Republica Moldova

GUVERNUL

HOTĂRÂRE Nr. HG694/2024
din 09.10.2024

cu privire la instituirea Sistemului informațional „Transplant”

Publicat : 17.10.2024 în MONITORUL OFICIAL Nr. 434-436 art. 821 Data intrării în vigoare

În temeiul art. 22 lit. c) și 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 HOTĂRĂȘTE:

1. Se instituie Sistemul informațional „Transplant”.

2. Se aprobă:

2.1. Conceptul Sistemului informațional „Transplant”, conform anexei nr. 1;

2.2. Regulamentul resursei informaționale ținute pe Sistemul informațional „Transplant”, conform anexei nr. 2.

3. La punctul 6 subpunctul 2) din Regulamentul privind organizarea și funcționarea Agenției de Transplant, aprobat prin Hotărârea Guvernului nr. 386/2010 (Monitorul Oficial al Republicii Moldova, 2010, nr. 78-80, art. 457), cu modificările ulterioare, textul „Sistemul informațional automatizat «Transplant»” se substituie cu textul „Sistemul informațional «Transplant»”.

4. Regulamentul privind modul de ținere a Registrului medical, aprobat prin Hotărârea Guvernului nr. 586/2017 (Monitorul Oficial al Republicii Moldova, 2017, nr. 277-288, art. 703), cu modificările ulterioare, se modifică după cum urmează:

4.1. la punctul 3, subpunctul 5) va avea următorul cuprins:

„5) Sistemul informațional «Transplant»” (SIT);”;

4.2. în tabelele de la punctele 8^1 și 10, textul „SIA Transplant” se substituie cu textul „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 1 ianuarie 2025.

PRIM-MINISTRU Dorin RECEAN

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării

economice și digitalizării Dumitru Alaiba

Ministrul sănătății Ala Nemerenco

Nr. 694. Chişinău, 9 octombrie 2024.

Anexa nr. 1

la Hotărârea Guvernului nr.694/2024

CONCEPTUL

Sistemului informațional „Transplant”

INTRODUCERE

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

Prezentul Concept determină scopul, obiectivele și funcțiile de bază ale Sistemului informațional „Transplant” (în continuare – *SIT*), obiectele informaționale, precum și scenariile de bază privind includerea datelor relevante în sistem, acesta este găzduit pe platforma tehnologică guvernamentală comună (MCloud) și integrat cu sistemele informaționale partajate relevante instituite de Guvern și cu alte sisteme informaționale de stat.

Capitolul I

DISPOZIȚII GENERALE

1. 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 al băncilor de țesuturi și/sau celule umane, autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane.

2. SIT este creat în următoarele scopuri:

2.1. asigurarea evidenței fișelor medicale ale pacienților ce donează un organ, țesut sau celule pentru primitorii care necesită un transplant de organ, țesut și celule umane în condițiile legii;

2.2. facilitarea participării la schimbul de organe, țesuturi și celule umane cu alte state, inclusiv cu statele Uniunii Europene;

2.3. asigurarea formării registrelor donatorilor și primitorilor de organe, țesuturi și celule umane;

2.4. asigurarea formării modulului de biovigilență pentru raportarea, investigarea, înregistrarea şi transmiterea informațiilor privind evenimentele şi reacțiile adverse grave, care pot influența calitatea şi siguranța organelor, țesuturilor şi celulelor umane utilizate la om;

2.5. asigurarea formării modulului de statistici și raportări ale activităților în domeniul transplantului de organe, țesuturi și celule umane și al activităților din cadrul reproducerii asistate medical;

2.6. asigurarea formării resurselor informaționale de stat privind starea sănătății populației.

3. Pentru prestatorii de servicii medicale autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane, SIT asigură:

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

3.2. gestionarea și actualizarea periodică a analizelor și a investigațiilor efectuate donatorilor și primitorilor;

3.3. implementarea automatizării pentru consumul datelor provenite din sistemele de apreciere a compatibilității imunohistochimice și izoserologice între donator și primitor la nivel de organ, țesut sau celulă umană;

3.4. evidența electronică a pacienților implicați în activitățile de donare, prelevare și transplant atât în țară, cât și în străinătate;

3.5. evidența electronică a stocurilor de medicamente necesare pentru primitorii de transplant;

3.6. evidența electronică națională a stocurilor de țesuturi și celule umane.

4. SIT oferă:

4.1. crearea și actualizarea periodică a fișei electronice a pacientului, în care se jurnalizează interacțiunile pacientului cu sistemul medical la nivel național;

4.2. generarea rapoartelor pentru monitorizarea activităților de prelevare și transplant;

4.3. generarea rapoartelor pentru monitorizarea activităților de reproducere asistată medical.

5. SIT folosește tehnologiile contemporane care permit utilizarea acestuia de prestatorii de servicii medicale și de băncile de țesuturi și/sau de celule umane, autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane, prin intermediul unui echipament IT convențional, fără necesitatea instalării programelor suplimentare.

6. Principiile de bază ale SIT sunt următoarele:

6.1. *principiul legitimității*, potrivit căruia funcțiile și operațiile efectuate de utilizatori sunt legale și conforme cu drepturile omului și cu legislația națională;

6.2. *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;

6.3. *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;

6.4. *principiul temeiniciei datelor*, prevede că introducerea și reactualizarea datelor în SIT se efectuează doar în baza înscrierilor din documentele acceptate ca surse de informații;

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

6.6. *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 niciun fel abordarea dezvoltării sistemului atât timp cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit;

6.7. *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 face prin protocoale și puncte de conexiune proiectate din start;

6.8. *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;

6.9. *principiul compatibilității*, conform căruia SIT trebuie să fie compatibil cu sistemele existente atât în țară, cât și peste hotarele ei;

6.10. *principiul orientării spre utilizator*, potrivit căruia structura, conținutul,

mijloacele de acces și navigarea sunt focalizate spre utilizatori;

6.11. *principiul extensibilității*, conform căruia componentele SIT oferă facilități de ajustare și extindere a funcționalităților existente;

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

6.13. *principiul consecutivității*, presupune elaborarea și implementarea proiectului în etape;

6.14. *principiul eficienței funcționării*, presupune optimizarea raportului dintre calitate și cost;

6.15. *principiul utilizării standardelor deschise*, se aplică pentru a asigura atât interoperabilitatea cu sistemele externe, cât și păstrarea informației, în conformitate cu legislația;

