoștințe

La finalizarea serviciilor, prestatorul va transmite beneficiarului documentația tehnică actualizată, necesară administrării, exploatării și mentenanței sistemului modernizat. Documentația va include, după caz:

- descrierea arhitecturii sistemului;
- configurațiile implementate;
- procedurile de instalare și actualizare;
- procedurile de backup și restaurare;
- instrucțiunile privind administrarea și exploatarea sistemului;
- lista modificărilor efectuate asupra aplicației și infrastructurii.

Ajustările și dezvoltările evolutive ale SIYK

Pe parcursul exploatării SIYK de către utilizatorii acestuia, au fost identificate o serie de module care se solicita a fi ajustate. Aceste intervenții au ca scop îmbunătățirea funcționalităților sistemului, optimizarea proceselor de lucru, adaptarea la modificările legislative și operaționale, precum și extinderea posibilităților de analiză și raportare privind activitatea desfășurată în cadrul CSPT.

Deci, pe întreaga durată a contractului, Beneficiarul va putea transmite Prestatorului cereri de modificare (Change Request) privind ajustarea, completarea, optimizarea sau dezvoltarea funcționalităților SIYK. Cererile de modificare vor fi comunicate în scris de către Beneficiar și vor descrie funcționalitatea solicitată, obiectivul urmărit și, după caz, rezultatul așteptat. Prestatorul va confirma recepționarea fiecărei cereri de modificare și în funcție de complexitatea solicitării, Prestatorul va analiza impactul asupra sistemului și va propune soluția tehnică de implementare, inclusiv estimarea efortului necesar, termenul de realizare și eventualele implicații asupra celorlalte componente ale sistemului.

Totodată, menționăm că Prestatorul trebuie să ia în considerare implementarea principiului celui mai mic privilegiu (Least Privilege), prin acordarea utilizatorilor, inclusiv conturilor administrative, doar a drepturilor necesare pentru îndeplinirea atribuțiilor aferente. De asemenea, în urma analizei aplicației, în comun cu Beneficiarul, va fi evaluată posibilitatea implementării autentificării multifactor (MFA), în funcție de nivelul de risc și particularitățile sistemului SIYK.

Avînd în vedere că solicitările de ajustare pot avea un impact asupra altor module și procese din cadrul sistemului, Prestatorul va analiza efectele fiecărei modificări asupra întregii aplicații și va implementa măsurile necesare pentru menținerea integrității datelor, compatibilității dintre componente și continuității funcționării sistemului. Fiecare ajustare implementată va fi însoțită după caz de documentația tehnică aferentă administrăreii și utilizării sistemului. În funcție de complexitatea acestora, solicitările vor fi încadrate în una dintre următoarele categorii.

Ajustări minore

Ajustările minore includ modificări care nu afectează arhitectura sistemului și care presupun completarea formularelor existente, introducerea unor cîmpuri suplimentare, modificarea nomenclatoarelor, ajustarea regulilor de validare, optimizarea interfețelor utilizator, modificarea rapoartelor existente sau implementarea unor optimizări punctuale.

Ajustări cu complexitate medie

Această categorie include modificări ale fluxurilor operaționale, implementarea unor reguli noi de business, modificări care implică mai multe module sau dezvoltarea unor rapoarte complexe.

Dezvoltări majore

Dezvoltările majore includ realizarea unor module noi, integrarea cu alte sisteme informaționale, implementarea unor procese funcționale noi, modificări arhitecturale sau alte dezvoltări care presupun un efort tehnic semnificativ.

Pentru ajustari/dezvoltari evolutive Prestatorul va analiza tehnic, va prezenta soluția propusă, estimarea resurselor și calendarul de implementare. Duratele implementării dezvoltărilor in urma cererilor va fi stabilită de comun acord între Beneficiar și Prestator, în funcție de complexitatea acestora.

Versiunile actualizate si funcționale ale sistemului intra automat în proprietatea Beneficiarului, iar Prestatorul executa operațiunile tehnice asupra acestora pana la finalizarea contractului **si acorda garanție asupra lor, în forma în care au fost predate, de cel puțin 6 luni** de la încetarea contractului. Cheltuielile generate de remedierea defecțiunilor aplicației apărute în perioada de garanție, în măsura în care acestea sunt cauzate de dezvoltările, modificările sau configurările

realizate de Prestator în cadrul prezentului contract, vor fi suportate de către Prestator.