Republica Moldova

GUVERNUL

HOTĂRÂRE Nr. HG885/2022
din 14.12.2022

cu privire la instituirea Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică

Publicat : 01.02.2023 în MONITORUL OFICIAL Nr. 25-27 art. 58 Data intrării în vigoare

MODIFICAT

HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25

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, Guvernul HOTĂRĂȘTE:

1. Se instituie Sistemul informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică.

2. Se aprobă:

1) Conceptul Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică, conform anexei nr. 1;

2) Regulamentul privind organizarea și funcționarea Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică, conform anexei nr. 2.

2^{1}. Se lichidează Registrul electronic de evidență a vaccinării împotriva COVID-19 și se instituie Registrul electronic național de vaccinuri în baza acestuia.

[Pct.2^{1} introdus prin HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

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:

1) pe tot parcursul textului, textul „SIA RVC-19” se substituie cu textul „SI SBTESP”;

2) la punctul 3, subpunctul 7) va avea următorul cuprins:

„7) Sistemul informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică”;

3) punctul 15 se completează cu subpunctul 7) cu următorul cuprins:

„7) fișa de anchetare epidemiologică a focarului de boală infecțioasă”.

4. Finanțarea Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică va fi asigurată din contul și în limitele mijloacelor aprobate anual Ministerului Sănătății, precum și din alte surse, conform legislației.

PRIM-MINISTRU Natalia GAVRILIȚA

Contrasemnează:

Ministrul sănătății Ala Nemerenco

Nr. 885. Chişinău, 14 decembrie 2022.

Anexa nr. 1

la Hotărârea Guvernului nr. 885/2022

CONCEPTUL

Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică

Capitolul I

INTRODUCERE

Supravegherea bolilor transmisibile și a evenimentelor de sănătate publică reprezintă un domeniu prioritar în supravegherea de stat a sănătății publice, așa cum este specificat în art. 5 din Legea nr. 10/2009 privind supravegherea de stat a sănătății publice. Prestatorii de servicii medicale, indiferent de tipul de proprietate și de forma de organizare juridică, sunt obligați să asigure o evidență separată a bolnavilor cu boli transmisibile și, în cazul depistării acestora, să notifice Agenția Națională pentru Sănătate Publică (în continuare – *ANSP*), prin raportarea acestora în decurs de 12 ore în Sistemul informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică (în continuare – *SI SBTESP*).

În acest sens, în Republica Moldova a fost elaborat și implementat sistemul național de supraveghere epidemiologică și control al bolilor transmisibile și evenimentelor de

sănătate publică, în baza Regulamentului aprobat prin Hotărârea Guvernului nr. 951/2013, care este gestionat de Ministerul Sănătății prin intermediul Agenției Naționale pentru Sănătate Publică.

Totodată, menționăm că la momentul actual Agenția Națională pentru Sănătate Publică nu dispune de un sistem informațional de colectare a datelor cu privire la înregistrarea cazurilor de boli transmisibile, iar metodele utilizate de aceasta au multiple deficiențe atât la nivel fizic, cât și operațional. Tehnologiile aplicate sunt depășite de timp, nu oferă funcționalități necesare în conformitate cu cadrul legal în domeniul supravegherii de stat în sănătate publică și nu sunt aliniate la cerințele actuale ale sistemelor informaționale naționale. Necesitatea stringentă pentru instituirea unui sistem informațional cu funcționalități noi a fost reconfirmată în contextul pandemiei de COVID-19 pentru monitorizarea situației epidemiologice și pentru coordonarea eficientă a răspunsului la nivel național și teritorial.

De menționat că domeniul de supraveghere a bolilor transmisibile este relevant și în contextul angajamentelor externe asumate de către Republica Moldova în conformitate cu articolul 114, capitolul 21 din Acordul de asociere între Republica Moldova, pe de o parte, şi Uniunea Europeană şi Comunitatea Europeană a Energiei Atomice şi statele membre ale acestora, pe de altă parte, ce se referă la cooperarea în domeniul privind supravegherea epidemiologică și controlul bolilor transmisibile, precum și la sporirea capacității de pregătire pentru amenințări și urgențe la adresa sănătății publice.

[Capitolul I modificat prin HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

Capitolul II

GENERALITĂȚI

1. Sistemul informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică (în continuare – *SI SBTESP*) reprezintă un sistem informațional constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, și este destinat să asigure înregistrarea, păstrarea, prelucrarea și utilizarea informațiilor cu privire la cazurile de boli infecțioase și evenimentele de sănătate publică, inclusiv intoxicații, toxiinfecții alimentare și boli profesionale acute.

2. SI SBTESP asigură digitalizarea proceselor de colectare, analiză, interpretare şi diseminare sistematică şi continuă a datelor despre sănătate cu privire la bolile transmisibile şi evenimentele de sănătate publică, în contextul răspândirii lor în timp, spațiu, grup de populație şi al analizei factorilor de risc de contractare a acestor boli, inclusiv în cadrul studiilor epidemiologice. Scopul general al SI SBTESP constă în îmbunătățirea procesului de evidență, de gestiune și de raportare a cazurilor cu privire la bolile transmisibile și evenimentele de sănătate publică.

3. SI SBTESP are următoarele obiective:

1) digitizarea, automatizarea și eficientizarea proceselor direcționate spre

îmbunătățirea prevenirii și controlului bolilor transmisibile și evenimentelor de sănătate publică;

2) dezvoltarea capacităților de evidență, gestionare, analiză și reacționare la evenimentele cu impact negativ asupra sănătății publice, supravegherea evenimentelor de sănătate publică, inclusiv prin implementarea sistemului de alertă precoce și răspuns rapid;

3) îmbunătățirea activității sistemului sănătății în contextul gestionării cazurilor de boli transmisibile şi evenimente de sănătate publică.

4. Datele din SI SBTESP pot fi prezentate autorităților administrației publice, persoanelor fizice și unităților de drept în modul stabilit de legislație.

5. Noțiunile principale utilizate în sensul prezentului Concept utilizează termenii definiți în Legea nr. 467/2003 cu privire la informatizare şi la resursele informaționale de stat şi în Legea nr. 71/2007 cu privire la registre, precum şi în Regulamentul privind sistemul național de supraveghere epidemiologică şi control al bolilor transmisibile şi evenimentelor de sănătate publică, aprobat prin Hotărârea Guvernului nr. 951/2013 și Hotărârea Guvernului nr. 30/2024 cu privire la sistemul de alertă precoce și răspuns rapid, instituit în legătură cu amenințările transfrontaliere grave pentru sănătate, la procedurile de notificare a alertelor și la procedurile de schimb de informații, consultare și coordonare a răspunsurilor la astfel de amenințări.

[Pct.5 modificat prin HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

6. Principiile de bază ale SI SBTESP sunt:

1) principiul legitimității – funcțiile și operațiile efectuate de utilizatori sunt legale și conforme cu drepturile omului și cu legislația națională;

2) principiul autenticității datelor – informațiile păstrate pe dispozitive de stocare a datelor sau pe suport de hârtie corespund stării reale a obiectelor;

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

4) principiul temeiniciei datelor – introducerea datelor în SI SBTESP se efectuează doar în baza înscrierilor din documentele acceptate ca surse de informații;

5) principiul auditului – înregistrarea informației despre schimbările care au loc, pentru a face posibilă reconstituirea istoriei unui set de date sau starea acestuia într-o etapă anterioară;

6) principiul independenței de platforma software – SI SBTESP poate fi construit pe baza modulelor elaborate la comandă (custom) sau a produselor software existente (COTS). Conceptul nu limitează în niciun fel abordarea dezvoltării SI SBTESP atât timp cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit;

7) principiul accesibilității și integrabilității – SI SBTESP, chiar dacă oferă funcționalități multiple, este construit ca un element integral și folosit de utilizatori prin intermediul interfețelor de acces definite;

8) principiul confidențialității informației – răspunderea personală în conformitate cu legislația a colaboratorilor responsabili de prelucrarea informației în SI SBTESP pentru utilizarea și difuzarea neautorizată a informației;

9) principiul compatibilității – SI SBTESP trebuie să fie compatibil cu sistemele existente moderne;

10) principiul orientării spre utilizator – structura, conținutul, mijloacele de acces și navigarea sunt focalizate pe utilizatori;

11) principiul extensibilității – componentele SI SBTESP oferă facilități de ajustare și extindere a funcționalităților existente pentru conformare cu necesitățile în continuă schimbare ale autorităților din domeniul sănătății;

12) principiul dezvoltării progresive – elaborarea SI SBTESP și modificarea permanentă a componentelor sale se efectuează în conformitate cu tehnologiile informaționale avansate;

13) principiul consecutivității – elaborarea și implementarea proiectului pe etape;

14) principiul eficienței funcționării – optimizarea raportului dintre calitate și cost;

15) principiul utilizării standardelor deschise – asigură atât interoperabilitatea cu sistemele externe, cât și păstrarea informației, în conformitate cu normele;

16) principiul securității informaționale – asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea SI SBTESP presupune rezistența la atacuri și protecția caracterului secret, a integrității și a pregătirii pentru lucru atât a SI SBTESP, cât și a datelor acestuia.

7. Sarcinile de bază realizate la exploatarea SI SBTESP sunt:

1) eficientizarea proceselor de gestiune și evidență a cazurilor de boli transmisibile și evenimentelor de sănătate publică;

2) automatizarea și digitizarea proceselor de gestiune și evidență a cazurilor de boli transmisibile și evenimentelor de sănătate publică;

3) crearea și dezvoltarea sursei informaționale de evidență și gestiune a cazurilor de boli infecțioase, de intoxicație, de toxiinfecție alimentară și profesională acută, a evenimentelor de sănătate publică, a investigațiilor de laborator, precum și a altor informații relevante, în vederea stocării, sistematizării, actualizării și asigurării unui nivel adecvat de protecție a datelor cu caracter personal;

4) standardizarea procedurilor, a formularelor și a nomenclatoarelor;

5) colectarea și procesarea informației privind determinanții stării de sănătate;

6) integrarea laboratoarelor, inclusiv din domeniul de sănătate publică în sistemul informațional comun;

7) monitorizarea apariției cazurilor noi sau a reapariției cazurilor de boli transmisibile supuse înregistrării şi notificării în sistemul de supraveghere epidemiologică, precum și a cazurilor de boli transmisibile de origine necunoscută;

8) monitorizarea evoluției unei situații epidemiologice provocate de boli transmisibile;

9) excluderea treptată a gestionării datelor pe suport de hârtie, prin utilizarea informațiilor și a documentelor electronice;

10) comunicarea rapidă între entitățile SI SBTESP, cu utilizarea mijloacelor electronice;

11) utilizarea potențialului tehnologiilor electronice contemporane la colectarea și procesarea datelor;

12) sporirea gradului de pregătire și de utilizare a tehnologiilor informaționale al personalului sistemului de sănătate;

13) dezvoltarea și acordarea serviciilor electronice cetățenilor, inclusiv prin depunerea solicitărilor în regim online;

14) asigurarea interoperabilității cu alte sisteme informaționale pentru livrarea și consumul de informații;

15) securizarea informațiilor cu accesibilitate limitată, prin implementarea unei politici de acces în sistem pentru fiecare entitate/utilizator în parte, în funcție de competențele specifice;

16) excluderea posibilităților de manipulare a datelor din SI SBTESP;

17) excluderea posibilităților de intervenție neautorizată asupra datelor din SI SBTESP;

18) excluderea posibilității modificării sau ștergerii istoricului datelor de jurnalizare a SI SBTESP.

8. Componentele ce formează SI SBTESP sunt următoarele:

1) Sistemul informațional de notificare a cazurilor de boli și a evenimentelor de sănătate publică – soluție informatică performantă pentru crearea și administrarea notificărilor despre cazurile de boli transmisibile, intoxicații acute neprofesionale exogene de etiologie chimică și evenimentele de sănătate publică. Aceasta presupune automatizarea procesului de înregistrare și gestiune a notificărilor și a informațiilor relevante, cum ar fi diagnosticul primar; diagnosticul final; simptomele/manifestările bolii; concluziile din anchetarea epidemiologică; încheierea cercetării cazului de intoxicație acută neprofesională

exogenă de etiologie chimică, cu emiterea procesului-verbal; rezultatele investigațiilor de laborator; informațiile cu privire la vaccinare și evidența administrării vaccinurilor; precum și evidența și diseminarea informațiilor cu privire la investigarea evenimentelor de sănătate publică;

[Pct.8 subpct.1) în redacția HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

2) Registrul electronic național de vaccinuri (în continuare – *RENV*) – registru electronic ce asigură înregistrarea setului de date necesare pentru evidența persoanelor vaccinate conform Programului național de imunizări din prima zi de viață cu vaccinurile de rutină și vaccinurile administrate la indicații epidemiologice. Acesta conține informații despre persoanele imunizate, vaccinurile administrate, programarea și planificarea vaccinării, precum și evidența stocurilor de vaccinuri și consumabile;

[Pct.8 subpct.2) în redacția HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

3) Sistemul informatic de laborator – sistem informatic pentru prelucrarea și stocarea informațiilor privind investigațiile și testele de laborator. Scopul acestuia constă în eficientizarea proceselor de înregistrare, prelucrare, evidență și expediere a informațiilor cu privire la investigațiile de laborator și a rezultatelor acestora. Sistemul informatic de laborator presupune gestiunea întregului ciclu de viață al unei solicitări/necesități de investigații în trei etape:

a) *preanalitic* – recepționarea înregistrărilor; prelevarea probelor; managementul solicitărilor;

b) *analitic* – generarea sarcinilor de investigații (work list); controlul și monitorizarea sarcinilor; interacțiunea cu echipamentul de laborator care realizează investigația; managementul calității; gestiunea alertei;

c) *postanalitic* – validarea clinică și tehnică a rezultatelor; emiterea rezultatelor/rapoartelor; notificarea pacienților și instituțiilor medicale prin diverse mijloace electronice; arhivarea;

4) Soluția informatică pentru monitorizarea incidenței unei boli transmisibile, a persoanelor supuse regimului de autoizolare, a contacților și a trasabilității cazurilor de boli transmisibile în cadrul evenimentelor de sănătate publică. Soluția asigură posibilitatea de configurare a monitorizării incidenței unei boli cunoscute sau necunoscute, precum și investigarea și înregistrarea datelor în legătură cu cazurile depistate, cu contactele și cu evenimentele. Monitorizarea prevede gestionarea cazului confirmat de boală sau a unei persoane aflate în regim de autoizolare și colectarea datelor referitoare la statutul de boală și la starea de sănătate a persoanelor. Aceasta presupune automatizarea procesului de contactare, cu completarea șabloanelor standard privind statutul cazului și a informațiilor privind evoluția bolii.

Capitolul III

SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII

SI SBTESP

9. Cadrul juridic al SI SBTESP include legislația națională, acordurile și convențiile internaționale la care Republica Moldova este parte, precum și actele normative ce reglementează sistemul de sănătate.

10. Crearea și funcționarea SI SBTESP este reglementată, în particular, de următoarele acte normative:

1) Constituția Republicii Moldova;

2) Legea ocrotirii sănătății nr. 411/1995;

3) Legea nr. 982/2000 privind accesul la informație;

4) Legea nr. 1069/2000 cu privire la informatică;

5) Legea nr. 467/2003 cu privire la informatizare şi la resursele informaționale de stat;

6) Legea nr. 71/2007 cu privire la registre;

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

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

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

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

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

12) Hotărârea Guvernului nr. 1128/2004 cu privire la aprobarea Concepției sistemului informațional medical integrat;

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

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;

15) Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind cadrul de interoperabilitate;

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

17) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de

jurnalizare (MLog);

18) Hotărârea Guvernului nr. 717/2014 privind platforma de dezvoltare a serviciilor electronice (PDSE);

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

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

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

22) Hotărârea Guvernului nr. 1090/2017 cu privire la organizarea și funcționarea Agenției Naționale pentru Sănătate Publică;

23) 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;

24) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

25) Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);

26) Hotărârea Guvernului nr. 375/2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;

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);

28) Hotărârea Guvernului nr. 152/2021 cu privire la aprobarea Conceptului serviciului guvernamental de livrare (MDelivery);

29) Ordinul ministrului sănătății nr. 190/2003 cu privire la instituirea structurii sistemului sănătății raionale/municipale, ce prevede structura și responsabilitățile secțiilor de informatică și statistică medicală din cadrul instituțiilor medicale publice;

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

31) Ordinul ministrului sănătății nr. 47/2016 cu privire la aprobarea Nomenclatorului prestatorilor privați de servicii de sănătate;

32) Ordinul ministrului sănătății nr. 1086/2016 cu privire la aprobarea regulamentelor-cadru de organizare și funcționare ale prestatorilor de servicii de sănătate;

33) Ordinul ministrului sănătății nr. 1087/721/2016 despre aprobarea Regulamentului privind înregistrarea persoanei la medicul de familie din instituția medico-sanitară ce prestează asistență medicală primară în cadrul asigurării obligatorii de asistență medical;

34) Ordinul ministrului sănătății nr. 1080/2017 cu privire la aprobarea Nomenclatorului Instituțiilor medico-sanitare publice de asistență medicală primară la nivel de raion;

35) Ordinul ministrului sănătății cu privire la întocmirea și prezentarea dărilor de seamă statistice medicale anuale de către instituțiile medico-sanitare, actualizat anual.

Capitolul IV

SPAȚIUL FUNCȚIONAL AL SI SBTESP

Secțiunea 1

Funcțiile de bază ale SI SBTESP

11. Funcțiile de bază ale SI SBTESP sunt:

1) formarea bazei de date a SI SBTESP ce reflectă notificările înregistrate cu privire la cazurile de boli transmisibile și evenimente de sănătate publică, cărora li se atribuie un număr de identificare, precum și informațiile cu privire la gestiunea acestora pe întreg ciclul de viață. Funcțiile de bază la formarea bazei de date sunt înregistrarea și actualizarea datelor și radierea obiectelor informaționale:

a) înregistrarea, notificarea și luarea în evidență primară în baza formularelor aprobate de Ministerul Sănătății. Constă în atribuirea numărului de identificare unic obiectului de evidență și în introducerea volumului stabilit de date în baza de date;

b) actualizarea datelor. Constă în actualizarea sistematică a bazei de date, în modificarea sau completarea datelor obiectelor informaționale;

c) scoaterea din evidență/arhivarea. Reprezintă schimbarea statutului obiectului informațional, și nu excluderea fizică a datelor despre obiect;

2) formarea bazei de date ce reflectă înregistrările cu privire la solicitările investigațiilor/analizelor de laborator. Constă în introducerea și actualizarea datelor și informațiilor ca urmare a efectuării proceselor de laborator:

a) înregistrarea și evidența solicitărilor investigațiilor/analizelor de laborator;

b) gestiunea probelor și a rezultatelor acestora;

c) crearea și gestionarea catalogului centralizat al investigațiilor de laborator;

d) asigurarea trasabilității, istoricului și corelării investigațiilor de laborator;

e) raportarea și interpretarea rezultatelor de laborator;

f) controlul și managementul proceselor;

3) formarea bazei de date ce reflectă înregistrările cu privire la procesul de vaccinare:

a) evidența și gestiunea informațiilor cu privire la vaccin;

b) evidența și gestiunea procesului de vaccinare;

c) generarea, descărcarea și imprimarea certificatului de vaccinare;

d) programarea pentru vaccinare;

e) evidența reacțiilor adverse la administrarea preparatelor imunobiologice;

4) formarea bazei de date ce permite monitorizarea contacților (*contact tracing*) pentru a întrerupe lanțurile de transmitere și prevenirea transmiterii ulterioare a maladiei:

a) investigarea focarelor și evenimentelor de sănătate publică generate de SI SBTESP;

b) monitorizare inteligentă a contacților;

c) identificarea relațiilor dintre înregistrările individuale cu focarele/evenimentele existente;

d) vizualizarea cazurilor și a contacților în regim de tablou de bord;

e) vizualizarea lanțurilor de transmitere;

f) generarea rapoartelor;

5) asigurarea informațională. Informația din SI SBTESP este accesibilă autorităților din domeniul sănătății, altor autorități publice, furnizorilor/destinatarilor/utilizatorilor de date, precum și participanților la SI SBTESP. Nivelul de acces la SI SBTESP este stabilit prin regulament și prin prevederile legislației;

6) administrarea informațională ce include următoarele acțiuni:

a) administrarea rolurilor și drepturilor utilizatorilor – gestionarea utilizatorilor SI SBTESP, individual pentru fiecare componentă, desfășurată conform regulamentului de organizare și funcționare;

b) administrarea nomenclatoarelor;

c) administrarea modelelor de documente;

d) alte activități de administrare și acces la funcționalitățile SI SBTESP:

- asigurarea calității informațiilor din contul creării şi menținerii componentelor SI SBTESP;

- protecția și securizarea informațiilor în toate etapele de formare a bazei de date a SI SBTESP, cu utilizarea metodelor de autentificare a utilizatorilor, de autorizare conform rolului atribuit, precum și cu utilizarea mecanismelor de protecție a datelor și a canalelor de conexiune;

7) asigurarea generării datelor statistice.

Toate modificările în SI SBTESP se păstrează în ordine cronologică.

Secțiunea a 2-a

Contururile funcționale ale SI SBTESP

12. SI SBTESP trebuie să asigure exercitarea funcțiilor specifice determinate de destinația sa, care sunt grupate în contururi funcționale specifice și realizate prin intermediul componentelor SI SBTESP.

13. Conturul „Sistemul informațional de notificare a cazurilor și evenimentelor de sănătate publică” include:

1) modulul notificări – componenta de bază a SI SBTESP care asigură crearea, înregistrarea, notificarea și gestionarea cazurilor de boală infecțioasă, a intoxicațiilor acute neprofesionale exogene de etiologie chimică, a evenimentelor de sănătate publică, a rezultatelor anchetei epidemiologice și a cercetării cazurilor notificate;,

[Pct.13 subpct.1) în redacția HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

2) modulul de hartă interactivă (*GIS*) – componenta responsabilă de reprezentarea geografică a informațiilor cu privire la situația epidemiologică, în corelare cu anumiți parametri;

3) modulul alerte – componenta responsabilă de alertarea/notificarea utilizatorilor cu privire la anumite evenimente care necesită gestionate sau despre care necesită ca aceștia să fie informați;

4) modulul de raportare – componenta pentru generarea rapoartelor statistice;

5) modulul de administrare – asigură funcționalitatea de gestionare a configurărilor de SI SBTESP, managementul utilizatorilor, al evenimentelor de audit, al alertelor, al clasificatoarelor etc.;

6) modulul de căutare – asigură capacitatea de căutare, în baza anumitor parametri, a informațiilor din SI SBTESP.

14. Conturul RENV va conține următoarele compartimente și module:

1) modulul de programare pentru vaccinare;

2) modulul de înregistrare a dozelor de vaccin;

3) modulul de înregistrare a evenimentelor adverse postimunizare;

4) modulul de generare a certificatelor de vaccinare sau de profilaxie;

5) modulul de raportare;

6) modulul de management al stocurilor de vaccinuri și consumabile ;

7) modulul de raportare grafică;

8) modulul de omologare a certificatelor de vaccinare;

9) modulul de planificare.

[Pct.14 în redacția HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

15. Conturul „Sistemul informatic de laborator” include:

1) modulul de înregistrare a probelor de laborator pentru investigare, cu generarea codului de bare;

2) modulul de înregistrare a rezultatelor de laborator;

3) modulul de eliberare a rezultatului investigației;

4) modulul de generare a rapoartelor investigațiilor de laborator;

5) modul de interoperabilitate.

16. Conturul „Monitorizarea cazurilor și a contacților” include:

1) modulul de evidență și gestiune a contacților;

2) modul de vizualizare a datelor;

3) modul privind lista cazurilor cu manifestări clinice și trasabilitatea cazurilor;

4) modul de contactare și de supervizare a cazurilor;

5) modulul de raportare – componenta pentru generarea și exportarea rapoartelor statistice.

Capitolul V

STRUCTURA ORGANIZAȚIONALĂ A SI SBTESP

17. Proprietarul SI SBTESP este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din acesta. Resursele financiare pentru dezvoltarea, mentenanța și exploatarea SI SBTESP sunt asigurate din bugetul de stat și din alte mijloace financiare, conform legii.

18. Posesorul SI SBTESP este Ministerului Sănătății, cu drept de gestionare și de utilizare a datelor și a resurselor conținute de acesta.

19. Deținătorul SI SBTESP este Agenția Națională pentru Sănătate Publică din subordinea Ministerului Sănătății, care este responsabilă de crearea, de administrarea, de mentenanța și de dezvoltarea SI SBTESP.

20. Administratorul tehnic al SI SBTESP este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care va asigura administrarea tehnică și menținerea SI SBTESP în conformitate cu Regulamentul privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat.

21. Posesorul asigură condițiile organizatorice și financiare pentru funcționarea SI SBTESP.

22. Registratorii SI SBTESP sunt lucrătorii medicali, personalul responsabil din cadrul prestatori de servicii medicale, prestatorii de servicii medicale departamentale, ai instituțiilor de asistență socială și de reabilitare/ recuperare, ai centrelor de plasament temporar, ai centrelor de sănătate publică, ai Agenției Naționale pentru Sănătate Publică, ai laboratoarelor medicale și ai Centrului Național de Transfuzie a Sângelui.

23. Utilizatorii SI SBTESP sunt Ministerul Sănătății și subdiviziunile subordonate acestuia, Ministerul Afacerilor Interne și subdiviziunile subordonate acestuia, Agenția Națională pentru Sănătate Publică, centrele de sănătate publică, Compania Națională de Asigurări în Medicină, Agenția Medicamentului și Dispozitivelor Medicale, prestatorii de servicii medicale departamentale, centrele de plasament temporar, laboratoarele medicale, Centrul Național de Transfuzie a Sângelui, instituțiile de asistență socială de reabilitare și recuperare, prestatorii de servicii medicale și subdiviziunile de sănătate ale autorităților administrației publice locale.

24. Destinatarii și utilizatorii datelor din SI SBTESP sunt autoritățile publice centrale și locale, persoanele fizice sau unitățile de drept mandatate cu dreptul de a primi informații conform prevederilor legale.

Capitolul VI

DOCUMENTELE SI SBTESP

25. Documentele utilizate de SI SBTESP sunt elaborate și aprobate de către Ministerul Sănătății în ordinea stabilită, și nu se limitează doar la cele listate mai jos.

26. Documentele de intrare a datelor inițiale sunt:

1) fișa de notificare urgentă despre depistarea cazului de boală infecțioasă,

intoxicație, toxiinfecție alimentară sau profesională acută, reacție adversă la administrarea preparatelor imunobiologice;

2) fișa de evidență a bolilor (intoxicațiilor) profesionale;

3) fișa de evidență a stocului de vaccinuri, diluanți, seringi;

4) fișa de anchetare epidemiologică a focarului de boală infecțioasă;

5) fișa medicală a bolnavului de staționar, cu anexele respective;

6) registrul de evidență a vaccinărilor;

7) registrul de evidență a bolilor infecțioase;

8) registrul de evidență a persoanelor cu intoxicație profesională sau cu boală profesională depistată, caz nou;

9) registrul de evidență a stocurilor primite de preparate imunobiologice, instrumente şi utilaje medicale în centrele de sănătate publică;

10) avizul despre bolnavul cu diagnosticul stabilit, caz nou, de tuberculoză activă;

11) avizul privind boala sau intoxicația profesională cronică;

12) actul de prelevare a probelor (mostrelor);

13) actul de înapoiere a probelor (mostrelor);

14) actul de decontare a probelor (mostrelor);

15) procesul-verbal de codificare a probelor (mostrelor);

16) procesul-verbal de recoltare a probelor de apă;

17) procesul-verbal de examinare a cazului (suspiciunii) de boală (intoxicație) profesională;

18) procesul-verbal de evidență a bolilor (intoxicațiilor) profesionale;

19) trimiterea la analiză;

20) trimiterea la investigații;

21) certificatul medical (de recuperare, de testare);

22) certificatul de vaccinare;

23) fișa de notificare urgentă despre depistarea cazului de intoxicație acută neprofesională exogenă de etiologie chimică.

[Pct.26 subpct.23) introdus prin HG904 din 30.12.24, MO569-571/31.12.24 art.1022;

în vigoare 31.01.25]

27. Documentele de ieșire sunt:

1) fișa de anchetare epidemiologică a focarului cu infecția HIV/SIDA;

2) fișa de anchetare epidemiologică a cazului de hepatită virală B, C şi D acută;

3) fișa de colectare a datelor epidemiologice a cazului de hepatită virală B, C și D cronică;

4) fișa de evidență a purtătorului cronic de germeni patogeni;

5) fișa de anchetare epidemiologică a focarului de boală infecțioasă;

6) registru investigațiilor;

7) registrul cazurilor de intoxicații;

8) registrul fișelor de declarații;

9) registrul de evidență a accidentelor la locul de lucru;

10) registrul de evidență a probelor de laborator;

11) Formularul privind rezultatele investigațiilor de laborator;

12) procesul-verbal de investigații;

13) procesul-verbal de recoltare;

14) trimiterea medicală pentru investigații;

15) certificatul medical (de recuperare, de testare);

16) certificatul de vaccinare;

17) rapoartele analitice și statistice;

17[1]) procesul-verbal privind cercetarea cazului de intoxicație acută neprofesională exogenă de etiologie chimică;

[Pct.27 subpct.17[1]) introdus prin HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

18) altele.

28. Documentele tehnologice sunt:

1) instrucțiunile metodice, ghidurile și regulamentele privind diferite nozologii;

2) protocoalele clinice naționale;

3) formularele și rapoartele aprobate de către Biroul Național de Statistică;

4) lista utilizatorilor și a drepturilor acestora;

5) înregistrările de audit ale activității SI SBTESP și ale utilizatorilor.

Capitolul VII

SPAȚIUL INFORMAȚIONAL AL SI SBTESP

Secțiunea 1

Obiectele informaționale ale SI SBTESP

29. Principalele obiecte informaționale ale SI SBTESP reprezintă totalitatea actelor oficiale care confirmă starea de sănătate a persoanei și includ:

1) fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică;

2) trimiterea/fișa de investigații de laborator;

3) certificate:

a) de vaccinare;

b) de recuperare;

c) de testare;

4) persoane fizice:

a) pacienți;

b) lucrători medicali;

5) unități de drept:

a) prestatori de servicii medicale;

b) prestatori de servicii sociale etc.

30. Atributele obiectului informațional „fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică” sunt:

1) numărul epidemiologic unic al notificării;

2) datele cu privire la diagnosticul primar;

3) datele de identificare a pacientului;

4) datele cu privire la înregistrarea cazului în SI SBTESP;

5) datele cu privire la simptomele și la manifestările bolii;

6) datele cu privire la diagnosticul final.

31. Atributele obiectului informațional „trimiterea/fișa de investigații de laborator” sunt:

1) numărul de identificare/înregistrare al investigației de laborator;

2) tipul analizei investigației de laborator;

3) datele de identificare a pacientului;

4) datele despre boală;

5) datele privind rezultatele de laborator.

32. Atributele obiectului informațional „certificate” sunt:

1) datele despre certificatul de vaccinare;

2) datele despre certificatul de recuperare;

3) datele despre certificatul de testare.

33. Atributele obiectului informațional „persoane fizice” sunt:

1) pacienți:

a) datele de identificare (IDNP, numele, prenumele, sexul, data nașterii);

b) datele demografice (cetățenia, tipul documentului de identificare, numărul documentului, data emiterii);

c) adresa de domiciliu și/sau de reședință temporară (localitatea, strada, blocul, apartamentul);

d) datele privind asigurarea medicală (categoria și statutul de asigurat, tipul de asigurare);

e) datele socioeconomice (locul de muncă/studiile);

2) lucrători medicali:

a) datele de identificare (IDNP, numele, prenumele, sexul, data nașterii);

b) datele demografice (cetățenia, tipul documentului de identificare, numărul documentului);

c) adresa de domiciliu și/sau de reședință temporară (localitatea, strada, blocul, apartamentul);

d) datele privind asigurarea medicală (categoria și statutul de asigurat, tipul de asigurare);

e) datele socioeconomice (locul de muncă/studiile).

34. Atributele obiectului informațional „unități de drept” prestatori de servicii medicale/sociale:

1) numărul de identificare de stat – IDNO;

2) denumirea;

3) codul IMS;

4) tipul;

5) numărul de telefon;

6) adresa poștală.

Secțiunea a 2-a

Identificatorii obiectelor informaționale

35. Identificatorul obiectului informațional „fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică” este constituit din numărul epidemiologic unic generat de către SI SBTESP și are următoarea structură: NNNNAA1XXXXXX, unde NNNN este codul instituției medicale care notifică cazul, AA reprezintă ultimele două cifre ale anului în care este generată alerta, 1 – cifra constantă, XXXXXX este numărul de ordine al cazului în instituția care a notificat și începe cu 000001 în fiecare an.

36. Identificatorul obiectului informațional „trimiterea/fișa de investigații de laborator” este constituit din numărul unic generat de către conturul „Sistemul informatic de laborator” a SI SBTESP și are următoarea structură: NNXXXXXX, unde NN este codul laboratorului care înregistrează investigația, XXXXXX este numărul de ordine a înregistrării și începe cu 000001 în fiecare an.

37. Identificatorul obiectului informațional „certificate” este constituit dintr-un număr unic generat de către conturul „RENV”, conform logicii și regulilor predefinite.

[Pct.37 în redacția HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

38. Pentru obiectele informaționale „persoane fizice” (pentru participanți persoane fizice) și „unități de drept” (pentru participanți persoane juridice și prestatori de servicii medicale) în SI BTESP sunt utilizate, respectiv: numărul de identificare de stat al „persoanei fizice” – IDNP (împrumutat din Registrul de stat al populației) și numărul de identificare de stat al „unității de drept” – IDNO (împrumutat din Registrul de stat al unităților de drept). Datele suplimentare necesare privind persoanele fizice şi unitățile de drept sunt accesibile din Registrul de stat al populației şi din Registrul de stat al unităților de drept în baza

numărului de identificare de stat respectiv.

Secțiunea a 3-a

Scenariile de bază asociate obiectelor informaționale

39. Obiectul informațional luat în evidență în SI SBTESP și scenariile de bază sunt descrise după cum urmează:

A. Pentru obiectul informațional *Fișa de notificare a cazului de boală infecțioasă, intoxicațiilor acute neprofesionale exogene de etiologie chimică și evenimentelor de sănătate publică*, scenariile de bază sunt:

1. Crearea notificărilor/înregistrarea se efectuează de către persoanele autorizate cu drept de înregistrare (rol de asistent al instituției medicale din numele medicului, medic), direct în sistem, sau prin intermediul platformei de interoperabilitate (MConnect) cu alte sisteme ce vor furniza datele respectând un anumit standard, conținând un set minim de date, privind următoarele cazuri de boli transmisibile și evenimentele de sănătate publică:

1) *boli transmisibile*:

a) boli prevenibile prin vaccinări;

b) boli cu transmitere sexuală;

c) hepatite virale;

d) infecția cu HIV/SIDA;

e) boli cu factor de transmitere alimentar;

f) boli cu factor de transmitere hidric şi care provin din mediul înconjurător;

g) alte boli transmisibile prin agenți neconvenționali;

h) boli cu transmitere aerogenă;

i) boli transmisibile care pot duce la apariția urgențelor de sănătate publică cu risc de răspândire internaționale;

j) boli transmise prin vectori;

k) zoonoze (comune pentru animale şi om);

l) alte boli transmisibile cu importantă pentru sănătatea publică, inclusiv bolile cauzate prin răspândire deliberată;

2) *probleme speciale de sănătate*:

a) boli diareice acute;

b) toxiinfecții alimentare;

c) infecții nosocomiale (infecții asociate asistenței medicale);

d) rezistență la antimicrobiene;

3) *evenimente de sănătate publică*:

intoxicații acute neprofesionale exogene de etiologie chimică.

2. Administrare/transfer notificare se realizează de către un utilizator cu rol de medic sau cu rol de epidemiolog ANSP și/sau Centrul de Sănătate Publică. Utilizatorii ANSP pot transfera cazul dintr-o instituție în alta și, de asemenea, pot atribui cazul transferat unei instituții din teritoriul administrativ.

3. Actualizarea datelor notificării cazului, are loc în cazul modificării unui atribut al acestuia. Această operațiune este realizată de către persoanele autorizate din SI SBTESP.

4. Monitorizarea epidemiologică se realizează de către un medic epidemiolog regional/raional, în limitele unui spațiu bine determinat, sau de către medicii specialiști/epidemiologi din cadrul ANSP.

5. Înregistrarea cazurilor de grup se realizează de către specialiștii ANSP din teritoriile administrative pentru a asigura monitorizarea în limitele unui spațiu bine determinat.

B. Pentru obiectul informațional *trimiterea/fișa de investigații de laborator* scenariile de bază sunt:

1) recepționarea cererii pentru investigație din sisteme externe;

2) recepționarea probelor la ghișeu, în laborator;

3) codificarea probelor și transmiterea în zona de investigare;

4) investigarea probelor;

5) validarea rezultatelor;

6) eliberarea rezultatelor la ghișeu;

7) transmiterea rezultatelor părților solicitante.

C. Pentru obiectul informațional certificate, scenariile de bază sunt:

1. vaccinarea/aplicarea vaccinului:

1) înregistrarea primară – de către registratori, în momentul adresării persoanei;

2) actualizarea datelor – de către registrator, la solicitarea deținătorului;

3) actualizarea datelor automat – presupune că persoana deține IDNP și un certificat cu un cod QR recunoscut sau eliberat în UE. În cazul verificărilor validate cu succes, în RENV se creează o inscripție nouă despre persoana vaccinată;

4) scoaterea din evidență și arhivarea – la radierea persoanei (deces, pierderea cetățeniei) pentru care s-a eliberat actul permisiv, la solicitarea deținătorului;

2. de recuperare:

1) înregistrarea primară de îmbolnăvire (pozitiv) – de către registratori, în momentul adresării persoanei;

2) actualizarea datelor de către registrator, la solicitarea deținătorului;

3) scoaterea din evidență a celor bolnavi, arhivarea;

3. de testare:

1) înregistrarea primară – de către registratori, în momentul adresării persoanei;

2) actualizarea datelor – de către registrator, la solicitarea deținătorului;

3) actualizarea datelor automat – presupune că persoana deține IDNP și un certificat cu un cod QR recunoscut sau eliberat în UE. În cazul verificărilor validate cu succes, în RENV se va crea o inscripție nouă despre statutul persoanei testate;

4) scoaterea din evidență și arhivarea datelor.

D. Pentru obiectul informațional persoane fizice, scenariile de bază sunt:

1. pacienți:

1) înregistrarea primară – de către registratori, în momentul adresării persoanei;

2) actualizarea datelor – de către registrator, la solicitarea deținătorului;

3) actualizarea datelor automat din cadrul Registrului de stat al populației;

4) scoaterea din evidență privind prezența cazului de boală infecțioasă și evenimentelor de sănătate publică și arhivarea datelor;

2. lucrători medicali:

1) înregistrarea primară – în momentul adresării persoanei la ANSP în baza cheiței electronice;

2) actualizarea datelor de către registrator/administrator, la solicitarea deținătorului prin cerere sau din acțiune proprie direct în SI SBTESP;

3) actualizarea datelor automat din cadrul Registrului de stat al populației prin actualizarea datelor personale de identificare a lucrătorului medical;

4) scoaterea din evidență/iradierea lucrătorului medical din sistem prin arhivarea datelor atribuite acțiunilor lucrătorului medical, și limitarea accesului asupra datelor cu caracter personal ale pacienților.

E. Pentru obiectul informațional unități de drept, scenariul de bază este:

prestatori de servicii medicale și prestatori de servicii sociale etc.:

1) înregistrarea primară – în baza nomenclatorului IMSP de către ANSP;

2) actualizarea datelor – la modificarea nomenclatorului IMSP prin adresare către ANSP;

3) scoaterea din evidență/radierea prestatorului de servicii medicale/sociale din sistem prin arhivarea datelor atribuite acțiunilor lucrătorului medical și limitarea accesului asupra datelor cu caracter personal ale pacienților.

[Pct.39 în redacția HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

Secțiunea a 4-a

Clasificatoarele SI SBTESP

40. Pentru a asigura veridicitatea și reducerea volumului informației stocate în SI SBTESP, se utilizează clasificatoarele și nomenclatoarele prezentate mai jos, care nu se limitează la:

1) internaționale:

a) Clasificatorul internațional al maladiilor;

b) Clasificatorul internațional al țărilor;

2) naționale:

a) Clasificatorul oficial al unităților administrativ-teritoriale ale Republicii Moldova;

b) Nomenclatorul prestatorilor de servicii medicale;

c) Nomenclatorul prestatorilor privați de servicii de sănătate;

d) Nomenclatorul investigațiilor de laborator;

e) Clasificatorul tipului prestatorilor de servicii medicale;

f) Clasificatorul tipurilor cazurilor;

g) Clasificatorul tipurilor de boli;

h) Clasificatorul condițiilor ce au favorizat infectarea;

i) Clasificatorul simptomelor neurologice;

j) Clasificatorul simptomelor respiratorii;

k) Clasificatorul simptomelor digestive;

l) Clasificatorul tipurilor de produse alimentare;

m) Clasificatorul surselor de apă;

n) Clasificatorul tipurilor parezelor/paraliziilor;

o) Clasificatorul tipurilor erupțiilor cutanate.

Secțiunea a 5-a

Interacțiunea SI SBTESP cu alte resurse informaționale

41. Schimbul de date dintre SI SBTESP 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 schimbului de date și al interoperabilității.

42. SI SBTESP asigură interacțiunea și schimbul de date cu următoarele resurse informaționale:

1) Sistemul informațional „Registrul de stat al populației”;

2) Sistemul informațional „Registrul de stat al unităților de drept”;

3) Sistemul informațional „Asigurarea obligatorie de asistență medicală”;

4) Sistemul informațional „Asistența medicală prespitalicească”;

5) Sistemul informațional „Asistența medicală spitalicească”;

6) Sistemul informațional „Asistența medicală primară”;

7) alte sisteme informaționale considerate necesare pentru implementarea și dezvoltarea SI SBTESP.

43. SI SBTESP utilizează următoarele sisteme informaționale partajate:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – serviciu reutilizabil, furnizat la nivelul platformei tehnologice guvernamentale comune, care are scopul de a oferi un mecanism integrator, securizat și flexibil de autentificare și control al accesului utilizatorilor în sistemele informaționale, inclusiv în serviciile electronice;

2) serviciul electronic guvernamental de semnătură electronică (MSign) – serviciu reutilizabil, furnizat la nivelul platformei tehnologice comune a Guvernului, care are scopul

de a oferi un mecanism integrator, securizat și flexibil pentru diferite soluții de aplicare și verificare a autenticității semnăturii electronice de către utilizatori (inclusiv în contextul utilizării sistemelor informaționale și a serviciilor electronice), oferite de către furnizorii de semnătură electronică în conformitate cu legislația;

3) serviciul electronic guvernamental de jurnalizare (MLog) – serviciu centralizat, reutilizabil, componentă a platformei tehnologice guvernamentale comune (MCloud), care are scopul de a oferi un mecanism securizat și flexibil de jurnalizare și audit, asigurând evidența evenimentelor, în contextul utilizării sistemelor informaționale;

4) serviciul guvernamental de notificare electronică (MNotify) – serviciu centralizat, reutilizabil, ce permite prestatorilor de servicii, autorităților și instituțiilor publice (expeditori) expedierea notificărilor utilizatorilor (destinatari) în vederea înștiințării acestora cu privire la evenimentele produse în legătură cu prestarea serviciilor sau a altor evenimente relevante destinatarilor;

5) platforma de interoperabilitate (MConnect) – soluție tehnică destinată asigurării schimbului de date dintre sistemele informaționale deținute de participanții la schimbul de date, în conformitate cu Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

6) alte servicii guvernamentale electronic considerate necesare pentru implementarea și dezvoltarea SI SBTESP.

Capitolul VIII

SPAȚIUL TEHNOLOGIC AL SI SBTESP

44. SI SBTESP se proiectează ca un sistem modular care asigură posibilitatea dezvoltării sale fără a afecta continuitatea funcționării. Arhitectura acestuia este concepută după schema-tip a infrastructurii informaționale a sistemului informațional, în conformitate cu cerințele legale.

Nivelele SI SBTESP:

45. La nivel conceptual, arhitectura SI SBTESP este definită pe trei niveluri:

1) nivelul de interfață – serverul pentru paginile web cu formularele utilizatorilor și cu informațiile din baza de date pentru vizualizare și utilizare prin intermediul browserului stației de lucru;

2) produsul program al nivelului de mijloc – serverul aplicațiilor care va susține partea client, ce deservește interfața bazei de date cu utilizatori, va transforma cererile utilizatorilor în limbaj de interpelare structurat și va primi datele de la baza de date și le va prezenta în formă comodă pentru percepție;

3) nivelul de jos – serverul bazei de date.

Rețeaua informațională de telecomunicații

46. Arhitectura complexului software, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către dezvoltatorii SI SBTESP, în comun cu posesorul și deținătorul, în etapele inițiale și în cele ulterioare de elaborare și de implementare a SI SBTESP.

Complexe tehnice de program

47. SI SBTESP conform schemei generale de reprezentare a conceptului tehnic, utilizează sistemele informaționale partajate (MPass, MSign, MLog, MNotify) și este găzduit pe platforma tehnologică guvernamentală comună (MCloud). SI SBTEP se integrează cu alte sisteme informaționale sau registre de stat prin intermediul platformei guvernamentale de interoperabilitate (MConnect).

Schema generală de reprezentare a conceptului tehnic

[Pct.47 modificat prin HG904 din 30.12.24, MO569-571/31.12.24 art.1022; în vigoare 31.01.25]

48. Platforma tehnologică a SI SBTESP va fi găzduită pe platforma tehnologică guvernamentală comună (MCloud), în conformitate cu Hotărârea Guvernului nr. 128/2014 cu privire la platforma tehnologică guvernamentală comună (MCloud).

Capitolul IX

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

A SI SBTESP

49. Prin securitatea informațională se înțelege protecția resurselor şi infrastructurii informaționale împotriva acțiunilor intenționate sau accidentale, cu caracter natural sau artificial, al căror rezultat cauzează daune participanților în procesul de schimb de informație.

50. Asigurarea securității informaționale va include totalitatea măsurilor juridice, organizatorice, economice şi tehnologice, orientate spre prevenirea pericolelor securității resurselor şi infrastructurii informaționale.

51. Pot fi delimitate următoarele probleme de asigurare a securități informaționale cu care se va confrunta SI SBTESP:

1) asigurarea confidențialității informației (prevenirea obținerii informațiilor de către persoanele care nu au drepturile şi competențele respective);

2) asigurarea integrității logice a datelor (prevenirea introducerii, actualizării şi ștergerii nesancționate a informației sau introducerea datelor denaturate);

3) asigurarea securității infrastructurii informaționale împotriva tentativelor de a defecta sau de a modifica funcționarea acesteia.

52. Mecanismele principale de securitate informațională utilizate sunt:

1) autentificarea şi autorizarea informației;

2) administrarea accesului la informație;

3) înregistrarea acțiunilor utilizatorilor sistemului informatic;

4) criptarea informației;

5) auditul informatic;

6) procedurile de restabilire, în caz de dezastru.

53. Veriga cea mai sensibilă supusă riscului în sistemul de securitate este factorul uman. Din aceste considerente, instruirea personalului la capitolul însușirii metodologiei rezistenței la amenințări informatice este un element important.

54. În procesul de elaborare a SI SBTESP, pentru asigurarea securității informaționale se va ține cont de algoritmii şi de protocoalele existente pe piață, cu respectarea cadrului legal, inclusiv:

1) Legea nr. 982/ 2000 privind accesul la informație;

2) Legea nr. 467/2003 cu privire la informatizare şi la resursele informaționale de stat;

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

4) Hotărârea Guvernului 1141/2017 pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii unităților de drept public în cadrul circulației electronice ale acestora.

55. Accesul la resursele SI SBTESP va fi asigurat şi autorizat prin intermediul unui sistem de utilizatori şi parole şi autorizarea prin certificat digital. Cu toate acestea, utilizatorii vor poseda drepturi distincte de acces în funcție de nivelul de securitate căruia îi corespund. Pentru fiecare grup de acces va exista posibilitatea de a defini rolurile şi drepturile utilizatorilor (chiar şi până la nivelul de acces la interfața utilizatorilor).

56. Accesul la informația bazei de date va fi limitat în funcţie de drepturile şi rolurile specifice grupurilor de acces. În acest caz, fiecare grup de utilizatori va avea acces la o interfață personalizată (diferită de cea a altor grupuri), pentru vizualizarea şi gestionarea informației bazei de date, precum şi de manipulare cu datele.

Orice modificare potențial periculoasă: modificarea informației unei înregistrări, marcarea la ștergere, adăugarea unor înregistrări noi etc. va fi documentată în registre electronice speciale (fişiere log), arătând momentul de timp şi utilizatorul care a efectuat modificarea potențial periculoasă. În cazul în care modificările potențial periculoase nu vor implica suprimarea fizică a datelor pentru fiecare înregistrare, va fi posibil de văzut utilizatorul care a efectuat ultima modificare. În consecință, sistemul informatic proiectat va

dispune de un instrument eficient care va da posibilitatea de a efectua o analiză a comportamentului utilizatorilor (sau a productivității lor).

57. La nivel fizic politica de asigurare a securități informaționale va fi realizată prin intermediul unor module automate de generare a copiilor de rezervă a fișierelor şi a bazelor de date aflate în producție. Administratorii SI SBTESP vor dispune de posibilitatea de definire a politicii de generare automată a copiilor de rezervă.

58. În vederea asigurării unui nivel adecvat al securități informaționale a SI SBTESP, se consideră binevenită elaborarea şi implementarea unei politici de asigurare a securități informaționale. Această politică va detalia totalitatea compartimentelor de securitate, rolurile, drepturile și obligațiile fiecărui actor al sistemului informatic.

Capitolul X

ÎNCHEIERE

59. Impactul SI SBTESP va consta în implementarea unei soluții moderne de gestiune şi automatizare a fluxurilor de date în sistemul de sănătate, precum și digitalizarea proceselor de colectare, analiză, interpretare şi diseminare sistematică şi continuă a datelor cu privire la bolile transmisibile şi evenimentele de sănătate publică, în scopul implementării măsurilor de sănătate publică, al îmbunătățirii calității informațiilor, inclusiv al relevanței, integrității, oportunității, exactității, accesibilității, comparabilității, coerenței acestora, precum și de a face mai transparent şi mai rapid procesul de luare a deciziilor.

60. Implementarea SI SBTESP va determina scăderea cheltuielilor generale, deoarece va crește fluxul de lucru în format electronic, fapt ce va duce la reducerea considerabilă a folosirii hârtiei şi a rechizitelor de birou şi la îmbunătățirea calității şi sporirii diversității mijloacelor de comunicare interinstituțională.

61. Implementarea SI SBTESP va aduce următoarele beneficii:

1) creșterea calității proceselor prin asigurarea interoperabilității cu registre demografice și alte resurse externe, a transparenței măsurilor de sănătate publică, cu eficientizarea managementului și a intervențiilor în sănătatea publică și a accesului la registrele privind morbiditatea prin boli transmisibile, precum și scurtarea timpului procedurilor de rutină și reducerea timpului de așteptare și acces la informație;

2) securizarea accesului la aplicații/date/sisteme/infrastructură, cu aplicarea politicilor de securitate, profilurilor de identitate şi a soluțiilor de gestiune a accesului;

3) oferirea de informații autentice, veridice, curente şi consistente Ministerului Sănătății și tuturor actorilor implicați din domeniul sănătății și alte domenii cum ar fi sănătatea animalelor și siguranța alimentelor, inspectoratul general al poliției de frontieră, inspectoratul general pentru situații excepționale etc.;

4) reducerea timpului de răspuns şi suport decizional ce presupune gestionarea situațiilor epidemiologice, evenimentelor și urgențelor de sănătate publică;

5) acces rapid, garantat la date şi informații indiferent de locație;

6) sporirea calității informațiilor, inclusiv a relevanței, integrității, oportunității, exactității, accesibilității, comparabilității, coerenței acesteia;

7) perfecționarea modului de păstrare şi diseminare a informațiilor prin asigurarea protecției informațiilor confidențiale, accesul nediscriminatoriu tuturor utilizatorilor la informații şi servicii, obiectivitate şi imparțialitate în diseminarea informaților;

8) consolidarea unei baze unice de date în domeniul sănătății cu privire la supravegherea epidemiologică a bolilor transmisibile și evenimentelor de sănătate publică și protejarea datelor în timp prin proceduri automatizate de salvare și restaurare.

Anexa nr. 2

la Hotărârea Guvernului nr. 885/2022

REGULAMENT

privind organizarea și funcționarea Sistemului

informațional de supraveghere a bolilor transmisibile și

evenimentelor de sănătate publică

I. DISPOZIȚII GENERALE

1. Regulamentul privind organizarea și funcționarea Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică (în continuare – *Regulament*) stabilește procedurile și mecanismele de înregistrare și evidență a informației sistematizate, acumulate în cadrul depistării, gestionării și supravegherii epidemiologice a bolilor transmisibile și evenimentelor de sănătate publică, precum și reglementează cerințele față de protecția datelor în procesul de colectare, acumulare, actualizare, prelucrare, păstrare și al schimbului 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 sănătăți 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. 951/2013 pentru aprobarea Regulamentului privind sistemul național de supraveghere epidemiologică și control al bolilor transmisibile și evenimentelor de sănătate publică, Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical.

3. Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică (în continuare – *SI SBTESP*) este resursa informațională de stat care reprezintă totalitatea informației sistematizate cu privire la boli infecțioase și evenimente de sănătate publică, inclusiv intoxicații, toxiinfecții alimentare și/sau profesionale acute, din momentul suspectării acestora.

4. Scopul SI SBTESP este digitizarea, automatizarea și eficientizarea proceselor direcționate spre îmbunătățirea prevenirii și controlului bolilor transmisibile și evenimentelor de sănătate publică, dezvoltarea capacităților de evidență, gestionare, analiză și reacționare la evenimentele cu impact negativ asupra sănătății publice, supravegherea evenimentelor de sănătate publică, inclusiv prin implementarea sistemului de alertă precoce și răspuns rapid, dezvoltarea și implementarea instrumentelor/soluțiilor tehnice flexibile și modulare, care ar permite îmbunătățirea activității sistemului sănătății.

5. SI SBTESP creează spațiul informațional necesar pentru participanții la SI SBTESP în vederea automatizării unor funcții realizate de aceștia prin implementarea tehnologiilor informaționale performante în domeniul supravegherii cazurilor de boli transmisibile și evenimentelor de sănătate publică.

II. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, EXPLOATĂRII ȘI UTILIZĂRII SI SBTESP ȘI ATRIBUȚIILE ACESTORA

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

1) proprietarul;

2) posesorul;

3) deținătorul;

4) administratorul tehnic;

5) registratorul;

6) utilizatorul.

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

8. Posesorul SI SBTESP este Ministerul Sănătății, cu drept de gestionare și de utilizare a datelor și a resurselor conținute de acestea și care asigură condițiile organizatorice și financiare pentru funcționarea și dezvoltarea acestuia.

9. Drepturile și obligațiile Posesorului sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și cu Hotărârea Guvernului nr. 148/2021 cu privire la organizarea și funcționarea Ministerului Sănătății.

10. Deținătorul SI SBTESP este Agenția Națională pentru Sănătate Publică din subordinea Ministerului Sănătății.

11. Deținătorul are următoarele atribuții:

1) asigură formarea resursei informaționale;

2) stabilește scopurile și sarcinile funcționale ale SI SBTESP;

3) monitorizează procesul de înregistrare și prelucrare a datelor în SI SBTESP;

4) verifică respectarea condițiilor de înregistrare, evidență și utilizare a datelor cu caracter personal;

5) asigură securitatea și protecția datelor din SI SBTESP în limitele competențelor;

6) autorizează și suspendă dreptul de acces la SI SBTESP;

7) stabilește măsurile tehnice și organizatorice de protecție și securitate a SI SBTESP;

8) elaborează și aprobă Planul de continuitate al SI SBTESP, instituie activități de control menite să diminueze riscurile privind integritatea datelor;

9) exercită alte atribuții necesare pentru asigurarea bunei funcționări a SI SBTEPS;

10) elaborează, coordonează și aprobă procedurile operaționale aferente gestionării și asigurării bunei funcționări a SI SBTESP;

11) stabilește regulile și procedurile specifice de acordare/suspendare/retragere/anulare a accesului la contururile SI SBTESP și de stabilire a rolurilor 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, cu Hotărârea Guvernului nr. 1090/2017 cu privire la organizarea și funcționarea Agenției Naționale pentru Sănătatea Publică și cu Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical.

13. Deținătorul asigură păstrarea SI SBTESP 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 SBTESP este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.

15. Registratorii SI SBTESP sunt lucrătorii medicali, persoanele responsabile din cadrul prestatorilor de servicii medicale, prestatorii de servicii medicale departamentale, ai

instituțiilor de asistență socială și de reabilitare și recuperare, ai centrelor de plasament temporar, ai centrelor de sănătate publică, ai laboratoarele medicale, ai Agenției Naționale pentru Sănătate Publică și ai Centrului Național de Transfuzie a Sângelui.

16. Registratorii au următoarele atribuții:

1) Asigură, în termenele și în condițiile stabilite, colectarea și introducerea informațiilor relevante în baza de date a SI SBTESP;

2) asigură autenticitatea, plenitudinea și integritatea datelor;

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

4) solicită posesorului autorizarea accesului, precum și suspendarea drepturilor de acces în SI SBTESP;

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

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

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

18. Registratorii SI SBTESP au următoarele drepturi:

1) să participe la dezvoltarea și la îmbunătățirea SI SBTESP;

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

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

4) să prezinte propuneri privind perfecționarea și eficientizarea SI SBTESP.

19. Utilizatorii SI SBTESP sunt Ministerul Sănătății și subdiviziunile subordonate acestuia, Ministerul Afacerilor Interne și subdiviziunile subordonate acestuia, Agenția Națională pentru Sănătate Publică, centrele de sănătate publică, Compania Națională de Asigurări în Medicină, Agenția Medicamentului și Dispozitivelor Medicale, prestatorii de servicii medicale departamentale, centrele de plasament temporar, laboratoarele medicale, Centrul Național de Transfuzie a Sângelui, instituțiile de asistență socială de reabilitare și recuperare, prestatorii de servicii medicale și subdiviziunile de sănătate ale autorităților administrației publice locale și alte instituții în baza unui acord semnat cu deținătorul SI SBTESP.

20. Utilizatorii SI SBTESP sunt obligați:

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

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

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

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

21. Utilizatorii SI SBTESP, în limitele competenței, au următoarele drepturi:

1) să participe la crearea, implementarea și dezvoltarea SI SBTESP;

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

3) să acceseze, să vizualizeze, să utilizeze și să prelucreze informațiile din SI SBTESP în conformitatea cu rolurile și drepturile stabilite;

4) să solicite și să primească de la posesorul și administratorul tehnic al SI SBTESP ajutor metodologic și practic privind problemele ce țin de funcționarea SI SBTESP.

III. REGIMUL JURIDIC DE UTILIZARE A DATELOR

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

23. Accesul la resursele informaționale ale SI SBTESP este segmentat pentru utilizatori interni și utilizatori externi.

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

24. Suspendarea dreptului de acces la SI SBTESP și/sau contururile acestuia se efectuează prin înaintarea cererii/demersului către posesor și/sau în una din următoarele situații:

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

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

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

4) după trei tentative greșite de autentificare;

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

6) în alte cazuri în limitele prevederilor legislative.

25. Lucrările profilactice 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 două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea utilizatorilor prin coordonarea prealabilă cu posesorul în situația nefuncționării sau funcționării necorespunzătoare a SI SBTESP.

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

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

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

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

4) la necesitate, datele vor fi actualizate, iar cele incomplete sau inexacte vor fi ulterior rectificate ori șterse;

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

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

IV. INTEROPERABILITATEA

CU ALTE SISTEME INFORMAȚIONALE

27. Pentru asigurarea actualizării operative și automate a conținutului informațional al SI SBTESP cu informație veridică, poate fi efectuată interacțiunea și sincronizarea datelor cu alte sisteme informaționale, importând automat sau exportând date spre verificare și/sau completare a conținutului informațional al SI SBTESP.

28. Schimbul de date dintre SI SBTESP și alte sisteme și resurse informaționale de stat se realizează prin intermediul platformei de interoperabilitate (MConnect).

29. Conectarea la platforma de interoperabilitate (MConnect) și, respectiv, schimbul de date dintre SI SBTESP și sistemele și resursele informaționale se asigură în conformitate cu prevederile Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate și ale Hotărârii Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect).

30. SI SBTESP realizează schimbul de date cu următoarele sisteme informaționale de stat:

1) Sistemul informațional „Registrul de stat al populației”;

2) Sistemul informațional „Registrul de stat al unităților de drept”;

3) Sistemul informațional „Asigurarea obligatorie de asistență medicală”;

4) Sistemul informațional „Asistența medicală prespitalicească”;

5) Sistemul informațional „Asistența medicală spitalicească”;

6) Sistemul informațional „Asistența medicală primară”;

7) alte sisteme informaționale considerate necesare pentru implementarea și dezvoltarea SI SBTESP.

31. SI SBTESP utilizează următoarele sisteme informaționale partajate:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass);

2) serviciul electronic guvernamental de semnătură electronică (MSign);

3) serviciul electronic guvernamental de jurnalizare (MLog);

4) serviciul guvernamental de notificare electronică (MNotify);

5) platforma de interoperabilitate (MConnect);

6) alte servicii guvernamentale electronice considerate necesare pentru implementarea și dezvoltarea SI SBTESP.

V. ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI DIN SI SBTESP

32. Măsurile de protecție și securitate a informației din SI SBTESP reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SI SBTESP și se efectuează neîntrerupt de către posesorul acestui sistem.

33. Obiecte ale asigurării protecției și securității informației din SI SBTESP se consideră:

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

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

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

34. Securitatea informațională a SI SBTESP se efectuează prin aplicarea metodelor și prin efectuarea acțiunilor descrise în Planul de continuitate al acestuia și, după caz, a procedurilor operaționale.

35. Protecția datelor se efectuează prin următoarele metode:

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

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

3) monitorizarea procesului de exploatare a SI SBTESP prin intermediul mecanismului de jurnalizare.

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

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

2) implementarea principalelor măsuri tehnico-organizatorice necesare pentru asigurarea funcționării SI SBTESP;

3) implementarea procedurilor interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din SI SBTESP;

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

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

VI. CONTROLUL ȘI RĂSPUNDEREA

37. Ținerea SI SBTESP este supusă controlului intern și extern. Controlul intern privind ținerea SI SBTESP se efectuează de către Agenția Națională pentru Sănătate Publică, care este posesorul SI SBTESP. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea SI SBTESP se efectuează de către instituții abilitate și certificate în domeniul auditului.

38. SI SBTESP se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

39. Responsabilitatea privind organizarea și funcționarea SI SBTESP se atribuie posesorului SI SBTESP, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea SI SBTESP.

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