6.16. *principiul egalității și nondiscriminării*, potrivit căruia toate ființele umane sunt egale în faţa legii şi au dreptul la protecţie şi beneficii egale;

6.17. *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 SIT

7. Crearea și funcționarea SIT este reglementată de următoarele acte normative:

7.1. Constituția Republicii Moldova;

7.2. Legea ocrotirii sănătății nr. 411/1995;

7.3. Legea nr. 1069/2000 cu privire la informatică;

7.4. Legea nr. 100/2001 privind actele de stare civilă;

7.5. Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

7.6. Legea nr. 71/2007 cu privire la registre;

7.7. Legea nr. 42/2008 privind transplantul de organe, țesuturi și celule umane;

7.8. Legea nr. 133/2011 privind protecția datelor cu caracter personal;

7.9. Legea nr. 121/2012 cu privire la asigurarea egalității;

7.10. Legea nr. 138/2012 privind sănătatea reproducerii;

7.11. Legea nr. 93/2017 cu privire la statistica oficială;

7.12. Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

7.13. Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

7.14. Legea nr. 148/2023 privind accesul la informațiile de interes public;

7.15. Hotărârea Guvernului nr. 272/2002 despre măsurile privind crearea sistemului informațional automatizat „Registrul de stat al unităților de drept”;

7.16. Hotărârea Guvernului nr. 735/2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova;

7.17. Hotărârea Guvernului nr. 916/2007 cu privire la Concepția Portalului guvernamental;

7.18. Hotărârea Guvernului nr. 386/2010 cu privire la instituirea Agenției de Transplant;

7.19. 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;

7.20. Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare şi control al accesului (MPass);

7.21. Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

7.22. Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

7.23. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

7.24. Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

7.25. Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical;

7.26. 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;

7.27. Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate

(MConnect);

7.28. 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);

7.29. 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”;

7.30. Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

7.31. Reglementarea tehnică „Procesele ciclului de viață al software-ului” (RT 38370656-002:2006), aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006;

7.32. Reglementările tehnice aprobate prin Ordinul ministrului dezvoltării informaționale nr. 94/2009.

Capitolul III

SPAȚIUL FUNCȚIONAL AL SIT

8. SIT realizează următoarele funcții:

8.1. formarea bazei de date a SIT:

8.1.1. luarea în evidență primară, care constă în atribuirea identificatorului unic obiectului de evidență și introducerea în baza de date a volumului stabilit de date;

8.1.2. actualizarea datelor, care presupune actualizarea sistematică a bazei de date după modificarea sau completarea datelor obiectelor de evidență;

8.1.3. scoaterea din evidență, care nu presupune excluderea fizică a datelor din registru, ci doar schimbarea statutului acestora. Informația în SIT se introduce numai în baza documentelor ce confirmă veridicitatea datelor, cu specificarea documentului în baza căruia s-a realizat actualizarea lor. Toate modificările în SIT se păstrează în ordine cronologică;

8.2. asigurarea informațională:

informația din resursa informațională SIT se pune la dispoziția destinatarilor, nivelul de acces fiind stabilit de Regulamentul resursei informaționale ținute pe Sistemul informațional „Transplant” și de prevederile legale;

8.3. asigurarea securității informației:

securitatea informației se asigură în toate etapele de colectare, păstrare și utilizare a resurselor informaționale de stat ce se referă la sfera de ocrotire a normelor de drept;

8.4. asigurarea funcționării.

9. SIT asigură preluarea și prelucrarea datelor din Registrul medical a următoarelor contururi funcționale:

9.1. înregistrarea, verificarea și reactualizarea datelor pacienților care necesită sau au beneficiat de un transplant de organ, țesut sau celule umane;

9.2. înregistrarea, verificarea și reactualizarea datelor persoanelor care donează un organ, țesut sau celule umane;

9.3. acumularea și reactualizarea informațiilor privind vizitele primitorilor de transplant la medicul specialist de profil, care verifică informațiile necesare pentru a completa și a reactualiza fișa electronică a pacientului;

9.4. generarea rapoartelor conform parametrilor selectați de utilizatori, prin comunicarea cu structurile bazelor de date care conțin informații relevante;

9.5. generarea rapoartelor cu privire la apariția reacțiilor și/sau a evenimentelor adverse grave, ce pot influența calitatea şi siguranța organelor, țesuturilor şi celulelor umane utilizate la om (biovigilența);

9.6. evidența pacienților care necesită sau au beneficiat de un transplant de organ, țesut sau celule umane;

9.7. evidența persoanelor care donează un organ, țesut sau celule umane;

9.8. preluarea 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 a investigațiilor imagistice efectuate, asigurând acces pentru vizualizarea lor în sistemul partajat;

9.9. evidența vizitelor primitorilor de transplant la medicul specialist de profil, care verifică informațiile necesare pentru a completa și a reactualiza fișa electronică a pacientului;

9.10. generarea rapoartelor privind donatorii în viață pentru comisia independentă de avizare;

9.11. generarea rapoartelor conform parametrilor selectați.

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ A SIT

10. Proprietarul SIT este statul.

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

12. Deținătorul SIT este Agenția de Transplant, care asigură crearea, mentenanța și monitorizarea exploatării eficiente a acestuia.

13. 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.

14. Registratorii datelor în SIT sunt:

14.1. prestatorii de servicii medicale autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane;

14.2. băncile de țesuturi și/sau celule umane autorizate pentru desfășurarea activităților de prelevare, prelucrare, testare, conservare, stocare și distribuire pentru utilizare la om.

15. Utilizatorii datelor sunt persoanele din cadrul prestatorilor de servicii medicale autorizați cu drept de vizualizare a datelor medicale.

16. Furnizorii datelor sunt persoanele din cadrul prestatorilor de servicii medicale cu drept de introducere a datelor medicale în sistemele informaționale ale prestatorilor (Sistemul informațional automatizat „Asistența medicală primară” și Sistemul informațional automatizat „Asistență medicală spitalicească”), care, prin realizarea interoperabilității cu SIT, furnizează datele interesate în fișierele medicale.

17. Destinatarii datelor sunt instituțiile statului cu drept de vizualizare a datelor medicale utilizate în scopuri științifice sau pentru crearea statisticilor naționale de domeniu (Ministerul Sănătății, Agenția Națională pentru Sănătate Publică, Compania Națională de Asigurări în Medicină, Agenția Medicamentului și Dispozitivelor Medicale).

