



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2022

Chișinău

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

În temeiul prevederilor 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.

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

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

2) pe tot cuprinsul Regulamentului, textul „SIA RVC-19” se substituie cu textul „SI SBTESP”;

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

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

5. 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

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

Capitolul I
INTRODUCERE

Supravegherea bolilor transmisibile și evenimentelor de sănătate publică reprezintă un domeniu prioritar în supravegherea de stat a sănătății publice, precum este stipulat 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 forma de organizare juridică, sunt obligați să asigure evidență separată a bolnavilor de boli transmisibile și, în cazul depistării acestora, să informeze Serviciul de Supraveghere de Stat a Sănătății Publice în decurs de 24 de ore.

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 (ANSP).

Totodată, menționăm că la moment ANSP nu dispune de un sistem informațional de colectare a datelor despre înregistrarea cazurilor de boli transmisibile, iar metodele utilizate de ANSP 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 COVID-19 pentru monitorizarea situației epidemiologice și 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 art. 114, capitolul 21 din Acordul de Asociere cu Uniunea Europeană (2014), care vizează cooperarea în domeniul privind supravegherea epidemiologică și controlul bolilor transmisibile, precum și sporirea capacității de pregătire pentru amenințări și urgențe la adresa sănătății publice.

Capitolul II GENERALITĂȚI

1. Sistemul informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică (în continuare – *SI SBTESP*) este un sistem informațional constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, care 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 boliprofesionale acute.

2. SI SBTESP asigură digitalizarea proceselor de colectare, analiză, interpretare și diseminare sistematică și continuă a datelor despre sănătate cu privire la bolile transmisibile și evenimentele de sănătate publică, în contextul răspândirii lor în timp, spațiu, grup de populație și 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, gestiune și raportare a cazurilor cu privire la boli transmisibile și evenimente 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 bolile transmisibile și evenimentele de sănătate publică.

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

5. Noțiunile principale, utilizate în sensul prezentului Concept, utilizează termenii definiți în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și Legea nr. 71/2007 cu privire la registre, precum și în Regulamentul privind sistemul național de supraveghere epidemiologică și control al bolilor transmisibile și evenimentelor de sănătate publică, aprobat prin Hotărârea Guvernului nr. 951/2013.

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 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 SI SBTESP – înregistrarea informației despre schimbările care au loc, pentru a face posibilă reconstituirea istoriei unui set de date sau starea lui la 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 nici un 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 spre 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 pregătirii pentru lucru atât a SI SBTESP, cât și a datelor acestuia.

7. Sarcinile de bază ce urmează a fi realizate la exploatarea SI SBTESP sunt următoarele:

- 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 boală infecțioasă, intoxicație, toxinfecție alimentară și profesională acută, evenimentelor de sănătate publică, investigațiilor de laborator, precum și altor informații relevante, în vederea stocării, sistematizării, actualizării și asigurării unui nivel adecvat de protecție a datelor cu caracter personal;
- 4) standardizarea procedurilor, formularelor și 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 reapariția cazurilor de boli transmisibile supuse înregistrării și notificării în sistemul de supraveghere epidemiologică, precum și a cazurilor de boli transmisibile de origine necunoscută;
- 8) monitorizarea evoluției unei situații epidemii prin boli transmisibile;
- 9) eliminarea treptată a gestionării datelor pe suport de hârtie, prin utilizarea informațiilor și documentelor electronice;
- 10) comunicarea rapidă între entitățile SI SBTESP, cu utilizarea mijloacelor electronice;
- 11) utilizarea potențialului tehnologiilor electronice contemporane în 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 către cetățeni, inclusiv prin depunerea solicitărilor în regim on-line;
- 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) eliminarea posibilităților de manipulare a datelor din SI SBTESP;

17) eliminarea 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 evenimentelor de sănătate publică – reprezintă o soluție informatică performantă pentru crearea și administrarea notificărilor despre cazurile de boli transmisibile și evenimentele de sănătate publică. Aceasta presupune automatizarea procesului de înregistrare și gestiune a notificărilor și a informațiilor relevante, cum ar fi, diagnostic primar; diagnostic final; simptome/manifestări ale bolii; concluzii din anchetarea epidemiologică; rezultatele investigațiilor de laborator, informații cu privire la vaccinare și evidența administrării vaccinurilor, dar și evidența și diseminarea informațiilor cu privire la investigarea evenimentelor de sănătate publică;

2) Registrul electronic de evidență a vaccinării împotriva COVID-19 (în continuare RVC-19)

– sistem informatic ce asigură înregistrarea setului de date necesar pentru evidența persoanelor vaccinate împotriva COVID-19. Registrul RVC-19 conține informații despre persoanele imunizate și vaccinurile administrate și este interconectat la platforma electronică de generare a certificatelor digitale de vaccinare împotriva COVID-19.

3) Sistemul informatic de laborator (în continuare - LIS) – sistem informatic pentru prelucrarea și stocarea informațiilor despre 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. LIS presupune gestiunea întregului ciclu de viață a unei solicitări/necesități de investigații în 3 etape:

a) pre-analitic – recepționarea înregistrărilor; prelevare probe; managementul solicitărilor;

b) analitica – generarea sarcinilor de investigații (work list); controlul și monitorizarea sarcinilor; interacțiunea cu echipamentul de laborator care realizează investigația; managementul calității; gestiune alerte;

c) post-analitica – validarea clinică și tehnică a rezultatelor; emitere rezultate/rapoarte; notificarea pacienților și instituțiilor medicale prin diverse mijloace electronice; arhivare.

4) Soluția informatică pentru monitorizarea incidenței unei boli transmisibile, persoanelor supuse regimului de autoizolare, contactilor, 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, contacte și evenimente. Monitorizarea prevede gestionarea cazului confirmat de boală, sau a unei persoane aflate în

regim de autoizolare și colectarea datelor despre statutul de boală, stării 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 este format din 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 din 29 iulie 1994;
- 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 și 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 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 desemnată electronică (MSign);

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

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

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

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

24) 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;

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

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

27) 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;

28) 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);

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

30) 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;

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

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

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

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

35) 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 medicală;

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

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 evenimentelor de sănătate publică, cărora li se atribuie un număr de identificare, și informațiilor cu privire la gestiunea lor, pe întreg ciclul de viață. Funcțiile de bază la formarea bazei de date sunt înregistrarea și actualizarea datelor, precum și radierea obiectelor informaționale:

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

b) actualizarea datelor. Constă în actualizarea sistematică a bazei de date, la 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 urmare a proceselor de laborator:

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

b) gestiunea probelor și 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 la vaccinare;
 - e) evidența reacțiilor adverse la administrarea preparatelor imunobiologice.
- 4) formarea bazei de date ce permite monitorizarea contactilor (*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 contactilor;
 - c) identificarea relațiilor dintre înregistrările individuale cu focarele/evenimentele existente;
 - d) vizualizarea cazurilor și contactilor în regim de tablou de bord;
 - e) vizualizarea lanțurilor de transmitere;
 - f) generarea rapoartelor.
- 5) asigurarea informațională. Informația din SI SBTESP este pusă la dispoziție autorităților din domeniul sănătății, altor autorități publice, furnizorilor/destinatarilor/utilizatorilor de date, precum și a participanților la SI SBTESP. Nivelul de acces la SI SBTESP este stabilit prin regulament și prevederile legislației.
- 6) administrarea informațională, care 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;
 - e) asigurarea calității informațiilor din contul creării și menținerii componentelor SI SBTESP;
 - f) protecția și securizarea informațiilor la toate etapele de formare a bazei de date a SI SBTESP, cu utilizarea metodelor de autentificare a utilizatorilor, de autorizare conform rolului atribuit, 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, grupate în contururi funcționale specifice, care sunt realizate prin intermediul componentelor SI SBTESP:

13. Conturul Sistemul Informațional de notificare a cazurilor și

evenimentelor de sănătate publică:

a) modulul notificări – componenta de bază a SI SBTESP, care asigură crearea, înregistrarea, notificarea și gestiunea cazurilor de boală infecțioasă, evenimentelor de sănătate publică și rezultatul anchetei epidemiologice;

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

c) modulul Alerte – componenta responsabilă de alertarea/notificarea utilizatorilor cu privire la anumite evenimente, care necesită gestionate, sau despre care necesită să fie informați;

d) modulul de raportare - componenta pentru generarea rapoartelor statistice;

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

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

14. Conturul Registrul electronic "Vaccinare Covid-19" va conține următoarele module și moduri:

a) modul de programare la vaccinare;

b) modului lista de așteptare;

c) modul de înregistrare a dozelor de vaccin;

d) modul de înregistrare a evenimentelor adverse post imunizare;

e) modul de generare a certificatelor COVID-19;

f) modulul de raportare;

g) modulul de management a stocurilor de vaccin;

h) modulul de raportare grafică.

15. Conturul Sistemul informațional de laborator:

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

b) modulul de înregistrare a rezultatelor de laborator;

c) modului de eliberare a rezultatului investigației;

d) modului de generare a rapoartelor investigațiilor de laborator;

e) modul de interoperabilitate.

16. Conturul Monitorizarea cazurilor și contactilor:

a) modulul de evidență și gestiune a contactilor;

b) modul de vizualizare a datelor;

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

d) modul de contactare și supervizare a cazurilor;

e) 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 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 Informațional este Agenția Națională pentru Sănătate Publică din subordinea Ministerului Sănătății, care este responsabilă de crearea, administrarea, mentenanța și dezvoltarea SI SBTESP informațional.

20. Administratorul tehnic al SI SBTESP este Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” care va asigura administrarea tehnică și menținerea SI SBTESP informațional 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 ai SI SBTESP sunt lucrătorii medicali, personalul responsabil din cadrul prestatorilor de servicii medicale, prestatorii de servicii medicale departamentale, instituțiilor de asistență socială și de reabilitare și recuperare, centrelor de plasament temporar, centrelor de sănătate publică, Agenției Naționale pentru Sănătate Publică, laboratoarele medicale, Centrul 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 Medicamentelor 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. Destinatari și utilizatori ai datelor din Sistem sunt autoritățile publice centrale și locale, persoanele fizice sau unităților de drept mandatate cu dreptul de a le primi informații conform prevederilor legale.

Capitolul VI DOCUMENTELE SI SBTESP

25. Documentele utilizate de SI SBTESP sunt documentele 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:

- a) fișa de notificare urgentă despre depistarea cazului de boală infecțioasă, intoxicație, toxiinfecție alimentară sau profesională acută, reacție adversă la administrarea preparatelor imunobiologice;
- b) fișa de evidență a bolilor (intoxicațiilor) profesionale;
- c) fișa de evidență a stocului de vaccinuri, diluanți, seringi;
- d) Fișa de anchetare epidemiologică a focarului de boală infecțioasă;
- e) fișa medicală a bolnavului de staționar cu anexe;
- f) registru de evidență a vaccinărilor;
- g) registru de evidență a bolilor infecțioase;
- h) registru de evidență a persoanelor cu intoxicație profesională sau boală profesională depistatăcaz nou;
- i) registru de evidență a stocurilor primite de preparate imunobiologice, instrumente și utilajemedicale în centrele de sănătate publică;
- j) aviz despre bolnavul cu diagnosticul stabilit caz nou de tuberculoză activă;
- k) aviz privind boala sau intoxicație profesională cronică;
- l) actul de prelevare a probelor (mostrelor);
- m) actul de înapoiere a probelor (mostrelor);
- n) actul de decontare a probelor (mostrelor);
- o) proces-verbal de codificare a probelor (mostrelor);
- p) proces-verbal de recoltare a probelor de apă;
- q) proces-verbal de examinare a cazului (suspiciunii) de boală (intoxicație) profesională;
- r) proces-verbal de evidență a bolilor (intoxicațiilor) profesionale;
- s) trimitere la analiză;
- t) trimitere la investigații;
- u) certificat medical (de recuperare, de testare);
- v) certificat de vaccinare.

27. Documentele de ieșire sunt:

- a) fișa de anchetare epidemiologică a focarului cu infecția HIV/SIDA;
- b) fișa de anchetare epidemiologică a cazului de hepatită virală B, C și D acută;
- c) fișa de colectare a datelor epidemiologice a cazului de hepatită virală B, C și D cronică;
- d) fișa de evidență a purtătorului cronic de germeni patogeni;
- e) fișa de anchetare epidemiologică a focarului de boală infecțioasă ;
- f) registru investigațiilor;
- g) registru cazurilor de intoxicații;
- h) registru fișelor de declarații;
- i) registru de evidență a accidentelor la locul de lucru;
- j) registru de evidență a probelor de laborator;
- k) Formular privind rezultatele investigațiilor de laborator;
- l) proces-verbal de investigații;
- m) proces-verbal de recoltare;
- n) trimitere medicală pentru investigații;
- o) certificat medical (de recuperare, de testare);
- p) certificat de vaccinare;
- q) rapoarte analitice și statistice;
- r) altele.

28. documente tehnologice sunt:

- a) instrucțiuni metodice, ghiduri și regulamente pe diferite nozologii;
- b) protocoale clinice naționale;
- c) formulare și rapoarte aprobate de către Biroul Național de Statistică;
- d) lista utilizatorilor și drepturilor acestora;
- e) înregistrările de audit ale activității SI SBTESP și utilizatorilor.

Capitolul VII

SPAȚIUL INFORMAȚIONAL AL SI SBTESP

Secțiunea 1

Obiectele informaționale ale SI SBTESP

29. Principalele obiecte informaționale ale SI SBTESP sunt:

Totalitatea actelor oficiale care confirmă starea de sănătate a persoanei și include următoarele:

- 1) fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică;
- 2) trimitere/fișa de investigații de laborator.
- 3) certificate:
 - a) de vaccinare;

- b) de recuperare;
- c) de testare;
- 4) persoane fizice și unități de drept:
 - a) pacienți;
 - b) lucrători medicali;
 - c) prestatori de servicii medicale;
 - d) prestatori de servicii sociale etc.

