GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2024

Chișinău

Cu privire la instituirea Sistemului Informațional Transplant

În temeiul prevederilor art. 22, lit. c) și lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12 art. 44), cu modificările ulterioare, Guvernul HOTĂRĂŞTE:

1. Se instituie Sistemul Informațional Transplant.

2. Se aprobă:

1) Conceptul Sistemului Informațional Transplant, conform anexei nr. 1;

2) Regulamentul Resursei Informaționale ținute pe Sistemul Informațional Transplant, conform anexei nr. 2.

3. Hotărârea Guvernului nr. 386/2010 cu privire la instituirea Agenției de Transplant (Monitorul Oficial al Republicii Moldova, 2010, nr. 78-80, art. 457) se modifică după cum urmează:

1) anexa nr. 1:

a) la punctul 6 subpunctul 2) cuvintele „ Sistemul informațional automatizat „Transplant”” se substituie cu cuvintele „Sistemul informațional Transplant”.

4. Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical (Monitorul Oficial al Republicii Moldova, 2017, nr. 277–288, art. 703) se modifică după cum urmează:

1) pe tot parcursul textului, cuvintele „Sistemul informațional automatizat „Transplant” (SIA Transplant)” se substituie cu cuvintele „Sistemul informațional Transplant (SIT)”.

5. Asigurarea funcționării Sistemului informațional Transplant se efectuează din contul și în limitele alocațiilor aprobate anual în acest scop în legea bugetului de stat, precum și din alte surse, conform legislației.

6. Prezenta hotărâre intră în vigoare la data de 01.01.2025.

Prim-ministru **DORIN RECEAN**

Contrasemnează:
Ministrul sănătății **Ala Nemerenco**

Anexa nr. 1

La Hotărârea Guvernului nr.____/_____

CONCEPTUL

Sistemului Informațional Transplant

Introducere

Instituirea Sistemului Informațional Transplant are drept scop proiectarea, dezvoltarea și menținerea unui sistem cu funcționalități specifice domeniului vizat, interoperabil cu alte sisteme informaționale, integrabil în structura Registrului medical, aprobat prin Hotărârea Guvernului nr. 586/2017, destinat prestatorilor de servicii medicale și băncilor de țesuturi și/sau de celule autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi sau celule umane.

Prezentul Concept determină scopul, obiectivele și funcțiile de bază ale Sistemului Informațional Transplant, obiectele informaționale, precum și scenariile de bază privind includerea datelor relevante în sistem, fiind plasat în MCloud să interacționeze cu alte sisteme informatice în scopul schimbului de date pe platforma guvernamentală MConnect utilizând serviciile electronice guvernamentale MSign, MPass, MLog și MNotify.

Capitolul I

Generalități

1. Sistemul Informațional Transplant (în continuare – SIT) reprezintă totalitatea de resurse și tehnologii informaționale, organizaționale, a sistemelor de colectare, stocare și transmitere a datelor și tehnologiilor de utilizare a acestora, a normelor de drept, precum și a infrastructurii implicate în susținerea activității informaționale din cadrul prestatorilor de servicii medicale și băncilor de țesuturi și/sau de celule autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi sau celule umane.

2. Abrevieri utilizate în text:

AT – Agenția de Transplant;

SIT – Sistemul Informațional Transplant;

UE – Uniunea Europeană;

EDQM – Directoratul European pentru Calitatea Medicamentelor și Asistenței Medicale al Consiliului Europei;

EHR – Electronic Health Record, - Dosarul Electronic al Pacientului sau Fișa Electronică a pacientului, care reprezintă totalitatea documentelor create ca urmare a interacțiunii între pacient și sistemul de sănătate. Sistemele EHR coordonează stocarea și regăsirea dosarului electronic individual cu ajutorul tehnologiei informației. Sistemele EHR reduc erorile medicale, îmbunătățesc eficienta actului medical, reduc costurile și promovează standardizarea serviciilor medicale;

ERA-EDTA – European Renal Association - European Dialysis and Transplant Association – Asociația Renală Europeană - Asociația Europeană de Dializă și Transplant;

ESOT – European Society for Organ Transplantation (Societatea Europeană pentru Transplantul de Organe;

EUROCET – Rețeua Europeană a Autorităților Competente pentru Țesuturi și Celule;

FOEDUS – Facilitating of Organs Exchange Donated in EU member States – Instrumentul European de schimb rapid de organe între statele membre ale UE;

IHE – Integrating the Healthcare Enterprise. IHE este o inițiativă a industriei medicale și a profesioniștilor din domeniul sănătății dedicată îmbunătățirii modului în care sistemele informatice medicale partajează informațiile. Sistemele construite conform specificațiilor IHE comunică între ele

mai bine, sunt mai ușor de implementat și oferă furnizorilor de servicii medicale posibilitatea de a folosi informațiile mai eficient în timp real.

3. În sensul prezentului Concept va fi utilizată noțiunea:

Acord informat – înțelegere reciprocă şi conştientă a părţilor implicate în actul medical, care urmează a fi respectată pe parcursul întregii perioade de prestație medicală atât de profesionistul medical, cât şi de pacient, și care trebuie să conțină obligator informația, expusă într-o formă accesibilă pentru pacient, cu privire la scopul, efectul scontat, metodele intervenţiei medicale, riscul potențial legat de ea, posibilele consecințe medico-sociale, psihologice, economice etc., precum şi procedeele alternative de tratament şi îngrijire medicală.

4. SIT va realiza:

1) formarea bazei de date la nivel național cu informații periodic actualizate, ce permit crearea fișierelor medicale ale pacienților ce donează un organ, țesut sau celule pentru primitorii, care necesită un transplant de organ, țesut sau celule în condițiile legii;

2) dirijarea și circulația eficientă a documentelor medicale;

3) obținerea operativă a informației actualizate;

4) participarea la schimbul de organe, țesuturi și celule umane între statele UE, cu care Republica Moldova are semnate acorduri de colaborare;

5) elaborarea și dezvoltarea în SIT a Registrelor Donatorilor și Primitorilor de organe, țesuturi și celule umane;

6) elaborarea și dezvoltarea modulului de biovigilență pentru raportarea, investigarea, înregistrarea şi transmiterea informațiilor despre evenimentele şi reacțiile adverse grave care pot influența calitatea şi siguranța organelor, țesuturilor şi celulelor umane utilizate la om;

7) elaborarea și dezvoltarea modulului de statistici și raportări a activităților în domeniul transplantului de organe, țesuturi și celule umane și activităților din cadrul reproducerii asistate medical;

8) aportul la constituirea resurselor informaționale de stat privind starea sănătății populației.

5. Pentru prestatorii de servicii medicale autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi sau celule umane, SIT va asigura:

1) gestionarea și actualizarea periodică a fișei electronice a pacientului (donatori și primitori);

2) gestionarea și actualizarea periodică a analizelor și investigațiilor efectuate donatorilor și primitorilor;

3) implementarea automatizării consumării datelor provenite din sistemele de apreciere a compatibilității imuno-histo-chimice și izo-serologice între donator și primitor la nivel de organ, țesut sau celulă umană;

4) evidența electronică a pacienților supuși activităților de donare, prelevare și transplant atât în țară, cât și peste hotarele ei;

5) evidența electronică a stocurilor de medicamente necesare primitorilor de transplant;

6) evidența electronică națională a stocurilor de țesuturi și celule umane.

6. SIT va oferi:

1) crearea și actualizarea periodică a fișei electronice a pacientului care jurnalizează interacțiunile pacientului cu sistemul medical la nivel național;

2) generarea rapoartelor pentru monitorizarea activităților de prelevare și transplant;

3) generarea rapoartelor pentru monitorizarea activităților de reproducere asistată medical.

7. SIT folosește tehnologiile contemporane, care permit utilizarea lui de prestatorilor de servicii medicale și băncilor de țesuturi și/sau de celule autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi sau celule umane prin intermediul unui echipament IT convențional, fără necesitatea instalării programelor suplimentare.

8. Principiile de bază ale SIT sunt următoarele:
1) ***principiul legitimității***, potrivit căruia funcțiile și operațiile efectuate de utilizatori sunt legale și conforme cu drepturile omului și legislația națională;
2) ***principiul autenticității datelor***, presupune că informațiile păstrate pe dispozitive de stocare a datelor sau pe suport de hârtie corespund stării reale a obiectelor din SIT;
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 acestora;
4) ***principiul temeiniciei datelor***, prevede că introducerea și reactualizarea datelor în SIT se efectuează doar în baza înscrierilor din documentele acceptate ca surse de informații;
5) ***principiul auditului sistemului***, presupune înregistrarea informației despre schimbările care au loc, pentru a face posibilă reconstituirea istoriei unui document sau starea lui la o etapă anterioară;
6) ***principiul independenței de platforma software***, conform căruia SIT poate fi construit pe baza modulelor elaborate la comandă sau a produselor software existente. Conceptul nu limitează în nici un fel abordarea dezvoltării sistemului atât timp, cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit;
7) ***principiul accesibilității și integrabilității***, presupune că SIT, chiar dacă oferă funcționalități multiple, este construit ca un element integral şi folosit de utilizatori prin intermediul unei interfețe unice. Acest principiu prevede că expansiunea și dezvoltarea sistemului se vor face prin protocoale și puncte de conexiune proiectate din start;
8) ***principiul confidențialității informației***, prevede răspunderea personală, în conformitate cu legislația, a colaboratorilor responsabili de prelucrarea informației în sistem pentru utilizarea și difuzarea neautorizată a informației;
9) ***principiul compatibilității***, conform căruia SIT trebuie să fie compatibil cu sistemele existente atât în țară, cât și peste hotarele ei;
10) ***principiul orientării spre utilizator***, potrivit căruia structura, conținutul, mijloacele de acces și navigarea sunt focalizate spre utilizatori;
11) ***principiul extensibilității,*** conform căruia componentele SIT oferă facilități de ajustare și extindere a funcționalităților existente;
12) ***principiul dezvoltării progresive***, potrivit căruia elaborarea sistemului și modificarea permanentă a componentelor sale se efectuează în conformitate cu tehnologiile informaționale avansate;
13) ***principiul consecutivității***, presupune elaborarea și implementarea proiectului pe etape;
14) ***principiul eficienței funcționării***, presupune optimizarea raportului dintre calitate și cost;
15) ***principiul utilizării standardelor deschise***, se aplică pentru a asigura atât interoperabilitatea cu sistemele externe, cât și păstrarea informației, în conformitate cu legislația;
16) ***principiul egalității și nondiscriminării***, potrivit căruia toate ființele umane sunt egale în faţa legii şi au dreptul la protecţie şi beneficii egale;
17) ***principiul securității informaționale***, 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 atât a SIT, cât și a datelor acestuia.