Capitolul V

DOCUMENTELE SIT

18. În cadrul SIT sunt utilizate documente de intrare, de ieșire și tehnologice. Acestea sunt actualizate în conformitate cu necesitățile domeniului și cu actele normative.

19. Documentele de intrare includ documentația medicală de evidență primară a instituțiilor ocrotirii sănătății.

20. Documentele de ieșire includ:

20.1. acordul informat cu privire la includerea pacientului în lista de așteptare pentru transplant de organe;

20.2. acordul informat pentru donarea și aplicarea tehnologiilor de reproducere asistată medical;

20.3. documentele extrase din registrele SIT:

20.3.1. Registrul național renal;

20.3.2. Registrul hepatic;

20.3.3. Registrul donatorilor de organe și țesuturi;

20.3.4. Registrul primitorilor de organe și țesuturi;

20.3.5. Registrul donatorilor de celule reproductive;

20.3.6. Registrul primitorilor de celule reproductive;

20.4. documente extrase din lista de așteptare;

20.5. lista de urgență și superurgență a primitorilor pentru transplant.

21. Documentele tehnologice care sunt generate de SIT sunt:

21.1. formularul de evidența lunară a ședințelor efectuate în centrele de dializă;

21.2. scorul renal și/sau scorul hepatic pentru oferta de atribuire a organului către echipa medico-chirurgicală;

21.3. cererea de țesuturi sau celule umane adresată băncilor de țesuturi și/sau celule umane;

21.4. fișa de prelevare emisă de centrele de prelevare, băncile de țesuturi și/sau celule umane;

21.5. fișa de procesare a grefei/grefelor emisă de băncile de țesuturi și/sau celule umane;

21.6. fișa de validare a grefei/grefelor (fișa produsului finit) emisă de băncile de țesuturi și/sau celule umane;

21.7. fișa de distribuire a grefei/grefelor emisă de băncile de țesuturi și/sau celule umane;

21.8. fișa de trasabilitate a grefei/grefelor emisă de băncile de țesuturi și/sau celule umane;

21.9. formulare de biovigilență pentru raportarea, investigarea, înregistrarea şi transmiterea informațiilor privind evenimentele şi/sau reacțiile adverse grave care pot influența calitatea şi siguranța organelor, țesuturilor şi celulelor umane utilizate la om.

22. SIT asigură funcționalitatea de raportare prin depozitul centralizat de date.

23. SIT asigură generarea datelor către instituțiile europene:

23.1. EDQM *(European Directorate for the Quality of Medicines & HealthCare*) – Directoratul European pentru Evaluarea Calității Medicamentelor și Ocrotirii Sănătății;

23.2. Platforma FOEDUS *(Platform Facilitating of Organs Exchange Donated in EU member States)* – platformă pentru facilitarea schimbului de organe între statele membre ale Uniunii Europene.

24. SIT generează rapoarte de activitate ale:

24.1. prestatorilor de servicii medicale autorizați pentru desfășurarea activităților de donare, prelevare și transplant de organe, țesuturi și celule umane;

24.2. băncilor de țesuturi și/sau celule umane autorizate pentru desfășurarea activităților de prelevare, prelucrare, testare, conservare, stocare și distribuire pentru utilizare la om.

25. Rapoartele reflectă următoarele aspecte:

25.1. diagnosticul conform Clasificatorului Internațional al Maladiilor CIM-10, CIM-11;

25.2. categoria de vârstă (1-18 ani, 19-35 de ani, 36-60 de ani, 60 de ani > etc.);

25.3. serviciile medicale acordate.

26. Prestatorii de servicii medicale și băncile de țesuturi și/sau celule umane autorizați 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 Agenției de Transplant.

Capitolul VI

SPAȚIUL INFORMAȚIONAL AL SIT

Secțiunea 1

Obiectele informaționale gestionate

27. Lista principalelor obiecte informaționale utilizate în SIT:

27.1. 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;

27.2. personal medical implicat în prestarea serviciilor medicale și a activităților de transplant autorizate;

27.3. medicamente specifice (imunosupresive, antivirale, hepatoprotectoare, anticorpi monoclonali etc.);

27.4. laboratoare clinice din cadrul prestatorului de servicii medicale;

27.5. centre/secții de dializă din cadrul prestatorului de servicii medicale;

27.6. centre/instituții medicale de investigații imagistice din cadrul prestatorului de servicii medicale.

28. Fiecare persoană în calitate de obiect informațional are un identificator numeric unic „Cod SIT” care este generat de aplicație în mod automat. „Codul SIT” este un element principal de pseudonimizare, ce reprezintă prelucrarea datelor cu caracter personal într-un mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică menite să asigure neatribuirea datelor cu caracter personal unei persoane fizice identificate sau identificabile. Codul SIT este utilizat constant în SIT. Obiectele împrumutate din alte sisteme informaționale respectă codificarea impusă de SI care le-a generat. În SIT ele se utilizează fără modificări.

29. Atributele obiectelor informaționale utilizate în SIT:

29.1. obiectul informațional „persoană fizică” – pacient, care include:

29.1.1. datele de identificare:

29.1.1.1. numărul de identificare de stat (IDNP);

29.1.1.2. numele, prenumele şi patronimicul;

29.1.1.3. sexul;

29.1.1.4. data nașterii;

29.1.1.5. grupa sangvină;

29.1.2. datele demografice:

29.1.2.1. cetățenia;

29.1.2.2. tipul documentului de identificare;

29.1.2.3. numărul documentului;

29.1.3. domiciliul/reședința temporară:

29.1.3.1. localitatea şi țara;

29.1.3.2. strada;

29.1.3.3. blocul;

29.1.3.4. apartamentul;

29.1.4. datele privind asigurarea medicală:

29.1.4.1. categoria de asigurat;

29.1.4.2. statutul de asigurat;

29.1.4.3. asigurator;

29.1.4.4. tipul de asigurare;

29.1.5. datele specifice despre sănătate:

29.1.5.1. date despre evidență;

29.1.5.2. date despre consultații şi examene medicale;

29.1.5.3. date despre organe, țesuturi și celule umane;

29.1.5.4 date despre diagnostice;

29.1.5.5. date despre examene de laborator;

29.1.5.6. date despre efectele adverse şi complicațiile în cadrul tratamentului;

29.2. obiectul informațional „persoană fizică” – personal medical, care include:

29.2.1. datele de identificare:

29.2.1.1. numărul de identificare de stat (IDNP);

29.2.1.2. numele, prenumele, patronimicul;

29.2.2. datele socioeconomice:

29.2.2.1. locul de muncă;

29.3. obiectul informațional „prestator servicii medicale”, care include:

29.3.1. numărul de identificare de stat (IDNO);

29.3.2. denumirea;

29.3.3. codul fiscal;

29.3.4. codul instituției medico-sanitare;

29.3.5. tipul;

29.3.6. numărul de telefon;

29.3.7. adresa poștală;

29.3.8. adresa electronică a persoanei juridice sau a întreprinzătorului individual;

29.4. obiectul informațional „medicamentele utilizate de către prestatorii serviciilor medicale”, care include:

29.4.1. ID-ul medicamentului (Nomenclator);

29.4.2. unitatea de măsură;

29.4.3. cantitatea în unitățile indicate;

29.4.4. data producerii medicamentului;

29.4.5. data expirării medicamentului;

29.4.6. stocul/factura din care a fost creat acest stoc gestionat;

29.4.7. codul medicamentului din Nomenclatorul de stat;

29.4.8. denumirea medicamentului;

29.4.9. substanța activă a medicamentului;

29.4.10. numărul cu care a fost înregistrat acest medicament;

29.4.11. forma farmaceutică a medicamentului;

29.4.12. compania producătoare a acestui medicament.

Secțiunea a 2-a

Scenariile de bază aferente obiectelor informaționale

30. Scenariile de bază ale principalelor procese-business sunt expuse în anexa nr. 1.

31. Lista rolurilor de business include persoane nominalizate responsabile de gestionarea datelor în SIT, care au stabilite reguli de securitate, corespunzător drepturilor de acces pentru:

31.1. introducerea datelor cu caracter personal și medical doar în spațiul SIT;

31.2. editarea datelor cu caracter personal și medical doar în spațiul SIT;

31.3. vizualizarea datelor cu caracter personal și medical.

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

33. Evidența și controlul înregistrărilor în modulele asociate rolurilor de business sunt interdependente și funcționează în cadrul aceluiași sistem unitar. Scenariul schemei logice este prezentat în anexa nr. 3.

34. Evidența activităților desfășurate în băncile de țesuturi şi/sau celule umane include:

34.1. înregistrarea etapelor lanțului, de la donare până la distribuția țesuturilor şi/sau

celulelor umane, efectuate în conformitate cu procedurile specifice fiecărui ţesut şi/sau celulă, inclusiv descrierea fiecărei etape de la recepționare până la distribuție şi evaluarea calitativă;

34.2. validarea produsului terapeutic prin control biologic şi descrierea funcțională;

34.3. certificarea fiecărui produs prin fișa produsului finit şi transmiterea ei odată cu distribuția țesutului și/sau celulelor umane;

34.4. înregistrarea privind destinația finală a țesuturilor și/sau celulelor umane distribuite;

34.5. identificarea la fiecare etapă a activităților desfășurate pentru fiecare unitate de țesut și/sau celule umane;

34.6. sistemul asigură trasabilitatea tuturor etapelor necesare pentru următoarele activități: codificarea, selectarea donatorului, procurarea, procesarea, conservarea, stocarea, distribuția şi transportul, incluzând şi aspectele privind controlul de calitate;

34.7. SIT asigură formarea Registrului băncilor de țesuturi și/sau celule umane.

Secțiunea a 3-a

Interacțiunea cu sistemele informaționale partajate

și cu resursele și sistemele informaționale de stat

35. În vederea asigurării funcționalității SIT și pentru preluarea datelor relevante din alte resurse informaționale de stat, acesta interacționează prin intermediul platformei de interoperabilitate (MConnect) cu următoarele resurse informaționale:

35.1. 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.;

35.2. 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;

35.3. Sistemul informațional automatizat „Asistența medicală primară și Sistemul informațional automatizat „Asistență medicală spitalicească” – pentru crearea și reactualizarea fișei pacientului, inclusiv a datelor de laborator și a investigațiilor imagistice, care jurnalizează interacțiunile pacientului cu sistemul medical la nivel național, precum și pentru generarea rapoartelor statistice necesare pentru monitorizarea activităților de prelevare și transplant etc.;

35.4. Sistemul informațional automatizat „Serviciul de sânge”– pentru consumul și partajarea datelor grupului sangvin și factorului Rhesus al persoanei, conform IDNP către Sistemul informațional automatizat „Asistența medicală primară” și Sistemul informațional

automatizat „Asistența medicală spitalicească”.

36. SIT este găzduit pe platforma tehnologică guvernamentală comună (MCloud) și este compatibil cu platforma de găzduire bazată pe tehnologii de tip container.

37. SIT interacționează cu următoarele platforme și sisteme informaționale partajate:

37.1. platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte sisteme informaționale și registre de stat;

37.2. serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice ieșite din sistem;

37.3. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în cadrul sistemului;

37.4. serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiilor (evenimentelor) produse în cadrul SIT;

37.5. Sistemul informațional „Catalogul semantic” – pentru evidența metadatelor ca resurse informaționale;

37.6. 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;

37.7. Serviciul guvernamental de notificare electronică (MNotify) – pentru primirea notificărilor electronice generate de alte sisteme informaționale cu care SIT comunică;

37.8. 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 SIT

38. La dezvoltarea SIT se aplică arhitectura multinivel, având cel puțin următoarele nivele: baza de date, logica de aplicație, interfața cu utilizatorul și principiile agile. Utilizarea unor astfel de arhitecturi și principii permite cuplarea redusă între componente. Responsabilitățile fiecărei componente sunt specializate și permit implementarea iterativă, operarea modificărilor și flexibilitatea în implementare.

39. SIT utilizează standarde deschise și este compatibil cu sistemele care, la fel, utilizează atât standarde nonproprietare, cât și standarde deja existente.

40. 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:

40.1. 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;

40.2. implementarea funcționalităților de arhivare (backup) și restabilire a datelor în caz de incidente.

41. SIT poate 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.

42. Sistemul de comunicații se bazează pe infrastructură și pe echipamentul rețelelor guvernamentale care includ posibilitatea conectării la internet. Infrastructura existentă este planificată în mod corespunzător, pentru a oferi nivelurile adecvate de performanță și capacitate.

43. Interfața de utilizare a SIT se adaptează automat la diverse rezoluții de afișare și este disponibilă în limbile română și rusă.