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

- 1) numărul epidemiologic unic al notificării;
- 2) date cu privire la diagnosticul primar;
- 3) date de identificare a pacientului;
- 4) date cu privire la înregistrarea cazului în SI SBTESP;
- 5) date cu privire la simptomele și manifestările bolii;
- 6) date cu privire la diagnosticul final.

31. Atributele obiectului informațional „trimitere/fișa de investigații de laborator”

- 1) numărul de identificare/înregistrare al investigației de laborator;
- 2) tipul analizei investigației de laborator;
- 3) date de identificare a pacientului;
- 4) date despre boală;
- 5) date privind rezultatele de laborator.

32. Atributele obiectului informațional „Certificate”:

- 1) date despre certificatul de vaccinare;
- 2) date despre certificatul de recuperare;
- 3) date despre certificatul de testare.

33. Atributele obiectului informațional „persoane fizice”:

- 1) pacienți:
 - a) date de identificare (IDNP, nume, prenume, sex, data nașterii);
 - b) date demografice (cetățenie, tipul documentului de identificare, numărul documentului, data emiterii);
 - c) adresa de domiciliu și/sau de reședință temporară (localitate, strada, bloc, apartament);
 - d) date privind asigurarea medicală (categoria și statutul de asigurat, tipul de asigurare);
 - e) date socioeconomice (locul de muncă/studii).
- 2) lucrători medicali:
 - a) date de identificare (IDNP, nume, prenume, sex, data nașterii);
 - b) date demografice (cetățenie, tipul documentului de identificare, numărul

documentului);

c) adresa de domiciliu și/sau de reședință temporară (localitatea, strada, bloc, apartament);

d) date privind asigurarea medical (categoria și statutul de asigurat, tipul de asigurare);

e) date socioeconomic (locul de muncă/studii).

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

a) numărul de identificare de stat – IDNO;

b) denumirea;

c) codul IMS;

d) tip;

e) număr de telefon;

f) adresă 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 Conturul SAE a SI SBTESP și care 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 care începe cu 000001 în fiecare an.

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

37. Identificatorul obiectului informațional „Certificate” este constituit dintr-un număr unic generat de către Conturul Registrul electronic „Vaccinare Covid-19” generat conform logicii și regulilor predefinite.

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 și unitățile de drept sunt accesibile din Registrul de stat al populației și 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. Scenariile de bază reprezintă lista evenimentelor aferente obiectului informațional luat în evidență în SI SBTESP, după cum urmează:

1. Notificarea cazurilor și evenimentelor de sănătate publică – reprezintă o soluția pentru crearea și administrarea notificărilor despre cazurile de boli transmisibile și evenimentele de sănătate publică. Aceasta presupune automatizarea procesului de înregistrare și gestiune a notificărilor și a informațiilor relevante, cum ar fi, diagnostic primar; diagnostic final; simptome/manifestări ale bolii; concluzii din anchetare; rezultatele investigațiilor de laborator, informații cu privire la vaccinare, dar și evidența și diseminarea informațiilor cu privire la investigarea evenimentelor de sănătate publică.

Scenariul de bază reprezintă notificarea evenimentelor cum sunt:

1. Boli transmisibile

- 1) boli prevenibile prin vaccinări;
- 2) boli cu transmitere sexuală;
- 3) hepatite virale;
- 4) infecția cu HIV/SIDA;
- 5) boli cu factor de transmitere alimentar;
- 6) boli cu factor de transmitere hidric și care provin din mediul înconjurător;
- 7) alte boli transmisibile prin agenți neconvenționali ;
- 8) boli cu transmitere aerogenă;
- 9) boli transmisibile care pot duce la apariția urgențelor de sănătate publică cu risc de răspândire internațională;
- 10) boli transmise prin vectori;
- 11) zoonoze (comune pentru animale și om);
- 12) alte boli transmisibile cu importanță pentru sănătatea publică, inclusiv bolile cauzate prin răspândire deliberată.

2. Probleme speciale de sănătate

- 1) infecții nosocomiale;
- 2) rezistență antimicrobiană;
- 3) reacții adverse și complicații postvaccinale.

3. Evenimente de sănătate publică

Intoxicație, toxiinfecție alimentară și profesională acută, evenimentelor de sănătate publică,

investigațiilor de laborator, precum și altor informații relevante, în vederea stocării, sistematizării și actualizării.

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

a) monitorizare epidemiologică – este realizat de către epidemiolog regional/raional pentru monitorizare în limita unui spațiu bine determinat sau epidemiolog național la nivel de țară;

b) cazuri de grup - este realizat de către medicul epidemiolog din teritoriile administrative pentru monitorizare în limita unui spațiu bine determinat sau epidemiolog național la nivel de țară.

2) gestiune evenimente de sănătate publică:

a) monitorizarea – este realizată de către toți actorii sistemului de sănătate, activități aplicate prioritar la nivel de individ, orientate spre preîntâmpinarea sau diminuarea probabilității apariției bolilor transmisibile sau netransmisibile, a răspândirii lor și spre prevenirea recidivelor și complicațiilor;

b) prevenire - activități aplicate prioritar la nivel de individ, orientate spre preîntâmpinarea sau diminuarea probabilității apariției bolilor transmisibile sau netransmisibile, a răspândirii lor și spre prevenirea recidivelor și complicațiilor;

c) identificare – realizată prin prisma sistemului de management în sănătate și cuprinde identificarea apariției riscului iminent de răspândire a unei boli sau a unui eveniment de sănătate care determină probabilitatea înaltă a unui număr mare de decese și unui număr mare de dizabilități în rândul populației afectate ori care determină expunerea largă la acțiunea unui agent biologic, chimic sau fizic ce poate cauza în viitor riscuri semnificative pentru un număr substanțial de persoane asupra populației afectate;

d) aplicarea măsurilor – ansamblu de măsuri cu caracter administrativ, economic, medical, social și de menținere a ordinii publice în caz de pericol sau declanșare a urgențelor de sănătate publică în scopul prevenirii, diminuării și lichidării consecințelor acestora.

Scenarii:

1) Înregistrarea unei notificări noi poate fi efectuată sau de către o persoană cu drept de înregistrare, direct în sistem, sau prin intermediul MConnect cu alte sisteme ce vor furniza datele respectând anumit standard. Notificările ce vor fi furnizate de către alte sisteme vor conține setul minim de date, ceea ce presupune că ele vor fi preluate în investigație sau transferate către alte instituții.

2) Înregistrarea anchetei are loc în timpul sau după efectuarea acesteia de către specialiști.

3) Solicitare de investigații de laborator și obținerea rezultatelor investigațiilor.