Capitolul II
Spațiul juridico-normativ al funcționării SI Transplant

9. Crearea și funcționarea SIT este reglementată de următoarele acte normative:
1) Constituția Republicii Moldova din 29 iulie 1994;
2) Legea nr. 411/1995 ocrotirii sănătății;
3) Legea nr. 1069/2000 cu privire la informatică;
4) Legea nr. 100/2001 privind actele de stare civilă;

5) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
6) Legea nr. 71/2007 cu privire la registre;
7) Legea nr. 241/2007 comunicațiilor electronice;
8) Legea nr. 42/2008 privind transplantul de organe, țesuturi și celule umane;
9) Legea nr. 133/2011 privind protecția datelor cu caracter personal;
10) Legea nr. 121/2012 cu privire la asigurarea egalității.
11) Legea nr. 138/2012 privind sănătatea reproducerii;
12) Legea nr. 93/2017 cu privire la Statistica oficială;
13) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
14) Legea nr. 124/2022 cu privire la identitatea electronică și serviciile de încredere;
15) Legea nr. 148/2023 privind accesul la informațiile de interes public;
16) Hotărârea Guvernului nr. 272/2002 despre măsurile privind crearea sistemului informațional automatizat „Registrul de stat al unităților de drept”;
17) Hotărârea Guvernului nr. 735/2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova;
18) Hotărârea Guvernului nr. 916/2007 cu privire la Concepția Portalului guvernamental;
19) Hotărârea Guvernului nr. 386/2010 cu privire la instituirea Agenției de Transplant;
20) Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
21) Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
22) Hotărârea Guvernului nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
23) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
24) Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare şi control al accesului (MPass);
25) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
26) Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical;
27) Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.
28) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
29) Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcţionare și utilizare a serviciului guvernamental de notificare electronică (MNotify);
30) Hotărârea Guvernului nr. 323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic”și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic”**;**
31) Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;
32) Ordinul Ministerului Dezvoltării Informaționale nr.78/2006 cu privire la aprobarea reglementării tehnice „Procesele ciclului de viață al software-ului" RT 38370656-002:2006”;
33) Ordinul Ministerul Tehnologiilor Informaționale și Comunicațiilor nr. 94/2009 cu privire la aprobarea unor reglementări tehnice;

34) Ordinul Ministerului Sănătății nr. 493/2011 privind întocmirea Listelor de așteptare pentru transplant renal, hepatic și cardiac;
35) Ordinul Ministerului Sănătății nr. 427/2017 cu privire la aprobarea Standardului privind organizarea și desfășurarea activităților de prelevare și transplant de organe, țesuturi și celule umane.

Capitolul III
Spațiul functional al SI Transplant

10. Categoriile datelor personale utilizate în SIT la introducerea în sistem a IDNP-ul persoanei sunt:
a) numele, prenumele, patronimicul;
b) grupul sangvin și factorul rezus;
c) data nașterii;
d) sexul;
e) seria și numărul actului de identitate înregistrat în baza de date a Registrului de stat al populației;
(buletin de identitate, pașaport, adeverință de naștere etc.)
f) data decesului;
g) domiciliul - înregistrarea actuală (adresa de domiciliu a părinților, după caz);
h) date privind asigurarea obligatorie de asistență medicală;
i) date privind cetățenia persoanei (inclusiv apatrizi, refugiați etc.)
11. Funcțiile de bază asigurate de SIT sunt următoarele:
1) înregistrarea, verificarea și reactualizarea datelor pacienților, care necesită sau au beneficiat de un transplant de organ, țesut sau celule umane;
2) înregistrarea, verificarea și reactualizarea datelor persoanelor, care donează un organ, țesut sau celule umane;
3) consumul din alte sisteme a datelor privind rezultatele analizelor de laborator documentate în Fișa electronică a pacientului cu stocarea lor în baza de date a SIT, precum și investigațiilor imagistice efectuate, asigurând acces pentru vizualizarea lor în sistemul partajant;
4) acumularea și reactualizarea informațiilor privind vizitele primitorilor de transplant la medicul specialist de profil, care verifică informațiile necesare pentru a completa și reactualiza Fișa Electronica a Pacientului;
5) generarea informației privind donatorul în viață pentru Comisia independentă de avizare;
6) generarea rapoartelor conform parametrilor selectați de utilizatori, prin comunicarea cu structurile bazelor de date care conțin informații relevante.
12. SIT asigură preluarea și prelucrarea datelor din Registrul medical a următoarelor contururi funcționale:
1) evidența și controlul sănătății persoanelor fizice („Starea Sănătății”). Datele evidenței pot fi găsite în Registrele Donatorilor și Primitorilor.
2) evidența și controlul prestatorilor de servicii medicale și băncilor de țesuturi și/sau de celule autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi sau celule umane. Datele evidenței pot fi găsite în modulul „Lista instituțiilor”;
3) evidența raportării activităților prestatorilor de servicii medicale și băncilor de țesuturi și/sau de celule autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi sau celule umane. Evidență dată se va regăsi în modulul „Stocului de țesuturi și/sau celule înregistrate de băncile de țesuturi și/sau celule umane”;
4) gestionarea Listelor de asteptare naționale pentru transplantul de organe, țesuturi și celule umane. Evidența Listei de așteptare este reflectată în Registrul Primitorilor;

5) evidența și controlul Stocului de medicamente necesare primitorilor de organe în perioada post-transplant. Evidența preparatelor imunosupresive cu indicarea stocului restant se efectuiază în modulul „Medicamente prescrise”;
6) monitorizarea Stocului de țesuturi și/sau celule umane din băncile autorizate pentru import și/sau export sau schimbului de țesuturi și/sau celule umane în cadrul UE;
7) biovigilența - reprezintă implementarea procedurilor de supraveghere și raportare cu privire la apariția reacțiilor și/sau evenimentelor adverse grave, ce pot influenţa calitatea şi siguranţa organelor, ţesuturilor şi celulelor umane utilizate la om.

Capitolul IV
Structura organizațională a SI Transplant

13. Proprietarul SIT este statul.
14. Posesorul SIT este Ministerul Sănătății, cu drept de gestionare a resurselor și care asigură condițiile organizatorice și financiare pentru funcționarea și dezvoltarea acestuia.

Posesorul SIT urmează să estimeze și să prezinte către Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” resursele TI necesare pentru găzduirea SIT pe platforma tehnologică guvernamentală comună (MCloud), pentru 6, 12, 18 luni. În baza estimărilor se vor planifica și se vor aloca resursele TI necesare. Urmare a dării în exploatare a SIT, Posesorul va încheia cu Administratorul tehnic Acordul privind administrarea tehnică și menținerea SIT, care va include activitățile minime privind administrarea tehnică și menținerea SIT, precum și volumul acestora. În baza Acordului vor fi estimate cheltuielile pentru administrare tehnică a SIT care urmează a fi acoperite din bugetul de stat, prin intermediul granturilor oferite Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică”, de către fondator.
15. Deținătorul SIT este Agenția de Transplant care asigură crearea, mentenanța și monitorizarea exploatării eficiente a acestuia.
16. Administratorul tehnic al SIT este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.
17. Registratorii datelor în SIT sunt:
a) prestatorii de servicii medicale autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane;
b) băncile de țesuturi și/sau celule umane autorizate pentru desfășurarea activităților de prelevare, prelucrare, testate, conservate, stocate și distribuite pentru utilizare la om.
18. Utilizatorii datelor sunt persoanele din cadrul prestatorilor de servicii medicale autorizați cu drept de vizualizare a datelor medicale.