44. Interfața de utilizare a SIT se implementează folosind tehnologiile care asigură funcționarea serviciului pe dispozitivele mobile.

45. Având în vedere locul SIT în cadrul resurselor informaționale de stat ale Republicii Moldova, este necesară disponibilitatea permanentă și accesul neîntrerupt la sistem. Din acest motiv, întreaga soluție este construită în regim de înaltă disponibilitate (24 de ore/zi, 7 zile/săptămână).

Capitolul VIII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SIT

46. Esența securității informaționale a SIT reflectă următoarele:

46.1. prin securitate informațională se înțelege protecția resurselor și a infrastructurii informaționale a SIT împotriva acțiunilor premeditate sau a celor accidentale, cu caracter natural sau artificial, care pot cauza prejudicii participanților la procesul de schimb informațional;

46.2. 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;

46.3. 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;

46.4. 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:

46.4.1. securitatea fizică se referă la protejarea infrastructurii fizice a sistemului prin aplicarea tuturor măsurilor de securitate;

46.4.2. securitatea informațională presupune protejarea informației prin aplicarea unor măsuri de securizare la nivel logic și prin utilizarea tehnologiilor informaționale. Aceasta include programele antivirus, delimitarea logică a subrețelelor, firewall, backup, sistemul de producție, controlul asupra folosirii programelor piratate, evidența și actualizarea licențelor produselor software;

46.4. 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 bază de utilizator și parolă, iar conexiunea se urmărește prin MPass sau MSign. Semnarea documentelor tehnologice generate de sistem se efectuează utilizând serviciul MSign prin intermediul semnăturii electronice calificate.

47. 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:

47.1. utilizarea ilegală a informației;

47.2. încălcarea tehnologiei de prelucrare a informației;

47.3. implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația ce însoțește aceste produse;

47.4. 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;

47.5. nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor hardware și/sau software de prelucrare a informației;

47.6. compromiterea credențialelor, a cheilor și a mijloacelor de protecție criptografică a informației;

47.7. scurgerea de informație prin canale tehnice;

47.8. 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;

47.9. nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;

47.10. tentativele de interceptare a informației în rețelele locale ale registratorilor sistemului și în liniile de comunicații, decodificarea ei și impunerea informației false;

47.11. utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție

a datelor, a mijloacelor de informatizare și comunicații la crearea și dezvoltarea infrastructurii informaționale;

47.12. accesul neautorizat la resursele informaționale care se află în bazele de date;

47.13. încălcarea restricțiilor legale ce țin de răspândirea informației.

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

48.1. asigurarea securității informației este realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017. Pentru gestiunea riscurilor de securitate este implementată o politica generală de securitate. Personalul implicat în utilizarea și în administrarea SIT este instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și pentru a stabili domeniile care necesită îmbunătățiri;

48.2. securitatea informațională asigură:

48.2.1. confidențialitatea informației, care presupune limitarea accesului la informație pentru persoanele fără drepturi și împuterniciri corespunzătoare;

48.2.2. integritatea logică a informației, adică prevenirea introducerii, modificării, copierii, actualizării și nimicirii neautorizate a informației;

48.2.3. integritatea fizică a informației;

48.2.4. protecția infrastructurii informaționale împotriva deteriorării și încercărilor de modificare a funcționării;

48.3. pentru îndeplinirea sarcinilor privind asigurarea securității informaționale a SIT se utilizează următoarele mecanisme:

48.3.1. dubla autentificare și autorizarea utilizatorului;

48.3.2. managementul accesului;

48.3.3. înregistrarea acțiunilor și auditul prin mecanisme de tip log;

48.3.4. primirea notificărilor electronice din sistemele informaționale cu care este stabilită interoperabilitatea cu ajutorul serviciului electronic MNotify.

49. Pericolele securității informaționale sunt:

49.1. colectarea și utilizarea ilegală a datelor;

49.2. încălcarea tehnologiei de prelucrare a datelor;

49.3. implementarea în produsele software și hardware a componentelor care

îndeplinesc funcții neprevăzute în documentația aferentă acestor produse;

49.4. elaborarea și răspândirea programelor ce afectează funcționarea normală a sistemelor informaționale și a comunicațiilor electronice, precum și a sistemelor securității informaționale;

49.5. nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a datelor și a comunicațiilor electronice;

49.6. influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;

49.7. compromiterea cheilor și a mijloacelor de protecție criptografică a informației;

49.8. scurgerea informației prin canale tehnice;

49.9. 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;

49.10. nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;

49.11. interceptarea datelor în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea unei informații false;

49.12. 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;

49.13. accesul nesancționat la resursele informaționale din băncile și bazele de date;

49.14. încălcarea restricțiilor legale privind răspândirea informației;

49.15. încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

50. SIT asigură realizarea următoarelor obiective de securitate:

50.1. autentificarea – garantează că zonele restricționate ale SIT sunt accesibile doar utilizatorilor cu identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass);

50.2. 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;

50.3. confidențialitatea – garantează că datele înregistrate în SIT nu pot fi accesate de o parte terță neautorizată;

50.4. integritatea – garantează că datele înregistrate în SIT nu au fost modificate sau alterate de o parte terță neautorizată;

50.5. nonrepudierea – garantează că datele înregistrate în SIT nu pot fi negate mai târziu.

51. Pentru atingerea obiectivelor de securitate, SIT dispune de mai multe mecanisme de securitate:

51.1. semnătura electronică – mecanism ce asigură integritatea și nonrepudierea datelor înregistrate în SIT;

51.2. 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;

51.3. antivirus/antispam – soluțiile hardware și/sau software care 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;

51.4. sistem de detectare a intruziunilor – sistem de detectare a accesului neautorizat la nivelul componentelor de sistem ale SIT;

51.5. comunicare sigură (transferuri de date) între serverele web și utilizatori – schimbul de informații confidențiale este securizat;

51.6. backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;

51.7. 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.

52. 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 utilizează funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).

53. Utilizatorii SIT sunt autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia. Utilizatorii și rolurile acestora sunt gestionate prin intermediul serviciului MPass. SIT preia rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).

