



Republica Moldova

GUVERNUL

HOTĂRÂRE Nr. 501
din 10-07-2024

**pentru aprobarea Conceptului Sistemului
informațional „Registrul național de cancer”
și a Regulamentului privind modalitatea de
ținere a Registrului național de cancer**

Publicat : 31-07-2024 în Monitorul Oficial Nr. 329-331 art. 654

În temeiul art. 22 lit. c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, al art. 16 alin. (1) din Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se instituie Sistemul informațional „Registrul național de cancer”.

2. Se aprobă:

2.1. Conceptul Sistemului informațional „Registrul național de cancer”, conform anexei nr. 1;

2.2. Regulamentul privind modalitatea de ținere a Registrului național de cancer, conform anexei nr. 2.

3. 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:

3.1. punctul 3 se completează cu subpunctul 10) cu următorul cuprins:

„10) Sistemul informațional „Registrul național de cancer” (SI RNC)”;

3.2. tabelul de la punctul 81 se completează cu poziția:

„IMSP Institutul Oncologic	Sistemul informațional „Registrul național de cancer (SI RNC);”
----------------------------	---

3.3. punctul 10 se completează cu poziția 10) cu următorul cuprins:

„10) Sistemul informațional „Registrul național de cancer” (SI RNC)	Ministerul Sănătății, Institutul Oncologic, Agenția Națională pentru Sănătate Publică, Compania Națională de Asigurări în Medicină, prestatorii de servicii medicale, subdiviziunile de sănătate ale autorităților administrației publice locale.”
---	--

4. Asigurarea funcționării Sistemului informațional „Registrul național de cancer” se efectuează din contul și în limitele alocațiilor aprobate în acest scop IMSP Institutul Oncologic, precum și din alte surse, conform legislației.

PRIM-MINISTRU

Dorin RECEAN

Contrasemnează:
Ministrul sănătății
Ministrul finanțelor

Ala Nemerenco
Petru Rotaru

Nr. 501. Chișinău, 10 iulie 2024.

Anexa nr. 1
la Hotărârea Guvernului nr.501/2024

CONCEPTUL
Sistemului informațional „Registrul național de cancer”
Capitolul I
INTRODUCERE

1. Conceptul Sistemului informațional „Registrul național de cancer” (în continuare – Concept) are drept scop crearea unui sistem integrat și integrabil în structura informatică națională și sectorială, destinat utilizării de către medicii specialiști și de către personalul medical, administrativ/de conducere, în vederea înregistrării, actualizării și interpretării datelor cu privire la maladiile oncologice la nivel populațional, orientat spre sprijinirea politicilor și a strategiilor naționale în domeniul sănătății, în corespundere cu practicile și politicile europene în acest domeniu.

2. Prezentul Concept determină scopul, obiectivele și funcțiile de bază ale Sistemului informațional „Registrul național de cancer” (în continuare – *SI RNC*), obiectele informaționale, precum și scenariile de bază privind includerea acestora în SI RNC, interacțiunea cu alte sisteme informaționale în vederea cooperării și a schimbului de date.

Capitolul II
DISPOZIȚII GENERALE

3. SI RNC reprezintă totalitatea resurselor și tehnologiilor informaționale interdependente, a metodelor și a personalului, destinate înregistrării, păstrării, prelucrării și furnizării informațiilor privind pacienții cu cancer și cu maladii oncologice.

4. SI RNC asigură digitalizarea proceselor de înregistrare, colectare, validare, depersonalizare, analiză, interpretare, precum și diseminare sistematică și continuă a datelor despre sănătatea cu privire la maladiile oncologice la adulți și copii. Scopul general al SI RNC constă în îmbunătățirea procesului de raportare, de evidență, de gestiune, de actualizare și de generare a rapoartelor cu privire la maladiile oncologice.

5. SI RNC este un sistem informațional al Registrului medical.

6. Noțiunile principale utilizate în prezentul Concept sunt următoarele:

6.1. *consimțământul subiectului datelor cu caracter personal* (acordul informat al pacientului) – manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

6.2. *date cu caracter personal* – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

6.3. *tumoră raportabilă* (în continuare – TR) – orice tumoră primară nou-diagnosticată pentru care, prin metode clinice și/sau de laborator, s-a stabilit un diagnostic raportabil (conform prevederilor pct. 29);

6.4. *caz aferent tumorii raportabile* – orice actualizare a cazului existent de TR (conform prevederilor pct. 29);

6.5. *validare* – verificarea corectitudinii și a gradului de completare pentru fiecare caz raportabil completat, care, obligatoriu, cuprinde volumul minim de date conform formularului electronic de raportare.

Alte noțiuni utilizate în prezentul Concept corespund termenilor definiți în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și în Legea nr. 71/2007 cu privire la registre.

7. SI RNC asigură dezvoltarea resursei informaționale și are următoarele obiective:

7.1. sistematizarea și actualizarea datelor cu privire la maladiile oncologice;

7.2. raportarea indicatorilor standardizați, comparabili la nivel național/internațional;

7.3. îmbunătățirea calității procesului de înregistrare și de validare, asigurând controlul calității datelor, eficientizarea procesului de raportare, conform standardelor regionale/europene/globale;

7.4. standardizarea formularului de înregistrare a cazului și a procedurii de raportare la nivel național;

7.5. dezvoltarea unui sistem informațional flexibil, care permite interconectarea în timp real cu alte sisteme informaționale la nivel național, cu deschiderea către alte sisteme informaționale, pentru a prelua și a transmite informații către acestea, cu îmbunătățirea calității prin furnizarea datelor actualizate;

7.6. generarea rapoartelor statistice și a rapoartelor necesare pentru monitorizarea stării de sănătate a populației și luarea deciziilor sau elaborarea politicilor în domeniul sănătății;

7.7. promovarea relațiilor de colaborare și a schimbului de date între instituțiile medicale la nivel național și asigurarea vizibilității (credibilității) datelor cu privire la cancer la nivel regional/european/global.

8. SI RNC folosește tehnologiile de ultimă generație care permit utilizarea acestuia de către prestatorii de servicii medicale din cadrul sistemului de sănătate al Republicii Moldova prin intermediul unui echipament IT convențional, fără necesitatea instalării programelor suplimentare (un computer personal cu sistem de operare comercial, conectat la internet).

9. Principiile de bază ale SI RNC sunt următoarele:

9.1. *principiul legalității*, potrivit căruia crearea și exploatarea SI RNC se efectuează în conformitate cu legislația națională;

9.2. *principiul autenticității datelor*, care presupune că informațiile păstrate pe dispozitivele de stocare a datelor sau pe suport de hârtie corespund stării reale a obiectelor din SI RNC;

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

9.4. *principiul temeiniciei datelor*, care prevede că introducerea datelor în SI RNC se efectuează doar în baza înscririlor din documentele acceptate ca sursă de informații;

9.5. *principiul auditului sistemului*, care presupune înregistrarea informației despre schimbările care au loc în scopul de a face posibilă reconstituirea istoriei unui document sau starea lui la o etapă anterioară;

9.6. *principiul independenței de platforma software*, conform căruia SI RNC poate fi construit pe baza modulelor elaborate la comandă sau în baza produselor software existente. Conceptul nu limitează în niciun fel abordarea dezvoltării SI RNC atât timp cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit;

9.7. *principiul accesibilității și al integrabilității*, care presupune că SI RNC oferă funcționalități multiple, este construit ca un element integral și este folosit de către utilizatori prin intermediul unei interfețe unice. Mai mult decât atât, acest principiu prevede că expansiunea și dezvoltarea SI RNC se vor face prin protocoale și prin puncte de conexiune proiectate din start;