Capitolul V
Documentele SI Transplant

19. În cadrul SIT sunt utilizate documente de intrare, ieșire și tehnologice. Acestea vor fi actualizate în conformitate cu necesitățile domeniului vizat și actele normative.
20. Documentele de intrare includ documentația medicală de evidență primară a instituțiilor ocrotirii sănătății.
21. Documentele de ieșire includ:
1) acordul informat cu privire la includerea pacientului în lista de așteptare pentru transplant de organe;
2) acordul informat pentru donarea și aplicarea tehnologiilor de reproducere asistată medical;
3) documente importate din registrele SIT:
a) Registrul Național Renal;

b) Registrul Donatorilor vii și cadaverici de organe și țesuturi;
c) Registrul Primitorilor de organe și țesuturi;
d) Registrul Donatorilor de Celule Reproductive;
e) Registrul Primitorilor de Celule Reproductive;
4) documente importate din Lista de așteptare;
5) Lista de urgență și super-urgență a primitorilor pentru transplant;
22. Documente tehnologice care sunt generate de SIT:
1) Formularul de evidența lunară a ședințelor efectuate în centrele de dializă;
2) Scorul renal sau Scorul hepatic pentru oferta de atribuire a organului către echipa medico-chirurgicală;
3) Cererea de țesuturi sau celule umane adresată băncilor de țesuturi și/sau celule umane;
4) Fișa de prelevare emisă de centrele de prelevare, băncile de țesuturi și/sau celule;
5) Fișa de procesare a grefelor emisă de băncile de țesuturi și/sau celule umane;
6) Fișa de validare a grefelor (fișa produsului finit) emisă de băncile de țesuturi și/sau celule umane;
7) Fișa de distribuire a grefei (lor) emisă de băncile de țesuturi și/sau celule umane;
8) Fișa de trasabilitate a grefei (lor) emisă de băncile de țesuturi și/sau celule umane;
9) Formulare de biovigilență pentru raportarea, investigarea, înregistrarea şi transmiterea informaţiilor despre evenimentele şi/sau reacţiile adverse grave care pot influenţa calitatea şi siguranţa organelor, ţesuturilor şi celulelor umane utilizate la om.
23. SIT va asigura funcționalitatea de raportare prin depozitul centralizat de date.
24. SIT va asigura generarea datelor către instituțiile europene:
1) EUROCET, ERA-EDTA, ESOT, EDQM (Newsletter Transplant);
2) Platforma FOEDUS-EOEO - instrument european pentru gestionarea schimburilor transfrontaliere de organe.
25. SIT generează rapoarte de activitate ale:
a) prestatorilor de servicii medicale autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane;
b) băncilor de țesuturi și/sau celule umane autorizate pentru desfășurarea activităților de prelevate, prelucrate, testate, conservate, stocate și distribuite pentru utilizare la om.
26. Rapoartele reflectă următoarele aspecte:
1) diagnosticul după Clasificatorul Internațional al Maladiilor CIM-10;
2) categoria de vârstă (1-18 ani, 19-35 ani, 36-60 ani, 60 ani > etc);
3) serviciile medicale acordate.
27. Prestatorii de servicii medicale și băncile de țesuturi și/sau celule umane autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane pot exporta rapoartele de activitate în format Excel pentru prezentarea lor la AT.

Capitolul VI
Spațiul informațional al SI Transplant

Secțiunea 1
Obiectele informaționale gestionate

28. Lista principalelor obiecte informaționale utilizate în SIT:
1) persoane fizice – pacienții (donatori și primitori), care beneficiază de servicii medicale în vederea donării sau primirii unui organ, țesut sau celule umane în scop terapeutic;
2) personal medical - implicat în prestarea serviciilor medicale și activităților de transplant autorizate;
3) organe, țesuturi și celule umane utilizate în scop terapeutic, în calitate de atribut al persoanei fizice (pacient);

4) medicamente specifice (imunosupresive, antivirale, hepatoprotectoare, anticorpi monoclonali etc.).
5) laboratoare clinice din cadrul prestatorului de servicii medicale;
6) centre/secții de dializă din cadrul prestatorului de servicii medicale;
7) centre/instituții medicale de investigatii imagistice din cadrul prestatorului de servicii medicale.
29. Fiecare persoană în calitate de obiect informațional va avea un identificator numeric unic „Cod SIT", care va fi generat de aplicație în mod automat. „Codul SIT" ca element principal de pseudonimizare conform prevederilor regulamentului UE 2016/679 GDPR va fi utilizat constant în SIT. Obiectele împrumutate din alte SI vor respecta codificarea impusă de SI care le-a generat. În SIT ele vor fi utilizate fără modificări.
30. Atributele obiectelor informaționale utilizate în SIT.
1) Obiectul informational „persoană fizică" – pacient
a) datele de identificare:
i) numărul de identificare de stat (IDNP);
ii) numele, prenumele şi patronimicul;
iii) sex;
iiii) data naşterii;
iiiii) grupa sangvină.
b) date demografice:
i) cetăţenie;
ii) tipul documentului de identificare;
iii) numărul documentului.
c) adresa de reşedinţă permanentă şi temporară:
i) localitatea şi ţara;
ii) strada;
iii) blocul;
iiii) apartamentul.
d) date privind asigurarea medicală:
i) categoria de asigurat;
ii) statutul de asigurat;
iii) asigurător;
iiii) tipul de asigurare.
e) date specifice despre sănătate:
i) date despre evidenţă;
ii) date despre consultaţii şi examene medicale;
iii) date despre diagnostice;
iiii) date despre examene de laborator;
iiiii) date despre efectele adverse şi complicaţiile în cadrul tratamentului.
2) Obiectul informational „persoană fizică" – personal medical
a) date de identificare:
i) numărul de identificare de stat (IDNP);
ii) numele;
iii) prenumele;
iiii) patronimicul.
b) date socioeconomice
i) locul de muncă.
3) Obiectul informational „prestator servicii medicale"
a) numărul de identificare de stat (IDNO);
b) denumirea;

c) codul fiscal;
d) codul IMS;
e) tip;
f) numărul de telefon;
g) adresa poştală;
h) adresa electronică a persoanei juridice sau a întreprinzătorului individual.

4) Obiectul informational „medicamentele aflate în gestiunea prestatorilor de servicii medicale”
a) ID-ul medicamentului (Nomenclator);
b) unitatea de măsură;
c) cantitatea în unitățile indicate;
d) data producerii medicamentului dat;
e) data expirării medicamentului;
f) stocul/factura din care a fost creat acest stoc gestionat;
g) codul medicamentului din Nomenclator;
h) numele medicamentului;
i) substanța activă a medicamentului;
j) numărul cu care a fost înregistrat acest medicament;
k) forma farmaceutică;
l) compania producătoare a acestui medicament.

Secțiunea 2
Scenariile de bază aferente obiectelor informaționale

31. Scenariile de bază a principalelor procese-business sunt prezentate în continuare în formă de schemă, prezentată în anexa nr. 1 la prezentul Concept.

32. Lista rolurilor de business va include persoane nominalizate responsabile pentru gestionarea datelor în SIT, care au stabilite reguli de securitate, corespunzător drepturilor de acces pentru:
1) introducerea datelor cu caracter personal și medical doar pe spațiul SIT;
2) editarea datelor cu caracter personal și medical doar pe spațiul SIT;
3) vizualizarea datelor cu caracter personal și medical.

33. Asocierea între rolurile de business existente în sistem și funcționalitățile necesare fiecărui rol, stabilește modul în care este realizată securitatea accesului la sistem, prezentată în anexa nr. 2 la prezentul Concept.

34. Evidența și controlul înregistrărilor în modulele asociate rolurilor de business vor fi interdependente și vor funcționa în cadrul aceluiași sistem unitar. Scenariul schemei logice este prezentată în anexa nr. 3 la prezentul Concept.

35. Evidența activităților desfăşurate în bancile de ţesuturi şi/sau celule umane va include:
1) înregistrarea etapelor lanţului, de la donare până la distribuţia ţesuturilor şi/sau celulor umane efectuate în conformitate cu procedurile specifice fiecărui ţesut şi/sau celulă cu descrierea fiecărei etape de la recepţionare până la distribuţie şi evaluarea calitativă;
2) validarea produsului terapeutic prin control biologic şi descrierea funcţională;
3) certificarea fiecărui produs prin Fişa produsului finit şi transmiterea ei odată cu distribuţia ţesutului sau celulelor umane;
4) înregistrarea privind destinaţia finală a ţesuturilor sau celulelor umane distribuite;
5) identificarea la fiecare stadiu al activităţilor desfăşurate pentru fiecărei unităţi de ţesut sau celule umane.
6) sistemul va asigura trasabilitatea tuturor etapelor necesare activităţilor: codificarea, selecţia donatorului, procurarea, procesarea, conservarea, stocarea, distribuţia şi transportul, incluzând şi aspectele privind controlul de calitate;

7) sistemul informațional al băncii de țesuturi și/sau celule umane reprezintă o bază de date specializată, adaptată, securizată care va fi integrabilă în SIT;
8) referința comună între SIT și sistemul informațional al băncii de țesuturi și/sau celule umane o va constitui IDNP-ul persoanei.

Secțiunea 3
Interacțiunea cu alte sisteme și platforme electronice guvernamentale

36. În vederea asigurării funcționalității SIT și pentru preluarea de date relevante din alte resurse informaționale de stat, acesta interacționează prin intermediul platformei de interoperabilitate (MConnect) cu următoarele resurse informaționale:
1) Registrul de stat al unităților de drept – pentru schimbul automatizat de date aferent informației privind înregistrarea și evidența de stat a persoanelor juridice prestatoare de servicii medicale, autorizate pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane etc.;
2) Registrul de stat al populației – pentru înregistrarea, căutarea și reactualizarea datelor pacienților, care necesită sau au beneficiat de transplant de organ, țesut sau celule umane, sau care donează un organ, țesut sau celule umane;
3) Sistemul Informațional Asistența Medicală Primară și Sistemul Informațional Asistență Medicală Spitalicească – pentru crearea și reactualizarea fișei pacientului inclusiv a datelor de laborator, investigațiilor imagistice, care jurnalizează interacțiunile pacientului cu sistemul medical la nivel național, generarea rapoartelor statistice necesare pentru monitorizarea activităților de prelevare și transplant etc.
4) Sistemul Informațional Servicii Sânge – pentru consumul și partajarea datelor grupului sangvin și factorului rezus al persoanei conform IDNP către SI AMP și SI AMS.
37. SIT este găzduit pe platforma tehnologică guvernamentală comună (MCloud) și este compatibil cu platforma de găzduire bazată pe tehnologii de tip container.
38. SIT va interacționa cu următoarele platforme și sisteme informaționale partajate:
1) platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte sisteme informaționale și registre de stat;
2) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice ieșite din sistem;
3) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în cadrul sistemului;
4) serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiilor (evenimentelor) produse în cadrul SIT;
5) Sistemul informațional „Catalogul semantic” a Agenției de Guvernare Electronică - în scopul asigurării interoperabilității pentru evidența metadatelor ca resurse informaționale și a schimbului de date cu alte sisteme și resurse informaționale de stat;
6) platforma de găzduire și partajare a documentelor (MDocs) – soluție guvernamentală destinată implementării unui mecanism centralizat de stocare pe platforma tehnologică comună (MCloud) și partajare online a documentelor rezultate din activitatea autorităților publice;
7) Serviciul guvernamental de notificare electronică (MNotify), aprobat prin Hotărârea Guvernului nr.376/2020 – pentru primirea notificărilor electronice generate de alte sisteme informaționale, cu care SIT comunică.
8) În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, Agenția de Transplant înregistrează activele semantice utilizate în SIT în Sistemul informațional „Catalogul semantic”.