54. Necesitatea importantă legată de securitate este păstrarea înregistrărilor de

audit pentru analiza integrității SIT și pentru monitorizarea activității utilizatorilor. SIT se bazează 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

55. SIT oferă beneficii importante părților implicate în activitățile de donare, prelevare și transplant de organe, țesuturi și celule umane și este caracterizat prin generarea următoarelor avantaje:

55.1. este proiectat și dezvoltat pe baza modelelor sectorului similar de activitate din țările Uniunii Europene;

55.2. urmărește eliminarea dosarelor în format de hârtie care sunt greu de gestionat;

55.3. urmărește implementarea unor mecanisme de monitorizare și control al calității pentru serviciile medicale de înaltă performanță oferite populației;

55.4. este prietenos în utilizare și se bazează pe cunoștințele utilizatorilor legate de navigarea pe internet;

55.5. asigură protecția datelor și are posibilitatea interoperabilității cu alte sisteme informatice;

55.6. asigură trasabilitatea prin sisteme de interconectare (web-servicii cu grad înalt de securitate) a activității medicale, în mod bidirecțional în toate etapele lanţului, de la donare până la transplant și monitorizare în timp real;

55.7. asigură calitatea serviciilor datorită implementării biovigilenței;

55.8. generează rapoarte statistice atât pentru managementul intern, cât și pentru autoritățile competente din domeniu.

56. SIT asigură modernizarea serviciilor medicale pentru domeniul de transplant în conformitate cu prevederile directivelor și recomandărilor Uniunii Europene în sectorul medical vizat, respectând în totalitate legislația.

Anexa nr. 1

la Conceptul Sistemului

informațional „Transplant”

Scenariile de bază ale principalelor procese-business

1. Scenariul prin care se realizează în mod dinamic fișa electronică a pacientului (FEP)

Vizita unui pacient la instituția medicală cu înregistrarea datelor din FEP este reprezentată în următoarea schemă:

2. Scenariul prin care datele existente într-un sistem se partajează către SIT prin notificare

Preluarea FEP din alte sisteme în baza IDNP-ului se efectuează conform notificării sistemului partajat către SIT prin intermediul serviciului MNotify (subpct. 37.7). După generarea „Codului SIT", datele medicale ale pacientului migrează către SIT doar după verificarea faptului dacă au fost introduse preliminar în sistem. În funcție de rezultatul obținut la interpelarea sistemului, pot fi vizualizate sau editate datele unui pacient existent în SIT sau se generează un cod SIT nou.

Anexa nr. 2

la Conceptul Sistemului

informațional „Transplant"

Asocierea între rolurile de business existente în SIT

și funcționalitățile necesare pentru fiecare rol

Nr. crt.	**Denumirea rolului-business**	**Funcționalități SIT datorate interoperabilității asigurate de Sistemul informațional automatizat „Asistența medicală spitalicească" și de Sistemul informațional automatizat „Asistența medicală primară"**
1.	Medic coordonator din cadrul Agenției de Transplant	Registrul donatorilor de organe și țesuturi umane Registrul primitorilor de organe și țesuturi umane Registrul de refuz
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 Sistemul informațional automatizat „Asistența medicală spitalicească" interconectat cu SIT pentru verificarea prezenței înregistrării datelor pacientului în Registrul de refuz
3.	Medicul laboratorului de histocompatibilitate antigenică (HLA) responsabil de introducerea datelor privind compatibilitatea imunohistochimică și izoserologică 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, a țesuturilor sau a 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 posttransplant	Registrul transplant renal – medicul nefrolog Registrul transplant hepatic – medicul hepatolog Registrul transplant cardiac – medicul cardiochirurg, cardiolog Submodulul „Stoc medicamente” – parte componentă a registrelor sus-menționate
8.	Medicul responsabil de realizarea transplanturilor de țesuturi (oftalmolog, ortoped, combustiolog, chirurg etc.)	Lista de 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 umane	Registrul țesuturilor stocate (cornee, os, ligamente, mușchi-tendon, amnion, piele, vase magistrale, periferice, valve cardiace)
12.	Persoana responsabilă din cadrul băncii de țesuturi și/sau celule reproductive	Registrul celulelor reproductive: gameți, embrioni, țesut reproductiv masculin (testicular) și feminin (ovarian) pentru evidența stocurilor de celule reproductive
13.	Medicul responsabil de vigilență	Modulul de biovigilență
14.	Administrator al Agenției de Transplant	Modulul de securitate informațională

Anexa nr. 3

la Conceptul Sistemul informațional „Transplant”

Scenariile evidenței și controlului înregistrărilor

în modulele asociate rolurilor de business

1. Scenariul de acces la sistem în baza autentificării prin intermediul parolei sau al MPass

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

3. Scenariul de generare a rapoartelor și a statisticilor

Prin acest scenariu sunt realizate rapoartele și statisticile privind:

3.1. evidența pacienților ce necesită un organ;

3.2. evidența centrelor de dializă;

3.3. evidența operațiilor de transplant efectuate;

3.4. evidența stocurilor de țesuturi;

3.5. evidența stocurilor de celule umane;

3.6. evidența donatorilor și primitorilor de organe, țesuturi, celule umane în scop terapeutic;

3.7. evidența stocurilor de medicamente necesare pacienților după transplant;

3.7. consultarea și actualizarea documentelor medicale ale pacienților aflați în listele de așteptare;

3.8. consultarea informațiilor legate de efectuarea operațiilor de transplant în străinătate;

3.9. interacțiunea cu platformele europene pentru gestionarea schimburilor de organe;

3.10. generarea rapoartelor personalizate și a statisticilor.

Anexa nr. 2

la Hotărârea Guvernului nr.694/2024

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 și obligațiile subiecților raporturilor juridice aferente creării și ținerii resursei informaționale; modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare și 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 în Conceptul Sistemului informațional „Transplant”.

3. Resursa informațională ținută pe Sistemul informațional „Transplant” (în continuare – *RISIT*) este resursa informaţională de stat care reprezintă totalitatea informației sistematizate cu privire la starea sănătății persoanelor care:

3.1. necesită transplant de organe, țesuturi și celule umane (primitorii);

3.2. donează organe, țesuturi și celulele umane (donatorii);

3.3. solicită să fie înregistrate în Registrul de refuz.

4. Prin intermediul RISIT Agenția de Transplant organizează și supraveghează evidența datelor referitoare la desfășurarea activităţilor de transplant la nivel naţional, în conformitate cu legislația, contribuind astfel la combaterea traficului ilicit de organe, ţesuturi şi celule umane.

5. Registrul de refuz, în calitate de modul funcțional RISIT, reprezintă o resursă informațională a persoanelor care au refuzat să devină donator de organe, țesuturi sau celule, după decesul lor.

