## Anexa nr. 2

La Hotărârea Guvernului nr.\_\_\_

**REGULAMENT**

**privind organizarea și funcționarea Sistemului informațional de supraveghere epidemiologică a bolilor transmisibile și evenimentelor de sănătate publică**

1. **DISPOZIȚII GENERALE**
2. Regulamentul privind organizarea și funcționarea Sistemului informațional automatizat de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică ”SI SBTESP” (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.
3. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută în Legea nr. 467/ 2003 cu privire la informatizare şi la resursele informaționale de stat, Legea nr. 71/ 2007 cu privire la registre, Legea nr. 133 /2011 privind protecția datelor cu caracter personal, Hotărîrea Guvernului nr. 1128/2004 „Cu privire la aprobarea Concepției Sistemului Informaţional Medical Integrat”, Hotărîrea Guvernului nr. 586 /2017 pentru aprobarea Regulamentului privind modul de ținere a Registrului medical, Hotărârea Guvernului nr. 951 din 25 noiembrie 2013, pentru aprobarea Regulamentului privind sistemul național de supraveghere epidemiologică și control al bolilor transmisibile și evenimentelor de sănătate publică, Hotărîrea Guvernului nr. 1123 /2010 „Privind aprobarea Cerințelor față de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal”.

În sensul prezentului Regulament se definesc următoarele noțiuni:

*notificare -* înregistrarea/notificarea urgentă despre depistarea cazului de boală infecțioasă, intoxicație, toxiinfecție alimentară și/sau profesională acută conform Formei de raportare 058/e ”Fișa de notificare urgentă despre depistarea cazului de boală infecțioasă, intoxicație alimentară și/sau profesională acută, reacție adversă după administrarea preparatelor imunobiologice” și generarea rezultatului anchetei epidemiologice;

*gestionarea electronică a notificărilor –* totalitatea acțiunilor legate de administrarea notificărilor prin intermediul platformei electronice sau al sistemelor informaționale automatizate;

*eveniment de sănătate publică –* manifestare a unei boli, sau situație care creează potențial pentru apariția unei boli;

*supraveghere epidemiologică –* proces de colectare, analiză, interpretare și diseminare sistematică și continuă a datelor despre sănătate cu privire la bolile transmisibile și evenimentelor de sănătate publică, în contextul răspîndirii lor în timp, spațiu, grup de populație și analizei factorilor de risc de contractare a acestei boli, inclusiv în cadrul studiilor epidemiologice, în scopul implementării măsurilor de sănătate publică;

*prevenire şi control al bolilor transmisibile –* ansamblu de măsuri, inclusiv investigaţii epidemiologice, orientate spre prevenirea sau reducerea riscului apariției, stoparea răspândirii bolilor transmisibile şi/sau eliminarea lor de pe teritoriul Republicii Moldova;

*autentificare –* verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;

*registrator –* persoană responsabilă de înregistrarea primară, împuterniciți cu atribuții partajate de introducere, modificare, radiere și/sau generare a informației în SI;

*utilizator –* persoană mandatată cu drept de acces, deplin sau partajat, asupra informației din resursa informațională;

*prelucrarea automatizată de date* – orice operațiune sau serie de operațiuni care se efectuează asupra datelor prin mijloace automatizate, precum: colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, blocarea, ștergerea sau distrugerea;

*securitate -* nivel necesar de integritate, selectivitate pentru protejarea datelor împotriva pierderilor, alterarilor, deteriorărilor și a accesului neautorizat. Securitatea sistemului presupune că acestea este rezistent la atacuri, informația este confidențială, integrală și în stare de lucru, atât la nivel de sistem, cît și la nivel de date;

*sistem informațional automatizat de supraveghere epidemiologică a bolilor transmisibile și evenimentelor de sănătate publică –* sistem informațional automatizat constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii aflate în interconexiune și care este destinat înregistrării, prelucrării, utilizării, păstrării, informațiilor cu privire la cazurile de notificare de boli transmisibile și evenimentelor de sănătate publică (în continuare SI SBTESP).

1. Sistemul este resursa informațională de stat care reprezintă totalitatea informației sistematizate cu privirede boli infecțioase și evenimentelor de sănătate publică, inclusiv intoxicații, toxiinfecții alimentare și/sau profesionale acute, din momentul suspectării acestora.
2. Scopul Sistemului 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.
3. Sistemul creează spațiul informațional necesar pentru participanții la Sistem 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.
4. **Subiecții raporturilor juridice în domeniul creării , exploatării și utilizării SBTESP, atribuțiile acestora**
5. Subiecții din domeniul creării, exploatării și al utilizării conținutului SBTESP sunt:
6. proprietarul;
7. posesorul;
8. deținătorul;
9. administrator tehnic
10. registratorul;
11. utilizatorul;
12. Proprietarul Sistemului este statul care realizează dreptul de proprietate, de gestionare și utilizare a datelor din SI SBTESP.
13. Posesorul Sistemului 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.
14. Drepturile și obligațiile Posesorului sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și Hotărîrea Guvernului nr. 148 din 25.08.2021 cu privire la organizarea și funcționarea Ministerului Sănătății.
15. Deținătorul Sistemului este Agenția Națională pentru Sănătate Publică din subordinea Ministerului Sănătății.
16. Deținătorul are următoarele atribuții:
17. asigură formarea resursei informaționale;
18. asigură condițiile organizatorice și financiare pentru funcționarea SBTESP;
19. stabilește obiectele informaționale de evidență a Sistemului și a conținutului acestora;
20. stabilește scopurile și sarcinile funcționale ale SBTESP;
21. monitorizează procesul de înregistrare și prelucrare a datelor în SBTESP;
22. verifică respectarea condițiilor de înregistrare, evidență și utilizare a datelor cu caracter personal;
23. asigură securitatea și protecția datelor din SBTESP în limita competențelor;
24. autorizează, suspendă și revocă dreptul de acces la SBTESP;
25. stabilește măsurile tehnice și organizatorice de protecție și securitate a SBTESP;

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

1. exercită alte atribuții necesare asigurării bunei funcționări ale SI SBTEPS;
2. asigură autorizarea/gestionarea, suspendarea și revocarea drepturilor de acces în SI SBTESP;
3. elaborează, coordonează și aprobă procedurile operaționale aferente gestionării și asigurării bunei funcționări a sistemului;
4. stabilește regulile și procedurile specifice de acordare/suspendare/retragere/anulare a accesului la contururile sistemului și de stabilire a rolurilor utilizatorilor.
5. 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.
6. Deținătorul asigură păstrarea SBTESP până la adoptarea deciziei privind lichidarea acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă, conform legislației.
7. Administrator tehnic al SI este Instituția publică ”Serviciul Tehnologia Informației și Securitate Cibernetică”, care îşi exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.
8. Registratorii ai Sistemului sunt lucrătorii medicali, persoanele responsabile din cadrul Prestatorilor de Servicii Medicale, Instituțiilor 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 Sîngelui.
9. Registratorii au următoarele atribuții:
10. asigură colectarea, introducerea informațiilor relevante în baza de date a SI, în termenele și condițiile stabilite;
11. asigură autenticitatea, plenitudinea și integritatea datelor;
12. raportează posesorului incidentele de infrastructură, erorile de sistem sau erorile cauzate de alți factori, în scopul remedierii acestora;
13. solicită posesorului autorizarea accesului, precum și suspendarea și revocarea drepturilor de acces în SI;
14. raportează posesorului sau administratorului tehnic problemele de sistem în utilizarea SI;
15. înaintează propuneri de îmbunătățire și dezvoltare a sistemului, participă în grupurile de lucru organizate în scopul dezvoltării SI;
16. Registratorii desemnează și informează posesorul despre numărul, numele, prenumele angajaților acestora cu atribuții de introducere nemijlocită a datelor în sistem.
17. Registratorii Sistemului au următoarele drepturi:
18. să participe la dezvoltarea, îmbunătățirea Sistemului;
19. să prezinte propuneri cu privire la inițierea modificărilor actelor normative care reglementează funcționarea Sistemului;
20. să solicite și să primească informația statistică cu privirile la înregistrările din sistem;
21. să prezinte propuneri privind perfecționarea și eficientizarea Sistemului.
22. Utilizatori ai SI 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, Instituțiile 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 sistemului.
23. Utilizatorii SI sunt obligați:
24. să utilizeze datele din Sistem conform scopului și destinației acestora;
25. să asigure securitatea și confidențialitatea informației vizualizate sau prelucrate în Sistem;
26. să înștiințeze imediat, posesorul și administratorul tehnic al Sistemului despre cazurile de încălcare a securității informaționale a Sistemului;
27. să informeze posesorul sistemului cu privire la orice situație, inclusiv de forță majoră, apărută, care ar putea afecta buna funcționare a Sistemului.
28. Utilizatorii sistemului, în limita competenței, au următoarele drepturi:
29. să participe la crearea, implementarea și dezvoltarea Sistemului;
30. să prezinte propuneri cu privire la inițierea modificărilor actelor normative existente care reglementează funcționarea Sistemului;
31. să acceseze, vizualizeze, utilizeze și să prelucreze informațiile din Sistem, în conformitatea cu rolurile și drepturile stabilite;
32. să solicite și să primească de la posesorul și administratorul tehnic al sistemului ajutor metodologic și practic pe probleme ce țin de funcționarea Sistemului;
33. **Regimul juridic de utilizare a datelor**
34. Utilizatorii sunt obligați să efectueze schimbul de date, cu caracter gratuit, prin intermediul platformei de interoperabilitate și să asigure condițiile tehnice necesare realizării schimbului de date.
35. Deținătorul Sistemului stabilește acordarea accesului la datele din registru în conformitate cu legislația în vigoare cu privire la schimbul de date și interoperabilitate;
36. Dreptul de acces la datele SI este segmentat pe unități de conținut, atribuind prerogative partajate de vizualizare, adăugare, redactare și ștergere.
37. Accesul la resursele informaționale ale SI este segmentat pentru utilizatori interni și utilizatori externi.
38. Dreptul de acces la SI SBTESP și contururile acestuia nu este unul permanent, acesta poate fi suspendat sau revocat. Introducerea și/sau modificarea datelor în 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.
39. Revocarea dreptului de acces la Sistem și/sau contururile acestuia se efectuează prin înaintarea cererii/demersului către posesor, în una din următoarele situații:
40. la încetarea/suspendarea raporturilor de serviciu/ de muncă ale utilizatorilor;
41. la intervenirea modificărilor raporturilor de serviciu/ de muncă când noile atribuții nu impun accesul la datele din Sistem;
42. la constatarea de către posesor a încălcării securității informaționale;
43. în alte cazuri în limitele prevederilor legislative.
44. Lucrările profilactice planificate în complexul de mijloace software şi hardware 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 Sistemului.
45. Condițiile pentru prelucrarea, stocarea și utilizarea datelor cu caracter personal.
46. datele cu caracter personal vor fi prelucrate în mod corect și conform prevederilor Legii 133/2011 „Cu privire la prelucrarea datelor cu caracter personal”;
47. colectarea datelor va fi efectuată doar în scopuri determinate și vor fi prelucrate doar în modul compatibil cu acest scop, cît și în scopuri statistice, de cercetare istorică sau științifică, care nu cu contravine prevederilor legii sus menționate;
48. 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.
49. la necesitate datele vor fi actualizate iar datele incomplete sau inexacte vor fi ulterior rectificate sau șterse.
50. stocarea datelor se va face cu respectarea garanțiilor de prelucrare a datelor, prevăzute de cadrul normativ ce reglementează acest domeniu.
51. la expirarea termenului de stocare, datele cu caracter personal urmează a fi distruse în modul stabilit de Legea 133/2011.