Capitolul VII
Spațiul tehnologic al SI Transplant

39. La dezvoltarea SIT se va aplica arhitectura multinivel, având cel puțin următoarele nivele: baza de date, logica de aplicație și interfața cu utilizatorul și principiile agile. Utilizarea unei astfel de arhitecturi și principii, va permite cuplarea redusă între componente. Responsabilitățile fiecărei componente sunt specializate și permite implementarea iterativă, operarea modificărilor și flexibilitate în implementare.
40. SIT va utiliza standarde deschise și va fi compatibil cu sistemele care, la fel, utilizează atât standarde nonproprietare, cât și standarde deja existente.
41. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către posesor în etapele ulterioare de dezvoltare a SIT, ținând cont de:
1) implementarea unei soluții bazate pe SOA (Service-Oriented Arhitecture – arhitectură software bazată pe servicii), care oferă posibilitatea reutilizării unor funcții ale SIT cu noi funcționalități, fără a afecta funcționarea SIT;
2) implementarea funcționalităților de arhivare (backup) și restabilire a datelor în caz de incidente.
42. SIT va putea fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori atât în regim normal de lucru, cât și în perioadele de vârf.
43. Sistemul de comunicații se va baza pe infrastructură și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării la Internet. Infrastructura existentă va fi planificată în mod corespunzător, pentru a oferi nivelurile adecvate de performanță și capacitate.
44. Interfața de utilizare a SIT se va adapta automat la diverse rezoluții de afișare și va fi disponibilă în limbile română și rusă.
45. Interfața de utilizare a SIT va fi implementată folosind tehnologiile, care vor asigura funcționarea serviciului pe dispozitivele mobile.
46. Având în vedere locul SIT în cadrul resurselor informaționale de stat ale Republicii Moldova, este necesară o disponibilitate permanentă și acces neîntrerupt la sistem. Din acest motiv, întreaga soluție va fi construită în regim de înaltă disponibilitate (24 de ore/zi, 7 zile/ săptămână).

Capitolul VIII
Asigurarea securității informaționale a SI Transplant

47. Esența securității informaționale a SIT constă în următoarele:
1) prin securitate informațională se înțelege protecția resurselor și a infrastructurii informaționale a SIT împotriva acțiunilor premeditate sau accidentale cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanților la procesul de schimb informațional;
2) noțiunea de securitate informațională a SIT include o serie de termeni, cum ar fi: măsuri, politici, tehnologii, puncte de control, structură organizațională, atribuții și funcții în sistem. Mijloacele de control pentru asigurarea securității informaționale a SIT sunt implementate;
3) colectarea, prelucrarea, stocarea și furnizarea datelor cu caracter personal se efectuează în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal;
4) pentru a atinge un nivel sporit al securității informaționale trebuie să se țină cont de cele două părți componente ale acesteia – securitatea fizică și securitatea informațională:
a) securitatea fizică se referă la protejarea infrastructurii fizice a sistemului, prin aplicarea tuturor măsurilor de securitate;
b) securitatea informațională presupune protejarea informației prin aplicarea unor măsuri de securizare la nivel logic, prin utilizarea tehnologiilor informaționale. Aceasta include programele antivirus, delimitarea logică a subrețelelor, firewall, backup, sistem de producție, controlul asupra folosirii programelor piratate, evidența și actualizarea licențelor produselor software;

c) securitatea aplicației presupune protejarea informației prin delimitarea accesului diferențiat la date, bazat pe roluri. În arhitectura sistemului sunt incluse mecanisme de securitate la nivelul aplicației care include cel puțin acces pe baza de utilizator și parolă, iar conexiunea se urmărește prin Mpass și Msign. Semnarea documentelor tehnologice generate de sistem se va efectua utilizând serviciul Msign prin intermediul token-ului personificat.

48. Pericolul informațional reprezintă un eveniment sau o acțiune posibilă, orientată spre cauzarea unui prejudiciu resurselor sau infrastructurii informaționale. Principalele pericole pentru securitatea informațională a SIT sunt:

1) utilizarea ilegală a informației;
2) încălcarea tehnologiei de prelucrare a informației;
3) implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația care însoțește aceste produse;
4) elaborarea și răspândirea la nivelul centrului de date a programelor ce pot afecta funcționarea normală a sistemelor informaționale și de comunicații, precum și a sistemelor de protecție a informației;
5) nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor hardware și/sau software de prelucrare a informației;
6) compromiterea credențialelor, a cheilor și a mijloacelor de protecție criptografică a informației;
7) scurgerea de informație prin canale tehnice;
8) implementarea dispozitivelor electronice de interceptare a informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor prin canalele de comunicații, precum și în încăperile de serviciu ale registratorilor sistemului;
9) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;
10) tentativele de interceptare a informației în rețelele locale ale registratorilor sistemului și în liniile de comunicații, decodificarea ei și impunerea informației false;
11) utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție a datelor, a mijloacelor de informatizare și comunicații la crearea și dezvoltarea infrastructurii informaționale;
12) accesul neautorizat la resursele informaționale care se află în bazele de date;
13) încălcarea restricțiilor legale ce țin de răspândirea informației.

49. SIT prevede următoarele cerințe și sarcini privind asigurarea securității informaționale:

1) asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017. Pentru gestiunea riscurilor de securitate va fi implementată o politica generală de securitate. Personalul implicat în utilizarea și administrarea SIT va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și a stabili domeniile care necesită îmbunătățiri;
2) securitatea informațională trebuie să asigure:
a) confidențialitatea informației, care presupune limitarea accesului la informație al persoanelor fără drepturi și împuterniciri corespunzătoare;
b) integritatea logică a informației, adică prevenirea introducerii, modificării, copierii, actualizării și nimicirii neautorizate a informației;
c) integritatea fizică a informației;
d) protecția infrastructurii informaționale împotriva deteriorării și încercărilor de modificare a funcționării;
3) pentru îndeplinirea sarcinilor privind asigurarea securității informaționale a SIT se utilizează următoarele mecanisme:
a) dubla autentificare și autorizarea utilizatorului;
b) managementul accesului;

c) înregistrarea acțiunilor și auditul prin mecanisme de tip log;
d) primirea notificărilor electronice din sistemele informaționale, cu care este stabilită interoperabilitatea cu ajutorul serviciului electronic MNotify.
50. Pericolele securității informaționale sunt:
1) colectarea și utilizarea ilegală a datelor;
2) încălcarea tehnologiei de prelucrare a datelor;
3) implementarea în produsele software și hardware a componentelor care îndeplinesc funcții neprevăzute în documentația aferentă acestor produse;
4) elaborarea și răspândirea programelor ce afectează funcționarea normală a sistemelor informaționale și a comunicațiilor electronice, precum și a sistemelor securității informaționale;
5) nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a datelor și a comunicațiilor electronice;
6) influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;
7) compromiterea cheilor și a mijloacelor de protecție criptografică a informației;
8) scurgerea informației prin canale tehnice;
9) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor, utilizând sistemele de comunicații, precum și în încăperile de serviciu ale autorităților administrației publice;
10) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;
11) interceptarea datelor în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea unei informații false;
12) utilizarea, la crearea și dezvoltarea infrastructurii informaționale de comunicații electronice, a tehnologiilor informaționale naționale și internaționale, a mijloacelor de protecție a informației și a mijloacelor de informatizare care nu sunt certificate;
13) accesul nesancționat la resursele informaționale din băncile și bazele de date;
14) încălcarea restricțiilor legale privind răspândirea informației;
15) încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.
51. SIT asigură realizarea următoarelor obiective de securitate:
1) autentificarea – garantează că zonele restricționate ale SIT vor fi accesibile doar utilizatorilor cu o identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass);
2) autorizarea – garantează că utilizatorii autentificați prin serviciul electronic guvernamental de autentificare și control al accesului (MPass) pot accesa serviciile și datele care corespund drepturilor lor de acces:
3) confidențialitatea – garantează că datele înregistrate în SIT nu pot fi accesate de o parte terță neautorizată;
4) integritatea – garantează că datele înregistrate în SIT nu au fost modificate sau alterate de o parte terță neautorizată;
5) nonrepudierea – garantează că datele înregistrate în SIT nu pot fi negate mai târziu.
52. Pentru atingerea obiectivelor de securitate, SIT dispune de mai multe mecanisme de securitate:
1) semnătura electronică – mecanism ce asigură integritatea și nonrepudierea datelor înregistrate în SIT;
2) firewall – filtrul firewall face parte din arhitectura tehnică a platformei tehnologice guvernamentale comune (MCloud) pentru a asigura un mecanism de apărare împotriva utilizatorilor externi neautorizați;