Capitolul II

SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ȘI UTILIZĂRII RISIT ATRIBUȚIILE, OBLIGAȚIILE ȘI DREPTURILE ACESTORA

6. Subiecții din domeniul creării și utilizării RISIT sunt:

6.1. proprietarul;

6.2. posesorul;

6.3. deținătorul;

6.4. administratorul tehnic;

6.5. registratorul;

6.6. destinatarul;

6.7. 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, cu Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical și cu Hotărârea Guvernului nr. 148/2021 cu privire la organizarea și funcționarea Ministerului Sănătății.

9.1. Posesorul este obligat:

9.1.1. să asigure efectuarea controlului intern privind ținerea RISIT;

9.1.2. să asigure condiții juridice pentru crearea și ținerea RISIT;

9.1.3. să informeze deținătorul despre modificările legislative care afectează funcționarea RISIT;

9.1.4. să informeze registratorii despre vulnerabilitățile RISIT.

9.2. Posesorul are dreptul:

9.2.1. să stabilească prioritățile de dezvoltare a RISIT;

9.2.2. să solicite deținătorului dezvoltarea funcționalităților noi în conformitate cu prioritățile de politici în domeniul sănătății și al asigurării obligatorii de asistență medicală;

9.2.3. să modifice documentația privind gestiunea și exploatarea RISIT;

9.2.4. să delege deținătorului RISIT și/sau registratorului dreptul de prelucrare a datelor cu caracter personal și de 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 are următoarele obligații:

11.1. asigură sprijinul tehnic și informativ pentru crearea și acordarea conturilor de acces la RISIT;

11.2. monitorizează procesul de înregistrare și prelucrare a datelor în RISIT;

11.3. verifică respectarea condițiilor de înregistrare, evidență și utilizare a datelor cu caracter personal;

11.4. asigură securitatea și protecția datelor din RISIT în limitele competențelor;

11.5. administrează rolurile și drepturile de acces corespunzătoare tipului de activitate în RISIT;

11.6. stabilește măsurile tehnice și organizatorice de protecție și securitate a RISIT;

11.7. elaborează și aprobă Planul de continuitate al RISIT, instituie activități de control menite să diminueze riscurile privind integritatea datelor;

11.8. exercită alte atribuții necesare pentru asigurarea bunei funcționări a RISIT;

11.9. elaborează, coordonează și aprobă procedurile operaționale aferente gestionării și asigurării bunei funcționări a RISIT;

11.10. stabilește regulile și procedurile specifice de acordare/suspendare/retragere/anulare a accesului la contururile RISIT și de stabilire a rolurilor registratorilor/utilizatorilor;

11.11. efectuează auditul securității RISIT privind gestiunea datelor cu caracter personal;

11.12. implementează generarea copiilor de rezervă ale RISIT pentru prelucrările automatizate ale datelor (copiile sunt stocate pe suport tehnic, păstrat în locuri protejate);

11.13. asigură, în caz de necesitate, restabilirea funcționalității RISIT în baza copiilor de rezervă generate în prealabil;

11.14. supraveghează respectarea cerințelor de securitate informațională de către registratori, documentează şi raportează 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 Centrului Național pentru Protecția Datelor cu Caracter Personal acest incident;

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

12. Deținătorul RISIT are dreptul:

12.1. să dezvolte, în funcție de competența sa, documentele normative aferente RISIT;

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

12.3. să supravegheze respectarea cerințelor de securitate a informației de către registratorii care formează RISIT și să fixeze cazurile şi tentativele de încălcare a acestora;

12.4. 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 al protecției datelor cu caracter personal;

12.5. să verifice autenticitatea şi veridicitatea datelor introduse în RISIT;

12.6. să solicite de la registratori actualizarea sau corectarea datelor din RISIT în caz de depistare a omiterilor şi a 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 asigură 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:

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

16.2. asigură autenticitatea, plenitudinea și integritatea datelor;

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

16.4. solicită deținătorului autorizarea accesului, precum și suspendarea drepturilor de acces în RISIT;

16.5. raportează posesorului problemele de sistem privind utilizarea RISIT;

16.6. 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, IDNP-ul angajaților acestora cu atribuții de registratori ai datelor în RISIT.

18. Registratorii RISIT au următoarele drepturi:

18.1. să participe la dezvoltarea și la îmbunătățirea RISIT;

18.2. să prezinte propuneri cu privire la inițierea modificărilor actelor normative care reglementează funcționarea RISIT;

18.3. să solicite și să primească informația statistică cu privire la înregistrările din

sistem;

18.4. să prezinte propuneri privind perfecționarea și eficientizarea RISIT.

19. Furnizorii de date către RISIT sunt persoanele autorizate conform următoarelor specificații, iar raportarea tuturor cazurilor este obligatorie:

19.1. persoane autorizate din cadrul prestatorilor de servicii medicale publice și private;

19.2. lucrătorii medicali, persoanele responsabile din cadrul prestatorilor de servicii medicale primare, spitalicești și servicii sânge;

19.3. persoane autorizate din cadrul băncilor de țesuturi și/sau celule umane, indiferent de domeniul de activitate și forma de proprietate;

19.4. persoane autorizate din cadrul laboratoarelor hematologice, virusologice, biochimice, indiferent de forma de proprietate, precum și al laboratoarelor de histocompatibilitate antigenică (HLA);

19.5. medicii din cadrul serviciului medico-legal.