1. **Interoperabilitatea cu alte sisteme Informaționale**
2. Pentru asigurarea actualizării operative şi automate a conținutului informațional al Sistemului cu informație veridică, poate fi efectuată interacțiunea şi sincronizarea datelor cu alte sisteme informaționale, importând automat sau exportând date spre verificare și/sau completare a conținutului informațional al Sistemului.
3. Consumul sau livrarea de date va fi realizată prin integrarea cu platforma guvernamentală de interoperabilitate Mconnect.
4. Conectarea la platforma de interoperabilitate (MConnect) și, respectiv, interconectarea sistemelor informaționale va fi asigurată prin decizia autorității competente - Agenția de Guvernare Electronică:
5. Sistemul informațional automatizat ”Registrul de stat al populației”;
6. Sistemul informațional automatizat ”Registrul de stat al unităților de drept”;
7. Sistemul informațional automatizat ”Asigurarea obligatorie de asistență medicală”;
8. Sistemul informațional automatizat ”Asistența medicală prespitalicească”;
9. Sistemul informațional automatizat ”Asistența medicală spitalicească”;
10. Sistemul informațional automatizat ”Asistența medicală primară”;
11. alte sisteme informaționale automatizate, considerate necesare pentru implementarea și dezvoltarea Sistemului.
12. În conformitate cu prevederile art.6 alin.(3) din Legea nr.142/2018: Participanții publici sunt obligați să efectueze schimbul de date, cu caracter gratuit, prin intermediul platformei de interoperabilitate și să asigure condițiile tehnice necesare realizării schimbului de date. În completarea celor expuse, art.29 alin.(2) din Legea nr.71/2007 cu privire la registre statuează că acordarea accesului la datele din registru se efectuează în conformitate cu legislația în vigoare cu privire la schimbul de date și interoperabilitate.
13. SI SBTESP utilizează următoarele sisteme informaționale partajate:
14. 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;
15. 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 digitale de către utilizatori (inclusiv în contextul utilizării sistemelor informaționale și a serviciilor electronice), oferite de către furnizorii de semnătură digitală în conformitate cu legislația;
16. 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, asigurînd evidența evenimentelor, în contextul utilizării sistemelor informaționale;
17. 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;
18. 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 Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
19. Alte servicii guvernamentale electronic considerate necesare pentru implementarea și dezvoltarea Sistemului.
20. **Asigurarea protecției și securității informației SBTESP**
21. Măsurile de protecție şi securitate a informaţiei din Sistem reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a Sistemului şi se efectuează neîntrerupt de către posesorul Sistemului.
22. Obiecte ale asigurării protecției şi securităţii informației din Sistem se consideră:
23. masivele informaţionale, indiferent de formele păstrării, bazele de date, suporturile materiale care conțin informații privind date cu caracter personal;
24. sistemele informaţionale, sistemele operaționale, sistemele de gestionare a bazelor de date şi alte aplicații care asigură activitatea Sistemului;
25. sistemele de telecomunicații, reţelele, inclusiv mijloacele de confecționare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informației.
26. Securitatea informațională a Sistemului se efectuează prin aplicarea metodelor și efectuarea acțiunilor descrise în Planul de continuitate al Sistemului și, după caz, a procedurilor operaționale.
27. Protecția datelor se efectuează prin următoarele metode:
28. prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;
29. utilizarea obligatorie a produselor de program licenţiate aprobate; orice solicitare de instalare a unui produs de program trebuie coordonată cu deținătorul tehnic;
30. monitorizarea procesului de exploatare al Sistemului prin intermediul mecanismului de jurnalizare efectuat de administratorul tehnic al acestuia.
31. Subiecții la utilizarea și exploatarea Sistemului asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:
32. identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;
33. implementarea principalelor măsuri tehnico-organizatorice necesare asigurării funcționării Sistemului;
34. implementarea procedurilor interne ce exclud cazurile de modificare nesancționată a mijloacelor software şi/sau a informației din Sistem;
35. informarea și instruirea utilizatorilor interni cu privire la mecanismele de asigurare a securității informaționale;
36. proceduri de control intern privind respectarea condițiilor de securitate informațională.
37. **Controlul și răspunderea**
38. Ținerea SI SBTESP este supusă controlului intern și extern. Controlul intern privind ținerea Sistemului se efectuează de către Agenția Națională pentru Sănătate Publică, care este posesorul Sistemului. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea SI SBTESP se efectuează de către instituții abilitate și certificate în domeniul auditului.
39. SI SBTESP se înregistrează în Registrul resurselor și sistemelor informaționale de stat.
40. Responsabilitatea privind organizarea și funcționarea SI SBTESP se atribuie posesorului Sistemului, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea Sistemului.
41. Toţi subiecții SI SBTESP, precum şi solicitantul informațiilor ce conțin date cu caracter personal poartă răspundere conform legislației în vigoare pentru prelucrarea, divulgarea, transmiterea informației din sistem persoanelor terțe, contrar prevederilor legislației în vigoare.