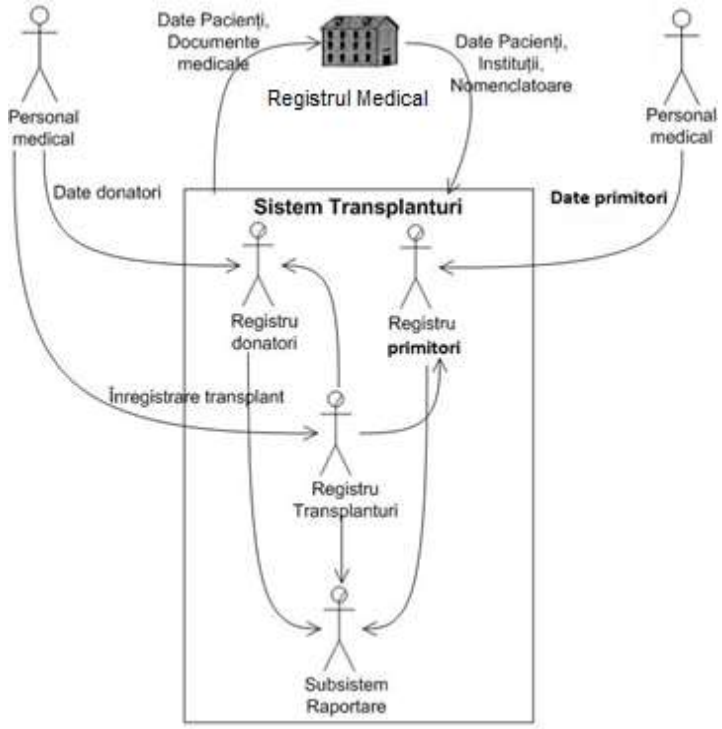
3) antivirus/antispam – soluțiile hardware și/sau software asigură protecția antivirus și antispam pentru toate serverele. Fișierele se scanează la încărcare în SIT. În cazul detectării unui fișier infectat, procedura de încărcare este oprită și fișierul – respins;
4) sistem de detectare a intruziunilor – sistem de detectare a accesului neautorizat la nivelul componentelor de sistem al SIT;
5) comunicare sigură (transferuri de date) între serverele web și utilizatori – schimbul de informații confidențiale este securizat;
6) backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;
7) instrument de înregistrare a evenimentelor de audit – toate activitățile desfășurate de către utilizatori, indiferent dacă au succes sau nu (cum ar fi conectările încercate, dar nereușite), sunt monitorizate și înregistrate în jurnalele SIT, cu acces limitat pentru utilizatorii neautorizați.
53. În cadrul SIT se asigură generarea și păstrarea înregistrărilor de audit ale securității pentru operațiile de prelucrare a datelor cu caracter personal în condițiile cadrului normativ în materie de protecție a datelor cu caracter personal. Înregistrările de audit ale operațiilor și rezultatele acestora pot fi accesate de către Centrul Național pentru Protecția Datelor cu Caracter Personal și puse la dispoziția acestuia în scopul investigării potențialelor încălcări ale regimului de prelucrare/protecție a datelor cu caracter personal. SIT va utiliza funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).
54. Utilizatorii SIT vor fi autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia. Utilizatorii și rolurile acestora vor fi gestionate prin intermediul serviciului MPass. SIT va prelua rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).
55. Necesitate importantă legată de securitate este păstrarea înregistrărilor de audit pentru analiza integrității SIT și pentru monitorizarea activității utilizatorilor. SIT se va baza pe un mecanism de înregistrări de audit dublu (intern și cu utilizarea serviciului electronic guvernamental de jurnalizare (MLog)), ce urmează practicile internaționale.

Capitolul IX
Încheiere

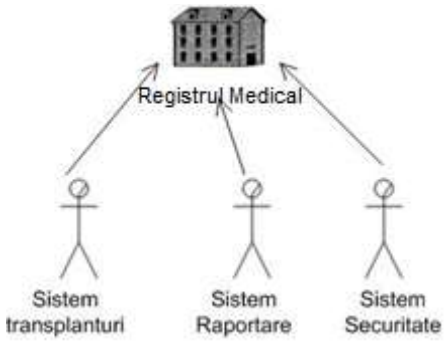
56. SIT va oferi beneficii importante părților implicate în activitățile de donare, prelevare și transplant de organe, țesuturi și celule umane și este caracterizat prin generarea avantajelor cum ar fi:
1) este proiectat și dezvoltat în baza modelelor sectorului similar de activitate din țările UE;
2) urmărește eliminarea mulțimii de dosare în format de hârtie care sunt greu de gestionat;
3) urmărește implementarea unor mecanisme de monitorizare și control al calității pentru serviciile medicale de înaltă performanță oferite populației;
4) este prietenos în utilizare și se bazează pe cunoștințele utilizatorilor legate de navigarea pe internet;
5) asigură protecția datelor și are posibilitatea interoperabilității cu alte sisteme informatice;
6) asigură trasabilitatea prin sisteme de interconectare (web-servicii cu grad înalt de securitate) a activității medicale, în mod bidirecțional la toate etapele lanţului, de la donare până la transplant și monitorizare în timp real;
7) asigură calitatea serviciilor datorită implementării biovigilenței;
8) generează rapoarte statistice atât pentru management intern, cât și pentru autoritățile competente din domeniu.
57. SIT va asigura modernizarea serviciilor medicale pentru domeniul de transplant în conformitate cu prevederile Directivelor și Recomandărilor UE în sectorul medical vizat, respectând în totalitate legislația Republicii Moldova.

Anexa nr. 1
la Conceptul SIT
nr.[…] din […] 2024

1) *Scenariul prin care se realizează în mod dinamic Fișa Electronică a Pacientului (EHR).*
Vizita unui pacient la instituția medicală și actualizarea datelor din Fișa Electronică a Pacientului (FEP) este reprezentată în următoarea schemă:



2) Preluarea FEP din alte sisteme în baza de IDNP concomitent oferindui-se un ”Cod SIT” oferă posibilitatea de a stabili dacă datele pacientului au fost introduse preliminar în sistem. În funcție de rezultatul obținut la interpelarea sistemului, pot fi vizualizate, editate datele unui pacient existent în SIT, sau se va adăuga un pacient nou.

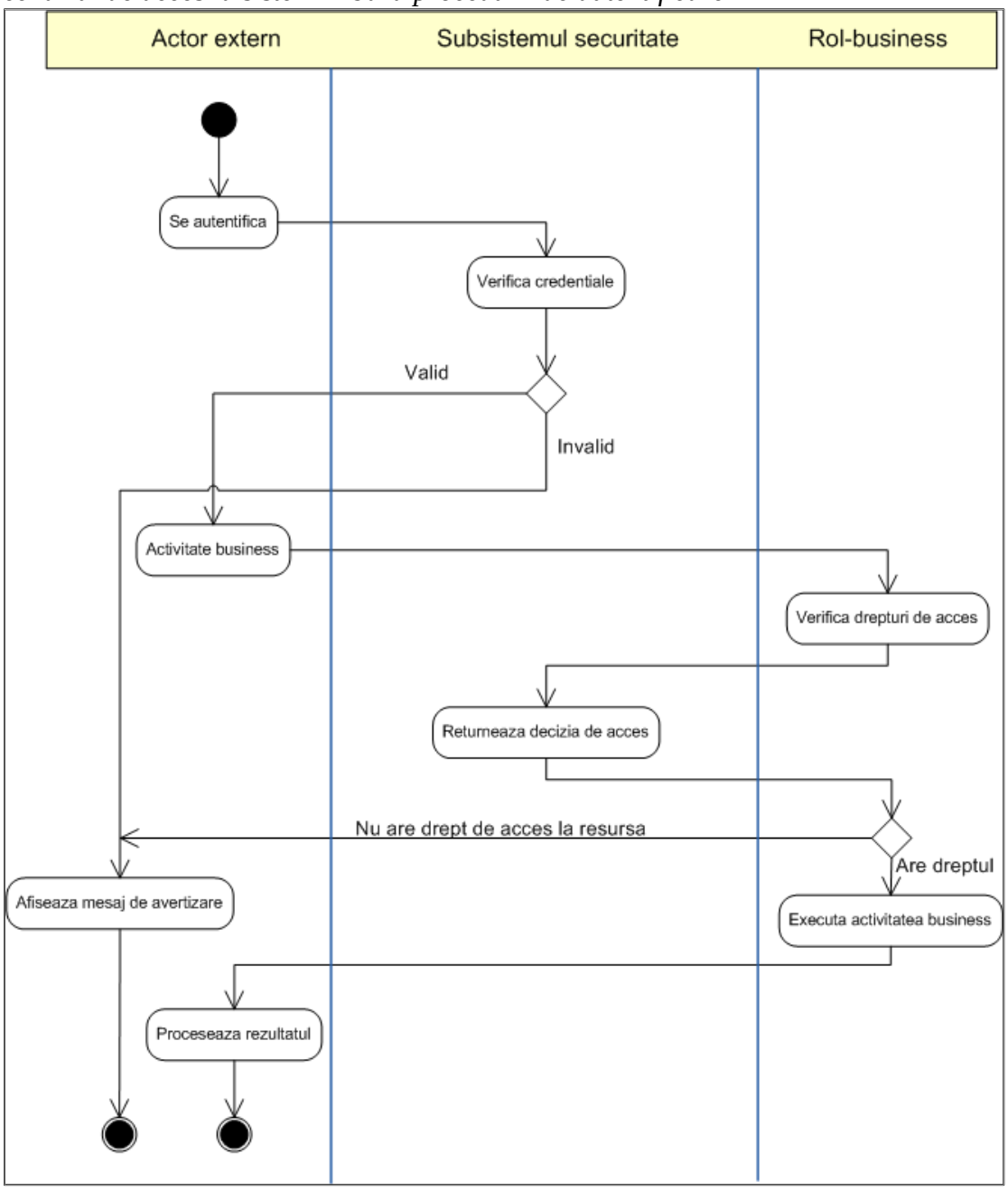


Anexa nr. 2
la Conceptul SIT
nr.[…] din […] 2024

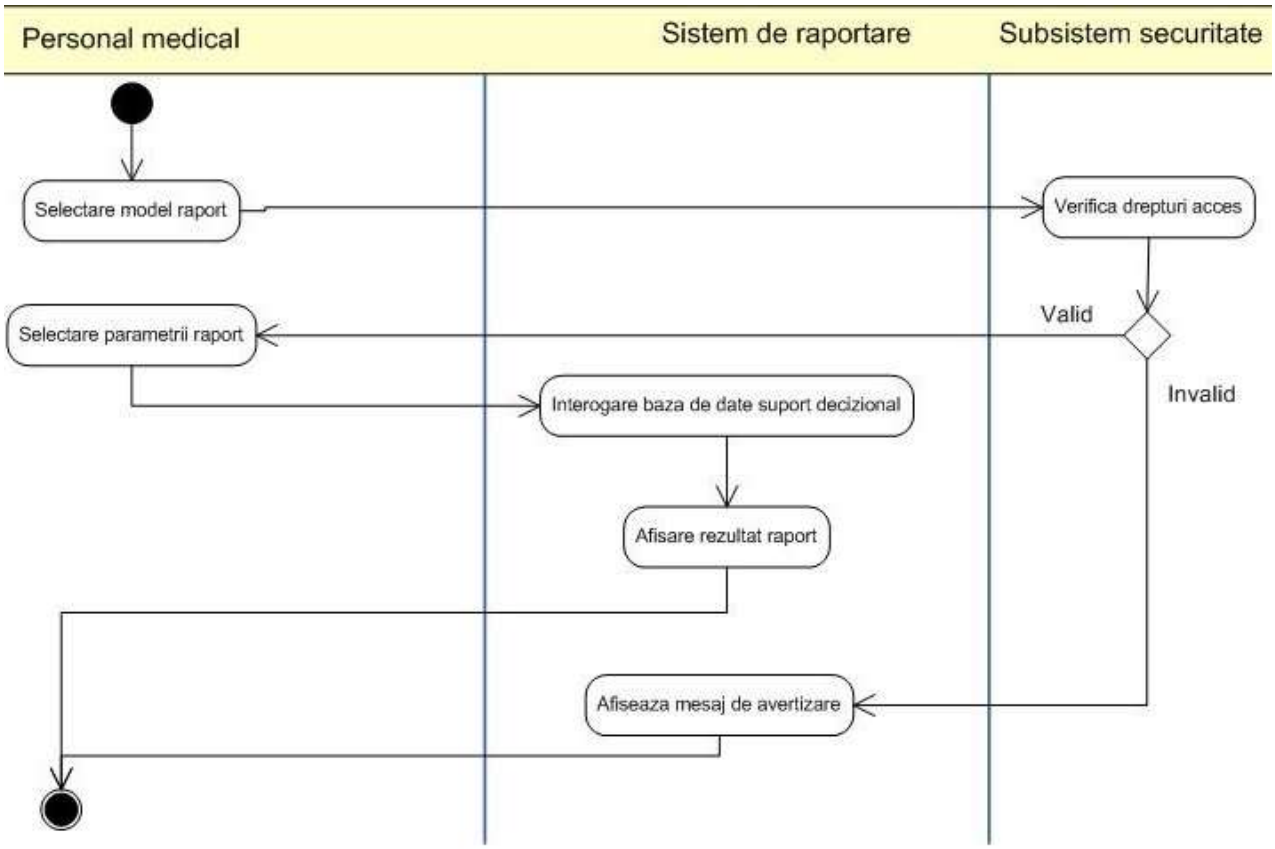
Nr. crt	Denumirea rolului-business	Funcționalități SIT datorate interoperabilității asigurate de SI AMS și SI AMP
1.	Medic coordonator din cadrul AT	Registrul Donatorilor de organe, țesuturi umane Registrul Primitorilor de organe, țesuturi umane Registrul de Refuz organe, țesuturi umane
2.	Coordonatorul de transplant numit de prestatorul de servicii medicale responsabil de identificarea și înregistrarea donatorilor pentru prelevarea organelor, țesuturilor, celulelor umane	Registrul electronic al pacienților aflați la tratament în secția de Terapie Intensivă este realizat prin SI AMS interconectat cu SIT pentru verificarea prezenței înregistrării datelor pacientului în Registrul de Refuz
3.	Medicul de laborator HLA responsabil de introducerea datelor privind compatibilitatea imuno-histo-chimică și izo-serologică între donator și primitor	Lista națională de urgențe în transplant Lista de așteptare a primitorilor de rinichi Lista de așteptare a primitorilor de cord Lista de așteptare a primitorilor de pancreas Lista de așteptare a primitorilor medulari
4.	Medicul responsabil de prelevarea organelor, țesuturilor sau celulelor umane	Registrul Donatorilor – Medicul echipei de prelevare Etichetele pentru organe, țesuturi sau celule umane
5.	Medicul responsabil de transplant de organe	Registrul Donatori Vii – Medicul echipei de transplant Registrul Primitori (listele de așteptare) Registrul Transplant Renal – Medicul echipei de transplant Registrul Transplant Hepatic – Medicul echipei de transplant Registrul Transplant Cardiac – Medicul echipei de transplant Registrul Transplant Pancreas – Medicul echipei de transplant
6.	Medicul responsabil de includerea primitorului în lista de așteptare pentru transplantul de organe	Registrul Național Renal – Medicul nefrolog Registrul Hepatic – Medicul hepatolog Registrul Diabetului – Medicul endocrinolog Registrul Cardiac – Medicul cardiochirurg
7.	Medicul responsabil de monitorizarea primitorilor de organ în perioada post-transplant	Registrul Transplant Renal – Medicul nefrolog Registrul Transplant Hepatic – Medicul hepatolog Registrul Transplant Cardiac – Medicul cardiochirurg, cardiolog Sub-modulul ”Stoc Medicamente” - parte componentă a registrelor menționate de mai sus
8.	Medicul responsabil de realizarea transplanturilor de țesuturi (oftalmolog, ortoped, combustiolog, chirurg etc.)	Lista așteptare transplant de cornee Registrele de evidență a transplanturilor de țesuturi realizate
9.	Medicul responsabil de selectarea donatorilor și primitorilor de celule reproductive	Registrul donatorilor de celule reproductive Registrul primitorilor de celule reproductive
10.	Medicul responsabil de utilizarea celulelor reproductive pentru reproducerea asistată medical	Registrul donatorilor de celule reproductive Registrul primitorilor de celule reproductive
11.	Persoana responsabilă din cadrul băncii de țesuturi și/sau celule	Registrul Țesuturilor Stocate (cornee, os, ligamente, mușchi-tendon, amnion, piele, vase magistrale, periferice, valve cardiace)
12.	Persoana responsabilă din cadrul băncii de țesuturi și celule reproductive	Registrul Celulelor Reproductive: gameți, embrioni, țesut reproductiv masculin (testicular) și femenin (ovarian) pentru evidența stocurilor de celule reproductive
13.	Medicul responsabil de vigilență	Modulul de Biovigilență
14.	Administrator AT	Modulul de securitate informațională

Anexa nr. 3
la Conceptul SIT
nr. […] din […] 2024

1) Scenariul de acces la sistem în baza procedurii de autentificare



2) Scenariul de acces la sistem în baza rolurilor de business.



3) Scenariul de generare a rapoartelor și statisticilor.

Prin acest scenariu sunt realizate rapoartele și statisticile privind:

- evidența pacienților ce necesită un organ;
- evidența centrelor de dializă;
- evidența operațiilor de transplant realizate;
- evidența stocurilor de țesuturi;
- evidența stocurilor de celule;
- evidența donatorilor și primitorilor de organe, țesuturi, celule umane în scop terapeutic;
- evidența stocurilor de medicamente necesare pacienților după transplant;
- consultarea și actualizarea documentelor medicale ale pacienților aflați în listele de așteptare;
- consultarea informațiilor legate de efectuarea operațiilor de transplant după hotarele țării;
- interacțiunea cu platformele europene pentru gestionarea schimburilor transfrontaliere de organe;
- generarea rapoartelor personalizate și statisticilor.

Anexa nr. 2
la Hotărârea Guvernului nr.___/_____

REGULAMENTUL
Resursei Informaționale ținute pe Sistemul Informațional Transplant

Capitolul I
Dispoziții generale

1. Regulamentul Resursei Informaționale ținute pe Sistemul Informaţional Transplant (în continuare - *Regulament*) cuprinde reglementări privind drepturile şi obligaţiile subiecților raporturilor juridice aferente creării şi ținerii resursei informaționale; modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare şi radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității resursei informaționale.
2. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută în Legea nr. 467/2003 cu privire la informatizare şi la resursele informaționale de stat, Legea nr. 71/2007 cu privire la registre, Legea nr. 42/2008 privind transplantul de organe, ţesuturi şi celule umane, Legea nr. 133/2011 privind protecția datelor cu caracter personal, Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical, precum și Conceptul SIT.
3. Resursa Informațională a Sistemului Informaţional Transplant (în continuare – *RISIT*) constituie un ansamblu de tehnologii informaţionale, mijloace tehnice şi metodologii, destinat gestionării informaţiei medicale în cadrul prestatorilor autorizați cu scopul evidenței, actualizării, analizei și raportării datelor în conformitate cu prevederile legale privind accesul la informaţiile cu caracter personal, în vederea realizării unei imagini corecte a resurselor (date privind donatorii și primitorii).
4. RISIT este resursa informaţională de stat care reprezintă totalitatea informației sistematizate cu privire la starea sănătății persoanelor:
   1) ce necesită transplant de organ/țesut/celulă (primitorii);
   2) care donează organul/țesutul/celulele (donatorii);
   3) care au solicitat să fie înregistrate în Registrul de Refuz. Cu ajutorul acestei resurse Agenţia de Transplant organizează şi supraveghează înregistrarea și reactualizarea permanentă a datelor privitoare la desfășurarea activităţilor de transplant la nivel naţional, în conformitate cu legislaţia, contribuind astfel combaterii traficului ilicit de organe, ţesuturi şi celule umane.
5. Registrul de Refuz RISIT, în calitate de modul funcțional RISIT, reprezintă o resursă informațională a persoanelor ce refuză să devină donator de organe, țesuturi sau celule după decesul său, datele cărora nu vor putea fi înregistrate în Registrul Donatorilor de nici un prestator autorizat. Modalitatea includerii, cât și radierii datelor din Registrul de Refuz se efectuează în baza unei cereri a subiectului deținător de date cu caracter personal pe suport de hârtie arhivat corespunzător procedurii în dosarul dedicat.

Capitolul II
Subiecții raporturilor juridice în domeniul creării, exploatării și utilizării RISIT
Atribuțiile, obligațiile și drepturile acestora

6. Subiecții din domeniul exploatării și utilizării RISIT sunt:
   1) proprietarul;
   2) posesorul;
   3) deținătorul;

4) administratorul tehnic;
5) registratorul;
6) destinatarul;
7) furnizorul de date.

7. Proprietarul RISIT este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din RISIT.

8. Posesorul RISIT este Ministerul Sănătății, cu drept de gestionare și de utilizare a datelor și a resurselor conținute de acestea și care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea sistemului informațional.

9. Drepturile și obligațiile Posesorului sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical și Hotărârea Guvernului nr. 148/2021 cu privire la organizarea și funcționarea Ministerului Sănătății.

1) Posesorul este obligat:
a) să asigure efectuarea controlului intern privind ținerea RISIT;
b) să asigure condiții juridice pentru crearea și ținerea RISIT;
c) să informeze deținătorul despre modificările legislative care afectează funcționarea RISIT;
d) să informeze registratorii despre vulnerabilitățile RISIT.

2) Posesorul are dreptul:
a) să stabilească prioritățile de dezvoltare a RISIT;
b) să solicite deținătorului dezvoltarea funcționalităților noi în conformitate cu prioritățile de politici în domeniul sănătății și asigurării obligatorii de asistență medicală;
c) să modifice documentația privind gestiunea și exploatarea RISIT;
d) să delege deținătorului RISIT și/sau registratorului dreptul de prelucrare a datelor cu caracter personal, asigurare a protecției datelor cu caracter personal.

10. Agenția de Transplant este deținătorul RISIT și asigură crearea, administrarea, mentenanța și dezvoltarea sistemului informațional.

11. Deținătorul RISIT este obligat:
1) asigură sprijinul tehnic și informativ pentru crearea și acordarea conturilor de acces la RISIT;
2) monitorizează procesul de înregistrare și prelucrare a datelor în RISIT;
3) verifică respectarea condițiilor de înregistrare, evidență și utilizare a datelor cu caracter personal;
4) asigură securitatea și protecția datelor din RISIT în limitele competențelor;
5) administrează rolurile și a drepturilor de acces corespunzătoare tipului de activitate în RISIT;
6) stabilește măsurile tehnice și organizatorice de protecție și securitate a RISIT;
7) elaborează și aprobă Planul de continuitate al RISIT, instituie activități de control menite să diminueze riscurile privind integritatea datelor;
8) exercită alte atribuții necesare pentru asigurarea bunei funcționări a RISIT;
9) elaborează, coordonează și aprobă procedurile operaționale aferente gestionării și asigurării bunei funcționări a RISIT;
10) stabilește regulile și procedurile specifice de acordare/suspendare/retragere/anulare a accesului la contururile RISIT și de stabilire a rolurilor registratorilor/utilizatorilor.
11) efectuează auditul securității RISIT privind gestiunea datelor cu caracter personal
12) implementează generarea copiilor de rezervă ale RISIT pentru prelucrările automatizate ale datelor din registru (copiile vor fi stocate pe suport tehnic, păstrat în locuri protejate);
13) asigură, în caz de necesitate, restabilirea funcționalității RISIT în baza copiilor de rezervă generate în prealabil;

14) supraveghează respectarea cerințelor de securitate informațională de către registratori, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora (incidentele de securitate), întreprinde măsurile necesare pentru prevenirea, limitarea şi lichidarea consecințelor. În termen de cel mult 72 de ore de la constatarea incidentului, notifică acest incident Centrului Național pentru Protecția Datelor cu Caracter Personal;

15) asigură dezvoltarea funcționalităților noi în sistemele informaționale deținute, în conformitate cu prioritățile stabilite de posesor.

12. Deținătorul RISIT are dreptul:

1) să dezvolte, în funcție de competenta sa, documentele normative aferente RISIT;

2) să propună soluții pentru perfecționarea şi eficientizarea procesului de funcționare a RISIT, precum şi să le pună în aplicare;

3) să supravegheze respectarea cerințelor de securitate a informației de către registratorii care formează RISIT, să fixeze cazurile şi tentativele de încălcare a acestora;

4) să inițieze procedura de suspendare a drepturilor de acces la RISIT dacă nu se respectă regulile, standardele şi normele general acceptate în domeniul securității informaționale și protecției datelor cu caracter personal;

5) să verifice autenticitatea şi veridicitatea datelor introduse în RISIT;

6) să solicite de la registratori actualizarea sau corectarea datelor din RISIT în caz de depistare a omiterilor şi erorilor.

13. Deținătorul asigură păstrarea RISIT până la adoptarea deciziei privind lichidarea acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

14. Administratorul tehnic al RISIT este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care va asigura administrarea tehnică și menținerea sistemului în conformitate cu cadrul normativ care reglementează domeniul.

15. Registratorii RISIT sunt persoanele autorizate din cadrul prestatorilor de servicii medicale publice și private să înregistreze și/sau să valideze datele în RISIT, precum și persoanele împuternicite de către deținătorul RISIT să înregistreze și/sau să valideze datele.

16. Registratorii au următoarele obligații:

1) asigură, în termenele și în condițiile stabilite, introducerea și validarea informațiilor relevante în baza de date a RISIT;

2) asigură autenticitatea, plenitudinea și integritatea datelor;

3) raportează posesorului incidentele de infrastructură, erorile de sistem sau erorile cauzate de alți factori, în scopul remedierii acestora;

4) solicită deținătorului autorizarea accesului, precum și suspendarea drepturilor de acces în RISIT;

5) raportează posesorului sau administratorului tehnic problemele de sistem privind utilizarea RISIT;

6) prezintă propuneri de îmbunătățire și dezvoltare a RISIT, participă în grupurile de lucru organizate în scopul dezvoltării acestuia.

17. Prestatorii desemnează și informează deținătorul despre numărul, numele, prenumele angajaților acestora cu atribuții de Registratori a datelor în RISIT.

18. Registratorii RISIT au următoarele drepturi:

1) să participe la dezvoltarea și la îmbunătățirea RISIT;

2) să prezinte propuneri cu privire la inițierea modificărilor actelor normative care reglementează funcționarea RISIT;

3) să solicite și să primească informația statistică cu privirile la înregistrările din sistem;

4) să prezinte propuneri privind perfecționarea și eficientizarea RISIT.

19. Furnizori ai datelor către RISIT sunt persoanele autorizate, după cum urmează, raportarea tuturor cazurilor fiind una obligatorie:

1) persoane autorizate din cadrul prestatorilor de servicii medicale publici și privați;

2) lucrătorii medicali, persoanele responsabile din cadrul prestatorilor de servicii medicale AMP, AMS, Servicii Sânge.

3) persoane autorizate din cadrul Biobăncilor indiferent de domeniu de activitate și forma de proprietate;

4) persoane autorizate din cadrul laboratoarelor hematologice, virusologice, biochimice, indiferent de forma de proprietate precum și laboratoarelor HLA;

5) medicii din cadrul serviciul medico-legal.

Furnizorii datelor sunt obligați să asigure corectitudinea şi autenticitatea datelor prezentate pentru a fi introduse în RISIT şi actualizarea acestora.

20. Destinatarii RISIT sunt Ministerul Sănătății și subdiviziunile subordonate acestuia, Agenția Națională pentru Sănătate Publică, Compania Națională de Asigurări în Medicină, Agenția Medicamentului și Dispozitivelor Medicale, mandatate cu dreptul de a primi informațiile conform prevederilor legale, în conformitate cu procedura stabilită pentru obținerea datelor.

21. Destinatarii RISIT sunt obligați:

1) să utilizeze datele din RISIT conform scopului și destinației acestora;

2) să asigure securitatea și confidențialitatea informației vizualizate sau prelucrate în RISIT;

3) să înștiințeze imediat posesorul și administratorul tehnic ai RISIT despre cazurile de încălcare a securității informaționale a RISIT;

4) să informeze posesorul RISIT cu privire la orice situație, inclusiv de forță majoră, apărută, care ar putea afecta buna funcționare a RISIT.

22. Destinatarii RISIT, în limitele competenței, au următoarele drepturi:

1) să participe la crearea, implementarea și dezvoltarea RISIT;

2) să prezinte propuneri cu privire la inițierea modificărilor actelor normative existente care reglementează funcționarea RISIT;

3) să vizualizeze, să utilizeze și să prelucreze informațiile din RISIT în conformitate cu rolurile și drepturile stabilite;

4) să solicite și să primească de la posesorul RISIT ajutor metodologic și practic privind problemele ce țin de funcționarea RISIT.

23. Registratorii autorizați pentru introducerea datelor personale ale pacienților din cadrul prestatorului de servicii în domeniul transplantului de organe/țesuturi/celule umane înainte de colectarea datelor informează pacienții despre realizarea drepturilor sale prin următorul mecanism:

1) dreptul de informare a subiectului datelor cu caracter personal:

a) pacientul este informat privind datele prestatorului de servicii, precum și scopul statistic sau științific al prelucrării datelor colectate, în care resursă informațională și sub ce formă care nu permite vizualizarea identității se va regăsi, cine va avea dreptul vizualizării sau prelucrării acestor date;

b) dreptul său de opoziție pentru a radia datele sale se realizează doar cu registratorul datelor căruia se adresează o cerere motivată de opoziție, arhivată de registrator ca motiv al radierii datelor anterior înregistrate.

2) dreptul de acces la datele cu caracter personal:

a) orice pacient are dreptul să obțină de la registrator, la cerere, fără întârziere şi în mod gratuit informația privind resursa informațională care operează datele sale, modul de pseudomimare ale identității sale, cine are dreptul accesării/completării datelor sale;

b) pacientul trebuie să își dea consimțământul ca datele privind starea de sănătate să fie prelucrate în scop de cercetare științifică, precum şi asupra posibilei amânări din acest motiv a comunicării informațiilor prevăzute în subpct 2), lit. a);

3) dreptul de intervenție asupra datelor cu caracter personal:

a) orice pacient are dreptul de a obţine de la registrator la cerere şi în mod gratuit datele sale:

b) de asemenea are dreptul să notifice terților cărora le-au fost dezvăluite datele cu caracter personal despre operaţiunile efectuate sau informațiile eronate existente.

4) dreptul de opoziție al subiectului datelor cu caracter personal:

a) orice pacient are dreptul de a se opune în orice moment, în mod gratuit, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care legea stabileşte altfel. Dacă opoziţia este justificată, prelucrarea efectuată de registrator nu mai poate viza aceste date.

b) orice pacient are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care îl vizează să fie prelucrate pentru prospectare comercială. Registratorul este obligat să informeze subiectul despre dreptul de a se opune unei astfel de lucrări înaintea dezvăluirii către terţi a datelor sale cu caracter personal.

5) dreptul de a nu fi supus unei decizii individuale:

orice pacient are dreptul de a cere anularea, în totalitate sau parțială, a oricărei decizii individuale care produce efecte juridice asupra drepturilor şi libertăților sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul şi altele.

6) accesul la justiție:

orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal efectuată ilegal sau căreia i-au fost încălcate drepturile şi interesele are dreptul de a sesiza instanța de judecată pentru repararea prejudiciilor materiale şi morale.

Capitolul III
Regimul juridic de utilizare a datelor

24. Dreptul de acces la datele RISIT este segmentat pe unități de conținut, atribuind prerogative partajate de vizualizare, adăugare, redactare și radiere.

25. Accesul la resursele informaționale ale RISIT este segmentat pentru utilizatori interni și utilizatori externi.

26. Dreptul de acces la RISIT și contururile acestuia nu este unul permanent, acesta poate fi suspendat. Introducerea și/sau modificarea datelor în RISIT de pe un nume de profil de utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure că profilul de utilizator, precum și eventual, semnătura electronică sunt confidențiale.

27. Suspendarea dreptului de acces la RISIT și/sau contururile acestuia se efectuează prin înaintarea cererii/demersului către deținător, și/sau în una din următoarele situații:

1) la încetarea/suspendarea raporturilor de serviciu/ de muncă ale utilizatorilor;

2) la intervenirea modificărilor raporturilor de serviciu/ de muncă când noile atribuții nu impun accesul la datele din RISIT;

3) după o perioadă inactivă, stabilită în timp (inacțiune în perioada de maximum 2 luni);

4) după trei tentative greșite de autentificare;

5) la constatarea de către deținător a încălcării securității informaționale;

6) în alte cazuri în limitele prevederilor legislative.

28. Lucrările profilactice planificate în complexul de mijloace software se efectuează după notificarea, în scris sau prin e-mail, a registratorilor de către deținător, în baza planului coordonat cu administratorul tehnic cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea utilizatorilor și coordonarea prealabilă cu deținătorul în situația nefuncționării sau funcționării necorespunzătoare a RISIT.

29. Condițiile pentru prelucrarea, stocarea și utilizarea datelor cu caracter personal sunt:

1) datele cu caracter personal vor fi prelucrate în mod corect și conform prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal;

2) colectarea datelor va fi efectuată doar în scopuri determinate și vor fi prelucrate doar în modul compatibil cu acest scop, cât și în scopuri statistice, de cercetare istorică sau științifică, care nu contravine prevederilor legii sus menționate;

3) datele colectate vor fi adecvate, pertinente și neexcesive, și vor fi folosite doar în ceea ce privește scopul pentru ce au fost colectate și prelucrate;

4) la necesitate datele vor fi actualizate iar datele incomplete sau inexacte vor fi ulterior rectificate sau radiate;

5) stocarea datelor se va face cu respectarea garanțiilor de prelucrare a datelor, prevăzute de cadrul normativ ce reglementează acest domeniu;

30. Termenul de păstrare a datelor se va aplica în conformitate cu reglementările aprobate de Ministerul Sănătății privind formularele de evidență medicală primară, ulterior RISIT în mod automatizat va depersonaliza și arhiva cazurile, în vederea asigurării disponibilității datelor de importanță pentru serviciul de sănătate publică.

Capitolul IV
Înregistrarea, modificarea, completarea și radierea datelor RISIT

31. Înregistrarea datelor în RISIT este efectuată de către utilizatorii cu rolul și permisiunile corespunzătoare după autentificarea în RISIT.

32. Înscrierile se efectuează în ordine cronologică, fiecărei înscrieri atribuindu-se data efectuării acesteia în sistem.

33. Modificarea și/sau completarea datelor din cadrul RISIT se efectuează în termenul stabilit conform legislației de către utilizatorii cu rolul și permisiunile corespunzătoare după autentificarea în RISIT.

34. RISIT asigură evidența tuturor modificărilor și/sau completărilor. Toate modificările operate în RISIT sunt păstrate în ordine cronologică, cu păstrarea nemijlocită a istoricului acestora. Modificarea și/sau completarea datelor nu afectează accesarea și vizualizarea informației din RISIT.

35. Orice modificare și/sau completare în RISIT se efectuează doar în temeiul documentelor justificative, cu indicarea motivului ce confirmă veridicitatea acțiunilor efectuate în sistem.

36. La expirarea termenului de păstrare în RISIT, datele se radiază din sistem, cu înregistrarea evenimentelor corespunzătoare și, ulterior cu arhivarea acestora conform legislației.

Capitolul V
Asigurarea protecției și securității informației RISIT

37. Măsurile de protecție şi securitate a informației din RISIT reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a RISIT şi se efectuează neîntrerupt de către posesorul RISIT.

38. Obiecte ale asigurării protecției și securității informației din RISIT se consideră:

1) masivele informaționale, indiferent de formele păstrării, bazele de date, suporturile materiale care conțin informații privind date cu caracter personal;

2) sistemele informaționale, sistemele operaționale, sistemele de gestionare a bazelor de date şi alte aplicații care asigură activitatea RISIT;

3) sistemele de telecomunicații, rețelele, inclusiv mijloacele de confecționare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informației.

39. Securitatea informațională a RISIT se efectuează prin aplicarea metodelor și efectuarea acțiunilor descrise în Planul de continuitate al RISIT și, după caz, a procedurilor operaționale.

40. Protecția datelor se efectuează prin următoarele metode:

1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;

2) utilizarea obligatorie a produselor de program licențiate aprobate; orice solicitare de instalare a unui produs de program trebuie coordonată cu deținătorul tehnic;

3) monitorizarea procesului de exploatare al RISIT prin intermediul mecanismului de jurnalizare.

41. Subiecții la utilizarea și exploatarea RISIT asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

1) identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

2) implementarea principalelor măsuri tehnico-organizatorice necesare asigurării funcționării RISIT;

3) implementarea procedurilor interne ce exclud cazurile de modificare nesancționată a mijloacelor software şi/sau a informației din RISIT;

4) informarea și instruirea utilizatorilor interni cu privire la mecanismele de asigurare a securității informaționale;

5) proceduri de control intern privind respectarea condițiilor de securitate informațională.

Capitolul VI
Controlul și răspunderea

42. Menținerea RISIT este supusă controlului intern și extern.

1) Controlul intern privind ținerea RISIT se efectuează de către Ministerul Sănătății, care este posesorul RISIT.

2) Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea RISIT se efectuează de către instituții abilitate și certificate în domeniul auditului.

43. RISIT se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

44. Responsabilitatea privind organizarea și funcționarea RISIT se atribuie deținătorului RISIT, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea RISIT.

45. Toți subiecții RISIT, precum și solicitantul informațiilor ce conțin date cu caracter personal poartă răspundere conform legislației pentru prelucrarea, divulgarea, transmiterea informației din RISIT persoanelor terțe contrar prevederilor legislației. Pentru încălcarea prezentului Regulament, persoanele vinovate răspund în conformitate cu legislaţia civilă, contravențională sau penală.

46. În cazul incidentelor de securitate, posesorul/deținătorul va întreprinde măsuri necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.