Furnizorii datelor sunt obligați să asigure corectitudinea şi autenticitatea datelor prezentate pentru a fi introduse în RISIT, precum 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:

21.1. să utilizeze datele din RISIT conform scopului și destinației acestora;

21.2. să asigure securitatea și confidențialitatea informației vizualizate sau prelucrate în RISIT;

21.3. să înștiințeze imediat posesorul RISIT despre cazurile de încălcare a securității informaționale a RISIT;

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

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

22.1. să participe la crearea, implementarea și dezvoltarea RISIT;

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

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

22.4. 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 exercitarea drepturilor lor prin următorul mecanism:

23.1. dreptul la informare cu privire la datele cu caracter personal:

23.1.1. 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 regăsește, cine are dreptul vizualizării sau prelucrării acestor date;

23.1.2. dreptul său de a se opune radierii datelor personale poate fi exercitat exclusiv față de registratorul de date, printr-o cerere motivată de opoziție, care va fi arhivată de acesta ca justificare pentru radierea datelor anterioare;

23.2. dreptul de acces la datele cu caracter personal:

23.2.1. fiecare pacient are dreptul să obțină de la registrator, la cerere, fără întârziere şi în mod gratuit, informația privind resursa informațională care prelucrează datele sale, modul de pseudonimizare a identității sale, persoanele cu drept de accesare/completare a datelor sale;

23.2.2. 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. 23.2.1;

23.3. dreptul de intervenție asupra datelor cu caracter personal:

23.3.1. fiecare pacient are dreptul de a obține datele sale, la cerere, de la registrator în mod gratuit;

23.3.2. dreptul să notifice terților cărora le-au fost dezvăluite datele cu caracter personal despre operațiunile efectuate sau informațiile eronate existente;

23.4. dreptul de opoziție al subiectului datelor cu caracter personal:

23.4.1. fiecare pacient are dreptul de a se opune în orice moment, în mod gratuit, din motive întemeiate şi legitime legate de situația sa particulară, prelucrării datelor cu caracter personal, cu excepția cazurilor în care legea stabilește altfel. Dacă opunerea pacientului este justificată, registratorul nu va mai avea acces la aceste date;

23.4.2. fiecare pacient are dreptul de a se opune în orice moment, în mod gratuit şi fără nicio justificare, prelucrării datelor sale personale în scopuri de marketing.

Registratorul este obligat să informeze subiectul despre acest drept, înainte de a dezvălui datele sale personale către terţe părți;

23.5. dreptul de a nu fi supus unei decizii individuale:

fiecare pacient are dreptul de a solicita anularea, totală sau parțială, a oricărei decizii individuale care îi afectează drepturile şi libertățile, dacă aceasta se bazează exclusiv pe prelucrarea automatizată a datelor cu caracter personal, destinată să evalueze anumite aspecte ale personalității sale, cum ar fi competența profesională, credibilitatea, comportamentul şi altele;

23.6. accesul la justiție:

fiecare 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 garantate de Legea nr. 133/2011 privind protecția datelor cu caracter personal 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, de adăugare, de redactare și de radiere.

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

26. Acordarea dreptului de acces la RISIT și contururile acestuia se efectuează în baza autorizării prestatorului de servicii medicale pentru activitățile desfășurate. 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 la contururile acestuia se realizează prin trimiterea cererii/demersului către deținător și/sau în una din următoarele situații:

27.1. după trei tentative greșite de autentificare;

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

28. Retragerea dreptului de acces la RISIT se efectuează:

28.1. la încetarea raporturilor de muncă ale utilizatorilor;

28.2. la intervenirea modificărilor raporturilor de muncă, când noile atribuții nu impun accesul la datele din RISIT.

29. Anularea dreptului de acces se efectuează după constatarea încălcării securității informaționale de către deținător.

30. Lucrările profilactice planificate în complexul de mijloace software se efectuează după notificarea de către deținător, în scris sau prin e-mail, a registratorilor, 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 prin coordonare prealabilă cu deținătorul, în cazul în care RISIT nu funcționează sau funcționează defectuos.

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

31.1. datele cu caracter personal se prelucrează în mod corect și conform prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal;

31.2. colectarea datelor se efectuează exclusiv în scopuri specifice și se prelucrează doar în mod compatibil cu aceste scopuri, inclusiv pentru analize statistice și de cercetare științifică, fără a contraveni prevederilor legii sus-menționate;

31.3. datele colectate sunt adecvate, pertinente și neexcesive și se folosesc doar în scopul pentru care au fost colectate și prelucrate;

31.4. stocarea datelor se face cu respectarea garanțiilor de prelucrare a datelor prevăzute de cadrul normativ ce reglementează acest domeniu.

32. Termenul de păstrare a datelor constituie 30 de ani, iar ulterior RISIT, în mod automatizat, depersonalizează și arhivează cazurile în vederea asigurării disponibilității datelor de importanță pentru serviciul de sănătate publică.

Capitolul IV

ÎNREGISTRAREA, MODIFICAREA, COMPLETAREA

ȘI RADIEREA DATELOR RISIT

33. Înregistrarea datelor în RISIT se realizează de către utilizatorii care au rolurile și permisiunile corespunzătoare, după autentificarea în RISIT.

34. Înscrierile se fac în ordine cronologică, fiecărei înscrieri atribuindu-i-se data efectuării acesteia în RISIT.

35. Modificarea și/sau completarea datelor din RISIT se efectuează de către utilizatorii care au rolurile și permisiunile corespunzătoare, după autentificarea în RISIT.

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

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

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

Capitolul V

ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI RISIT

39. 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.

40. Obiecte ale asigurării protecției şi securității informației din RISIT se consideră:

40.1. masivele informaționale, indiferent de formele păstrării, bazele de date, suporturile materiale care conțin informații privind datele cu caracter personal;

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

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

41. Securitatea informațională a RISIT se realizează prin aplicarea metodelor și prin efectuarea acțiunilor descrise în Planul de continuitate al acestuia și a procedurilor operaționale.

42. Protecția datelor se efectuează prin următoarele metode:

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

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

42.3. monitorizarea procesului de exploatare a RISIT prin intermediul mecanismului de jurnalizare.

43. Subiecții, în procesul de utilizare și exploatare a RISIT, asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

43.1. identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

43.2. implementarea principalelor măsuri tehnico-organizatorice necesare pentru

asigurarea funcționării RISIT;

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

43.4. informarea și instruirea utilizatorilor interni cu privire la mecanismele de asigurare a securității informaționale;

43.5. proceduri de control intern privind respectarea condițiilor de securitate informațională.

Capitolul VI

CONTROLUL ȘI RĂSPUNDEREA

44. Ținerea RISIT este supusă controlului intern și extern:

44.1. controlul intern privind ținerea RISIT se efectuează de către Ministerul Sănătății, care este posesorul RISIT;

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

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

46. 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 acestuia.

47. Toți subiecții RISIT, precum și solicitantul informațiilor ce conțin date cu caracter personal, poartă răspundere pentru prelucrarea, divulgarea, transmiterea informației din RISIT persoanelor terțe, contrar prevederilor legislației.

48. În cazul incidentelor de securitate, posesorul/deținătorul întreprinde măsuri necesare pentru depistarea sursei de producere a incidentului, efectuează analiza acestuia și înlătură cauzele incidentului de securitate, cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal.