***Proiect***

**GUVERNUL REPUBLICII MOLDOVA**

HOTĂRÎREnr.\_\_\_\_\_

din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2017

Chişinău

**privind aprobarea Regulamentului „Sistemului Informațional Medical Integrat”**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

În temeiul art. 22 pct. 1) și pct. 2) din Legea nr. 467–XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările și completările ulterioare, Guvernul,

 **HOTĂRĂŞTE:**

**1.** Se aprobă Regulamentul „Sistemului Informațional Medical Integrat” (se anexează);

**2.** Controlul asupra executării prezentei hotărîri se pune în sarcina Ministerului Sănătății.

**PRIM MINISTRU Pavel FILIP**

Contrasemnează:

Ministrul sănătăţii Ruxanda GLAVAN

 Ministrul tehnologiei informaţiei

 şi comunicaţiilor

Anexa

la Hotărîrea Guvernului

nr.\_\_\_\_\_\_\_din \_\_\_\_\_\_\_\_\_\_\_\_\_\_2017

 **REGULAMENTUL**

**”Sistemului Informaţional Medical Integrat”**

**I. Dispoziţii generale**

    1. Regulamentul cu privire la Sistemul Informaţional Medical Integrat (în continuare – S.I.M.I.) stabileşte modul de colectare (actualizare) şi analiză a datelor despre evenimentele ce au loc în sistemul de sănătate şi transformării lor în informaţii utilizate în procesul de luare a deciziilor privind profilaxia maladiilor, tratamentul şi reabilitarea pacienţilor, gestionarea eficientă a resurselor din instituţiile medico-sanitare publice şi private.

    2. S.I.M.I. este sistem integrat unic de evidenţă şi control automatizat al ocrotirii sănătăţii în Republica Moldova.

    3. S.I.M.I. este interconectat cu serviciul electronic guvernamental autentificare şi control al accesului (MPass), conform Hotărîrii Guvernului nr. 1090 din 31 decembrie 2013, cu Registrul de Stat al Populaţiei şi Compania Naţională de Asigurări în Medicină.

    4. S.I.M.I. este organizat astfel încît să asigure ca procesele de înregistrare şi acces să fie simple, eficiente, accesibile şi transparente.

    5. În sensul prezentului Regulament, noţiunile de bază utilizate semnifică:

*bază de date* – totalitatea datelor corelate, ce corespund anumitor reguli, care stabilesc principii generale de descriere, păstrare şi prelucrare a datelor;

*identificator* – cod artificial, creat sau generat după anumite reguli pentru fiecare categorie de obiecte, ce asigură identificarea unică şi stabilă a obiectului în decursul întregului ciclu de existenţă ca resursă informaţională;

*obiect informaţional* – reflectare virtuală de esenţe real existente, atît materiale, cît şi nemateriale;

*sistem informaţional automatizat* – totalitatea mijloacelor de program şi a echipamentelor destinate pentru prelucrarea informaţiei, resurselor informaţionale şi infrastructurii utilizatorului;

*securitate* – nivel necesar de integritate, selectivitate, accesibilitate şi eficienţă pentru protejarea datelor de pierderi, alterări, deteriorări şi de acces nesancţionat. Securitatea sistemului demonstrează faptul că sistemul este rezistent la atacuri, informaţia este confidenţială, integrală şi în stare de lucru, atît la nivel de sistem cît şi la nivel de date, prezentate în această informaţie;

*resursă informaţională* – totalitatea obiectelor informaţionale ce se referă la registrul dat, evenimentelor ce au loc cu obiectele informaţionale şi sînt reflectate în registru, precum şi atributele obiectelor informaţionale ce descriu starea lor la fiecare moment de timp concret.

    6. S.I.M.I. creează un spaţiu informaţional unitar şi constituie unica sursă oficială de informaţii privind funcţiile publice/posturile şi persoanele care le deţin pentru participanţii la S.I.M.I. şi pentru toate sistemele informaţionale ale autorităţilor publice care utilizează şi prelucrează astfel de tipuri de date.

    7. Regulamentul formulează sarcinile de bază ale S.I.M.I., stabileşte subiecţii raporturilor juridice în domeniul creării şi funcţionării acestuia, drepturile şi obligaţiile posesorului, deţinătorului şi ale participanţilor la S.I.M.I., obiectele informaţionale şi lista datelor incluse în acesta, procedurile de colectare şi gestiune a datelor, interoperabilitatea cu alte registre şi sisteme informaţionale, modalitatea de ţinere şi asigurare a funcţionării S.I.M.I., precum şi metodele de protecţie a datelor din acesta.

    8. Sarcinile de bază ale S.I.M.I. constau în formarea bazei de date (colectarea, introducerea şi stocarea datelor), actualizarea pe parcursul formării resursei informaţionale, exploatarea (procesarea, sistematizarea, generalizarea, furnizarea şi analiza datelor) şi asigurarea creării şi funcţionării bazei de date naţionale integrate distribuite în funcție de rolurile necesare din sistemul medical național.

**II. Subiecţii raporturilor juridice de ținere a S.I.M.I.**

    9. Proprietarul S.I.M.I. este statul, care îşi realizează dreptul de proprietate, de gestionare şi utilizare a datelor din prezentul Registru.

    10. Posesorul şi deţinătorul S.I.M.I. este Ministerul Sănătăţii.

    11. Registratori ai S.I.M.I. sînt:

    a) Ministerul Sănătăţii;

    b) Instituţiile medico-sanitare publice şi private de asistenţă medicală primară şi specializată de ambulator;

    c) Instituţiile mecido-sanitare publice şi private de asistenţă medicală spitalicească;

    d) medicii şi asistentele medicale din cadrul IMS respective, specificate la art.11 lit. b)-c);

    12. Furnizorii datelor S.I.M.I. sînt instituţiile medico-sanitare publice şi private de asistenţă medicală primară şi specializată de ambulator şi instituţiile medico-sanitare publice şi private de asistenţă medicală spitalicească.

    13. Destinatari ai datelor S.I.M.I. sînt: Guvernul RM, Ministerul Sănătăţii, Centrul Naţional de Management în Sănătate, Biroul Naţional de Statistică, Compania Naţională de Asigurări în Medicină, Direcţiile raionale şi municipale a Sănătăţii.

**III. Obligaţiile şi drepturile subiecţilor raporturilor juridice**

    14. În funcţie de rolurile atribuite, participanţii S.I.M.I. sînt obligaţi:

       a) să asigure colectarea, introducerea şi prelucrarea informaţiei relevante în baza de date a S.I.M.I., conform Manualului de utilizare pus la dispoziţia participanţilor S.I.M.I., precum şi în termenele coordonate cu posesorul acestuia;

       b) să asigure autenticitatea şi veridicitatea datelor colectate şi introduse în S.I.M.I.;

       c) să  asigure actualizarea datelor introduse în S.I.M.I.;

       d) la solicitarea deţinătorului SIMI, să întreprindă demersurile pentru introducerea în SIMI a altor componente necesare deținătorului;

       e) să asigure și să organizeze accesul autorizat al utilizatorilor SIMI în limitele nivelului de responsabilitate aferent funcției deținute în sistemul medical;

       f) să efectueze acţiunile de asigurare a securităţii informaţiei, să documenteze cazurile şi tentativele de încălcare a acesteia, precum şi să întreprindă măsurile ce se impun pentru prevenirea şi lichidarea consecinţelor;

       g) să asigure accesul securizat la informaţia conţinută în S.I.M.I., respectarea condiţiilor de securitate şi a regulilor de exploatare a acestuia;

      h) să ia măsurile organizatorice şi tehnice necesare pentru asigurarea regimului de confidenţialitate şi securitate a datelor cu caracter personal în conformitate cu instrucţiunile deţinătorului S.I.M.I.;

       i) să efectueze deservirea tehnică a locurilor de muncă conectate la S.I.M.I., să înlăture, în caz de necesitate, defecţiunile tehnice ale echipamentelor tehnice respective;

       j) să utilizeze informaţia obţinută din baza de date a S.I.M.I. doar în scopurile stabilite de legislaţia în vigoare;

       k) să raporteze imediat, în formă verbală şi scrisă, deţinătorului S.I.M.I. despre cazurile de încălcare a securităţii informaţionale a S.I.M.I. (incidentele de securitate);

      l) să aducă la cunoştinţa deţinătorului S.I.M.I., în termen de o zi, orice situaţie de forţă majoră (incidente aflate în afara ariei de competenţă a participantului) care ar putea influenţa în mod negativ exercitarea funcţiilor participantului;

 m) în cazul producerii incidentelor de securitate vor fi întreprinse măsurile necesare pentru depistarea sursei de producere a incidentului. Va fi efectuată analiza acestuia şi vor fi înlăturate cauzele incidentului de securitate cu informarea a autorităților abilitate.

    15. Fiecare participant are dreptul:

      a) să participe la implementarea şi dezvoltarea S.I.M.I.;

       b) să înainteze posesorului S.I.M.I. propuneri privind modificarea şi/sau completarea actelor legislative şi normative care reglementează funcţionarea S.I.M.I.;

       c) să solicite şi să primească de la deţinătorul S.I.M.I. ajutor metodologic şi practic privind funcţionarea acestuia;

      d) să prezinte propuneri deţinătorului S.I.M.I. privind perfecţionarea şi eficientizarea funcţionării acestuia.

**IV. Obligaţiile şi drepturile deţinătorului S.I.M.I.**

    16. Deţinătorul S.I.M.I. este obligat

       a) să asigure sprijinul tehnic si informativ pentru crearea conturilor de acces a utilizatorilor SIMI, cu atribuirea rolurilor şi drepturilor de acces corespunzătoare tipului de activitate;

      b) să efectueze operațiuni de monitorizare şi supraveghere a accesărilor informaţiei din S.I.M.I., să identifice încălcările comise şi să întocmească un raport privind datele accesate. În baza acestor rapoarte va participa alături de echipele tehnice la corectarea problemelor identificate;

      c) să asigure susţinerea metodologică şi practică prin elaborarea de proceduri, reguli şi instrucţiuni vizavi de introducerea, acumularea, păstrarea, completarea, corectarea, sistematizarea şi utilizarea datelor, precum şi de funcţionarea S.I.M.I.;

      d) să asigure funcţionarea şi ţinerea S.I.M.I. în conformitate cu cadrul normativ în vigoare;

      e) să asigure funcţionarea neîntreruptă a S.I.M.I.;

      f) să asigure integrarea cu alte sisteme informaţionale relevante;

      g) să dezvolte continuu S.I.M.I. prin identificarea, implementarea şi integrarea noilor componente și mecanisme de gestionare a datelor asociate domeniului medical;

      h) să acorde suportul necesar persoanelor autorizate, care au acces la S.I.M.I., privind utilizarea complexului de mijloace software aferente acestuia;

       i) să informeze participanţii la S.I.M.I. despre modificările condiţiilor tehnice de funcţionare a acestuia;

       j) să asigure implementarea măsurilor organizatorice şi tehnice necesare pentru asigurarea regimului de confidenţialitate şi securitate a datelor cu caracter personal în conformitate cu dispoziţiile Legii privind protecţia datelor cu caracter personal şi Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal aprobate de Guvern;

     k) să înregistreze și să verifice corespondența reală a următoarelor date din S.I.M.I.:

       -- datele generale despre instituţiile medicale;

       - numărul de identificare de stat (IDNO);

       - denumirea;

       - Cod fiscal;

       - Cod IMS;

       - tip;

       - numărul de telefon;

       - adresa poştală şi, opţional, cea electronică a persoanei juridice sau a întreprinzătorului individual.

       -- Planuri, Nomenclatoare şi formulare:

       - planuri de imunizări;

       - planuri de vaccinare;

       - programe de sănătate;

       - grupe de investigaţii;

       - grupe de diagnostic;

       - grupe de servicii;

       - grupurile de medicamente;

       - diverse nomenclatoare asociate;

       - formulare asociate;

     l) să asigure accesul securizat la  informaţia conţinută în S.I.M.I., respectarea condiţiilor de securitate şi regulilor de exploatare a acestuia;

     m) să utilizeze informaţia obţinută din baza de date a S.I.M.I. doar în  scopurile stabilite de legislaţia în vigoare.

     n) să examineze adresărilor primite referitoare la deficienţele tehnice ale S.I.M.I.;

     o) să asigure, în condiţiile legii, procesul de înregistrare în S.I.M.I. şi accesul la informaţiile înscrise în acesta.

     p) să efectueze auditul securităţii S.I.M.I. privind gestiunea datelor cu caracter personal;

      q) să genereze, copiile de rezervă a bazei de date a S.I.M.I. şi mijloacelor software folosite pentru prelucrările automatizate ale datelor din S.I.M.I. (copiile vor fi stocate pe suport tehnic păstrat în locuri protejate);

      r) să asigure restabilirea funcţionalităţii S.I.M.I., în caz de necesitate, în baza copiilor de rezervă generate în prealabil;

 s) să supravegheze respectarea cerinţelor de securitate informaţională de către participanţi, să documenteze şi să raporteze cazurile şi tentativele de încălcare a acestora (incidentele de securitate), să întreprindă măsurile necesare pentru prevenirea, limitarea şi lichidarea consecinţelor;

    17. Deţinătorul S.I.M.I. are dreptul:

       a) să dezvolte, în funcţie de competenţa sa, legislaţia cu privire la S.I.M.I.;

       b) să propună soluţii pentru perfecţionarea şi eficientizarea procesului de funcţionare a S.I.M.I., precum şi să le pună în aplicare;

       c) să supravegheze respectarea cerinţelor de securitate a informaţiei de către participanţii la S.I.M.I., să fixeze cazurile şi tentativele de încălcare a acestora;

       d) să iniţieze procedura de suspendare a drepturilor de acces la S.I.M.I. pentru utilizatorii care nu respectă regulile, standardele şi normele general acceptate în domeniul securităţii informaţionale;

      e) să verifice autenticitatea şi veridicitatea datelor introduse de participanţii la S.I.M.I.;

       f) să solicite de la participanţi actualizarea sau corectarea datelor din baza de date a S.I.M.I. în caz de depistare a omiterilor şi erorilor.

**V. Obiectele informaţionale şi datele de stocare în S.I.M.I.**

    18. Totalitatea obiectelor informaţionale, care reprezintă resursa informaţională a S.I.M.I., este determinată de destinaţia lui şi include următoarele obiecte:

    1) persoanele fizice:

       colaboratori medicali;

       pacienţi;

    2) instituţiile medicale:

       spitale;

       centre ale medicilor de familie, ambulatorii;

       întreprinderi şi instituţii farmaceutice;

       alte instituții medicale de interes pentru S.I.M.I, ex. laboratoare, centre de recuperare şi dispensare etc;

    3) medicamentele;

    4) serviciile medicale;

    5) documentele:

       certificatul medical constatator al naşterii;

       fişa medicală personală;

       fişa gravidei;

       fişa copilului;

       fişa de imunizări;

       poliţa de asigurare;

       certificatul concediului de boală;

       certificatul medical de deces;

    19. Atributele obiectului informaţional „persoană fizică – pacient” sînt:

     1) date de identificare:

       a) numărul de identificare de stat (IDNP);

       b) numele, prenumele şi patronimicul;

       c) sex;

       d) data naşterii;

       e) grupa sangvină;

     2) date demografice:

       a) cetăţenie;

       b) tip document de identificare;

       c) nr. document;

       d) data cînd a fost emis şi data cînd expiră documentul;

     3) adresa de reşedinţă permanentă şi temporară:

       a) localitatea;

       b) strada;

       c) bloc;

       d) apartament;

     4) date privind asigurarea medicală:

       a) categoria asigurat;

       b) statut asigurat;

       c) asigurator;

       d) tip asigurare;

     5) date socio-economice:

       a) locul de muncă/studii;

     6) date specifice despre sănătate:

       a) date despre evidenţă;

       b) date despre triaj;

       c) date despre consultaţii şi examene medicale;

       d) date despre diagnostice;

       e) date despre examene de laborator;

       f) date despre efectele adverse şi complicaţiile la tratament;

       g) date despre programele de sănătate;

     7) date administrative specifice despre pacienţii spitalizaţi:

       a) date despre prezentarea şi înregistrare;

       b) date despre internare;

       c) date despre mişcarea intraspitalicească;

       d) date despre externare;

    20. Atributele obiectului informaţional „persoană fizică – colaborator medical” sînt:

     1) date de identificare:

       a) numărul de identificare unic;

       b) numărul de identificare de stat (IDNP);

       c) numele;

       d) prenumele;

       e) patronimic;

       f) sex;

       g) data naşterii;

       h) grupa sangvină;

     2) date demografice:

       a) cetăţenie;

       b) tip document de identificare;

       c) nr. document;

     3) adresa de reşedinţă permanentă şi temporară:

       a) localitatea;

       b) strada;

       c) bloc;

      d) apartament;

       e) număr de telefon fix/fax;

       f) număr de telefon mobil;

     4) date privind asigurarea medicală:

       a) categoria asigurat;

       b) statut asigurat;

       c) asigurator;

       d) tip asigurare;

     5) date socio-economice:

       a) locul de muncă/studii;

    21. Atributele obiectului informaţional „instituţiile medicale - centre ale medicilor de familie, ambulatorii şi spitale” sînt:

       a) numărul de identificare de stat (IDNO);

       b) denumirea;

       c) Cod fiscal;

       d) Cod IMS;

       e) tip;

       f) numărul de telefon;

       g) adresa poştală;

 e) electronică a persoanei juridice sau a întreprinzătorului individual.

    22. Atributele obiectului informaţional „medicamente” sînt:

       a) id-ul medicamentului (Nomenclator);

       b) unitatea de măsură;

       c) cantitatea în unitățile indicate;

       d) prețul unei unități minime fără TVA;

       e) prețul total;

       f) data producerii medicamentului dat;

       g) data expirării medicamentului;

       h) stocul/factură din care a fost creat acest stoc gestionat;

       i) unitatea minimă de distribuție;

       j) numărul de unități de măsură din acest stoc;

       k) codul medicamentului din nomenclator;

       l) numele medicamentului;

       m) substanța activă a medicamentului;

       n) unitatea elementară a medicamentului;

       o) numărul sub care a fost înregistrat acest medicament;

       p) forma farmaceutică;

       q) compania producătoare a acestui medicament;

       r) dacă e nevoie sau nu de rețetă pentru eliberare;

       s) dacă este sau nu substanță activă;

    23. Atributele obiectului informaţional „servicii medicale” sînt:

       a) cod serviciu medical;

       b) cod instituţiei medico-sanitare;

       c) numărul de identificare unic al colaboratorului medical;

    24. Atributele obiectului informaţional „documente” sînt determinate de elementele formularelor aprobate de către instituţiile abilitate.

**VI. Interoperabilitatea cu alte sisteme informaţionale**

    25. Pentru asigurarea actualizării operative şi automate a conţinutului informaţional al S.I.M.I. cu informaţie veridică, se realizează interacţiunea şi sincronizarea datelor cu următoarele sisteme informaţionale automatizate:

    a) Sistemului Informaţional Automatizat ”Registrul de stat al populaţiei”, care acordă acces la datele despre persoanele fizice, adresa de domiciliu şi documentele eliberate acestora;

    b) Sistemul Informaţional Automatizat ”Asigurarea Obligatorie de Asistenţă Medicală”, deținut de Compania Naţională de Asigurări în Medicină, care acordă acces la datele despre asigurarea medicală.

**VII. Modalitatea de ţinere și accesul la S.I.M.I.**

    26. S.I.M.I. este ţinut electronic în limba de stat.

    27. Principalele proceduri de ţinere a S.I.M.I. includ introducerea iniţială, actualizarea, excluderea, păstrarea în arhivă şi utilizarea datelor în modul stabilit.

    28. Introducerea iniţială a datelor în S.I.M.I. are loc în următoarele cazuri:

    A. persoana fizică

       pentru colaborator medical - la prima angajare în instituţia medicală;

       pentru pacient - la adresarea iniţială în instituţia medicală;

    B. Instituţia medicală

       Luarea iniţială în evidenţă a unităţii de drept are loc la momentul creării acesteia.

    C. Medicamentele

       Punerea iniţială în evidenţă a medicamentelor se efectuează la momentul livrării acestora de către furnizor.

    D. Serviciul medical

       Evidenţa serviciului medical se efectuează la prestarea acestuia de către instituţiile medicale.

    E. Documentul

       Punerea iniţială în evidenţă are loc la întocmire.

    29. Actualizarea datelor S.I.M.I. constă în introducerea sistematică a modificărilor (rectificărilor şi completărilor) după cum urmează:

    A. persoana fizică

       înregistrarea decesului persoanei fizice;

       schimbarea domiciliului;

       schimbarea datelor personale de identificare;

       schimbul informaţional interdepartamental.

    B. Instituţia medicală

       reorganizare  (fuziune, alipire, separare, divizare, transformare) a unităţii de drept;

       schimbare a denumirii;

       schimbare a adresei juridice;

       documentare cu toate tipurile de documente (de înregistrare, licenţe etc.);

       schimbare a formei de proprietate;

       schimbare a conducătorilor;

       schimbare a tipului de activitate;

       înregistrare a filialelor sau reprezentanţelor;

       schimbul informaţional interdepartamental.

    C. Medicamentele

       Actualizarea datelor are loc la modificarea datelor medicamentelor.

    D. Documentul

       la declararea nulă a documentului;

       la schimbarea termenului de valabilitate.

    30. Arhivarea datelor din S.I.M.I. are loc în următoarele cazuri:

    1) persoana fizică - pacient

 a) la plecarea definitivă din ţară;

       b) în cazul decesului persoanei fizice;

2) persoana fizică – colaborator medical

 a) la încetarea activităţii medicale;

    3) Instituţia medicală

       drept rezultat al lichidării unităţii de drept.

    4) Medicamentele

       la încetarea producerii;

       la interzicerea importării în ţară.

    5) Documentul

       la expirarea termenului;

       în caz de nimicire.

    31. Termenele de păstrare a datelor în sistem sînt identice cu termenele de păstrare a documentelor pe suport de hîrtie stabilite de legislaţia în vigoare.

    32. Evidenţa obiectelor informaţionale se ţine conform Manualului de utilizare a S.I.M.I., care conţine instrucţiuni privind introducerea, modificarea şi vizualizarea datelor în baza de date, elaborat în cadrul procesului de dezvoltare a S.I.M.I. şi pus la dispoziţia participanţilor la S.I.M.I. prin intermediul sistemului informaţional în cauză.

    33. La prelucrarea informaţiei, utilizatorii S.I.M.I. au obligaţia asigurării protecţiei datelor cu caracter personal conform Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

    34. În caz de pierdere, nimicire sau deteriorare a datelor S.I.M.I. acestea urmează a fi restabilite, despre care fapt se va face menţiunea respectivă.

    35. Toate modificările operate în S.I.M.I. se păstrează în ordine cronologică.

    36. Accesul la resursele S.I.M.I. este asigurat şi autorizat prin intermediul sistemului certificatelor electronice a cheilor publice. La începutul sesiunii de lucru fiecare utilizator trece procedura de  autentificare în sistem, prin care se verifică corectitudinea identificatorului atribuit utilizatorului dat. În caz de neconfirmare a autenticităţii utilizatorului, conectarea la S.I.M.I. nu se permite.

    37. Răspunderea pentru veridicitatea şi corectitudinea datelor şi informaţiilor raportate, precum şi pentru respectarea termenelor de raportare revine registratorilor S.I.M.I..

    38. Pentru asigurarea funcţionării eficiente şi neîntrerupte a S.I.M.I., schimbul informaţional de date dintre participanţii la S.I.M.I. şi baza  de date este asigurat în regim nonstop.

    39. Schimbul informaţional se efectuează cu utilizarea complexului de mijloace software şi hardware specializat, prin intermediul sistemului de telecomunicaţii al autorităţilor publice.

    40. Funcţionarea S.I.M.I. este suspendată de către administratorul central de sistem sau de către administratorul tehnic al S.I.M.I. în următoarele cazuri:

       a) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software şi hardware al S.I.M.I.;

       b) la apariţia circumstanţelor de forţă majoră;

       c) la încălcarea cerinţelor sistemului securităţii informaţiei, dacă aceasta prezintă pericol pentru funcţionarea S.I.M.I.;

       d) în cazul apariţiei dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware al S.I.M.I.;

       e) la cererea posesorului sau a deţinătorului S.I.M.I..

    41. Lucrările profilactice în complexul de mijloace software şi hardware se efectuează după notificarea în scris sau prin e-mail a participanţilor la S.I.M.I. cu cel puţin 2 zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil.

    42. În cazul apariţiei circumstanţelor de forţă majoră, precum şi a dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware al S.I.M.I., din vina terţelor persoane, este posibilă suspendarea funcţionării S.I.M.I., cu informarea ulterioară prin telefon, e-mail sau în  scris a participanţilor la S.I.M.I. conectaţi.

    43. Revocarea dreptului de acces la S.I.M.I. pentru utilizatorii participanţilor la S.I.M.I. se efectuează în una dintre următoarele situaţii:

       a) în temeiul cererii (demersului) conducătorului acestuia;

       b) la încetarea raporturilor de serviciu/ de muncă ale utilizatorului;

       c) la intervenirea modificărilor raporturilor de serviciu/de muncă cînd noile atribuţii nu impun accesul la datele din S.I.M.I.;

       d) la constatarea încălcării de către utilizatorul participantului la S.I.M.I. a sistemului securităţii informaţionale a S.I.M.I..

    44. Lucrările necesare de deconectare a mijloacelor software de la locul de muncă al participantului la S.I.M.I. sistat se execută în termenul coordonat cu respectivul participant.

**VIII. Securitatea şi integritatea informaţiei din S.I.M.I.**

    45. Pentru asigurarea funcţionării eficiente şi neîntrerupte a S.I.M.I., accesul la date este asigurat continuu.

    46. Schimbul informaţional se efectuează numai cu utilizarea complexului de mijloace software şi hardware specializat.

    47. Măsurile de protecţie şi securitate a informaţiei din S.I.M.I. reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a S.I.M.I..

    48. Protecţia informaţiei din S.I.M.I. se efectuează în felul următor:

    a) prevenirea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor din S.I.M.I. transmise prin aceste reţele;

    b) excluderea accesului neautorizat la datele din S.I.M.I., asigurată prin folosirea mijloacelor speciale tehnice şi de program;

    c) prevenirea distrugerii, modificării datelor sau a defecţiunilor în funcţionarea complexului tehnic şi de program, prin folosirea mijloacelor de protecţie speciale, inclusiv a programelor antivirus prin organizarea sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă;

    d) prevenirea acţiunilor intenţionate şi/sau neintenţionate ale utilizatorilor, care pot conduce la distrugerea sau modificarea datelor din S.I.M.I..

    49. Asigurarea securității și integrității informației din S.I.M.I. este condiționată de Standardele internaționale SM ISO/CEI 27001:2014 „Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe” și SM ISO/CEI 27002:2014 „Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei”.

    50. Copiile de siguranţă ale bazei de date (backup) vor fi efectuate zilnic, conform graficului, începînd cu ora 00:00. Mentenanța și profilaxia echipamentelor se va realiza de două ori pe an şi în caz de necesitate.

    51. În procesul de ţinere a S.I.M.I. se va asigura securitatea datelor cu caracter personal, în conformitate cu Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, cu Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal” în conformitate cu Politica de securitate a datelor cu caracter personal în cadrul Ministerului Sănătăţii, aprobată prin Ordinul Ministerului Sănătăţii nr.797 din 17 octombrie 2016.

**IX. Controlul și responsabilitatea**

    52. Persoanele responsabile de ţinerea S.I.M.I. și registratorii sînt obligate să prevină accesul nesancţionat la datele din S.I.M.I., utilizarea ilegală, difuzarea, modificarea sau nimicirea lor.

    53. Pentru deteriorarea, falsificarea, nimicirea şi alte acţiuni ilegale întreprinse asupra informaţiei ce se conţine în S.I.M.I., persoana responsabilă poartă răspundere în conformitate cu legislaţia.

    54. Controlul intern asupra modului de ținere a S.I.M.I. se efectuează de către Ministerul Sănătăţii. Controlul extern asupra modului de ținere a S.I.M.I. se efectuează de către autoritatea administraţiei publice abilitată prin lege.

    55. Răspunderea pentru corectitudinea şi veridicitatea informaţiilor din bazele de date existente pînă la crearea S.I.M.I., care au devenit parte componentă a bazei de date a S.I.M.I., o poartă deţinătorii precedenți ai acestor baze de date.