4) Transfer. În unele cazuri persoanele se deplasează cu sediul în alte locații ceea ce presupune că este posibilă modificarea instituției de evidență a cazului. În cazul dat se efectuează procedura de transfer dintr-o instituție în alta. În istoria notificării se vor păstra toate transferurile. Transferul poate fi efectuat de un utilizator din instituția de evidență a cazului sau de utilizatori din CSP din

arealul de care este responsabil. Utilizatorii din ANSP poate necondiționat să transfere cazul dintr-o instituție în alta.

5) Înregistrare cazuri de grup – este realizat de către specialiștii CSP din teritoriile administrative pentru monitorizare în limita unui spațiu bine determinat sau specialiștii ANSP la nivel de țară.

2. Gestionare evenimente de sănătate publică:

1) monitorizarea – este realizată de către toți actorii sistemului de sănătate, activități aplicate prioritar la nivel de individ, orientate spre preîntâmpinarea sau diminuarea probabilității apariției bolilor transmisibile sau netransmisibile, a răspândirii lor și spre prevenirea recidivelor și complicațiilor;

2) prevenire – activități aplicate prioritar la nivel de individ, orientate spre preîntâmpinarea sau diminuarea probabilității apariției bolilor transmisibile sau netransmisibile, a răspândirii lor și spre prevenirea recidivelor și complicațiilor;

3) identificare – realizată prin prisma sistemului de management în sănătate și cuprinde identificarea apariției riscului iminent de răspândire a unei boli sau a unui eveniment de sănătate care determină probabilitatea înaltă a unui număr mare de decese și unui număr mare de dizabilități în rândul populației afectate ori care determină expunerea largă la acțiunea unui agent biologic, chimic sau fizic ce poate cauza în viitor riscuri semnificative pentru un număr substanțial de persoane asupra populației afectate;

4) aplicarea măsurilor – ansamblu de măsuri cu caracter administrativ, economic, medical, social și de menținere a ordinii publice în caz de pericol sau declanșare a urgențelor de sănătate publică în scopul prevenirii, diminuării și lichidării consecințelor acestora.

5) reprezentarea grafică a situației în spațiu, prezintă un raport grafic cu date agregate pe harta Moldovei, cu posibilitate de definire a anumitor parametri.

6) alerte. Modul ce conține anumite reguli și parametri predefiniți, ce generează alerte în dependență de spațiu, timp, cantitatea persoanelor depistate cu maladii identice sau parametrul evenimentului.

7) rapoarte. Modul ce permite generarea datelor atât agregate cât și dezagregate.

După finisarea monitorizării cazului, cazul este arhivat, iar păstrarea datelor se va aplica în conformitate cu reglementările aprobate de Ministerul Sănătății privind formularele de evidență medicală primară, ulterior SI SBTESP în mod automatizat va depersonaliza și arhiva cazurile, în vederea asigurării disponibilității datelor de importanță pentru serviciul de sănătate publică.

3. Registrul electronic de evidență a vaccinării împotriva COVID-19 (în continuare RVC-19) – sistem informatic ce asigură înregistrarea setului de date necesar pentru evidența persoanelor vaccinate împotriva COVID-19. Registrul RVC-19 conține informații despre persoanele imunizate și vaccinurile administrate și este interconectat la platforma electronică de generare a certificatelor digitale de vaccinare împotriva COVID-19, cu următoarele componente:

- înregistrare vaccinare;
- omologare certificate;
- programare;
- lista de așteptare;
- rapoarte detaliate și agregate;
- modificare date;
- eliberare certificate.

Componenta de vaccinare conține date demografice despre persoana vaccinată, vaccinul aplicat și instituția în care și când s-a efectuat vaccinarea.

Omologarea certificatelor conține informația despre vaccinare în altă țară, date demografice a persoanei și în cazurile omologării manuale se aplica o doza noua de vaccin cu indicarea lui, instituția și data efectuării acesteia.

Programarea conține date despre persoana programata, locul și data pentru efectuarea vaccinării.

Lista de așteptare conține date despre persoana care este dispusa sa fie vaccinată.

Rapoartele sunt dimensionate atât ca conținut fie agregat fie dezagregat, cât și în spațiu și timp, în dependență de rolul și instituția utilizatorului.

Scenarii:

1) Aplicarea vaccinului.

La prezentarea primară a persoanei la punctul de vaccinare, operatorul completează datele demografice, în cazul persoanei ce deține IDNP se identifică prin extragerea datelor din RSP sau în cazul persoanei fără IDNP se utilizează opțiune *Act fără IDNP, și datele despre vaccinul aplicat persoanei.

La prezentarea următoare a persoanei la punctul de vaccinare, operatorul caută persoana în registru, după identificare, se efectuează o înregistrare doar cu indicarea vaccinului aplicat persoanei.

2) Omologare.

Este o funcționalitate ce permite înregistrarea vaccinării efectuate peste hotare. Ficționalitatea este posibilă atât în regim manual cât și automat.

Înregistrarea automată presupune că persoana deține IDNP și un certificat cu QR recunoscut sau eliberat în UE. Persoana accesează pagina dedicată și scanează QR. Dacă conținutul QR este valid, atunci persoanei i se solicită să introducă IDNP și să permită procesarea datelor. În cazul verificărilor validate cu succes, în registru se va crea o inscripție noua despre persoana vaccinată.

Înregistrarea manuală presupune că persoana se prezintă la o instituție medicală ce vaccinează, prezintă certificatul de vaccinare eliberat în orice țară și actul de identitate. Operatorul v-a înregistra aceste certificate cu condiția că persoanei i se aplică o doză nouă cu inscripția respectivă în registru.

3) Programare

Programarea poate fi efectuată de către persoană sau de către un operator din instituția medicală.

În cazul când persoana se programează de sine stătător, el accesează o pagină dedicată, se identifică și selectează locul și timpul unde dorește să se vaccineze. După înregistrarea cu succes pe ecran se va afișa mesajul respectiv cu datele relevante programării. Dacă persoana a indicat e-mail atunci pe adresa indicată se va expedia un mesaj de confirmare cu datele relevante programării.

În cazul programării de către operator, operatorul va opera doar în limitele instituției în care activează, ceea ce presupune că el poate programa doar la punctele de vaccinare ale instituției. Se face înscrierea datelor personale a persoanei și se va indica punctul de vaccinare și ora.

4) Lista de așteptare

Persoana accesează o pagină dedicată în care completează datele personale, de contact și instituția medicală de evidență primară. După completare, persoana va indica una sau mai multe opțiuni cheie de disponibilitate pentru vaccinare: dorește să se vaccineze la medicul de familie, dorește să se vaccineze la locul de trai sau este disponibil indiferent de loc și instituție.

Pe de altă parte, operatorii listei de așteptare, în baza la anumiți criterii, pot selecta persoanele din lista de așteptare pentru contactarea lor și invitare la vaccinare.

5) Modificare date

Modificarea datelor se efectuează prin identificarea persoanei după identificatorul unic și redactarea datelor introduse în registru, fie date despre vaccinare fie date demografice.

6) Rapoarte

În sistem există două tipuri de rapoarte. Primul tip se referă la datele nominale și este accesibil doar instituțiilor medicale ce vaccinează cu accesarea listei persoanelor vaccinate doar de instituția medicală. Al doilea tip sunt rapoartele statistice sau agregate, care sunt accesibile absolut pentru toate instituțiile.

7) Eliberare certificate

Eliberarea certificatelor se face în baza la identificarea persoanei după doi parametri, identificator unic și data naștere. Această opțiune este disponibilă atât de pe pagina oficială de descărcare a certificatelor COVID 19 cât și pentru utilizatorii registrului.

Păstrarea datelor personale la moment sunt condiționate și reglementate de faptul necesității eliberării certificatelor COVID-19 și necesității vaccinării repetate.

4. Laborator – sistem informatic pentru prelucrarea și stocarea informațiilor despre 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. Presupune gestiunea întregului ciclu de viață a unei solicitări/necesități de investigații în 3 etape:

a) pre-analitic – recepționarea înregistrărilor; prelevare probe;

managementul solicitărilor;

b) analitica – generarea sarcinilor de investigații (work list); controlul și monitorizarea sarcinilor; interacțiunea cu echipamentul de laborator care realizează investigația; managementul calității; gestiune alerte;

c) post-analitica – validarea clinică și tehnică a rezultatelor; emitere rezultate/rapoarte; notificarea pacienților și instituțiilor medicale prin diverse mijloace electronice; arhivare.

Sistemul asigură operațiunile necesare:

- 1) programarea probelor;
- 2) înregistrare și etichetare (cod de bare) cu atribuirea unui număr unic atât pentru probe planificate, cât și pentru cele neprogramate;
- 3) atribuirea fiecărei probe a unei liste de parametri definiți cu indicarea unei anumite metode de analiză;
- 4) distribuirea probelor cu analize alocate subdiviziunilor specifice, executanți, dispozitive;
- 5) introducerea rezultatelor analizei;
- 6) verificarea rezultatelor introduse prin compararea acestora cu criteriile specificate, prevenind erorile tehnice la introducerea rezultatelor;
- 7) conectarea fiecărui rezultat obținut cu procedurile relevante de management al calității și de asigurare a calității (verificarea, calibrarea echipamentelor de măsurare, controlul calității și admiterea la analiza consumabilelor, disponibilitatea și valabilitatea materialelor de referință, evidența graficelor de control);
- 8) validarea rezultatelor introduse în conformitate cu responsabilitatea angajaților;
- 9) emiterea de protocoale (rapoarte) cu rezultatele testelor;
- 10) realizarea diferitelor rapoarte privind rezultatele activităților;
- 11) asigurarea schimbului de date și interoperabilitatea cu alte sisteme informatice electronice.

Scenariu:

- 1) persoana se prezintă la laborator, la ghișeu;
- 2) se prelevează material pentru investigare;
- 3) se creează o cerere pentru investigare cu indicarea parametrilor necesari și materialul investigat;
- 4) proba se codifică și se transmite în zona de investigare;
- 5) proba se recepționează către investigare și se efectuează investigarea;
6. după înregistrarea rezultatelor investigației, rezultatul se validează;
7. după validarea rezultatelor, la ghișeu se eliberează rezultatele.

Alternativ:

- 1) cererea pentru investigație vine din sisteme externe; 2) în laborator, la ghișeu, se recepționează probele;
- 3) proba se codifică și se transmite în zona de investigare;
- 4) proba se recepționează către investigare și se efectuează investigarea;

- 5) după înregistrarea rezultatelor investigației, rezultatul se validează;
- 6) după validarea rezultatelor, la ghișeu se eliberează rezultatele;
- 7) rezultatele se transmit către sistemele de unde a venit solicitarea.

5. Monitorizarea cazurilor și contactilor

Persoanelor supuse regimului de autoizolare, contactilor, 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, contacte și evenimente. Monitorizarea prevede gestionarea cazului confirmat de boală, sau a unei persoane aflate în regim de autoizolare și colectarea datelor despre statutul de boală, stării de sănătate a persoanelor. Aceasta presupune automatizarea procesului de contactare, cu completarea șabloanelor standard privind statutul cazului și a informațiilor privind evoluția bolii și din notificarea cazurilor și evenimentelor de sănătate publică sau cazurile de grup, ce oferă utilizatorilor instrumente necesare pentru a:

- 1) vizualiza cazul critic, contactul, și înregistrările privind un focar;
- 2) înregistra datele care sunt absolut esențiale pentru a monitoriza un focar;
- 3) crea vizualizări pentru a ajuta în monitorizarea unui focar;
- 4) urmări activitățile de monitorizare pentru un focar specific;
- 5) identifica relațiile între înregistrările unui focar individual.

Pentru a utiliza efectiv instrumentul, trebuie percepute conceptele utilizate în cadrul investigației și monitorizarea focarului.

Următoarea listă definește conceptele critice pentru gestionarea unui focar:

1) Caz: Un caz este o persoană care întrunește definiția de caz epidemiologic pentru un focar de o anumită maladie.

2) Cluster: Un cluster este o grupare de cazuri, contacte și evenimente care dispun de expuneri existente sau relații de contact pentru un anumit focar. În general, clusterelor sunt create atunci când există o relație potențială în baza evidențelor, dar nu sunt sigur privind modul în care evidențele se corelează.

3) Contact: Un contact este o persoană despre care se crede că este în situație de risc din cauza expunerii la un caz sau un eveniment.

4) Vizualizarea datelor. O vizualizare a datelor este o diagramă sau un grafic care afișează relațiile din cadrul focarului și lanțurile de transmitere. După ce ați creat cazuri, contacte și evenimente și relațiile între acestea cu direcția și nivelul de certitudine a transmiterii, sistemul poate genera o rețea de relații drept un lanț al graficului de transmitere.

5) Eveniment: Un eveniment este o adunare specifică în comunitate unde se crede că a avut loc transmiterea unei maladii care stă la baza focarului. Exemple de evenimente tipice includ clinici, concerte, funeralii, piețe, adunări în masă, școli și evenimente sportive.

6) Monitorizare: O monitorizare este un exercițiu realizat de monitorii contactelor pentru a urmări sănătatea fiecărui contact drept urmare a potențialei expuneri. Frecvența și durata unei monitorizări este determinată de boala

suspectată, care servește drept sursă a focarului.

7) Focar: Un focar de o maladie implică survenirea în exces a cazurilor de boală în comparație cu așteptarea obișnuită. Focarele de boli sunt de obicei cauzate de o infecție, transmisă prin contact de la persoană la persoană, contact de la animal la persoană sau din mediul ambiant sau alte medii. Focarele pot surveni și drept expunere la agenți chimici sau materiale radioactive. Ocazional, cauza unui focar nu este cunoscută, chiar și după investigații minuțioase.

Scenariu:

1) Gestionarea focarelor – funcționalitatea este pentru a crea o nouă incidență de boală cunoscută sau necunoscută. După ce este creată, se setează focarul ca fiind activ pentru a începe investigarea și înregistrarea datelor privind cazuri, contacte și evenimente. Focarele de asemenea poate fi creat în baza la șabloane de focare pentru un șir de boli care implică transmiterea de la om la om și un șablon general pentru boli necunoscute. Este posibil de asemenea crea și șabloane noi în dependență de necesitățile unei investigații.

2) Gestionare cazuri – funcționalitatea oferă epidemiologilor și managerilor de date instrumente pentru a gestiona datele cazului.

Modulul cu privire la caz urmărește informațiile personale, de locație și cele epidemiologice pentru o persoană în timp în legătură cu un focar specific. Acesta de asemenea urmărește formularul de investigare a cazului și relațiile cu alte cazuri, contacte și evenimente.

Cu ajutorul funcționalității de gestionare a cazurilor, este posibil de adăugați, modificat și șterge cazuri. De asemenea este posibil de a stabili relații cu alte cazuri, contacte și evenimente. De exemplu, vizualizare relațiile unui caz cu alte cazuri, contacte sau evenimente, sau partaja relații existente între două persoane. Modulul Cazuri de asemenea include vizualizarea mișcării cazului (în baza istoricului adresei), linia cronologică a datelor importante în istoria epidemiologică și câteva rapoarte.

8) Gestionare contacte – contactele sunt persoanele cu care este asociat un caz. Uneori contactele încep să dea dovadă de semne de boală și devin un caz și respectiv contactul este transformat în caz.

Cazurile ar putea avea unul sau mai multe contacte. Contactele sunt relevante doar când sunt legate de un caz sau un eveniment; din aceste considerente, trebuie de adăugat contactul de la un caz sau un eveniment. Contactele cazului, fie că în listă liniară sau individual, reprezintă o parte importantă a managementului focarului. De exemplu, dacă se dorește să se partajeze contactele selectate, se poate utiliza lista Contacte caz. Dacă se dorește să se modifice un contact, se poate utiliza Detalii caz pentru contactul specific.

Aceste vizualizări permit să se vizualizeze înregistrările contactelor în cadrul unui focar selectat, pentru a iniția acțiuni sau pentru a vedea rapoarte.

Lista Contacte caz: o singură locație pentru a vizualiza toate înregistrările contactelor ce țin de un caz. Detalii contact: o singură locație pentru a vizualiza înregistrările contactului pentru o anumită persoană ce ține de un caz.

9) Gestionare clustere - funcționalitatea oferă posibilitatea de a grupa împreună cazuri, contacte și evenimente cu relații existente în clustere. Utilizând clusterelor, este posibil de a descrie în continuare legăturile între un set de transmițeri, care se crede că este legat de un factor semnificativ.

Utilizând funcționalitatea se cere doar să se definească un nume și descrierea când este creat clusterul, ceea ce permite să fie urmărite legăturile între cazuri, contact și evenimente pentru orice model care apare pe parcursul procesului de investigare a focarului.

După închiderea focarului păstrarea datelor se va aplica în conformitate cu reglementările aprobate de Ministerul Sănătății privind formularele de evidență medicală primară, ulterior SI SBTESP în mod automatizat va depersonaliza și arhiva cazurile, în vederea asigurării disponibilității datelor de importanță pentru serviciul de sănătate publică.

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, dar care nu se limitează la:

- 1) internaționale:
 - a) Clasificatorul internațional al maladiilor;
 - b) Clasificatorul internațional al țărilor.
- 2) naționale:
 - a) Clasificatorul oficial a unităților administrativ – teritoriale ale Republicii Moldova;
 - c) Nomenclatorul prestatorilor de servicii medicale;
 - d) Nomenclatorul prestatorilor privați de servicii de sănătate;
 - e) Nomenclatorul investigațiilor de laborator;
 - f) Clasificatorul tipului prestatorilor de servicii medicale;
 - g) Clasificatorul tipurilor cazurilor;
 - h) Clasificatorul tipurilor de boli;
 - i) Clasificatorul condițiilor ce au favorizat infectarea;
 - j) Clasificatorul simptomelor neurologice;
 - k) Clasificatorul simptomelor respiratorii;
 - l) Clasificatorul simptomelor digestive;
 - m) Clasificatorul tipurilor de produse alimentare;
 - n) Clasificatorul surselor de apă;
 - o) Clasificatorul tipurilor parezelor/paraliziilor;
 - p) 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 SISBTESP.

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 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, autoritățile și instituțiile publice (Expeditori) expedierea notificărilor către utilizatori (Destinatari) în vederea înștiințării acestora, despre evenimentele produse în legătură cu prestarea serviciilor sau altor evenimente relevante destinatarilor;

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

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

Capitolul VIII

SPAȚIUL TEHNOLOGIC AL SI SBTESP

44. SI SBTESP este proiectat 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 3 niveluri:

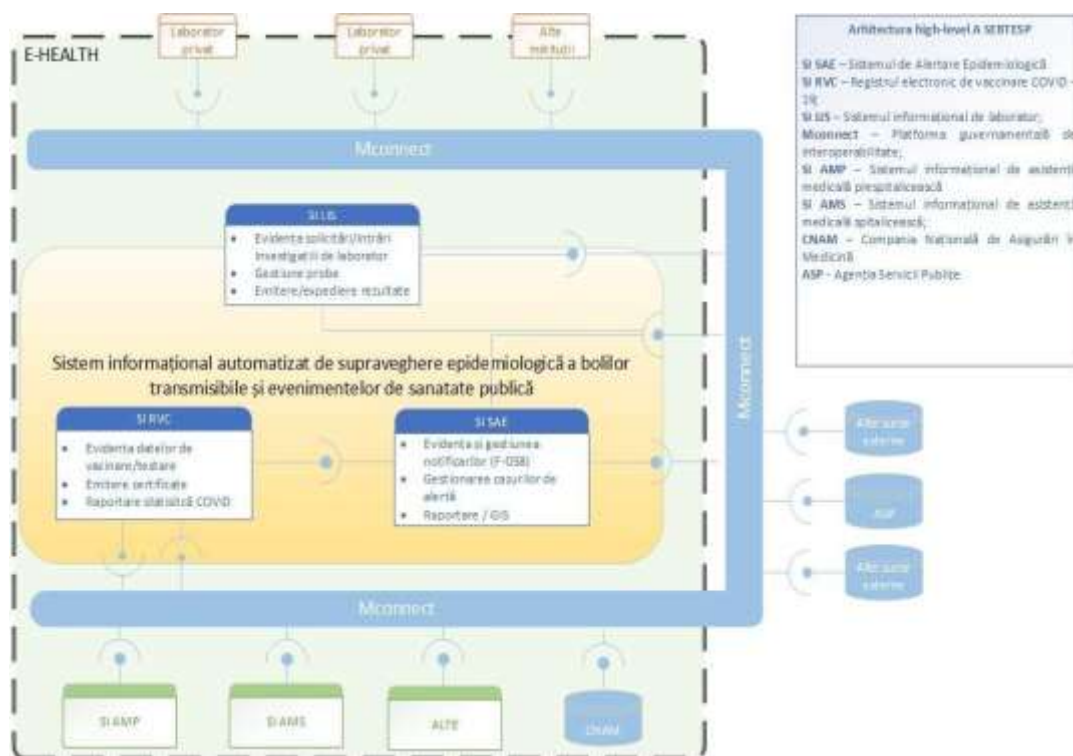
- 1) nivelul de interfață – serverul pentru paginile web cu formularele utilizatorilor și informațiile din baza de date pentru vizualizare și utilizare prin intermediul browserului stației de lucru;
- 2) produsul program al nivelului de mijloc – serverul aplicațiilor care va susține partea client, ce 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, la etapele inițiale și ulterioare de elaborare și 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

48. Platforma tehnologică a SI SBTESP va fi găzduit 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 informaționale și infrastructurii de acțiuni intenționate sau accidentale, cu caracter natural sau artificial, al căror rezultat cauzează daune participanților la procesul de schimb de informație.

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

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

- 1) asigurarea confidențialității informației (prevenirea obținerii informațiilor de către persoanele care nu au drepturile și competențele respective);
- 2) asigurarea integrității logice a datelor (prevenirea introducerii, actualizării și ștergerii nesancționate a informației sau introducerea datelor denaturate);

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

52. Mecanismele principale de securitate informațională utilizate vor fi:

- 1) autentificarea și 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 la risc în sistemul de securitate este factorul uman. Din aceste considerente, instruirea personalului la capitolul însușirii metodicii rezistenței la amenințări informatice este un element foarte important.

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

- 1) Legea nr. 982/ 2000 privind accesul la informație;
- 2) Legea nr. 467/ 2003 cu privire la informatizare și 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. Reieșind din cele expuse, accesul la resursele SI SBTESP trebuie să fie asigurat și autorizat prin intermediul unui sistem de utilizatori și parole și autorizare 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 trebuie să existe posibilitatea de a defini rolurile și drepturile utilizatorilor (chiar și până la nivelul de acces la interfața utilizatorilor).

56. Accesul la informația bazei de date trebuie să fie limitat, în funcție de drepturile și 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 și gestionarea informației bazei de date, precum și de manipulare cu datele.

Orice modificare potențial periculoasă: modificarea informației unei înregistrări, marcarea la ștergere, adăugarea unor înregistrări noi etc. trebuie să

fie documentată în registre electronice speciale (fișiere log), arătând momentul de timp și utilizatorul care a efectuat modificarea potențial periculoasă. În caz că 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 securității informaționale trebuie să fie realizată prin intermediul unor module automate de generare a copiilor de rezervă a fișierelor și bazelor de date aflate în producție. Administratorii SI SBTESP trebuie să dispună de posibilitatea de a-și defini politica de generare automată a copiilor de rezervă.

58. În vederea asigurării unui nivel adecvat al securității informaționale a SI SBTESP se consideră binevenită elaborarea și implementarea unei politici de asigurare a securității 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 și automatizare a fluxurilor de date în sistemul de sănătate precum și digitalizarea proceselor de colectare, analiză, interpretare și diseminare sistematică și continuă a datelor cu privire la bolile transmisibile și evenimentele de sănătate publică, în scopul implementării măsurilor de sănătate publică, îmbunătățirea calității informațiilor, inclusiv a relevanței, integrității, oportunității, exactității, accesibilității, comparabilității, coerenței acestora, a face mai transparent și mai rapid procesul de luare 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 și a rechizitelor de birou și la îmbunătățirea calității și sporirea 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 și a soluțiilor de gestiune a accesului;

3) oferirea de informații autentice, veridice, curente și 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 și suport decizional ce presupune gestionarea situațiilor epidemiologice, evenimentelor și urgențelor de sănătate publică;

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

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

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

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.

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 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 10/2009 privind supravegherea de stat a sănătății publice, Legea nr. 133/2011 privind protecția datelor cu caracter personal, Hotărârea Guvernului nr. 1128/2004 cu privire la aprobarea Concepției Sistemului Informațional Medical Integrat, Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, Hotărârea Guvernului nr. 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 de boli infecțioase și evenimentelor 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, III. ATRIBUȚIILE ACESTORA

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

- 1) proprietarul;
- 2) posesorul;
- 3) deținătorul;
- 4) administrator tehnic;
- 5) registratorul;
- 6) utilizatorul.

7. Proprietarul SI SBTESP este statul care realizează dreptul de proprietate, de gestionare și utilizarea 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 aceste 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 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 limita competențelor;

6) autorizează, 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 asigurării bunei funcționări ale SI SBTESP;

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 conturile 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, Hotărârea Guvernului nr. 1090/2017 cu privire la organizarea și funcționarea Agenției Naționale pentru Sănătatea Publică și 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. Administrator 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 ai SI SBTESP sunt lucrătorii medicali, persoanele responsabile din cadrul prestatorilor de servicii medicale, prestatorii de servicii medicale departamentale, instituțiilor de asistență socială și de reabilitare și recuperare, centrelor de plasament temporar, centrelor de sănătate publică, laboratoarele medicale, Agenției Naționale pentru Sănătate Publică, Centrului Național de Transfuzie a Sângelui.

16. Registratorii au următoarele atribuții:

1) asigură colectarea, introducerea informațiilor relevante în baza de

date a SI SBTESP, în termenele și condițiile stabilite;

- 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 în utilizarea SI SBTESP;
- 6) înaintează propuneri de îmbunătățire și dezvoltare a SI SBTESP, participă în grupurile de lucru organizate în scopul dezvoltării SI.

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, 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 privire la înregistrările din sistem;
- 4) să prezinte propuneri privind perfecționarea și eficientizarea SI SBTESP.

19. Utilizatorii ai 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 Medicamentelor 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 al 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 limita 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, vizualizeze, utilizeze și să prelucreze informațiile din SI SBTESP, în conformitate cu rolurile și drepturile stabilite;
- 4) să solicite și să primească de la posesorul și administratorul tehnic al SI SBTESP ajutor metodologic și practic pe probleme ce țin de funcționarea SI SBTESP.

IV. 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 și 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 133/2011 privind protecția datelor cu caracter personal;

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

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

4) la necesitate datele vor fi actualizate, iar datele incomplete sau inexacte vor fi ulterior rectificate sau 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, ulterior SI SBTESP în mod automatizat va depersonaliza și arhiva cazurile, în vederea asigurării disponibilității datelor de importanță pentru serviciul de sănătate publică.

V. 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 HG 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.

VI. 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 și 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 efectuarea acțiunilor descrise în Planul de continuitate al SI SBTESP 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 denaturarea datelor;

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

3) monitorizarea procesului de exploatare al 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 asigurării 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.

VII. 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.

**Notă informativă la proiectul Hotărârii de Guvern
cu privire la instituirea Sistemului Informațional de Supraveghere a Bolilor Transmisibile
și Evenimentelor de Sănătate Publică**

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului
Ministerul Sănătății și Agenția Națională pentru Sănătate Publică.
2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite
<p>Supravegherea bolilor transmisibile și evenimentelor de sănătate publică reprezintă un domeniu prioritar în supravegherea de stat a sănătății publice, precum este stipulat 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 forma de organizare juridică, sunt obligate să asigure evidență separată a bolnavilor de boli transmisibile și, în cazul depistării acestora, să informeze Serviciul de Supraveghere de Stat a Sănătății Publice în decurs de 24 de ore. 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 (ANSP).</p> <p>Totodată, sistemul informatic utilizat de ANSP pentru colectarea datelor despre înregistrarea cazurilor de boli transmisibile are multiple deficiențe atât la nivel fizic, cât și operațional. Sistemele de operare și 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 COVID-19 pentru monitorizarea situației epidemiologice și coordonarea eficientă a răspunsului la nivel național și teritorial.</p> <p>De menționat că, domeniul de supraveghere a bolilor transmisibile este relevant și în contextul angajamentelor externe asumate de către Republica Moldova; în conformitate cu art. 114, capitolul 21 din Acordul de Asociere cu Uniunea Europeană (2014), cooperarea vizează și componentul de supraveghere epidemiologică și controlul bolilor transmisibile, precum și sporirea capacității de pregătire pentru amenințări și urgențe la adresa sănătății publice.</p>
3. Principalele prevederi ale proiectului și evidențierea elementelor noi
<p>Prin prevederile prezentului proiect este stabilit modul de organizare și mecanismul de funcționare a Sistemului Informațional de Supraveghere Epidemiologică a Bolilor Transmisibile și Evenimentelor de Sănătate Publică (SI SBTESP).</p> <p>Acest sistem va asigura digitalizarea proceselor de colectare, analiză, interpretare și diseminare sistematică și continuă a datelor despre sănătate cu privire la bolile transmisibile și evenimentele de sănătate publică, în contextul răspândirii lor în timp, spațiu, grup de populație și analizei factorilor de risc de contractare a acestor boli. Este conceput ca un sistem unic de gestiune și evidență în domeniul supravegherii epidemiologice de stat al maladiilor transmisibile, care acoperă business-procese referitoare atât la activitatea ANSP, cât și la relațiile cu prestatorii de servicii medicale din sectoarele asistenței medicale.</p> <p>Scopul general al SI SBTESP constă în îmbunătățirea procesului de evidență, gestiune și raportare a cazurilor cu privire la boli transmisibile și evenimente de sănătate publică. Sistemul are următoarele obiective:</p> <p>1) digitizarea, automatizarea și eficientizarea proceselor direcționate spre îmbunătățirea prevenirii și controlului bolilor transmisibile și evenimentelor de sănătate publică;</p>

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 bolile transmisibile și evenimentele de sănătate publică.

Sistemul informațional SBTESP este format din următoarele **componente**:

1) *Sistemul informațional de notificare a cazurilor și evenimentelor de sănătate publică* – reprezintă o soluție informatică performantă pentru crearea și administrarea notificărilor despre cazurile de boli transmisibile și evenimentele de sănătate publică;

2) *Registrul electronic de evidență a vaccinării împotriva COVID-19* (în continuare RVC-19) – sistem informatic ce asigură înregistrarea setului de date necesar pentru evidența persoanelor vaccinate împotriva COVID-19. Registrul RVC-19 conține informații despre persoanele imunizate și vaccinurile administrate și este interconectat la platforma electronică de generare a certificatelor digitale de vaccinare împotriva COVID-19;

3) *Sistemul informatic de laborator* (în continuare LIS) – sistem informatic pentru prelucrarea și stocarea informațiilor despre 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;

4) *Soluția informatică pentru monitorizarea incidenței unei boli transmisibile* – persoanelor supuse regimului de autoizolare, contactilor, 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, contacte și evenimente.

De menționat, că *Registrul electronic de evidență a vaccinării împotriva COVID-19* a fost dezvoltat pe parcursul anului 2021 cu suportul partenerilor internaționali, resursele fiind alocate de către Organizația Mondială a Sănătății. În prezent, SI RVC-19 este un registru funcțional și nu necesită dezvoltarea ulterioară. Odată cu aprobarea proiectului de hotărâre de guvern, SIRVC-19 va fi integrat și va deveni parte componentă a Sistemului Informațional de Supraveghere a Bolilor Transmisibile și Evenimentelor de Sănătate Publică, având interferențe cu alte componente ale sistemului instituit, pentru a exclude fragmentarea sistemelor informatice aferente domeniului de boli transmisibile.

Conceptul SI SBTESP stabilește scopul, sarcinile și funcțiile sistemului, structura organizațională și baza normativă, necesare pentru crearea, implementarea, exploatarea și menținerea acestuia; definește obiectele informaționale și lista datelor care se păstrează în sistem; stabilește interacțiunea cu alte sisteme informaționale, în scopul colaborării și asigurării schimbului de date. Totodată, sunt stabilite elementele de infrastructura tehnologică și măsurile de asigurare a securității, confidențialității și integrității datelor prelucrate în cadrul sistemului, cu respectarea cerințelor față de asigurare a securității datelor cu caracter personal conform Hotărârii Guvernului nr.1123/2010.

Regulamentul privind organizarea și funcționarea SI SBTESP stabilește modul de înregistrare și evidență a datelor pentru toate componentele sistemului, circuitul electronic al documentelor în cadrul sistemului, precum și schimbul de informații cu alte sisteme informatice deținute de autoritățile din domeniul sănătății și alte autorități publice.

4. Fundamentarea economico-financiară

Finanțarea Sistemului Informațional de Supraveghere a Bolilor Transmisibile și Evenimentelor de Sănătate Publică, va fi asigurată din contul și în limita mijloacelor aprobate anual Ministerului Sănătății precum și din alte surse, conform legislației.

5. Modul de încorporare a actului în cadrul normativ în vigoare

Aprobarea proiectului Hotărârii de Guvern va impune aprobarea unor acte normative.

6. Avizarea și consultarea publică a proiectului

Proiectul a fost plasat spre consultare publică de către Ministerul Sănătății în ordinea prevederilor Legii nr. 239/2008 privind transparența în procesul decizional.

În conformitate cu prevederile Regulamentului Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, prezentul proiect a fost avizat de către Ministerul Finanțelor, Ministerul Economiei, Agenția de Guvernare Electronică și Serviciul Tehnologia Informației și Securitate Cibernetică, Centrul Național pentru Protecția Datelor cu Caracter Personal.

7. Constatările expertizei anticorupție

Informația referitoare la concluziile expertizei anticorupție a fost inclusă după recepționarea raportului de expertiză anticorupție în sinteza obiecțiilor și propunerilor/recomandărilor la proiectul de hotărâre.

8. Constatările expertizei juridice

Informația referitoare la concluziile expertizei juridice privind compatibilitatea proiectului de hotărâre cu alte acte normative în vigoare, precum și respectarea normelor de tehnică legislativă a fost inclusă după recepționarea expertizei juridice în sinteza obiecțiilor și propunerilor/recomandărilor la proiectului de hotărâre.

Ministru

Ala NEMERENCO