9.8. *principiul confidențialității informației*, care prevede răspunderea personală, în conformitate cu legislația, a colaboratorilor responsabili de prelucrarea datelor în SI RNC, de utilizarea și difuzarea neautorizată a informației;

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

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

9.11. *principiul extensibilității*, conform căruia componentele SI RNC oferă facilități de ajustare și de extindere a funcționalităților existente pentru conformare la necesitățile în continuă schimbare ale sistemului de sănătate;

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

9.13. *principiul consecutivității*, care presupune elaborarea și implementarea proiectului pe etape;

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

9.15. *principiul utilizării standardelor deschise*, care se aplică pentru a asigura interoperabilitatea cu sistemele externe și păstrarea informației în conformitate cu normele în vigoare;

9.16. *principiul egalității și nondiscriminării*, potrivit căruia toate ființele umane sunt egale în fața legii și au dreptul la protecție și la beneficii egale;

9.17. **principiul securității informaționale**, care presupune asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, a denaturării, a distrugerii și a utilizării neautorizate. Securitatea SI RNC presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirea pentru lucru atât a SI RNC, cât și a datelor acestuia.

Capitolul III

CADRUL NORMATIV AL SI RNC

10. Cadrul normativ al SI RNC este fundamentat pe legislația națională, inclusiv pe cea de profil și din domeniul tehnologiei informației și comunicațiilor, precum și pe tratatele și convențiile internaționale la care Republica Moldova este parte. Acestea sunt:

10.1. Constituția Republicii Moldova;

10.2. Legea ocrotirii sănătății nr. 411/1995;

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

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

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

10.6. Legea nr. 10/2009 privind supravegherea de stat a sănătății publice;

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

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

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

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

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

10.12. Hotărârea Guvernului nr. 1128/2004 cu privire la aprobarea Concepției Sistemului Informațional Medical Integrat;

10.13. Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

- 10.14. 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;
- 10.15. Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate;
- 10.16. Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 10.17. Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- 10.18. Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- 10.19. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
- 10.20. Hotărârea Guvernului nr. 717/2014 privind platforma de dezvoltare a serviciilor electronice (PDSE);
- 10.21. Hotărârea Guvernului nr. 1291/2016 cu privire la Programul național de control al cancerului pentru anii 2016-2025;
- 10.22. Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
- 10.23. Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical;
- 10.24. Hotărârea Guvernului nr. 1090/2017 cu privire la organizarea și funcționarea Agenției Naționale pentru Sănătate Publică;
- 10.25. 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;
- 10.26. Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
- 10.27. Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);
- 10.28. Hotărârea Guvernului nr. 413/2020 cu privire la aprobarea Regulamentului privind utilizarea, administrarea și dezvoltarea Portalului guvernamental al cetățeanului;
- 10.29. Ordinul ministrului sănătății cu privire la întocmirea și prezentarea dărilor de seamă statistice medicale anuale de către instituțiile medico-sanitare, actualizat anual;
- 10.30. Ordinul ministrului sănătății nr. 1086/2016 cu privire la aprobarea Regulamentelor-cadru de organizare și funcționare ale prestatorilor de servicii de sănătate;
- 10.31. Ordinul ministrului sănătății nr. 87/2023 cu privire la aprobarea Regulamentului-cadru de organizare și funcționare a Instituției Medico-Sanitare Publice (în continuare – IMSP) spitalicești;
- 10.32. Ordinele ministrului sănătății cu privire la aprobarea Nomenclatoarelor prestatorilor de asistență medicală primară și spitalicească;
- 10.33. Standardul SM ISO/CEI/IEEE 15288;
- 10.34. Reglementarea tehnică „Procese ciclului de viață al software-ului” (RT 38370656-002:2006) aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78 din 01.06.2006.

Capitolul IV

SPAȚIUL FUNCȚIONAL AL SI RNC

11. Funcțiile de bază asigurate de SI RNC sunt următoarele:

11.1. *înregistrarea sistemică și continuă*, validarea datelor cu privire la orice caz nou de TR și a episoadelor referitoare aferente (totalizarea actualizărilor eventuale pe cazuri concrete);

11.2. *luarea în evidență primară* – atribuirea identificatorului unic obiectului de evidență și introducerea volumului minim stabilit de date în baza de date a SI RNC;

11.3. *actualizarea datelor* – actualizarea sistematică a bazei de date, modificarea/completarea datelor/obiectelor informaționale;

11.4. *schimbarea statutului obiectului informațional* – modificarea informației introduse în SI RNC numai în baza formularului de raportare care confirmă veridicitatea datelor cu referire la documentația medicală în baza căreia a avut loc raportarea/actualizarea datelor, păstrându-se în ordine cronologică;

11.5. *asigurarea informațională* – oferirea informației din SI RNC utilizatorilor doar în conformitate cu prevederile legislației;

11.6. *asigurarea calității informațiilor*, a datelor înregistrate și menținerea acurateței și a gradului de completare a obiectelor informaționale incluse în SI RNC;

11.7. *protecția și securizarea informațiilor* cu utilizarea metodelor de autentificare a utilizatorilor, de autorizare conform rolului atribuit în SI RNC și cu utilizarea mecanismelor de protecție a datelor și a canalelor de conexiune;

11.8. *accesul la date deschise*;

11.9. *utilizarea datelor* – accesarea informației depersonalizate va fi disponibilă cercetătorilor și publicului care este interesat de date statistice (incidența, mortalitatea, supraviețuirea sau prevalența în cancer). Această informație va fi diseminată în literatura de specialitate, în mass-media, prin intermediul bazelor de date sau al website-urilor sub forma rapoartelor și articolelor;

11.10. *generarea rapoartelor statistice* care conțin informații relevante.

12. SI RNC trebuie să asigure exercitarea funcțiilor specifice, ținând cont de destinația sa și fiind definite de următoarele componente funcționale:

12.1. *administrarea reperelor informaționale* implică formarea bazei de date necesare pentru dezvoltarea/evidența/actualizarea informațiilor și a datelor cu privire la TR, a actelor normative naționale și internaționale, a prestatorilor de servicii medicale, indiferent de forma juridică de administrare (publică sau privată) etc.;

12.2. *managementul SI RNC* asigură evidența și elaborarea elementelor descriptive și a indicatorilor standardizați de raportare, publicarea rapoartelor anuale/actualizate, oferirea datelor cu privire la oncologie;

12.3. *analiza datelor SI RNC* și interpretarea acestora pentru a asigura furnizarea informației în vederea elaborării sau a ajustării politicilor în sănătate, știință și utilizarea informației pentru conduita pacientului, etc.

Capitolul V

SPAȚIUL ORGANIZATORIC AL SI RNC

13. Funcțiile de bază privind formarea și exploatarea SI RNC sunt divizate între proprietarul, posesorul, deținătorul, administratorul tehnic, furnizorii de date, registratorii și destinatarii acestuia.

14. Proprietarul SI RNC este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din cadrul acestuia. Resursele financiare pentru dezvoltarea și mentenanța SI RNC sunt asigurate din fondurile asigurării obligatorii de asistență medicală, din proiecte de asistență internațională și din alte mijloace financiare, conform cadrului normativ.

15. Ministerul Sănătății este posesorul SI RNC și asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea acestuia.

16. IMSP Institutul Oncologic (în continuare – *Institutul Oncologic*) este deținătorul SI RNC și asigură crearea, administrarea, mentenanța și dezvoltarea acestuia în conformitate cu prevederile cadrului normativ.

17. Administratorul tehnic al SI RNC este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile conform cadrului normativ în materie de administrare tehnică și de menținere a sistemelor informaționale de stat.

18. Registratorii sunt următoarele categorii de utilizatori ai SI RNC:

18.1. persoanele din cadrul Institutului Oncologic autorizate să înregistreze și/sau să valideze datele în SI RNC și să genereze rapoarte în conformitate cu nivelul de acces atribuit;

18.2. persoanele împuternicite de către deținătorul SI RNC să înregistreze și/sau să valideze datele cu privire la cazurile de cancer și episoadele aferente.

19. Furnizorii de date către SI RNC sunt prestatorii serviciilor de sănătate, indiferent de forma juridică de organizare, după cum urmează:

19.1. persoanele autorizate din cadrul Institutului Oncologic;

19.2. persoanele autorizate din cadrul asistenței medicale primare (în continuare – AMP), asistenței medicale specializate de ambulatoriu (în continuare – AMSA), asistenței medicale spitalicești (în continuare – AMS), precum și a instituțiilor medico-sanitare departamentale și private;

19.3. persoanele autorizate din secțiile de anatomie patologică de categoriile I, II și III;

19.4. persoanele autorizate din cadrul laboratoarelor de citologie, al cabinetelor de imagistică și medicină nucleară, al laboratoarelor hematologice și biochimice, indiferent de forma juridică de organizare;

19.5. persoanele autorizate din cadrul laboratoarelor anatomopatologice din AMS și Centrul de Medicină Legală.

Furnizorii de date sunt obligați să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi introduse în SI RNC și actualizarea acestora.

20. Pentru asigurarea plenitudinii informației în cadrul SI RNC, furnizorii de date menționați în pct. 19 vor prezenta, în mod obligatoriu, toate cazurile de TR și de episoade aferente, în modul stabilit.

21. Destinatarii datelor din SI RNC sunt Ministerul Sănătății, Institutul Oncologic, prestatorii serviciilor medicale implicate în tratamentul pacienților oncologici, Agenția Națională pentru Sănătate Publică, Compania Națională de Asigurări în Medicină, subdiviziunile de sănătate ale autorităților administrației publice locale și persoanele mandatate cu dreptul de a primi informațiile conform prevederilor legale.

22. Accesul la SI RNC poate fi activ și pasiv.

Institutul Oncologic și registratorii autorizați în modul corespunzător dețin acces activ la SI RNC, fapt care le permite înregistrarea, actualizarea și verificarea datelor despre TR și episoadele aferente acestora, proiectarea, construirea, implementarea, operarea și întreținerea SI RNC, asigurarea securității, a protecției și a integrității datelor din SI RNC.

Accesul pasiv permite vizualizarea și extragerea informației din SI RNC de către subiecții indicați în scopul exercitării atribuțiilor corespunzătoare nivelului de acces prestabilit.

23. Administrarea SI RNC va fi asigurată de către posesor și deținător până la adoptarea deciziei despre lichidare a SI RNC. Statul de personal al SI RNC este stabilit de către Institutul Oncologic și include operatori, medici oncologi, asistenți medicali, programatori IT, specialiști în domeniul biostatisticii și în domeniul epidemiologiei, în conformitate cu fișa postului.

Capitolul VI

CLASIFICAREA DOCUMENTELOR SI RNC

24. În cadrul SI RNC se utilizează:

24.1. documente de intrare, care includ formularul de înregistrare a cazului;

24.2. documente de ieșire, care includ:

24.2.1. rapoarte statistice și analitice;

24.2.2. liste pe categoriile solicitate;

24.3. documente tehnologice, care includ:

24.3.1. glosare de termeni și definiții;

24.3.2. notificări privind înregistrarea unui caz nou în SI RNC;

24.3.3. șabloane ale formularelor de înregistrare a cazului;

24.3.4. documente privind descrierea procesului de înregistrare a cazului;

24.3.5. documente tehnologice privind parametrii de sistem;

24.3.6. ghiduri de utilizare și administrare a SI RNC;

24.3.7. registrul cu înregistrări privind acțiunile și interacțiunea utilizatorilor interni;

24.3.8. rapoarte și statistici agregate privind utilizarea SI RNC;

24.3.9. alte documente necesare pentru funcționarea și dezvoltarea SI RNC.

25. Documentele utilizate în cadrul SI RNC vor fi actualizate în conformitate cu necesitățile din domeniul vizat și în strictă concordanță cu legislația.

Capitolul VII

SPAȚIUL INFORMAȚIONAL

Secțiunea 1

Obiectele informaționale ale SI RNC

26. Spațiul informațional al SI RNC cuprinde totalitatea obiectelor informaționale cu atributele și identificadorii săi.

27. Obiectul informațional al SI RNC este caracterizat prin următoarele particularități de bază:

27.1. *unicitate* – particularitate ce semnifică existența identificadorului unic care deosebește obiectul respectiv de alte obiecte similare;

27.2. *stare* – particularitate descrisă printr-un set de proprietăți variabile ale obiectului, luate în considerare în SI RNC;

27.3. *comportament* – particularitate descrisă printr-o listă de evenimente/scenarii prin care trece acesta și care sunt luate în considerare în SI RNC.

28. Obiectele informaționale care reprezintă resursele informaționale ale SI RNC sunt determinate conform destinației și, după caz, vor fi preluate de la autoritățile și instituțiile care le dețin nemijlocit. Obiectele informaționale se recunosc după un număr de identificare unic, specific fiecărui obiect separat.

29. Obiectele informaționale ale SI RNC sunt următoarele:

29.1. cazul de TR – cazul înregistrat și validat în SI RNC.

Reflectarea informațiilor despre TR, care este definită drept orice tumoră malignă conform Clasificării Internaționale a Maladiilor pentru Oncologie, ediția a 3-a (în continuare – ICD-O-3), cod morfologic „/3” sau tumoră *in situ* conform ICD-O-3, cod morfologic „/2” sau tumoră cu evoluție imprevizibilă ori comportament necunoscut conform ICD-O-3, cod morfologic „/1” sau tumoră benignă a creierului și a altor părți ale sistemului nervos central conform ICD-O-3, cod morfologic „/0”, cu excepția hemangioamelor și a leziunilor chistice.

Codificarea tumorilor la persoane cu vârsta cuprinsă între 0 și 19 ani va fi realizată în conformitate cu Clasificarea Internațională a Maladiilor pentru Oncologie, ediția a 3-a (ICD-O-3) și cu Clasificarea Internațională a Cancerelor Pediatriche, ediția a 3-a (în continuare – ICC-3).

Clasificările și nomenclatoarele sus-menționate vor fi actualizate conform ultimilor recomandări internaționale;

29.2. episoadele aferente TR;

29.3. furnizorii de date;

29.4. registratorii SI RNC;

29.5. utilizatorii SI RNC.

Utilizatorul intern (activ) este colaboratorul subdiviziunii care gestionează SI RNC, iar utilizatorul extern (pasiv) este persoana care vizualizează și extrage informația.

30. SI RNC urmează să asigure unicitatea, integritatea și consistența datelor stocate și procesate.

31. Fiecărui obiect informațional i se va atribui un identificator unic, generat automat de SI RNC. Obiectele informaționale preluate din alte sisteme informaționale vor fi identificate în conformitate cu regulile sistemului în care au fost introduse/create.

31.1. Identificatorul obiectului informațional „caz de TR” este numărul de ordine al cazului (unic) generat automat;

31.2. identificatorul obiectului informațional „episod aferent TR” este actualizarea eventuală pe caz concret TR;

31.3. identificatorul obiectului informațional „furnizor de date al SI RNC” este numărul de identificare de stat al persoanei fizice (în continuare – IDNP), preluat din Registrul de stat al populației;

31.4. identificatorul obiectului informațional „registrator al SI RNC” (operator, asistent medical, medic oncolog, epidemiolog, analist de date din cadrul SI RNC) este IDNP-ul persoanei fizice, preluat din Registrul de stat al populației;

31.5. identificatorul obiectului informațional „utilizator SI RNC” este numărul de identificare de stat al unității de drept (în continuare – IDNO), preluat din Registrul de stat al unităților de drept sau, după caz, IDNP.

Secțiunea a 2-a

Scenariile asociate obiectelor informaționale

32. Scenariile de bază reprezintă lista evenimentelor referitoare la obiectele înregistrate în SI RNC și care corespund următoarelor criterii:

32.1. *luarea inițială în evidență a cazului de TR* se face la apariția unui caz nou, obiect al SI RNC, cu atribuirea numărului unic de înregistrare și se efectuează de către operatori, medici oncologi și asistenți medicali ai SI RNC;

32.2. *actualizarea informațiilor* se efectuează prin introducerea sistematică a modificărilor/rectificărilor/completărilor în baza de date a SI RNC în conformitate cu episoadele aferente survenite;

32.3. *scoaterea/radierea obiectului informațional* din evidență și transferarea datelor are loc prin intermediul formularului de raportare (în continuare – *fRNC*), prin argumentare și cu efectuarea unei mențiuni speciale în SI RNC;

32.4. *raportare*, se realizează prin elaborarea rapoartelor finale pentru anul gestionat. Rapoartele pot fi generate după validarea tuturor datelor, dar nu mai târziu de un an de la validarea acestora.

33. Furnizorii de date vor iniția fluxul de informații spre secția de înregistrare a SI RNC prin intermediul site-ului web dedicat, prin interacțiunea sistemelor informaționale sau prin intermediul altor metode disponibile, iar personalul secției de înregistrare va valida informația primită și va atribui un număr unic de înregistrare a cazului nou de TR sau a episodului aferent acesteia, pentru a fi inclus în baza de date activă din SI RNC.

Actualizarea informației are loc pe măsura recepționării de la furnizorii de date și a validării acesteia de către registratori. Radierea/corecția datelor despre obiectul informațional din evidență și transferarea datelor acestuia poate avea loc doar cu autorizarea deținătorului SI RNC.

Secția analitică va prelucra statistic datele din SIRNC, va genera rapoarte cu periodicitate variabilă pentru rapoartele regulate sau la cerere și va asigura suport pentru cercetările științifice în domeniu.

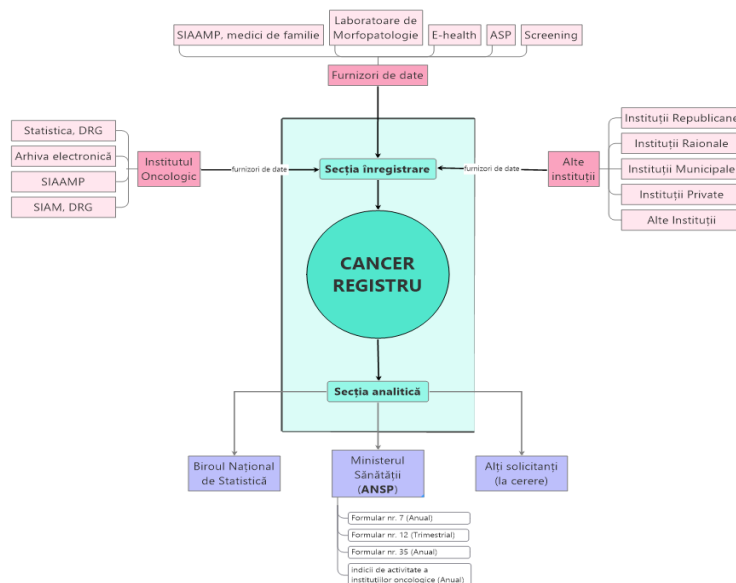


Figura 1. Fluxul informațional asociat obiectelor informaționale

Secțiunea a 3-a Datele SI RNC

34. Datele SI RNC reprezintă totalitatea caracteristicilor obiectului informațional și includ următoarele informații:

34.1. date despre furnizorii de date care raportează:

34.1.1. numele prestatorului de servicii medicale;

34.1.2. IDNO prestatorului de servicii medicale;

34.1.3. numele și prenumele medicului care completează fRNC;

34.1.4. data, luna și anul raportării;

34.1.5. codul unic de identificare a medicului care completează fRNC;

34.2. date despre pacient:

34.2.1. numele și prenumele pacientului;

34.2.2. IDNP-ul pacientului (după caz);

34.2.3. data, luna și anul nașterii pacientului;

34.2.4. genul pacientului;

34.2.5. adresa de domiciliu și/sau reședința temporară a pacientului;

34.3. date despre cazul de tumoră sau episoadele aferente TR:

34.3.1. data primei consultații (adresări);

34.3.2. data confirmării anatomopatologice (histologice) sau citologice/hematologice (după caz);

34.3.3. certitudinea diagnosticului – clasificarea și modul cum a fost confirmat diagnosticul;

34.3.4. codul diagnosticului;

34.3.5. topografia tumorii;

34.3.6. lateralitatea tumorii;

34.3.7. morfologia tumorii;

34.3.8. codul morfologiei;

34.3.9. comportamentul tumorii;

34.3.10. gradul de diferențiere histologică;

34.3.11. imunofenotipul;

34.4. determinarea stadiului cazului de TR sau episoadele aferente TR conform Clasificării Internaționale: tumori, noduli și metastaze (în continuare – *TNM*):

34.4.1. stadiul clinic al *TNM* ;

34.4.2. stadiul patologic al *TNM*;

34.4.3. stadiul non*TNM* pentru limfoame și leucemii;

- 34.5. evoluția și tratamentul cazului de TR:
 - 34.5.1. tratamentele aplicate;
 - 34.5.2. intenția tratamentului;
 - 34.5.3. data inițierii tratamentului;
 - 34.5.4. tipul tratamentului;
 - 34.5.5. statutul vital;
 - 34.5.6. data decesului;
 - 34.5.7. cauza decesului;
- 34.6. date despre registratorii și utilizatorii SI RNC:
 - 34.6.1. numele și prenumele persoanei;
 - 34.6.2. IDNP-ul;
 - 34.6.3. funcția deținută;
 - 34.6.4. cronologia acțiunilor.

Secțiunea a 4-a **Clasificatoarele SI RNC**

35. Pentru a asigura autenticitatea și reducerea volumului informației stocate în SI RNC, se utilizează următoarele clasificatoare și nomenclatoare:

- 35.1. Clasificatoare internaționale:
 - 35.1.1. ICD-X – Clasificarea internațională a maladiilor, ediția X;
 - 35.1.2. ICD-O-3 – Clasificarea internațională a maladiilor oncologice, ediția a 3-a;
 - 35.1.3. ICC-3 – Clasificarea internațională a cancerelor pediatrice, ediția a 3-a;
 - 35.1.4. stadializarea TNM – Clasificarea TNM a Tumorilor Maligne, ediția 8;
 - 35.1.5. stadializarea cancerelor pediatrice recomandat prin Consensul de la Toronto;
 - 35.1.6. ICD-X-AM – Clasificarea internațională a maladiilor, ediția X, modificarea Australiană;
- 35.2. nomenclatoare:
 - 35.2.1. ale prestatorilor de servicii medicale;
 - 35.2.2. ale unităților administrativ-teritoriale.

Secțiunea a 5-a **Interacțiunea SI RNC cu alte resurse informaționale**

36. Schimbul de date dintre SI RNC și alte sisteme și resurse informaționale de stat se realizează prin intermediul platformei de interoperabilitate (MConnect), în conformitate cu prevederile cadrului normativ care reglementează domeniul interoperabilității și al schimbului de date.

37. Pentru a asigura funcționalitatea SI RNC este necesară interacțiunea cu următoarele sisteme informaționale:

- 37.1. Sistemul informațional automatizat „Asistența medicală spitalicească” (SIA AMS); Sistemul informațional automatizat „Asistență medicală primară” (SIA AMP); Sistemul informațional automatizat „Registrul de screening de cancer de col uterin”, precum și cu alte registre de screening oncologic, din momentul când vor deveni funcționale;
- 37.2. sistemele informaționale ale Companiei Naționale de Asigurări în Medicină;
- 37.3. Sistemul informațional automatizat „Registrul de stat al populației”;
- 37.4. alte sisteme informaționale din cadrul instituțiilor medicale și nonmedicale, indiferent de forma de proprietate (de exemplu: sistemele informaționale ale laboratoarelor morfologice, ale spitalelor private etc.), care furnizează informații relevante pentru SI RNC.

38. SI RNC utilizează și interacționează cu următoarele sisteme informaționale partajate:

- 38.1. platforma de interoperabilitate (MConnect) – în vederea interoperabilității și schimbului de date cu alte sisteme și resurse informaționale de stat;

38.2. serviciul electronic guvernamental de jurnalizare (MLog) – în scopul evidenței evenimentelor supuse jurnalizării;

38.3. serviciul electronic guvernamental integrat de semnătură electronică (MSign) – în vederea semnării electronice a actelor întocmite în SI RNC care necesită semnarea;

38.4. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – în vederea autentificării participanților la SI RNC;

38.5. portalul guvernamental al cetățeanului – în scopul transmiterii și afișării informației medicale personale a persoanei fizice;

38.6. serviciul guvernamental de notificare electronică (MNotify) – în vederea notificării utilizatorilor evenimentele din SI RNC;

38.7. portalul guvernamental unic de date deschise (date.gov.md) – pentru publicarea și punerea la dispoziția persoanelor interesate a datelor publice referitoare la resursa informațională.

39. Datele cu caracter personal din SI RNC nu sunt publice, accesibilitatea acestora este limitată și se acordă în condițiile Legii nr. 133/2011 privind protecția datelor cu caracter personal.

40. Toate activitățile efectuate de către utilizatori, fie cu succes, fie fără succes (încercările de logare nereușită), vor fi monitorizate și înregistrate în jurnalele cu acces limitat ale SI RNC.

Capitolul VIII

SPAȚIUL TEHNOLOGIC AL SI RNC

41. Spațiul tehnologic al SI RNC este caracterizat de următoarele aspecte generale:

41.1. SI RNC este găzduit de platforma tehnologică guvernamentală comună (MCloud), în conformitate cu Hotărârea Guvernului nr. 128/2014;

41.1.1. spațiul tehnologic al SI RNC constă în stabilirea metodelor de asigurare a integrabilității acestuia și de suport pentru buna lui funcționare, conform criteriilor de performanță și de utilizare a sistemelor de acest tip. Spațiul tehnologic se referă la problema calității și a securității informației în cadrul SI RNC. În sensul funcționării corecte și al asigurării accesului echitabil la SI RNC, Ministerul Sănătății este responsabil de evaluarea situației din cadrul instituțiilor furnizoare de date și de recomandările de ordin tehnic către acestea;

41.1.2. fiecare registrator dispune de acces la SI RNC, bazat pe apartenența la un grup de securitate;

41.1.3. conexiunea la rețeaua internet a SI RNC este de bandă largă, pentru a menține la cel mai înalt nivel indicii de performanță și accesibilitatea;

41.1.4. accesul la resursele informaționale ale SI RNC se realizează prin conexiunea la internet, asigurată de către prestatorii naționali de asemenea servicii;

41.1.5. SI RNC dispune de servicii de comunicare care asigură buna funcționare: gestiunea și funcționalitatea fluxurilor de lucru, a fluxurilor documentelor și ale înregistrărilor.

42. SI RNC este proiectat ca un sistem modular și se bazează pe componente integrate, fiind compatibil cu tehnologia de cloud computing, care asigură posibilitatea dezvoltării sale, fără a afecta continuitatea funcționării, și permite operarea modificărilor și implementarea acestora.

43. SI RNC urmează să fie dezvoltat, ținând cont de prioritățile posesorului/deținătorului.

44. Arhitectura SI RNC este compusă din trei niveluri, caracterizată prin următoarele componente de bază, care sunt interdependente, realizează schimbul reciproc de date și sunt grupate după cum urmează:

44.1. nivelul de prezentare a datelor – reprezentat de interfețele destinate utilizatorilor;

44.2. nivelul aplicațiilor – destinat pentru executarea proceselor de business-logică a SI RNC, pentru accesarea, prelucrarea, transformarea datelor și pentru asigurarea coerenței și a preciziei acestora;

44.3. nivelul de date – destinat pentru stocarea și actualizarea datelor în sistemul de gestionare a bazelor de date relaționale.

45. Platforma tehnică a SI RNC va utiliza tehnologii bine cunoscute și general acceptate și va fi compatibilă cu sisteme care la fel utilizează standarde nonproprietary și standarde deja existente.

46. Arhitectura platformei software, lista de produse software și mijloacele tehnice utilizate pentru crearea infrastructurii informaționale sunt determinate de către posesor/deținător în etapele ulterioare de dezvoltare a SI RNC, ținând cont de următoarele aspecte:

46.1. implementarea unei soluții care să se bazeze pe arhitectura software orientată spre servicii (*service oriented architecture*), ce oferă posibilitatea reutilizării unor funcții ale SI RNC în cadrul altor procese sau permite extinderea acestuia cu noi funcționalități, fără a perturba funcționarea sa;

46.2. implementarea funcționalităților de arhivare a informațiilor, crearea copiilor de rezervă și restaurarea datelor în caz de incidente;

46.3. utilizarea aplicațiilor și a infrastructurii software bazate pe licențe perpetue pentru toate produsele software incluse în SIRNC și care să asigure suportul producătorilor;

46.4. asigurarea operaționalității/funcționalității sistemelor IT în cazul unor perturbări (defecțiuni hardware, coruperi de date) sau permisiunea extensiilor ulterioare pentru un centru alternativ folosit în cazul unor dezastre naturale;

46.5. asigurarea protecției corespunzătoare a datelor confidențiale, limitarea accesului la informațiile din sistemul de producție SI RNC conform unei matrice de drepturi, în funcție de roluri, și monitorizarea acestuia, astfel încât să prevină divulgarea sau utilizarea neautorizată a datelor din SI RNC;

46.6. asigurarea următoarelor funcționalități generale:

46.6.1. partajarea eficientă a informației între utilizatorii SI RNC;

46.6.2. crearea fluxurilor de proces automatizate suportate de aplicații;

46.6.3. accesul online, pe baza serviciilor web, la informațiile utile utilizatorilor;

46.6.4. oferirea suportului tehnic sigur (mentenanța pentru corectarea erorilor și asigurarea completărilor necesare) și scalabil, astfel încât să susțină numărul necesar de utilizatori;

46.6.5. administrarea identității utilizatorilor și controlul accesului la toate resursele SI RNC;

46.6.6. administrarea și operarea infrastructurii și a componentelor soluției la costuri reduse;

46.7. implementarea următoarelor caracteristici generice:

46.7.1. principii standard ale industriei de profil pentru utilizarea prietenoasă;

46.7.2. facilități de securitate și de administrare a SI RNC;

46.7.3. facilități de management al datelor (informațiilor), cu particularitățile de protecție corespunzătoare.

47. Tipurile principale de standarde tehnologice utilizate sunt:

47.1. standarde ale datelor;

47.2. standarde ale metadatelor (SM ISO/IEC 11179-1; SM ISO/IEC 11179-2; SM ISO/IEC 11179-3; SM ISO/IEC 11179-4; SM ISO/IEC 11179-5; SM ISO/IEC 11179-6);

47.3. standarde privind schimburile de informații;

47.4. standarde privind căutarea informațiilor;

47.5. standarde de calitate;

47.6. standarde de securitate;

47.7. standarde de multilingvism.

48. Conformitatea cu standardele tehnologice constă în:

48.1. susținerea interfeței browserului public pentru accesare;

48.2. utilizarea standardelor internet și WWW – HTML, TCP/IP, SMTP;

48.3. utilizarea standardelor naționale și internaționale privind calitatea și securitatea.

Capitolul IX

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

A SI RNC

49. Securitatea informațională a SI RNC constă în următoarele:

49.1. prin securitate informațională se înțelege protecția resurselor și a infrastructurii informaționale a SI RNC împotriva acțiunilor premeditate sau accidentale cu caracter natural sau artificial, care cauzează prejudicii participanților la procesul de schimb informațional;

49.2. noțiunea de securitate informațională a SI RNC include o serie de termeni ca: măsuri, politici, tehnologii, puncte de control, structură organizațională, atribuții și funcții în SI RNC. Identificarea acestor mijloace de control este necesară pentru a asigura securitatea informațională și pentru a le implementa în SI RNC;

49.3. 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;

49.4. 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:

49.4.1. securitatea fizică se referă la protejarea infrastructurii fizice a SI RNC, prin aplicarea tuturor măsurilor de securitate;

49.4.2. securitatea informațională presupune protejarea informației prin aplicarea unor măsuri de securizare la nivel logic, precum și 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;

49.4.3. securitatea aplicației presupune protejarea informației prin delimitarea accesului diferențiat la date, bazat pe roluri. În arhitectura SI RNC sunt incluse mecanisme de securitate la nivelul aplicației, care presupun autentificarea utilizatorilor doar prin intermediul serviciului MPass.

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

50.1. colectarea și/sau utilizarea ilegală a informației;

50.2. încălcarea tehnologiei de prelucrare a informației;

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

50.4. 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;

50.5. nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor software de prelucrare a informației;

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

50.7. scurgerea de informație prin canale tehnice;

50.8. implementarea dispozitivelor electronice de interceptare a informației în mijloacele tehnice de prelucrare, de păstrare și de transmitere a datelor prin canalele de comunicații, precum și în încăperile de serviciu ale registratorilor SI RNC;

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

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

50.11. utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție a datelor, a mijloacelor de informatizare și comunicații la crearea și dezvoltarea infrastructurii informaționale;

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

50.13. încălcarea restricțiilor legale ce țin de răspândirea informației.

51. SI RNC prevede următoarele cerințe și sarcini privind asigurarea securității informaționale:

51.1. securitatea informațională trebuie să se conformeze cerințelor legislației Republicii Moldova, precum și standardelor internaționale care nu contravin legii și permit sporirea gradului de securitate;

51.2. securitatea informațională trebuie să asigure:

51.2.1. confidențialitatea informației, care presupune limitarea accesului la informație al persoanelor fără drepturi și împuterniciri corespunzătoare;

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

51.2.3. integritatea fizică a informației;

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

51.3. pentru îndeplinirea sarcinilor privind asigurarea securității informaționale a SI RNC, se utilizează următoarele mecanisme;

51.3.1. dubla autentificare și autorizarea utilizatorului;

51.3.2. managementul accesului;

51.3.3. înregistrarea acțiunilor și auditul prin intermediul mecanismelor serviciului MLog.

Capitolul X ÎNCHEIERE

52. Impactul SI RNC constă în implementarea unei soluții moderne de gestiune și de automatizare a fluxurilor de date în sistemul de sănătate, precum și digitalizarea proceselor de colectare, de analiză, de interpretare și de diseminare sistematică și continuă a datelor cu privire la toate cazurile de boli oncologice și TR, în scopul colectării, înregistrării și prelucrării, în cadrul Institutului Oncologic, a datelor legate de incidența, prevalența și mortalitatea prin cancer la nivel național.

53. Ținând cont de complexitatea SI RNC, implementarea acestuia va fi efectuată pe etape.

În etapa inițială, va fi elaborat mecanismul de raportare a cazului de tumoră malignă de către instituțiile medicale, urmat de mecanismul de vizualizare a datelor și informațiilor.

Celelalte etape vor fi determinate ulterior, în funcție de mijloacele financiare disponibile.

54. SI RNC oferă beneficii importante părților implicate în sistemul de sănătate publică și de avantaje de ordin strategic, dintre care:

54.1. este creat și dezvoltat în baza unei analize amănunțite, realizate împreună cu personalul medical, pentru a cuprinde și a optimiza întreaga activitate, urmând modele moderne ale aceluiași sector din țările Uniunii Europene;

54.2. urmărește eliminarea mulțimii de dosare pe hârtie, care sunt greu de gestionat;

54.3. urmărește organizarea eficientă a timpului;

54.4. urmărește implementarea unor mecanisme de monitorizare și control al calității serviciilor medicale oferite;

54.5. urmărește modernizarea serviciilor medicale în aceeași direcție, similar țărilor Uniunii Europene în sectorul dat, respectând în totalitate legislația Republicii Moldova;

54.6. este ușor de utilizat, fiind adaptat la cunoștințele utilizatorilor legate de navigarea pe internet;

54.7. asigură în permanență protecția datelor și are posibilitatea interoperabilității cu alte sisteme informaționale;

54.8. asigură trasabilitatea prin sisteme de interconectare (servicii web cu grad înalt de securitate), oferind informații utile și exacte privind evoluția și statutului pacientului oncologic și privind istoricul medical în timp real;

54.9. contribuie la realizarea unei imagini corecte a resurselor prin intermediul generării de rapoarte complexe;

54.10. prin implementarea SI RNC la nivel național, se realizează o platformă informatică cu un nivel înalt de acuratețe a datelor medicale, deschisă pentru extinderea și interconectarea unor sisteme actuale/viitoare din domeniul sănătății.

55. În perioada de trecere de la sistemul existent de raportare statistică la raportarea prin depozitul centralizat de date SI RNC, se va asigura funcționalitatea de raportare prin emiterea rapoartelor statistice existente (inclusiv fRNC).

Anexa nr. 2
la Hotărârea Guvernului nr.501/2024

REGULAMENT
privind modalitatea de ținere a Sistemului informațional
Registrul național de cancer

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind modalitatea de ținere a Registrului național de cancer (în continuare – *Regulament*) stabilește procedurile și mecanismele de înregistrare și de evidență a informației sistematizate, acumulate în cadrul depistării, gestionării și supravegherii epidemiologice a maladiilor oncologice, precum și reglementează cerințele față de protecția datelor în procesul de colectare, acumulare, actualizare, prelucrare și de păstrarea acestora, precum și față de schimbul autorizat de date cu alte sisteme informaționale.

2. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Legea nr. 71/2007 cu privire la registre, Legea nr. 10/2009 privind supravegherea de stat a sănătății publice, Legea nr. 133/2011 privind protecția datelor cu caracter personal, Hotărârea Guvernului nr. 1128/2004 cu privire la aprobarea Concepției Sistemului informațional medical integrat, 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.

3. Sistemul informațional „Registrul național de cancer” (în continuare – *SI RNC*) este resursa informațională de stat care reprezintă totalitatea informației sistematizate cu privire la maladiile oncologice și include datele cu privire la tumorile raportabile (în continuare – *TR*), inclusiv orice episod aferent acestora, precum și totalitatea documentelor și a mijloacelor de identificare.

4. Scopul SI RNC este de a asigura digitalizarea proceselor de colectare, validare, depersonalizare, analiză, interpretare și diseminare sistematică și continuă a datelor despre sănătate privind maladiile oncologice la adulți și copii, precum și îmbunătățirea procesului de raportare, evidență, gestiune, actualizare și generare a rapoartelor cu privire la bolile oncologice.

5. SI RNC creează spațiul informațional necesar pentru participanții la SI RNC, în vederea automatizării unor funcții realizate de aceștia prin implementarea tehnologiilor informaționale performante în domeniul supravegherii tuturor cazurilor de boli oncologice și TR.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE
ÎN DOMENIUL CREĂRII, EXPLOATĂRII ȘI UTILIZĂRII
SI RNC ȘI ATRIBUȚIILE ACESTORA

6. Subiecții din domeniul creării, exploatării și utilizării conținutului SI RNC sunt:

- 6.1. proprietarul;
- 6.2. posesorul;
- 6.3. deținătorul;
- 6.4. administratorul tehnic;
- 6.5. registratorul;
- 6.6. destinatarul;
- 6.7. furnizorul datelor.

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

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

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 SI RNC;

9.1.2. să asigure condiții juridice pentru crearea și ținerea Registrului național de cancer (în continuare – RNC);

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

9.1.4 să informeze registratorii despre vulnerabilitățile SI RNC.

9.2. Posesorul are dreptul:

9.2.1. să stabilească prioritățile de dezvoltare a SI RNC;

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

9.2.3. să modifice documentația privind gestiunea și exploatarea SI RNC;

9.2.4. să delege deținătorului SI RNC și/sau registratorului dreptul de prelucrare a datelor cu caracter personal, precum și de asigurare a protecției acestora.

10. Institutul Oncologic este deținătorul SI RNC și asigură crearea, administrarea, mentenanța și dezvoltarea acestuia.

11. Deținătorul are următoarele atribuții:

11.1 asigură formarea resursei informaționale;

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

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

11.4. asigură securitatea și protecția datelor din SI RNC, în limitele competențelor;

11.5. autorizează și suspendă dreptul de acces la SI RNC;

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

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

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

11.9. elaborează, coordonează și aprobă procedurile operaționale privind gestionarea și asigurarea bunei funcționări a SI RNC;

11.10. stabilește regulile și procedurile specifice de acordare/suspendare/retragere/anulare a accesului la conturile SI RNC, precum și rolurile utilizatorilor.

12. Drepturile și obligațiile deținătorului sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și cu Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical.

13. Deținătorul asigură păstrarea SI RNC 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 SI RNC este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care asigură administrarea tehnică și menținerea SI RNC conform cadrului normativ care reglementează domeniul.

15. Registratorul SI RNC se consideră persoana autorizată din cadrul Institutului Oncologic să înregistreze și/sau să valideze datele în SI RNC, precum și persoanele împuternicite de către deținătorul SI RNC să înregistreze și/sau să valideze datele cu privire la cazurile de TR și episoade aferente.

16. Registratorii au următoarele atribuții:

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

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 SI RNC;

16.5. raportează posesorului sau administratorului tehnic problemele de sistem privind utilizarea SI RNC;

16.6. prezintă propuneri de îmbunătățire și de dezvoltare a SI RNC, participă în grupurile de lucru organizate în scopul dezvoltării acestuia.

17. Registratorul desemnează și informează posesorul despre numărul, numele, prenumele angajaților cu atribuții de introducere nemijlocită a datelor în SI RNC.

18. Registratorii SI RNC au următoarele drepturi:

18.1. să participe la dezvoltarea și îmbunătățirea SI RNC;

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

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

18.4. să prezinte propuneri privind îmbunătățirea și eficientizarea SI RNC.

19. Furnizori de date pentru SI RNC sunt lucrătorii medicali și persoanele autorizate, care sunt obligați să raporteze toate cazurile. Din categoria aceasta fac parte:

19.1. persoanele autorizate din cadrul Institutului Oncologic;

19.2. lucrătorii medicali, persoanele responsabile din cadrul prestatorilor de servicii medicale cum ar fi Asistența medicală primară (în continuare – AMP), Asistența medicală specializată de ambulatoriu (în continuare – AMSA), Asistența medicală spitalicească (în continuare – AMS), prestatorii de servicii medicale departamentală, precum și cei ai centrelor de sănătate publică;

19.3. lucrătorii medicali din secțiile de anatomie patologică de categoriile I, II și III;

19.4. persoanele autorizate din cadrul laboratoarelor de citologie, al laboratoarelor de morfopatologie, al cabinetelor de imagistică și medicină nucleară, al laboratoarelor hematologice și biochimice, indiferent de forma de proprietate;

19.5. medicii din cadrul laboratoarelor anatomopatologice ale AMS și ale Centrului de Medicină Legală.

Furnizorii de date sunt obligați să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi introduse în SI RNC, precum și actualizarea acestora.

20. Destinatarii SI RNC sunt Ministerul Sănătății, Institutul Oncologic, Agenția Națională pentru Sănătate Publică, Compania Națională de Asigurări în Medicină, prestatorii de servicii medicale, subdiviziunile de sănătate ale autorităților administrației publice locale, persoanele mandatate cu dreptul de a primi informațiile conform prevederilor legale și procedurii stabilite pentru obținerea datelor.

21. Destinatarii SI RNC sunt obligați:

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

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

21.3. să înștiințeze imediat posesorul și administratorul tehnic al SI RNC despre cazurile de încălcare a securității informaționale a SI RNC;

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

22. Destinatarii SI RNC, în limitele competențelor, au următoarele drepturi:

22.1. să participe la crearea, implementarea și dezvoltarea SI RNC;

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

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

22.4. să solicite și să primească de la posesorul SI RNC ajutor metodologic și practic privind problemele ce țin de funcționarea SI RNC.

Capitolul III

REGIMUL JURIDIC DE UTILIZARE A DATELOR

23. Dreptul de acces la datele SI RNC este segmentat pe unități de conținut, atribuind prerogative partajate de vizualizare, de adăugare, de redactare și de ștergere.

24. Accesul la resursele informaționale ale SI RNC este segmentat pentru utilizatori interni și utilizatori externi.

Utilizatorii interni sunt utilizatorii care accesează datele deținute de către Institutul Oncologic în vederea înregistrării, a actualizării și a verificării datelor despre TR și despre episoadele aferente acestora. Utilizatorii interni sunt: deținătorul, registratorul și alți utilizatori ale căror drepturi de acces sunt definite în prezentul Regulament și în alte acte normative.

Utilizatorii externi sunt utilizatorii care accesează datele prin platforma de interoperabilitate pentru a vizualiza și a extrage informația.

Dreptul de acces la SI RNC și contururile acestuia nu sunt permanente și pot fi suspendate. Introducerea și/sau modificarea datelor în SI RNC de pe un nume de profil de utilizator străin este strict interzisă, urmând a fi considerate ca acces neautorizat.

Furnizorii de date și utilizatorii urmează să se asigure că profilul de furnizor sau de utilizator, precum și, eventual, semnătura electronică sunt confidențiale.

25. Suspendarea dreptului de acces la SI RNC și/sau contururile acestuia se efectuează prin înaintarea cererii/demersului de către utilizatorul intern către deținător și/sau în una dintre următoarele situații:

25.1. la încetarea/suspendarea raporturilor de serviciu/de muncă ale furnizorului sau ale utilizatorului;

25.2. la intervenirea modificărilor în raporturile de serviciu/de muncă, când noile atribuții nu impun accesul la datele din SI RNC;

25.3. după o perioadă inactivă, stabilită în timp (inacțiune în perioada de maximum 6 luni);

25.4. după 3 tentative greșite de autentificare;

25.5. la constatarea de către posesor a încălcării securității informaționale;

25.6. în alte cazuri, în limitele prevederilor legislative.

26. Lucrările de mentenanță planificate în complexul de mijloace software se efectuează după notificarea, în scris sau prin e-mail, a registratorilor de către posesor, în baza planului coordonat cu administratorul tehnic cu cel puțin 2 zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările de mentenanță neplanificate se efectuează la solicitarea utilizatorilor prin coordonarea prealabilă cu posesorul, în situația nefuncționării sau funcționării necorespunzătoare a SI RNC.

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

27.1. prelucrarea datelor cu caracter personal se va realiza în mod corect și conform prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal;

27.2. colectarea datelor va fi efectuată doar în scopuri determinate și vor fi prelucrate doar în modul compatibil cu acest scop, precum și în scopuri statistice, de cercetare istorică sau științifică, care nu contravin prevederilor legii sus-menționate;

27.3. datele colectate vor fi adecvate, pertinente și neexcesive și se vor folosi doar în scopul pentru care au fost colectate și prelucrate;

27.4. actualizarea datelor se va efectua la necesitate, iar cele incomplete sau inexacte fiind ulterior rectificate ori șterse;

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

Termenul de păstrare al datelor se va aplica în conformitate cu reglementările aprobate de Ministerul Sănătății privind formularele de evidență medicală primară, iar ulterior SI RNC, în mod automatizat, va depersonaliza și va arhiva cazurile pentru a asigura disponibilitatea datelor de importanță pentru serviciul de sănătate publică.

Capitolul IV **ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII** **INFORMAȚIEI DIN SI RNC**

28. Măsurile de protecție și securitate a informației din SI RNC reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SI RNC și se efectuează neîntrerupt de către posesorul acestuia.

29. Obiecte ale asigurării protecției și securității informației din SI RNC se consideră:

29.1. volumul informațional, indiferent de formele păstrării, bazele de date, suporturile materiale care conțin informații privind date cu caracter personal;

29.2. sistemele informaționale, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații care asigură activitatea SI RNC;

29.3. sistemele de telecomunicații, rețelele, inclusiv mijloacele de creare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

30. Securitatea informațională a SI RNC se efectuează cu ajutorul metodelor și acțiunilor descrise în Planul de continuitate al acestuia (elaborat odată cu implementarea SI RNC) și, după caz, a procedurilor operaționale.

31. Protecția datelor se efectuează prin următoarele metode:

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

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

31.3. monitorizarea procesului de exploatare a SI RNC prin intermediul mecanismului de jurnalizare.

32. Subiecții, în procesul de utilizare și exploatare SI RNC, asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

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

32.2. implementarea principalelor măsuri tehnico-organizatorice necesare pentru asigurarea funcționării SI RNC;

32.3. implementarea procedurilor interne ce exclud cazurile de modificare nesanționată a mijloacelor software și/sau a informației din SI RNC;

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

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

33. Pentru îndeplinirea sarcinilor privind asigurarea securității informaționale a SI RNC sunt folosite următoarele mecanisme:

33.1. autentificarea și autorizarea;

33.2. dirijarea accesului;

33.4. înregistrarea acțiunilor și auditul securității;

33.5. criptarea informației.

34. Sistemul complex al securității informaționale asigură:

34.1. integritatea logică a informației;

34.2. integritatea fizică a informației;

34.3. protecția infrastructurii informaționale, în cazul tentativelor de deteriorare sau modificare a funcționării SI RNC.

35. Autoritatea/instituția care utilizează SI RNC desemnează o persoană responsabilă de implementarea și monitorizarea respectării prevederilor normelor de securitate informațională.

36. Normele de securitate informațională se aduc la cunoștința fiecărui utilizator și se semnează de acesta. Fiecare utilizator este obligat să cunoască normele de securitate informațională și procedurile care trebuie respectate în strictă concordanță cu politica de securitate.

37. Persoana responsabilă care implementează și monitorizează respectarea prevederilor normelor de securitate informațională asigură instruirea angajaților privind metodele și procedeele de contracarare a pericolelor informaționale.

38. Procedura de înregistrare este realizată prin autentificare și autorizare, care sunt aspecte critice pentru securitatea SI RNC, asigurând că doar persoanele autorizate au acces în SI RNC, și este efectuată numai de către utilizatorii cu rolul și permisiunile corespunzătoare după autentificare în SI RNC.

39. Procedura de modificare și completare are loc după procedura de înregistrare și este efectuată de către utilizatorii cu rolul și cu permisiunile corespunzătoare după autentificarea în SI RNC.

40. Procedura de radiere a datelor în SI RNC este un proces esențial pentru asigurarea securității SI RNC și pentru protejarea confidențialității informațiilor. În același timp, SI RNC va asigura istoricul datelor în scopuri statistice și științifice.

41. Procedura de interacțiune cu furnizorii de date are loc prin mecanisme tehnice în regim unilateral/bilateral, ținând cont de necesități, cum ar fi conexiunile și schimbul de informații cu bazele Sistemului informațional automatizat „Asistența medicală primară”, Sistemului informațional automatizat „Asistența medicală spitalicească”, Registrului de stat al populației etc.

Capitolul V

ÎNREGISTRAREA, MODIFICAREA COMPLETAREA ȘI RADIEREA DATELOR SI RNC

42. Înregistrarea datelor în SI RNC se efectuează de către utilizatorii cu rolul și cu permisiunile corespunzătoare, după autentificarea în SI RNC.

43. Înscrierile se efectuează în ordine cronologică, fiecărei înscrieri atribuindu-i-se data efectuării acesteia în SI RNC.

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

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

46. Orice modificare și/sau completare în SI RNC se efectuează doar în baza documentelor justificative, cu indicarea motivului ce confirmă veridicitatea acțiunilor efectuate în SI RNC.

47. La expirarea termenului de păstrare în SI RNC, datele se radiază din SI RNC, cu înregistrarea evenimentelor corespunzătoare și cu arhivarea ulterioară a acestora conform legislației.

Capitolul VI

CONTROLUL ȘI RĂSPUNDEREA

48. Ținerea SI RNC este supusă:

48.1. controlului intern care se efectuează de către Ministerul Sănătății, fiind posesorul SI RNC;

48.2. controlului extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea SI RNC, care se efectuează de către instituțiile abilitate și certificate în domeniul auditului.

49. SI RNC se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

50. Responsabilitatea privind organizarea și funcționarea SI RNC este atribuită posesorului SI RNC, care elaborează tipul și modelul documentelor corespunzătoare, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea SI RNC.

51. Toți subiecții SI RNC, precum și solicitantul informațiilor cu caracter personal poartă răspundere, conform legislației, pentru prelucrarea, divulgarea și transmiterea informației din SI RNC persoanelor terțe, contrar prevederilor legislației. Pentru încălcarea prezentului Regulament, persoanele vinovate poartă răspundere disciplinară, contravențională sau penală conform legislației.