## Anexa nr. 1

La Hotărârea Guvernului nr.\_\_\_\_

## **Conceptul**

## **Sistemului Informațional de Supraveghere a Bolilor Transmisibile și Evenimentelor de Sănătate Publică**

**Capitolul I**

**Dispoziții generale**

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 boli profesionale acute.
2. SBTESP asigură digitalizarea proceselor de colectare, analiză, interpretare şi diseminare sistematică şi continuă a datelor despre sănătate cu privire la bolile transmisibile şi evenimentele de sănătate publică, în contextul răspândirii lor în timp, spaţiu, grup de populaţie şi analizei factorilor de risc de contractare a acestor boli, inclusiv în cadrul studiilor epidemiologice. Scopul general al SBTESP constă în îmbunătățirea procesului de evidență, gestiune și raportare a cazurilor cu privire la boli transmisibile și evenimente de sănătate publică.
3. Sistemul are următoarele obiective:
4. digitizarea, automatizarea și eficientizarea proceselor direcționate spre îmbunătățirea prevenirii și controlului bolilor transmisibile și evenimentelor de sănătate publică;
5. 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;
6. îmbunătățirea activității sistemului sănătății în contextul gestionării cazurilor de bolile transmisibile şi evenimentele de sănătate publică.
7. Datele din sistemul SBTESP pot fi prezentate autorităților administrației publice, persoanelor fizice și juridice, în modul stabilit de legislația Republicii Moldova.
8. Noțiunile principale, utilizate în sensul prezentului Concept, semnifică următoarele:

*complex de mijloace tehnice de program -* totalitate de mijloace tehnice şi de mijloace de program care asigură realizarea proceselor informaţionale;

*clasificator –* totalitatea semnificaţiilor unor sau altor caracteristici ale obiectului şi codurilor digitale sau literale ce corespund acestora;

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

*identificator al obiectului registrului* - unul din atributele obiectului informaţional care este unic şi rămîne invariabil pe parcursul întregii perioade de existenţă a obiectului în registru;

*obiect informațional* – reflectarea virtuală a obiectului înregistrării în cadrul resursei informaţionale;

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

*securitate cibernetică -* ansamblul unitar al normelor de drept şi etico-morale, al măsurilor organizatorice (administrative) şi al mijloacelor tehnice de program, orientate spre contracararea pericolelor ce amenință sistemul şi spre minimizarea eventualelor prejudicii care ar putea fi cauzate utilizatorilor şi posesorilor de informații.

*supraveghere epidemiologică* – proces 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 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, limitarea răspândirii bolilor transmisibile şi eliminarea lor de pe teritoriul Republicii Moldova.

1. Principiile de bază ale Sistemului Informațional

Principiile de bază ale sistemului sunt următoarele:

1. principiul legitimității – funcțiile și operațiile efectuate de utilizatori sunt legale și conforme cu drepturile omului și legislația națională în vigoare;
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 sistem se efectuează doar în baza înscrierilor din documentele acceptate ca surse de informații;
5. principiul auditului sistemului – 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 – Sistemul 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 sistemului atât timp cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit;
7. principiul accesibilității și integrabilității – Sistemul, 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 în vigoare, a colaboratorilor responsabili de prelucrarea informației în sistem pentru utilizarea și difuzarea neautorizată a informației;
9. principiul compatibilității – Sistemul 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 Sistemului 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 sistemului 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 în vigoare;
16. principiul securității informaționale – asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirii pentru lucru atât a Sistemului, cât și a datelor acestuia.
17. Sarcinile de bază ce urmează a fi realizate la exploatarea Sistemului sunt următoarele:
18. eficientizarea proceselor de gestiune și evidență a cazurilor de boli transmisibile și evenimentelor de sănătate publică;
19. automatizarea și digitizarea proceselor de gestiune și evidență a cazurilor de boli transmisibile și evenimentelor de sănătate publică;
20. crearea și dezvoltarea sursei informaționale de evidență și gestiune a cazurilor de boală infecțioasă, intoxicație, toxiinfecție 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;
21. standardizarea procedurilor, formularelor și nomenclatoarelor;
22. colectarea şi procesarea informaţiei privind determinanţii stării de sănătate;
23. integrarea laboratoarelor, inclusiv din domeniul de sănătate publică în sistemul informaţional comun;
24. monitorizarea apariţiei cazurilor noi sau reapariţia cazurilor de boli transmisibile supuse înregistrării şi notificării în sistemul de supraveghere epidemiologică, precum și a cazurilor de boli transmisibile de origine necunoscută;
25. monitorizarea evoluţiei unei situaţii epidemii prin boli transmisibile;
26. eliminarea treptată a gestionării datelor pe suport de hârtie, prin utilizarea informațiilor și documentelor electronice;
27. comunicarea rapidă între entitățile sistemului, cu utilizarea mijloacelor electronice;
28. utilizarea potenţialului tehnologiilor electronice contemporane în colectarea și procesarea datelor;
29. sporirea gradului de pregătire și de utilizare a tehnologiilor informaționale al personalului sistemului de sănătate;
30. dezvoltarea și acordarea serviciilor electronice către cetățeni, inclusiv prin depunerea solicitărilor în regim on-line;
31. asigurarea interoperabilității cu alte sisteme informaționale pentru livrarea și consumul de informații;
32. securizarea informațiilor cu accesibilitate limitată, prin implementarea unei politici de acces în sistem pentru fiecare entitate/utilizator în parte, în funcție de competențele specifice;
33. eliminarea posibilităților de manipulare a datelor din sistem;
34. eliminarea posibilităților de intervenție neautorizată asupra datelor din Sistem;
35. excluderea posibilității modificării sau ștergerii istoricului datelor de jurnalizare a Sistemului.
36. Componentele ce formează sistemul SBTESP, sunt următoarele:
37. **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 vaccinelor, dar și evidența și diseminarea informațiilor cu privire la investigarea evenimentelor de sănătate publică;
38. **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*.*
39. **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, evidența 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:
40. *pre-analitic* – recepționarea înregistrărilor; prelevare probe; managementul solicitărilor;
41. *analitica* – generarea sarcinilor de investigații (work list); controlul și monitorizarea sarcinilor; interacțiunea cu echipamentul de laborator care realizează investigația; managementul calității; gestiune alerte;
42. *post-analitica* – validarea clinică și tehnică a rezultatelor; emitere rezultate/rapoarte; notificarea pacienților și instituțiilor medicale prin diverse mijloace electronice; arhivare.
43. **Soluția informatică pentru monitorizarea incidenței unei boli transmisibile**, persoanelor supuse regimului de autoizolare, contacților, 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 II**

**Cadrul normativ-juridic al Sistemului informațional de supraveghere a bolilor transmisibile și evenimentelor de sănătate publică**

1. Cadrul juridic al Sistemului este format din legislația națională, acordurile și convențiile internaționale la care Republica Moldova este parte, precum și actele normative ce reglementează sistemul de sănătate.
2. Crearea și funcționarea Sistemului este reglementată, în particular, de următoarele acte legislative și normative:
3. Constituția Republicii Moldova din 29 iulie 1994;
4. Legea nr. 71/2007 cu privire la registre;
5. Legea nr. 467/ 2003 cu privire la informatizare şi la resursele informaţionale de stat;
6. Legea nr.411/1995 Ocrotirii sănătății;
7. Legea nr.982/2000 privind accesul la informație;
8. Legea nr.1069/2000 Cu privire la informatică;
9. Legea nr.412/2004 Cu privire la Statistica oficială;
10. Legea nr.10/2009 privind supravegherea de stat a sănătăţii publice;
11. Legea nr.133/2011 privind protecția datelor cu caracter personal;
12. Legea nr. 91/2014 privind semnătura electronică și documentul electronic;
13. Legea nr. 142/2018 Cu privire la schimbul de date și interoperabilitate;
14. Hotărârea Guvernului nr. 1128/2004 Cu privire la aprobarea Concepției Sistemului Informaţional Medical Integrat;
15. Hotărârea Guvernului nr.632/2004 Despre aprobarea Politicii de edificare a societății informaționale în Republica Moldova;
16. Hotărârea Guvernului nr. 1123/2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal”;
17. Hotărârea Guvernului nr.656/2012 „Cu privire la aprobarea Programului privind Cadrul de Interoperabilitate”;
18. Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
19. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
20. Hotărârea Guvernului nr. 201/2017 „Privind aprobarea Cerințelor minime obligatorii de securitate cibernetică”;
21. Hotărârea Guvernului nr. 586/2017 pentru aprobarea Regulamentului privind modul de ţinere a Registrului medical;
22. Hotărârea Guvernului nr. 1090/2017 cu privire la organizarea și funcționarea Agenției Naționale pentru Sănătate Publică;
23. Hotărârea Guvernului nr. 414/2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat”;
24. Hotărârea Guvernului nr. 211/2019 „Privind platforma de interoperabilitate (MConnect);
25. Hotărârea Guvernului nr. 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);
26. Ordinul MS 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;
27. Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006;
28. Ordinul MS nr. 466/2015 cu privire la aprobarea Nomenclatorului instituțiilor medico-sanitare spitalicești;
29. Ordinul MS Cu privire la întocmirea și prezentarea dărilor de seamă statistice medicale anuale de către instituțiile medico-sanitare, actualizat anual;
30. Ordin MS nr. 47/2016 Cu privire la aprobarea Nomenclatorului prestatorilor privați de servicii de sănătate;
31. Ordinul MS nr. 1086/2016 cu privire la aprobarea Regulamentelor-cadru de organizare și funcționare ale prestatorilor de servicii de sănătate;
32. Ordinul MS nr. 1087/721/2016 despre aprobarea Regulamentului privind înregistrarea persoanei la medicul de familie din instituția medico-sanitară ce prestează asistență medicală primară în cadrul asigurării obligatorii de asistență medical;
33. Ordinul MS nr. 1080/2017 Cu privire la aprobarea Nomenclatorului Instituțiilor medico-sanitare publice de asistență medicală primară la nivel de raion.
34. Tipurile principale de standarde tehnologice care vor fi utilizate de Sistem, sunt următoarele
35. standardul datelor;
36. standardul metadatelor;
37. standardele schimburilor de informații;
38. standardele căutării informațiilor;
39. standardele de calitate;
40. standardele de securitate;
41. standardele de multilingvism.
42. Conformitatea cu aceste standarde constă în:
43. susținerea interfeței *browser*-ului public pentru accesare;
44. XML ca mijloc principal pentru integrarea datelor;
45. utilizarea standardelor internet și WWW-HTML, TCP/IP, SMTP;
46. utilizarea standardelor naționale și internaționale privind calitatea și securitatea.

**Capitolul III**

**Spațiul informațional al sistemului informațional automatizat**

**Secțiunea 1. Funcțiile de bază ale Sistemului**

1. Funcțiile de bază ale Sistemului sunt:
2. formarea bazei de date a Sistemului 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 ciclu de viață. Funcțiile de bază la formarea bazei de date sunt înregistrarea și actualizare datelor, precum și radierea obiectelor informaționale:
3. 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 Sistemului;
4. actualizarea datelor. Constă în actualizarea sistematică a bazei de date, la modificarea sau completarea datelor obiectelor informaționale;
5. scoaterea din evidență/arhivarea. Reprezintă schimbarea statutului obiectului informațional, și nu excluderea fizică a datelor despre obiect.
6. 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:
7. înregistrarea și evidența solicitărilor investigațiilor/analizelor de laborator;
8. gestiunea probelor și rezultatelor acestora;
9. crearea și gestionarea catalogului centralizat al investigațiilor de laborator;
10. asigurarea trasabilității, istoricului și corelării investigațiilor de laborator;
11. raportarea și interpretarea rezultatelor de laborator;
12. controlul și managementul proceselor.
13. formarea bazei de date ce reflectă înregistrările cu privire la procesul de vaccinare:
14. evidența și gestiunea informațiilor cu privire la vaccin;
15. evidența și gestiunea procesului de vaccinare;
16. generarea, descărcarea și imprimarea certificatului de vaccinare;
17. programarea la vaccinare;
18. evidența reacțiilor adverse la administrarea preparatelor imunobiologice.
19. formarea bazei de date ce permite monitorizarea contacților (*contact tracing*) pentru a întrerupe lanțurile de transmitere și prevenirea transmiterii ulterioare a maladiei:
20. investigarea focarelor și evenimentelor de sănătate publică generate de sistem;
21. monitorizare inteligentă a contacților;
22. identificarea relațiilor dintre înregistrările individuale cu focarele/evenimentele existente;
23. vizualizarea cazurilor și contacților în regim de tablou de bord;
24. vizualizarea lanțurilor de transmitere;
25. generarea rapoartelor.
26. asigurarea informațională. Informația din Sistem este pusă la dispoziție autorităților din domeniul sănătății, altor autorități publice, furnizorilor/destinatarilor/utilizatorilor de date, precum și a participanților la Sistem. Nivelul de acces la Sistem este stabilit prin regulament și prevederile legislației.
27. administrarea informațională, care include următoarele acțiuni:
28. administrarea rolurilor și drepturilor utilizatorilor – gestionarea utilizatorilor Sistemului, individual pentru fiecare componentă, desfășurată conform regulamentului de organizare și funcționare;
29. administrarea nomenclatoarelor;
30. administrarea modelelor de documente;
31. alte activități de administrare și acces la funcționalitățile Sistemului:
32. asigurarea calității informațiilor din contul creării şi menținerii componentelor Sistemului;
33. protecția și securizarea informațiilor la toate etapele de formare a bazei de date a Sistemului, 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;
34. asigurarea generării datelor statistice.

Toate modificările în sistem se păstrează în ordine cronologică.

**Secțiunea 2. Contururile funcționale ale Sistemului informațional automatizat**

1. Sistemul trebuie să asigure exercitarea funcțiilor specifice determinate de destinația sa, grupate în contururi funcționale specifice, care sunt realizate prin intermediul componentelor Sistemului:
2. **Conturul Sistemul Informațional de notificare a cazurilor și evenimentelor de sănătate publică:**
3. modulul notificări – componenta de bază a Sistemului, care asigură crearea, înregistrarea, notificarea și gestiunea cazurilor de boală infecțioasă, evenimentelor de sănătate publică (Anexa 1) și rezultatul anchetei epidemiologice;
4. modulul de hartă interactivă (GIS) – componenta responsabilă de reprezentarea geografică a informațiilor cu privire la situația epidemiologică, în corelare cu anumiți parametri;
5. modulul Alerte – componenta responsabilă de alertarea/notificarea utilizatorilor cu privire la anumite evenimente, care necesită gestionate, sau despre care necesită să fie informați;
6. modulul de raportare - componenta pentru generarea și exportarea rapoartelor statistice;
7. modulul de administrare – asigură funcționalitatea de gestionare a configurărilor de sistem, managementul utilizatorilor, evenimentelor de audit, managementul alertelor, managementul clasificatoarelor, etc.;
8. modulul de căutare - asigură capacitatea de căutare, în baza anumitor parametri, a informațiilor din sistem.
9. **Conturul Registrul electronic ”Vaccinare Covid-19”** va conține următoarele module și moduri:
10. modul de programare la vaccinare;
11. modului lista de așteptare;
12. modul de înregistrare a dozelor de vaccin;
13. modul de înregistrare a evenimentelor adverse post imunizare;
14. modul de generare a certificatelor COVID-19;
15. modulul de raportare;
16. modulul de management a stocurilor de vaccin;
17. modulul de raportare grafică.
18. **Conturul Sistemul informațional de laborator:**
19. modulul de înregistrare a probelor de laborator pentru investigare cu generarea codului de bare;
20. modulul de înregistrare a rezultatelor de laborator;
21. modului de eliberare a rezultatului investigației;
22. modului de generare a rapoartelor investigațiilor de laborator;
23. modul de interoperabilitate.
24. **Conturul Monitorizarea cazurilor și contacților:**
25. modulul de evidență și gestiune a contacților;
26. modul de vizualizare a datelor;
27. modul privind lista cazurilor cu manifestări clinice și trasabilitatea cazurilor;
28. modul de contactare și supervizare a cazurilor;
29. modulul de raportare - componenta pentru generarea și exportarea rapoartelor statistice.

**Capitolul IV**

**Structura organizațională a Sistemului informațional automatizat**

1. Proprietarul Sistemului este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din acesta. Resursele financiare pentru dezvoltarea, mentenanța și exploatarea Sistemului sunt asigurate din bugetul de stat și alte mijloace financiare, conform legii.
2. Posesorul Sistemului este Ministerului Sănătății, cu drept de gestionare și de utilizare a datelor și a resurselor conținute de acesta.
3. Deținătorul Sistemului Informațional este Agenția Națională pentru Sănătate Publică din subordinea Ministerului Sănătății, care este responsabilă de crearea, administrarea, mentenanța și dezvoltarea sistemului informațional și poate exercita atribuțiile administratorului tehnic și ale utilizatorului sistemului informațional.
4. Administratorul tehnic al sistemului este Instituția publică ”Serviciul Tehnologia Informației și Securitate Cibernetică”, care va asigura administrarea tehnică a sistemului informațional, mentenanța sistemului, dezvoltarea sistemului și implementarea cerințelor de securitate stabilite de actele normative în domeniu.
5. Posesorul și deținătorul asigură condițiile organizatorice și financiare pentru funcționarea Sistemului.
6. Registratorii ai Sistemului sunt lucrătorii medicali, personalul responsabil din cadrul Prestatori 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.
7. Utilizatorii Sistemului 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.
8. Destinatari și utilizatori ai datelor din Sistem sunt autoritățile publice centrale și locale, persoanele fizice sau juridice mandatate cu dreptul de a le primi informații conform prevederilor legale.

**Capitolul V**

**Documentele Sistemului**

1. Documentele utilizate de Sistem sunt documentele elaborate si aprobate de către Ministerul Sănătății în ordinea stabilita și nu se limitează doar la cele listate mai jos.
2. Documentele de intrare a datelor inițiale sunt:
3. Fişa de notificare urgentă despre depistarea cazului de boală infecțioasă, intoxicație, toxiinfecție alimentară sau profesională acută, reacție adversă la administrarea preparatelor imunobiologice;
4. Fișa de evidenţă a bolilor (intoxicațiilor) profesionale;
5. Fișa de evidenţă a stocului de vaccinuri, diluanți, seringi;
6. Fișa de anchetare epidemiologică a focarului de boală infecțioasă;
7. Fișa medicală a bolnavului de staționar cu anexele;
8. Registru de evidenţă a vaccinărilor;
9. Registru de evidenţă a bolilor infecțioase;
10. Registru de evidenţă a persoanelor cu intoxicație profesională sau boală profesională depistată caz nou;
11. Registru de evidenţă a stocurilor primite de preparate imunobiologice, instrumente şi utilaje medicale în Centrele de Sănătate Publică;
12. Aviz despre bolnavul cu diagnosticul stabilit caz nou de tuberculoză activă;
13. Aviz privind boala sau intoxicație profesională cronică;
14. Actul de prelevare a probelor (mostrelor);
15. Actul de înapoiere a probelor (mostrelor);
16. Actul de decontare a probelor (mostrelor);
17. Proces-verbal de codificare a probelor (mostrelor);
18. Proces-verbal de recoltare a probelor de apă;
19. Proces-verbal de examinare a cazului (suspiciunii) de boală (intoxicație) profesională;
20. Proces-verbal de evidentă a bolilor (intoxicațiilor) profesionale;
21. Trimitere la analiză;
22. Trimitere la investigații;
23. Certificat medical (de recuperare, de testare);
24. Certificat de vaccinare.
25. Principalele documente de ieșire sunt:
26. Fişa de anchetare epidemiologică a focarului cu infecția HIV/SIDA;
27. Fişa de anchetare epidemiologică a cazului de hepatită virală B, C şi D acută;
28. Fișa de colectare a datelor epidemiologice a cazului de hepatită virală B, C și D cronică;
29. Fişa de evidenţă a purtătorului cronic de germeni patogeni;
30. Fişa de anchetare epidemiologică a focarului de boală infecțioasă ;
31. Registru investigațiilor;
32. Registru cazurilor de intoxicații;
33. Registru fișelor de declarații;
34. Registru de evidenţă a accidentelor la locul de lucru;
35. Registru de evidenţă a probelor de laborator;
36. Formular privind rezultatele investigațiilor de laborator;
37. Proces-verbal de investigații;
38. Proces-verbal de recoltare;
39. Trimitere medicală pentru investigații;
40. Certificat medical (de recuperare, de testare);
41. Certificat de vaccinare;
42. Rapoarte analitice și statistice;
43. Altele.
44. Documente tehnologice:
45. instrucțiuni metodice, ghiduri și regulamente pe diferite nozologii;
46. protocoale clinice naționale;
47. formulare și rapoarte aprobate de către Biroul Național de Statistică;
48. lista utilizatorilor și drepturilor acestora;
49. înregistrările de audit ale activității sistemului și utilizatorilor.

**Capitolul VI**

**Resursa informațională**

**Secțiunea 1. obiectele informaționale ale Sistemului**

1. Principalele obiecte informaționale ale Sistemului sunt:

Totalitatea obiectelor informaționale, care constituie resursa informațională, este determinată de destinația Sistemului și include cel puțin următoarele:

1. fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică;
2. trimitere/fișa de investigații de laborator.
3. certificate:
4. de vaccinare;
5. de recuperare;
6. de testare;
7. persoane fizice și juridice:
8. pacienți;
9. lucrători medicali;
10. prestatori de servicii medicale;
11. prestatori de servicii sociale, etc..
12. Atributele obiectului informațional ”fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică”:
13. numărul epidemiologic unic al notificării;
14. date cu privire la diagnosticul primar;
15. date de identificare a pacientului;
16. date cu privire la înregistrarea cazului în SI;
17. date cu privire la simptomele și manifestările bolii;
18. date cu privire la diagnosticul final.
19. Atributele obiectului informațional ”trimitere/fișa de investigații de laborator”
20. numărul de identificare/înregistrare al investigației de laborator;
21. tipul analizei investigației de laborator;
22. date de identificare a pacientului;
23. date despre boală;
24. date privind rezultatele de laborator.
25. Atributele obiectului informațional ”Certificate”:
26. date despre certificatul de vaccinare;
27. date despre certificatul de recuperare;
28. date despre certificatul de testare.
29. Atributele obiectului informațional ”persoane fizice și juridice”:
30. pacienți:
* date de identificare (IDNP, nume, prenume, sex, data nașterii);
* date demografice (cetățenie, tipul documentului de identificare, numărul documentului, data emiterii);
* adresa de reședință permanentă și temporară (localitate, strada, bloc, apartament);
* date privind asigurarea medicală (categoria și statutul de asigurat, tipul de asigurare);
* date socioeconomice (locul de muncă / studii).
1. lucrători medicali:
* date de identificare (IDNP, nume, prenume, sex, data nașterii);
* date demografice (cetățenie, tipul documentului de identificare, numărul documentului);
* adresa de reședință permanentă și temporară (localitatea, strada, bloc, apartament);
* date privind asigurarea medical (categoria și statutul de asigurat, tipul de asigurare);
* date socioeconomic (locul de muncă / studii).
1. prestatori de servicii medicale/ sociale:
* numărul de identificare de stat – IDNO;
* denumirea;
* codul fiscal;
* codul IMS;
* tip;
* număr de telefon;
* adresă poștală.

**Secțiunea 2. Identificatorii obiectelor informaționale**

1. 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 al 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.
2. 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.
3. 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.
4. Identificatorul obiectului informațional persoane fizice și juridice este constituit din:
5. numărul de identificare de Stat al persoanei juridice (IDNO), denumirea, adresa poștală, în cazul acesta există - pentru participanții persoane juridice și prestatori de servicii medicale;
6. numărul de identificare de Stat al persoanei fizice (IDNP), nume, prenume, adresa de domiciliu și reședință - pentru participanții persoane fizice.

**Secțiunea 3. Scenariile de bază asociate obiectelor informaționale**

1. Scenariile de bază reprezintă lista evenimentelor aferente obiectului informațional luat în evidență în Sistem, după cum urmează:
2. fișa de notificare a cazului de boală infecțioasă și evenimentelor de sănătate publică (caz de boală);
3. înregistrarea cazului – este realizat de către medic, în cazul depistării cazului de boală transmisibilă, prin completarea datelor de notificare, date a persoanei notificate, diagnostice, rezultatele investigațiilor, simptomatică și alte date aferente înregistrării;
4. realizarea anchetării epidemiologice – este realizat de către epidemiolog, prin completarea rezultatelor anchetării și finalizarea cazului;
5. monitorizare epidemiologică – este realizat de către epidemiolog regional/raional pentru monitorizare în limita unui spațiu bine determinat sau epidemiolog național la nivel de țară;
6. 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.
7. gestiune evenimente de sănătate publică:
8. 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 şi spre prevenirea recidivelor şi complicaţiilor;
9. prevenire - activități aplicate prioritar la nivel de individ, orientate spre preîntâmpinarea sau diminuarea probabilității apariției bolilor transmisibile sau netransmisibile, a răspândirii lor şi spre prevenirea recidivelor şi complicaţiilor;
10. identificare – realizată prin prisma sistemului de management în sănătate și cuprinde identificarea apariției riscul iminent de răspândire a unei boli sau a unui eveniment de sănătate care determină probabilitatea înaltă a unui număr mare de decese şi unui număr mare de dizabilități în rândul populaţiei 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 populaţiei afectate;
11. aplicarea măsurilor - ansamblu de măsuri cu caracter administrativ, economic, medical, social şi de menținere a ordinii publice în caz de pericol sau declanșare a urgenţelor de sănătate publică în scopul prevenirii, diminuării şi lichidării consecinţelor acestora.
12. investigații de laborator – la solicitarea persoanelor fizice/juridice, sau în baza trimiterilor emise de către personalul medical din cadrul instituțiilor prestatoare de servicii medicale se asigură recepția și înregistrarea cererilor și solicitărilor pentru investigații de laborator, efectuarea investigațiilor și emiterea rezultatelor;
13. gestiune certificate – presupune organizarea evidență și monitorizarea , cap-coadă a procesului de vaccinare și a vaccinurilor utilizate, dar și generarea emiterea și descărcarea certificatelor cu privire la vaccinare, recuperare sau testare;
14. monitorizare contacți – monitorizarea a unui individ sau a unui grup de indivizi infectați sau care se consideră, în baza unor raționamente, a fi infectați cu o boală contagioasă sau posibil contagioasă de alţi indivizi în vederea prevenirii sau limitării transmiterii bolii către indivizii neizolați.

**Secțiunea 5. Clasificatoarele Sistemului**

1. Pentru a asigura veridicitatea și reducerea volumului informației stocate în Sistem, se utilizează clasificatoarele și nomenclatoarele prezentate mai jos dar ,care nu se limitează la :
2. internaționale:
3. Clasificatorul internațional al maladiilor;
4. Clasificatorul internațional al țărilor.
5. alte:
6. Clasificatorul oficial a unităților administrativ – teritoriale ale Republicii Moldova;
7. Nomenclatorul instituțiilor medico-sanitare;
8. Nomenclatorul prestatorilor privați de servicii de sănătate;
9. Nomenclatorul investigațiilor de laborator;
10. Clasificatorul tipului instituțiilor medicale;
11. Clasificatorul tipurilor cazurilor;
12. Clasificatorul tipurilor de boli;
13. Clasificatorul condițiilor ce au favorizat infectarea;
14. Clasificatorul simptomelor neurologice;
15. Clasificatorul simptomelor respiratorii;
16. Clasificatorul simptomelor digestive;
17. Clasificatorul tipurilor de produse alimentare;
18. Clasificatorul surselor de apă;
19. Clasificatorul tipurilor parezelor/paraliziilor;
20. Clasificatorul tipurilor erupțiilor cutanate

**Secțiunea 6. Interacțiunea Sistemului informațional cu alte resurse informaționale automatizate**

1. Structura și arhitectura de interoperabilitate high-level a Sistemului conform anexei nr. 1.
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 completare a conținutului informațional al Sistemului.
3. Consumul sau livrarea de date va fi realizată prin integrarea cu platforma guvernamentală de interoperabilitate Mconnect.
4. SI SBTESP asigură interacțiunea și schimbul de date cu următoarele resurse informaționale automatizate:
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 SI SBTESP.
12. SI SBTESP utilizează următoarele servicii electronice guvernamentale de platformă:
13. 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;
14. 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;
15. 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;
16. 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;
17. 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;
18. Alte servicii guvernamentale electronic considerate necesare pentru implementarea și dezvoltarea SI SBTESP.

**Capitolul VII**

**Spațiul tehnologic al Sistemului**

**Secțiunea 1. Dispoziții generale**

1. Sistemul 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 automatizat, în conformitate cu cerințele legale.
2. La nivel conceptual, arhitectura Sistemului este definită pe 3 niveluri:
3. 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;
4. produsul program al nivelului de mijloc – serverul aplicațiilor care va susține partea client, ce deservește interfața BD cu utilizatorii, va transforma cererile utilizatorilor în interpelări SQL și va primi datele de la baza de date și le va prezenta în formă comodă pentru percepție;
5. nivelul de jos – serverul bazei de date.
6. Componenta Centrală a infrastructurii sistemului este găzduită de către administratorul tehnic şi asigură procesarea şi stocarea centralizată a datelor aferente Sistemului. Componentele distribuite reprezintă punctele de acces către componenta centrală prin canale securizate, asigurate de către administratorul tehnic.
7. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către dezvoltatorii Sistemului, în comun cu posesorul și deținătorul, la etapele inițiale și ulterioare de elaborare și implementare a Sistemului.

**Secțiunea a 2-a. Platforma tehnologică**

1. Sistemul Informațional de Supraveghere a Bolilor Transmisibile și Evenimentelor de Sănătate Publică 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).

**Secțiunea 3. Asigurarea securității informației**

1. Prin securitatea informaţională se înţelege protecţia resurselor informaţionale şi infrastructurii de acţiuni intenţionate sau accidentale, cu caracter natural sau artificial, al căror rezultat cauzează daune participanţilor la procesul de schimb de informaţie.
2. Asigurarea securității informaționale va include totalitatea măsurilor juridice, organizatorice, economice şi tehnologice, orientate spre prevenirea pericolelor securităţii resurselor şi infrastructurii informaționale.
3. Pot fi delimitate următoarele probleme de asigurare a securităţii informaţionale cu care se va confrunta Sistemul:
4. asigurarea confidențialității informației (prevenirea obţinerii informaţiilor de către persoanele care nu au drepturile şi competenţele respective);
5. asigurarea integrităţii logice a datelor (prevenirea introducerii, actualizării şi ştergerii nesancţionate a informaţiei sau introducere a datelor denaturate);
6. asigurarea securităţii infrastructurii informaţionale de tentative de a defecta sau de a modifica funcţionarea acesteia.
7. Mecanismele principale de securitate informaţională utilizate vor fi:
8. autentificarea şi autorizarea informaţiei;
9. administrarea accesului la informaţie;
10. înregistrarea acţiunilor utilizatorilor sistemului informatic ;
11. criptarea informaţiei;
12. auditul informatic;
13. procedurile de restabilire, în caz de dezastru.
14. 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.
15. În procesul de elaborare a Sistemului, pentru asigurarea securității informaționale se va ține cont de algoritmii şi protocoalele existente pe piață cu respectarea cadrului legal al Republicii Moldova, inclusiv:
16. Legea nr. 982-XIV din 11 mai 2000 privind accesul la informaţie;
17. Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat;
18. Legea nr. 91/2014 privind semnătura electronică și documentul electronic;
19. Hotărârea Guvernului 1141/2017 pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora”.
20. Reieşind din cele expuse, accesul la resursele Sistemului trebuie să fie asigurat şi autorizat prin intermediul unui sistem de utilizatori şi parole şi autorizare prin certificat digital. Cu toate acestea, utilizatorii vor poseda drepturi distincte de acces, în funcţie de nivelul de securitate căruia îi corespund. Pentru fiecare grup de acces trebuie să existe posibilitatea de a defini rolurile şi drepturile utilizatorilor (chiar şi pînă la nivelul de acces la interfaţa utilizatorilor).
21. Accesul la informația bazei de date trebuie să fie limitat, în funcţie de drepturile şi rolurile specifice grupurilor de acces. În acest caz, fiecare grup de utilizatori va avea acces la o interfaţă personalizată (diferită de cea a altor grupuri), pentru vizualizarea şi gestionarea informaţiei bazei de date, precum şi de manipulare cu datele.
22. Orice modificare potenţial periculoasă: modificarea informaţiei unei înregistrări, marcarea la ştergere, adăugarea unor înregistrări noi etc. trebuie să fie documentată în registre electronice speciale (fişiere log), arătînd momentul de timp şi utilizatorul care a efectuat modificarea potenţial periculoasă. În caz că modificările potenţial periculoase nu vor implica suprimarea fizică a datelor pentru fiecare înregistrare va fi posibil de văzut utilizatorul care a efectuat ultima modificare. În consecinţă, sistemul informatic proiectat va dispune de un instrument eficient care va da posibilitatea de a efectua o analiză a comportamentului utilizatorilor (sau a productivităţii lor).
23. La nivel fizic politica de asigurare a securităţii informaţionale trebuie să fie realizată prin intermediul unor module automate de generare a copiilor de rezervă a fişierelor şi bazelor de date aflate în producţie. Administratorii Sistemului trebuie să dispună de posibilitatea de a-şi defini politica de generare automată a copiilor de rezervă.
24. În vederea asigurării unui nivel adecvat al securităţii informaţionale a Sistemului se consideră binevenită elaborarea şi implementarea unei politici de asigurare a securităţii informaţionale. Această politică va detalia totalitatea compartimentelor de securitate, rolurile, drepturile şi obligaţiile fiecărui actor al sistemului informatic.

**Capitolul VII Impactul general**

1. Impactul SI SBTESP va consta în implementarea unei soluţii moderne de gestiune şi automatizare a fluxurilor de date în sistemul de sănătate precum și digitalizarea proceselor de colectare, analiză, interpretare şi diseminare sistematică şi continuă a datelor cu privire la bolile transmisibile şi evenimentele de sănătate publică, în scopul implementării măsurilor de sănătate publică, îmbunătăţirea calității informaţiilor, inclusiv a relevanței, integrităţii, oportunităţii, exactității, accesibilității, comparabilității, coerenței acestora, a face mai transparent şi mai rapid procesul de luare deciziilor.
2. Implementarea SI SBTESP va determina scăderea cheltuielilor generale deoarece va crește fluxul de lucru în format electronic, fapt ce va duce la reducerea considerabilă a folosirii hârtiei şi a rechizitelor de birou şi la îmbunătăţirea calității şi sporirea diversității mijloacelor de comunicare interinstituțională.
3. Implementarea SI SBTESP va aduce următoarele beneficii:
4. 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;
5. securizarea accesului la aplicații/date/sisteme/infrastructură, cu aplicarea politicilor de securitate, profilurilor de identitate şi a soluțiilor de gestiune a accesului;
6. oferirea de informaţii autentice, veridice, curente şi consistente Ministerului Sănătății și tuturor actorilor implicați din domeniul sănătății și alte domenii cum ar fi sănătatea animalelor și siguranța alimentelor, inspectoratul general al poliției de frontieră, inspectoratul general pentru situații excepționale, etc;
7. reducerea timpului de răspuns şi suport decizional ce presupune gestionarea situațiilor epidemiologice, evenimentelor și urgențelor de sănătate publică;
8. acces rapid, garantat la date şi informaţii indiferent de locație;
9. sporirea calității informaţiilor, inclusiv a relevanței, integrităţii, oportunităţii, exactității, accesibilității, comparabilității, coerenței acesteia;
10. perfecționarea modului de păstrare şi diseminare a informaţiilor prin asigurarea protecţiei informaţiilor confidenţiale, acces nediscriminatoriu tuturor utilizatorilor la informaţii şi servicii, obiectivitate şi imparţialitate în diseminarea informaţilor;
11. consolidarea unei baze unice de date în domeniul sănătății cu privire la supravegherea epidemiologică a bolilor transmisibile și evenimentelor de sănătate publică și protejarea datelor în timp prin proceduri automatizate de salvare și restaurare.

Anexa nr. 1: Structura și arhitectura de interoperabilitatea *high-level* a Sistemului:

