Suvestinė redakcija nuo 2023-04-07

Įsakymas paskelbtas: TAR 2021-06-07, i. k. 2021-13018

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL LIETUVIŠKOJO SNOMED CT ŽODYNO INFORMACINĖS SISTEMOS MODERNIZAVIMO IR MEDICINOS NOMENKLATŪRŲ IR KLASIFIKATORIŲ VALDYMO INFORMACINĖS SISTEMOS NUOSTATŲ BEI MEDICINOS NOMENKLATŪRŲ IR KLASIFIKATORIŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2021 m. birželio 7 d. Nr. V-1343
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 8 straipsnio 3 dalimi, 30 straipsniu, 32 straipsnio 2 dalimi, 33 straipsnio 1 dalimi, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 32–34 punktais ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais:

1. N u s p r e n d ž i u modernizuoti Lietuviškojo SNOMED CT žodyno informacinę sistemą į Medicinos nomenklatūrų ir klasifikatorių valdymo informacinę sistemą.

2. T v i r t i n u pridedamus:

2.1. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos nuostatus;

2.2. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos duomenų saugos nuostatus.

3. P a v e d u Lietuvos medicinos bibliotekos direktoriui:

3.1. paskirti Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos saugos įgaliotinį, administratorių;

3.2. per 6 mėnesius nuo šio įsakymo įsigaliojimo parengti ir teisės aktų nustatyta tvarka suderinti bei Lietuvos Respublikos sveikatos apsaugos ministerijai pateikti tvirtinti:

3.2.1. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos naudotojų administravimo taisyklių projektą;

3.2.2. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių projektą;

3.2.3. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos veiklos tęstinumo valdymo plano projektą.

4. P r i p a ž į s t u netekusiais galios:

4.1. Lietuvos Respublikos sveikatos apsaugos ministro 2013 m. spalio 9 d. įsakymą

Nr. V- 926 „Dėl Lietuviškojo SNOMED CT žodyno informacinės sistemos nuostatų patvirtinimo“;

4.2. Lietuvos Respublikos sveikatos apsaugos ministro 2013 m. spalio 28 d. įsakymą Nr. V- 983 „Dėl Lietuviškojo SNOMED CT žodyno informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

Sveikatos apsaugos ministras Arūnas Dulkys

SUDERINTA
Lietuvos Respublikos ekonomikos ir inovacijų ministerijos
2021-05-07 raštu Nr. (4.6-82Mr)-3-2143

SUDERINTA
Valstybinės duomenų apsaugos inspekcijos
2021-05-10 raštu Nr. 2R-2345 (3.2.Mr)

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos
2021-05-13 raštu Nr. (4.1)6K-388

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2021 m. birželio 7 d. įsakymu Nr. V-1343

MEDICINOS NOMENKLATŪRŲ IR KLASIFIKATORIŲ VALDYMO INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos nuostatai (toliau – Nuostatai) nustato Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos (toliau – Informacinė sistema) steigimo teisinį pagrindą, tikslą, uždavinius, asmens duomenų tvarkymo tikslą, pagrindines funkcijas, organizacinę, informacinę ir funkcinę struktūrą, duomenų teikimo ir naudojimo tvarką, duomenų saugos reikalavimus, finansavimą, modernizavimą ir likvidavimą.

2. Informacinė sistema tvarkoma vadovaujantis šiais teisės aktais:

2.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679);

2.2. Lietuvos Respublikos civiliniu kodeksu;

2.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

2.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

2.5. Lietuvos Respublikos sveikatos sistemos įstatymu;

2.6. Lietuvos Respublikos kibernetinio saugumo įstatymu;

2.7. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ (toliau – Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas);

2.8. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas);

2.9. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas);

2.10. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatais, patvirtintais Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarimu Nr. 1057 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų patvirtinimo“;

2.11. kitais teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, saugojimą bei sunaikinimą.

3. Nuostatuose vartojamos sąvokos ir jų apibrėžtys:

3.1. **SNOMED CT** – sisteminė medicinos klinikinių terminų nomenklatūra (angl. *Systematized Nomenclature of Medicine – Clinical Terms*).

3.2. **„SNOMED International“** – pelno nesiekianti organizacija, kuriai nuosavybės teise priklauso SNOMED CT ir kuri yra atsakinga už SNOMED CT palaikymą ir vystymą.

3.3. **LOINC** – tarptautinė laboratorinių tyrimų nomenklatūra, kuria vadovaujantis identifikuojami klinikiniai tyrimai ir keičiamasi standartizuotais klinikinių tyrimų duomenimis (angl. *Logical Observation Identifiers Names and Codes*).

3.4. **Informacinės sistemos naudotojas** – Lietuvos medicinos bibliotekos darbuotojas, dirbantis pagal darbo sutartį, ar kitas asmuo, Informacinės sistemos veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

3.5. **Išorinis Informacinės sistemos naudotojas** – su Lietuvos medicinos biblioteka darbo santykiais nesusijęs asmuo, Informacinės sistemos veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

3.6. **Vidinis Informacinės sistemos naudotojas** – Lietuvos medicinos bibliotekos darbuotojas, dirbantis pagal darbo sutartį, Informacinės sistemą veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

3.7. Kitos Nuostatuose vartojamos sąvokos apibrėžtos Civiliniame kodekse, Valstybės informacinių išteklių valdymo įstatyme ir Reglamente (ES) 2016/679, Lietuvos Respublikos įstatymuose ir kituose teisės aktuose, reglamentuojančiuose sveikatos sistemą ir informacinių sistemų steigimą, saugą ir administravimą.

4. Informacinės sistemos steigimo pagrindas – Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. spalio 17 d. įsakymas Nr. V-908 „Dėl Nacionalinio SNOMED CT terminologijos valdymo centro paskyrimo“.

5. Informacinės sistemos tikslas – suteikti prieigą prie Informacinės sistemos, elektroniniu būdu tvarkant ir teikiant SNOMED CT ir LOINC tarptautines ir lietuviškąsias versijas bei ėminių, mėginių, tyrimų metodų, tyrimų gabenimo ir kt. klasifikatorius (toliau – Medicinos nomenklatūros ir klasifikatoriai).

6. Informacinės sistemos uždaviniai:

6.1. elektroniniu būdu tvarkyti tarptautinius standartus atitinkančias Medicinos nomenklatūras ir klasifikatorius;

6.2. teikti sveikatinimo veiklą vykdančioms įstaigoms Medicinos nomenklatūras ir klasifikatorius, sudarant sąlygas įsidiegti juos Lietuvos informacinėse sveikatos sistemose bei naudoti elektroniniuose sveikatos įrašuose, siekiant užtikrinti vienodą medicininės informacijos turinio interpretaciją įvairiose e. sveikatos srityse.

7. Pagrindinės Informacinės sistemos funkcijos:

7.1. tvarkyti ir redaguoti Medicinos nomenklatūrų ir klasifikatorių turinį;

7.2. susieti SNOMED CT nacionalinius plėtinius ir terminus į hierarchinę struktūrą;

7.3. importuoti į lietuvių kalbą išverstas SNOMED CT ir LOINC, užtikrinant sąsajas ir loginius ryšius tarp skirtingų medicinos terminų;

7.4. atlikti Medicinos nomenklatūrų ir klasifikatorių terminų, identifikatorių, pavadinimų ir kodų paiešką;

7.5. valdyti skirtingų Medicinos nomenklatūrų ir klasifikatorių terminų, kodų, identifikatorių susiejimą (angl. *mapping*);

7.6. formuoti medicinos terminų ir pavadinimų duomenų rinkinius;

7.7. tvarkyti Informacinės sistemos tvarkytojo išduotų lietuviškosios ir tarptautinės SNOMED CT versijos licencijų (toliau – Licencijų) duomenis;

7.8. teikti duomenis Elektroninei sveikatos paslaugų ir bendradarbiavimo informacinei sistemai (toliau – ESPBI IS);

7.9. apdoroti duomenis ir formuoti ataskaitas;

7.10. administruoti Informacinės sistemos naudotojus.

8. Asmens duomenų tvarkymo Informacinėje sistemoje tikslai:

8.1. vienoda Informacinės sistemos naudotojų identifikacija;

8.2. vienoda Informacinės sistemos duomenų gavėjų identifikacija, išduodant Licencijas ir teikiant duomenis apie išduotas Licencijas tarptautinei sveikatos terminologijos standartų plėtros organizacijai „SNOMED International“ Licencijų administravimo tikslais;

8.3. Licencijos suteiktų teisių ir Informacinės sistemos duomenų gavėjų kontrolė, siekiant užtikrinti efektyvų medicinos nomenklatūrų ir klasifikatorių naudojimo valdymą bei apskaitą nepriklausomai nuo duomenų gavimo būdo;

8.4. Informacinės sistemos naudotojų informavimo užtikrinimas, kai to reikia Licencijų ar medicinos nomenklatūrų ir klasifikatorių administravimo paslaugoms teikti.

II SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINĖ STRUKTŪRA

9. Informacinės sistemos ir joje saugomų asmens duomenų valdytojas ir tvarkytojas – Lietuvos medicinos biblioteka (toliau – Informacinės sistemos valdytojas ir tvarkytojas).

Punkto pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

10. Informacinės sistemos duomenų teikėjai:

10.1. Informacinės visuomenės plėtros komitetas, teikiantis Valstybės informacinių išteklių sąveikumo platformos (toliau – VIISP) (valdytoja – Lietuvos Respublikos ekonomikos ir inovacijų ministerija) duomenis, nustatytus Nuostatų 23.1 papunktyje;

10.2. fiziniai asmenys, siekiantys gauti Licenciją naudoti SNOMED CT, teikia pirminius duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose, nustatytus Nuostatų 23.2 papunktyje;

10.3. fiziniai asmenys, norintys naudoti LOINC ir medicinos klasifikatorius, teikia pirminius duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose, nustatytus Nuostatų 23.4 papunktyje;

10.4. juridiniai asmenys, siekiantys gauti Licenciją naudoti SNOMED CT, teikia pirminius duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose, nustatytus Nuostatų 23.3 papunktyje;

10.5. juridiniai asmenys, norintys naudoti LOINC ir medicinos klasifikatorius, teikia pirminius duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose, nustatytus Nuostatų 23.5 papunktyje.

11. Informacinės sistemos valdytojas turi Valstybės informacinių išteklių valdymo įstatyme ir Reglamente (ES) 2016/679 nurodytas teises ir pareigas.

12. Lietuvos medicinos biblioteka, veikianti kaip Informacinės sistemos valdytojas, vykdo šias funkcijas:

Punkto pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

12.1. priima sprendimus, susijusius su Informacinės sistemos kūrimu, plėtra, likvidavimu, modernizavimu, priežiūra, administravimu, ir kontroliuoja jų vykdymą;

12.2. tvirtina su Informacinės sistemos veikla, informacinių ir ryšių technologijų infrastruktūra susijusius dokumentus;

12.3. tvirtina Informacinės sistemos kūrimo, plėtros planus ir projektus, Informacinės sistemos tvarkymo ir administravimo veiklos planus ir ataskaitas bei kontroliuoja jų vykdymą;

12.4. analizuoja teisines, technines, technologines, metodines ir organizacines Informacinės sistemos tvarkymo problemas ir pagal savo kompetenciją priima sprendimus, kurių reikia Informacinės sistemos veiklai užtikrinti;

12.5. išduoda Licencijas;

Papunkčio pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

12.6. teisės aktų nustatyta tvarka teikia informaciją apie Informacinės sistemos veiklą;

12.7. atlieka kitas Nuostatuose ir kituose teisės aktuose, susijusiuose su Informacinės sistemos valdymu, nustatytas funkcijas.

13. Informacinės sistemos tvarkytojas turi Valstybės informacinių išteklių valdymo įstatyme, Reglamente (ES) 2016/679 nurodytas teises ir pareigas.

14. Lietuvos medicinos biblioteka, veikianti kaip Informacinės sistemos tvarkytojas, vykdo šias funkcijas:

14.1. rengia su Informacinės sistemos veikla, informacinių ir ryšių technologijų infrastruktūra, duomenų tvarkymu ir sauga susijusių dokumentų projektus;

14.2. rengia Informacinės sistemos kūrimo, plėtros planus ir projektus, Informacinės sistemos tvarkymo bei administravimo veiklos planus ir ataskaitas;

14.3. užtikrina duomenų teikimą ESPBI IS nustatytu duomenų teikimo būdu ir formatu;

14.4. užtikrina, kad Informacinės sistemos duomenys būtų tvarkomi vadovaujantis Nuostatais, Nuostatuose nurodytais kitais įstatymais ir teisės aktais;

14.5. organizuoja vidinių Informacinės sistemos naudotojų mokymą;

14.6. tvarko asmens duomenis tik pagal Informacinės sistemos asmens duomenų valdytojo dokumentais įformintus nurodymus, įskaitant susijusius su asmens duomenų perdavimu į trečiąją valstybę ar tarptautinei organizacijai, išskyrus atvejus, kai tai daryti reikalaujama pagal Europos Sąjungos arba valstybės narės teisę, kuri yra taikoma Informacinės sistemos duomenų tvarkytojui;

14.7. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikoma atitinkama konfidencialumo prievolė;

14.8. imasi visų priemonių, kurių reikalaujama pagal Reglamento (ES) 2016/679 32 straipsnį – techninėmis ir organizacinėmis priemonėmis užtikrina duomenų saugą, tvarkomų asmens duomenų konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo netyčinio arba neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų ir nuo bet kokio kito neteisėto tvarkymo, taip pat saugų duomenų perdavimą kompiuteriniais tinklais;

14.9. atsižvelgdama į asmens duomenų tvarkymo pobūdį, Informacinės sistemos asmens duomenų valdytojo nustatyta tvarka, taikydama tinkamas technines ir organizacines priemones, padeda Informacinės sistemos asmens duomenų valdytojui įvykdyti Informacinės sistemos duomenų valdytojo prievolę atsakyti į prašymus pasinaudoti Reglamento (ES) 2016/679 III skyriuje nustatytomis duomenų subjekto teisėmis;

14.10. Informacinės sistemos asmens duomenų valdytojo nustatyta tvarka padeda Informacinės sistemos asmens duomenų valdytojui užtikrinti Reglamento 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdama į asmens duomenų tvarkymo pobūdį ir Informacinės sistemos asmens duomenų tvarkytojo turimą informaciją. Informuoja raštu ir (ar) el. paštu (nedelsiant, bet ne vėliau kaip per 24 valandas) Informacinės sistemos asmens duomenų valdytoją pagal Reglamento 33 straipsnio 2 dalį apie įvykusį asmens duomenų saugumo pažeidimą ir pateikia pranešimą Informacinės sistemos asmens duomenų valdytojo nustatyta tvarka;

14.11. nebevykdydama Informacinės sistemos asmens duomenų tvarkytojo funkcijų, atsižvelgdama į tvarkomų Informacinės sistemos asmens duomenų valdytojo nurodymus, Informacinės sistemos asmens duomenų tvarkytojas sunaikina arba grąžina tvarkomų asmens

duomenų Informacinės sistemos valdytojui visus asmens duomenis ir sunaikina turimas jų kopijas, išskyrus atvejus, kai pagal Europos Sąjungos ar Lietuvos Respublikos teisės aktus yra nustatyta pareiga juos saugoti;

14.12. atlieka kitas Nuostatuose ir kituose teisės aktuose, susijusiuose su Informacinės sistemos valdymu, nustatytas funkcijas.

Punkto pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

15. Išorinių Informacinės sistemos naudotojų teisės ir pareigos:

15.1. gauti prieigą prie Informacinės sistemos;

15.2. gauti prieigą prie medicinos nomenklatūrų ir klasifikatorių;

15.3. gauti informaciją apie Informacinėje sistemoje tvarkomus savo asmens duomenis;

15.4. reikalauti ištaisyti netikslius duomenis, kaip nurodyta Nuostatų 42 punkte;

15.5. tvarkyti (teikti naujus, tikslinti, papildyti) savo Informacinėje sistemoje kaupiamus asmens duomenis.

III SKYRIUS
INFORMACINĖS SISTEMOS INFORMACINĖ STRUKTŪRA

16. Informacinę struktūrą sudaro Informacinės sistemos duomenų saugykloje saugomos duomenų bazės:

16.1. SNOMED CT terminų, sujungtų į hierarchinę struktūrą, duomenų bazė;

16.2. lietuviškosios ir tarptautinės LOINC versijos identifikatorių, pavadinimų ir kodų duomenų bazė;

16.3. medicinos klasifikatorių duomenų bazė;

16.4. Licencijų ir Licencijų gavėjų duomenų bazė;

16.5. administravimo, ataskaitų ir statistinės informacijos duomenų bazė.

17. SNOMED CT terminų, sujungtų į hierarchinę struktūrą, duomenų bazėje tvarkomi SNOMED CT terminai ir jų tarpusavio sąsajos.

18. Lietuviškosios ir tarptautinės LOINC versijos identifikatorių, pavadinimų ir kodų duomenų bazėje tvarkomi identifikatoriai, pavadinimai ir kodai.

19. Medicinos klasifikatorių duomenų bazėje tvarkomi kodai ir pavadinimai.

20. Licencijų ir Licencijų gavėjų duomenų bazėje tvarkomi juridinių ir fizinių asmenų duomenys:

20.1. Licencijos identifikacinis numeris;

20.2. Licencijos gavėjo pavadinimas (esant juridiniam asmeniui) arba Licencijos gavėjo vardas ir pavardė (esant fiziniam asmeniui);

20.3. Licencijos gavėjo Juridinių asmenų registro kodas (esant juridiniam asmeniui) arba Licencijos gavėjo asmens kodas (esant fiziniam asmeniui);

20.4. Licencijos gavėjo gyvenamosios vietos adresas (esant fiziniam asmeniui) arba buveinės adresas (esant juridiniam asmeniui);

20.5. Licencijos išdavimo data;

20.6. Licencijos panaikinimo data;

20.7. kontaktinio asmens vardas ir pavardė (esant juridiniam asmeniui);

20.8. kontaktinio asmens telefono ryšio numeris;

20.9. kontaktinio asmens elektroninio pašto adresas.

21. Administravimo, ataskaitų ir statistinės informacijos duomenų bazėje tvarkomi:

21.1. vidinių Informacinės sistemos naudotojų duomenys (naudotojo identifikacinis kodas, slaptažodis, vardas, pavardė, kontaktinis telefono ryšio numeris, kontaktinis elektroninio pašto

adresas, pareigos) ir Medicinos nomenklatūrų ir klasifikatorių naudojimo duomenys (intensyvumas, terminų koregavimas, peržiūra ir tvirtinimas);

21.2. išorinių Informacinės sistemos naudotojų duomenys (naudotojo identifikacinis kodas, slaptažodis, vardas, pavardė, telefono ryšio numeris, elektroninio pašto adresas).

22. Administravimo, ataskaitų ir statistinės informacijos duomenų bazėje tvarkomi Informacinės sistemos komponentais sukurti duomenys:

22.1. Informacinės sistemos vidinių naudotojų veiksmų audito duomenys: veiksmo data, laikas, pobūdis (duomenų įrašymas, koregavimas, trynimas, naikinimas), naudotojo, susijusio su veiksmu, identifikacinis kodas, veiksmo rezultatas; naudotojų / administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas;

22.2. Informacinės sistemos veiksmų, veikimo sutrikimų ir kiti techniniai duomenys;

22.3. duomenų teikimo Informacinės sistemos duomenų gavėjams faktą patvirtinantys duomenys: duomenų teikimo tipas, data, laikas, duomenų apsikeitimo požymis (pavyko / nepavyko).

23. Informacinės sistemos duomenų teikėjai teikia šiuos duomenis:

23.1. VIISP teikia autentifikuotų Informacinės sistemos naudotojų duomenis (asmens kodas, vardas, pavardė);

23.2. fiziniai asmenys, siekiantys gauti Licenciją naudoti SNOMED CT, teikia asmens duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose (gyvenamosios vietos adresas, telefono ryšio numeris, elektroninio pašto adresas);

23.3. juridiniai asmenys, siekiantys gauti Licenciją naudoti SNOMED CT, teikia juridinio asmens duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose (adresas, kontaktinio asmens vardas ir pavardė, kontaktinio asmens telefono ryšio numeris, kontaktinio asmens elektroninio pašto adresas);

23.4. fiziniai asmenys, norintys naudoti LOINC ir medicinos klasifikatorius, teikia asmens duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose (telefono ryšio numeris, elektroninio pašto adresas);

23.5. juridiniai asmenys, norintys naudoti LOINC ir medicinos klasifikatorius, teikia asmens duomenis, nekaupiamus valstybės informacinėse sistemose ir registruose (buveinės adresas, kontaktinio asmens vardas ir pavardė, kontaktinio asmens telefono ryšio numeris, kontaktinio asmens elektroninio pašto adresas).

IV SKYRIUS
INFORMACINĖS SISTEMOS FUNKCINĖ STRUKTŪRA

24. Informacinės sistemos funkcinę struktūrą sudaro:

24.1. Medicinos terminų, identifikatorių, pavadinimų ir kodų paieškos posistemė;

24.2. Licencijų, Informacinės sistemos naudotojų ir Licencijų gavėjų administravimo ir ataskaitų posistemė;

24.3. SNOMED CT terminų ir jų tarpusavio sąryšių tvarkymo posistemė;

24.4. LOINC identifikatorių, pavadinimų ir kodų tvarkymo posistemė;

24.5. Medicinos klasifikatorių tvarkymo posistemė;

24.6. Medicinos nomenklatūrų ir klasifikatorių duomenų teikimo posistemė;

24.7. Terminų susiejimo posistemė;

24.8. Terminų rinkinių formavimo posistemė.

25. Medicinos terminų, identifikatorių, pavadinimų ir kodų paieškos posistemės funkcijos:

25.1. SNOMED CT terminų paieška pagal pasirinktus kriterijus;

25.2. SNOMED CT terminų, sinonimų ir jų sąsajų peržiūra;

25.3. LOINC identifikatorių, pavadinimų ir kodų paieška pagal pasirinktus kriterijus;

25.4. LOINC identifikatorių, pavadinimų ir kodų peržiūra;

25.5. medicinos klasifikatorių pavadinimų ir kodų paieška pagal pasirinktus kriterijus;

25.6. medicinos klasifikatorių pavadinimų ir kodų peržiūra.

26. Licencijų, Informacinės sistemos naudotojų ir Licencijų gavėjų administravimo ir ataskaitų posistemės funkcijos:

26.1. Informacinės sistemos naudotojų ir Licencijų gavėjų teisių tvarkymas, Licencijų išdavimas;

26.2. Informacinės sistemos naudotojų ir Licencijų gavėjų duomenų ir SNOMED CT archyvavimas;

26.3. ataskaitų pagal suvestus parametrus formavimas;

26.4. suformuotų ataskaitų sąrašų pateikimas;

26.5. ataskaitų peržiūra ekrane;

26.6. ataskaitų spausdinimas;

26.7. duomenų eksportavimas pagal nustatytą formatą;

26.8. nuasmenintų duomenų finansinei ir statistinei analizei naudojimo užtikrinimas;

26.9. Informacinės sistemos naudotojų tapatybės nustatymas, pasitelkiant VIISP priemones ar naudojant Informacinės sistemos naudotojo identifikacinį kodą arba elektroninį pašto adresą ir slaptažodį.

27. SNOMED CT terminų ir jų tarpusavio sąryšių tvarkymo posistemės funkcijos:

27.1. SNOMED CT terminų bei jų tarpusavio sąsajų peržiūra;

27.2. SNOMED CT terminų bei jų tarpusavio sąsajų redagavimas ir tvirtinimas;

27.3. egzistuojančių ir naujų SNOMED CT terminų vertimas.

28. LOINC identifikatorių, pavadinimų ir kodų tvarkymo posistemės funkcijos:

28.1. LOINC identifikatorių, pavadinimų ir kodų paieška ir peržiūra;

28.2. LOINC identifikatorių, pavadinimų ir kodų redagavimas, versijų valdymas;

28.3. naujų LOINC terminų sudarymas;

28.4. egzistuojančių ir naujų LOINC terminų vertimas;

28.5. LOINC versijų valdymas.

29. Medicinos klasifikatorių tvarkymo posistemės funkcijos:

29.1. medicinos klasifikatorių terminų, identifikatorių, pavadinimų ir kodų peržiūra, redagavimas ir tvirtinimas;

29.2. medicinos klasifikatorių paieška ir peržiūra;

29.3. medicinos klasifikatorių redagavimas, versijų valdymas;

29.4. medicinos klasifikatorių vertimas (taikoma tarptautiniams klasifikatoriams);

29.5. naujų medicinos klasifikatorių sudarymas.

30. Medicinos nomenklatūrų ir klasifikatorių duomenų teikimo posistemę sudaro:

30.1. SNOMED CT terminų ir jų tarpusavio sąsajų duomenų teikimo komponentas, kurio funkcijos:

30.1.1. SNOMED CT įkėlimas į Informacinę sistemą;

30.1.2. SNOMED CT terminų ir jų sąsajų konvertavimas į formatą, nustatytą Informacinės sistemos tvarkytojo ir duomenų gavėjo sudarytoje sutartyje (toliau – Duomenų teikimo sutartis);

30.1.3. Informacinės sistemos duomenų (Medicinos nomenklatūrų ir klasifikatorių terminai, identifikatoriai, pavadinimai ir kodai, duomenys apie jų tarpusavio sąsajas bei išduotų Licencijų duomenys, išvardyti Nuostatų 19.1–19.5 papunkčiuose) automatinis teikimas ESPBI IS ir sveikatinimo veiklą vykdančių įstaigų informacinėms sistemoms.

30.2. LOINC identifikatorių, pavadinimų ir kodų duomenų teikimo komponentas, kurio funkcijos:

30.2.1. LOINC identifikatorių, pavadinimų ir kodų įkėlimas į Informacinę sistemą;

30.2.2. LOINC identifikatorių, pavadinimų ir kodų automatinis teikimas ESPBI IS ir sveikatinimo veiklą vykdančių įstaigų informacinėms sistemoms;

30.3. medicinos klasifikatorių duomenų teikimo komponentas, kurio funkcijos:

30.3.1. medicinos klasifikatorių įkėlimas į Informacinę sistemą;

30.3.2. medicinos klasifikatorių automatinis teikimas ESPBI IS ir sveikatinimo veiklą vykdančių įstaigų informacinėms sistemoms.

31. Terminų susiejimo posistemės funkcijos:

31.1. terminų ir klasifikatorių paieška ir peržiūra;

31.2. terminų ir klasifikatorių sąsajų valdymas;

31.3. naujų terminų ir klasifikatorių sąsajų sudarymas.

32. Terminų rinkinių formavimo posistemės funkcijos:

32.1. terminų duomenų paketo iš nomenklatūros ar klasifikatoriaus duomenų suformavimas, sujungiant dalį tos pačios ar kelių nomenklatūrų bei klasifikatorių terminus;

32.2. suformuotų terminų duomenų paketų publikavimas duomenų mainų komponente.

V SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ TEIKIMAS IR NAUDOJIMAS

33. Informacinės sistemos duomenys Lietuvos Respublikos sveikatos apsaugos ministerijai (ESPBI IS), „SNOMED International“, sveikatos priežiūros institucijoms, kitiems fiziniams ir juridiniams asmenims (toliau – duomenų gavėjai) gali būti teikiami šiais būdais:

33.1. Informacinės sistemos duomenų ieškant ir juos peržiūrint kompiuterio ekrane pagal Informacinės sistemos duomenų gavėjo pateiktą užklausą neperduodant pačių duomenų;

33.2. Informacinės sistemos duomenis perduodant duomenų perdavimo kanalu pagal Informacinės sistemos duomenų gavėjo pateiktą užklausą;

33.3. Informacinės sistemos duomenis, nurodytus Nuostatų 20 punkte, perduodant pagal Informacinės sistemos duomenų gavėjo pateiktą užklausą ir atsižvelgiant į Informacinės sistemos duomenų gavėjui teikiamą informaciją.

34. Informacinės sistemos tvarkytojas teikia duomenų išrašus, pagal šios sistemos duomenis parengtas ataskaitas, apibendrintą, susistemintą ar kitaip apdorotą informaciją, Informacinės sistemos duomenų teikėjų pateiktus dokumentus ir (arba) jų kopijas.

35. Informacinėje sistemoje kaupiami duomenys teikiami tokio turinio ir formato, kokie yra saugomi ir naudojami Informacinėje sistemoje. Tais atvejais, kai teikiamų duomenų turinys ir forma neatitinka Informacinės sistemos duomenų gavėjų poreikių arba Informacinės sistemos duomenų gavėjas neturi techninių galimybių reikiamai apdoroti gaunamų duomenų, taip pat kai teikiamos informacijos turinys ir forma neatitinka kitų juridinių ar fizinių asmenų, kurie kreipiasi dėl tokios informacijos ir siekia ją pakartotinai panaudoti, poreikių, Informacinėje sistemoje kaupiami duomenys teikiami vadovaujantis Valstybės informacinių išteklių valdymo įstatymo 35 straipsnio nuostatomis.

36. Informacinės sistemos duomenų gavėjams Informacinės sistemos duomenys, išskyrus asmens duomenis, teikiami pagal duomenų teikimo sutartį (daugkartinio teikimo atveju) arba Informacinės sistemos duomenų gavėjo rašytinį prašymą (vienkartinio teikimo atveju). Duomenų teikimo sutartyje nurodomas Informacinės sistemos duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų Informacinės sistemos duomenų apimtis. Prašyme nurodomas duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, prašomų pateikti duomenų apimtis.

37. Informacinės sistemos asmens duomenis teikiant pagal sutartį, turi būti nurodyta asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų asmens duomenų apimtis. Informacinės sistemos asmens duomenis teikiant pagal gavėjo prašymą,

turi būti nurodyta asmens duomenų naudojimo tikslas, teikimo bei gavimo teisinis pagrindas ir prašomų pateikti asmens duomenų apimtis.

38. Informacinės sistemos asmens duomenys tvarkomi vadovaujantis Reglamentu (ES) 2016/679 ir kitais teisės aktais, reglamentuojančiais asmens duomenų gavimą ir teikimą. Informacinės sistemos asmens duomenys teikiami duomenų gavėjams vadovaujantis Reglamento (ES) 2016/679 nustatytais reikalavimais ir teisėto tvarkymo kriterijais bei kitais teisės aktais, reglamentuojančiais asmens duomenų teikimą fiziniams ir juridiniams asmenims. Informacinės sistemos asmens duomenys neteikiami, jeigu duomenų gavėjui gauti šiuos duomenis nėra teisinio pagrindo, numatyto Lietuvos Respublikos įstatymuose ir (ar) Europos Sąjungos teisės aktuose. Kai atsisakoma teikti Informacinėje sistemoje tvarkomus duomenis, asmeniui, pateikusiam prašymą juos gauti, pranešama apie priimtą sprendimą atsisakyti tenkinti prašymą ir suteikiama informacija apie tokio sprendimo apskundimo tvarką. Atsisakymas teikti duomenis gali būti skundžiamas teismui Lietuvos Respublikos įstatymų nustatyta tvarka.

39. Licencijų gavėjams Informacinės sistemos duomenys, t. y. SNOMED CT ir duomenys apie jų tarpusavio ryšius, teikiami pagal duomenų teikimo sutartį (daugkartinio teikimo atveju) arba Informacinės sistemos duomenų gavėjo rašytinį prašymą (vienkartinio teikimo atveju).

40. Informacinės sistemos duomenų gavėjai privalo Informacinės sistemos duomenis naudoti tik taip, kaip nustatyta Duomenų teikimo sutartyje. Informacinės sistemos duomenų gavėjas negali keisti iš Informacinės sistemos gautų duomenų ir juos naudodamas privalo nurodyti duomenų šaltinį.

41. Informacinės sistemos duomenys pakartotinio panaudojimo tikslais (statistinėms ataskaitoms) teikiami pagal duomenų teikimo sutartis, kuriose nurodomas duomenų gavimo teisinis pagrindas, tvarka, duomenų naudojimo tikslas ir apimtis, formatas ir gavimo būdas. Teikiami asmens duomenys nuasmeninami (pavyzdžiui, asmens kodas nėra teikiamas, vardas ir pavardė pakeičiami žodžiais „fizinis asmuo“ ir kt.).

42. Duomenų gavėjai, duomenų subjektai ir kiti asmenys turi teisę reikalauti ištaisyti netikslius duomenis. Fizinis ar juridinis asmuo, pastebėjęs netikslius duomenis, rašytiniu prašymu (pateiktu elektroninių ryšių priemonėmis, patvirtinančiomis besikreipiančiojo tapatybę, arba rašytiniu kreipimusi pateikiant prašymą asmeniškai atsakingam Informacinės sistemos tvarkytojo darbuotojui ir asmens tapatybę patvirtinantį dokumentą (įsitikinus besikreipiančiojo asmens tapatybe, asmens dokumentas grąžinamas), arba rašytiniu kreipimusi paštu, pateikiant asmens tapatybę patvirtinančio dokumento kopiją, patvirtintą teisės aktų nustatyta tvarka, turi kreiptis į Informacinės sistemos tvarkytoją, kuris, gavęs informaciją apie nustatytus jam perduotus netikslius duomenis, privalo per 5 darbo dienas nuo prašymo ir jame nurodytus faktus patvirtinančių dokumentų gavimo ištaisyti nurodytus netikslumus ir informuoti apie tai ištaisyti netikslius duomenis reikalavusį fizinį ar juridinį asmenį paštu arba elektroniniu paštu.

43. Informacinės sistemos duomenys Informacinės sistemos duomenų gavėjams teikiami neatlygintinai.

44. Informacinės sistemos duomenys Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių, trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami Valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka, o asmens duomenys – ir Reglamento (ES) 2016/679 bei kitų teisės aktų, reglamentuojančių asmens duomenų teikimą, nustatyta tvarka.

45. Informacinės sistemos duomenys, įskaitant asmens duomenis, neteikiami, jeigu Informacinės sistemos duomenų gavėjui gauti šiuos duomenis nėra teisinio pagrindo, numatyto Lietuvos Respublikos įstatymuose ir (ar) Europos Sąjungos teisės aktuose. Kai atsisakoma teikti Informacinėje sistemoje tvarkomus duomenis asmeniui, pateikusiam prašymą juos gauti, pranešama apie priimtą sprendimą atsisakyti tenkinti prašymą ir suteikiama informacija apie tokio sprendimo

apskundimo tvarką. Atsisakymas teikti Informacinės sistemos duomenis gali būti skundžiamas Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

46. Informacinės sistemos duomenų teikimas negali būti apribotas kitaip, negu nustato „SNOMED International“ licencinė sutartis, Lietuvos Respublikos įstatymai ar Europos Sąjungos teisės aktai. Atsisakymas teikti Informacinės sistemos duomenis turi būti motyvuojamas „SNOMED International“ licencinės sutarties teisiniu pagrindu, Lietuvos Respublikos įstatymų ar Europos Sąjungos teisės aktų normomis. Atsisakymą teikti Informacinės sistemos duomenis galima skųsti „SNOMED International“ licencinės sutarties ir Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGA

47. Informacinės sistemos duomenų saugaus tvarkymo reikalavimų laikymasis užtikrinamas vadovaujantis:

47.1. Reglamento (ES) 2016/679 nustatyta tvarka;

47.2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

47.3. Asmens duomenų teisinės apsaugos įstatymu;

47.4. Kibernetinio saugumo įstatymu;

47.5. Lietuvos standartais ir tarptautiniais standartais, reglamentuojančiais saugų informacinės sistemos duomenų tvarkymą.

48. Informacinės sistemos duomenų sauga organizuojama vadovaujantis Informacinės sistemos duomenų saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, parengtais ir patvirtintais vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimais.

49. Už Informacinės sistemos duomenų saugą teisės aktų nustatyta tvarka atsako Informacinės sistemos valdytojas ir tvarkytojas.

50. Tvarkant ir saugant Informacinėje sistemoje duomenis, turi būti imamasi duomenų saugos organizacinių, programinių, techninių, patalpų apsaugos ir administracinių priemonių, skirtų Informacinės sistemos duomenų konfidencialumui, prieinamumui, vientisumui ir autentiškumui užtikrinti ir apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, naudojimo, atskleidimo, taip pat bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų Informacinėje sistemoje saugomų duomenų pobūdį.

Punkto pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

51. Informacinėje sistemoje Licencijos gavėjo ir kontaktinio asmens duomenys pradedami kaupti nuo Licencijos išdavimo datos ir yra saugomi iki Licencijos panaikinimo datos.

52. Informacinėje sistemoje išorinio Informacinės sistemos naudotojo duomenys pradedami kaupti nuo išorinio Informacinės sistemos naudotojo registracijos Informacinėje sistemoje datos ir yra saugomi ne ilgiau, nei to reikalauja asmens duomenų tvarkymo tikslai arba iki išorinio Informacinės sistemos naudotojo prašymo panaikinti duomenis Informacinės sistemos tvarkytojui pateikimo.

53. Informacinėje sistemoje vidinio naudotojo asmens duomenys pradedami saugoti nuo teisių naudoti Informacinę sistemą darbuotojui, dirbančiam pagal darbo sutartį, suteikimo iki darbo sutarties nutraukimo.

54. Licencijų ir statistinės ataskaitos su asmens duomenimis, pateiktos „SNOMED International“, tvarkomos dvejus metus po ataskaitų parengimo.

55. Pasibaigus asmens duomenų tvarkymo terminams, nurodytiems Nuostatų 52, 53, 54, punktuose, asmens duomenys ir ataskaitos yra perkeliami į Informacinės sistemos duomenų archyvą, kuriame saugomi 3 metus. Suėjus terminui, duomenys sunaikinami, išskyrus tuos, kurie Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka turi būti perduoti valstybės archyvams.

56. Vidiniai Informacinės sistemos naudotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams.

VII SKYRIUS
INFORMACINĖS SISTEMOS FINANSAVIMAS

57. Informacinės sistemos kūrimas, diegimas, tobulinimas ir plėtra finansuojama Lietuvos Respublikos valstybės biudžeto ir Europos Sąjungos struktūrinių fondų lėšomis.

58. Informacinės sistemos eksploatacija finansuojama Lietuvos Respublikos valstybės biudžeto lėšomis.

VIII SKYRIUS
INFORMACINĖS SISTEMOS MODERNIZAVIMAS IR LIKVIDAVIMAS

59. Informacinė sistema modernizuojama ir likviduojama Valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo nustatyta tvarka.

60. Likviduojamos Informacinės sistemos duomenys perduodami kitai informacinei sistemai, kuri steigiama vietoj likviduojamos, arba sunaikinami, arba perduodami valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

61. Duomenų subjektų teisių, įtvirtintų Reglamente (ES) 2016/679, įgyvendinimo tvarką tvirtina Informacinės sistemos valdytojas.

62. Informacinės sistemos tvarkytojas ne rečiau kaip kartą per metus iki kiekvienų einamųjų metų pabaigos atnaujina (tikslina ar papildo) Nuostatus, atsižvelgdamas į susijusių teisės aktų ir (arba) Informacinės sistemos funkcionalumų pasikeitimus.

_____

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2021 m. birželio 7 d. įsakymu Nr. V-1343

MEDICINOS NOMENKLATŪRŲ IR KLASIFIKATORIŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Informacinės sistemos elektroninės informacijos saugos politikos tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti Informacinės sistemos duomenis, užtikrinant tvarkomos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

3. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. Informacinės sistemos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. Informacinės sistemos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. Informacinės sistemos tvarkymo kontrolė;

5.4. Informacinės sistemos paslaugų ir naudojimosi Informacinės sistemos elektronine informacija kontrolės užtikrinimas;

5.5. Informacinės sistemos tvarkomų asmens duomenų apsauga;

5.6. Informacinės sistemos veiklos tęstinumo užtikrinimas;

5.7. Informacinės sistemos naudotojų mokymas.

6. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojas.

7. Informacinės sistemos valdytojas atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

8. Informacinės sistemos tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą saugos politiką įgyvendinančiuose dokumentuose (toliau – saugos dokumentai) nustatyta tvarka.

9. Saugos nuostatai taikomi Informacinės sistemos valdytojui ir tvarkytojui – Lietuvos medicinos bibliotekai (Kaštonų g. 7, 01107 Vilnius), Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriams, Informacinės sistemos naudotojams, Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams.

Punkto pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

10. Lietuvos medicinos biblioteka, kaip Informacinės sistemos valdytoja, vykdo šias funkcijas:

Punkto pakeitimai:
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654

10.1. organizuoja Informacinės sistemos veiklą ir jai vadovauja;

10.2. rengia ir tvirtina teisės aktus, susijusius su duomenų sauga, ir prižiūri, kad Informacinės sistemos duomenys būtų tvarkomi vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais;

10.3. tvirtina Saugos nuostatus, saugos dokumentus ir kitus teisės aktus, susijusius su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu);

10.4. nagrinėja ir apibendrina Informacinės sistemos tvarkytojo pasiūlymus dėl Informacinės sistemos tobulinimo;

10.5. skiria Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorių arba paveda juos paskirti Informacinės sistemos tvarkytojui;

10.6. vykdo kitas Saugos reikalavimuose, Informacinės sistemos nuostatuose nustatytas funkcijas.

11. Lietuvos medicinos biblioteka, kaip Informacinės sistemos tvarkytoja, vykdo šias funkcijas:

11.1. atlieka Informacinės sistemos nuostatuose nustatytas funkcijas;

11.2. užtikrina tinkamą Informacinės sistemos sąveiką su kitomis informacinėmis sistemomis;

11.3. užtikrina saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

11.4. užtikrina, kad Informacinė sistema veiktų nepertraukiamai, organizuoja techninę priežiūrą;

11.5. rengia Informacinės sistemos saugos dokumentų projektus ir teikia tvirtinti Informacinės sistemos valdytojui;

11.6. užtikrina saugos dokumentų ir kitų valdytojo priimtų teisės aktų, susijusių su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

11.7. pagal kompetenciją įgyvendina Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

11.8. pagal kompetenciją užtikrina Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą);

11.9. atsako už informacijos tvarkymo Informacinėje sistemoje teisėtumą ir duomenų saugą;

11.10. ne rečiau kaip kartą per metus organizuoja saugos dokumentų peržiūrėjimą ir aktualizavimą;

11.11. atlieka kitas Informacinės sistemos valdytojo pavestas Informacinės sistemos nuostatuose, Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

12. Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą) užtikrina Informacinės sistemos saugos įgaliotinis.

13. Informacinės sistemos saugos įgaliotinis, užtikrindamas Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą), vykdo šias funkcijas:

13.1. koordinuoja ir prižiūri elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

13.2. teikia Informacinės sistemos valdytojui pasiūlymus dėl dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios, informacinių technologijų saugos reikalavimų atitikties vertinimo;

13.3. atlieka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

13.4. teikia Informacinės sistemos tvarkytojo vadovui siūlymus dėl Saugos nuostatų ir Informacinės sistemos saugos dokumentų priėmimo arba keitimo;

13.5. organizuoja Informacinės sistemos rizikos įvertinimą ir rengia rizikos įvertinimo ataskaitą;

13.6. supažindina Informacinės sistemos administratorius ir Informacinės sistemos naudotojus su Saugos nuostatų ir saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

13.7. organizuoja Informacinės sistemos naudotojų mokymus elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

13.8. registruoja elektroninės informacijos saugos (kibernetinio saugumo) incidentus, įvykusius Informacinėje sistemoje;

13.9. koordinuoja elektroninės informacijos saugos (kibernetinio saugumo) incidentų, įvykusių Informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo (kibernetinio saugumo) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetinio saugumo) incidentais;

13.10. pagal kompetenciją teikia Informacinės sistemos administratoriui ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos ir kibernetinio saugumo politikos įgyvendinimu;

13.11. atlieka kitas Informacinės sistemos tvarkytojo vadovo pavestas Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

14. Saugos įgaliotinis negali atlikti Informacinės sistemos administratoriaus funkcijų.

15. Informacinės sistemos administratorius vykdo šias funkcijas:

15.1. atsako už Informacinės sistemos funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą;

15.2. diegia ir prižiūri programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

15.3. suteikia teisę Informacinės sistemos naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

15.4. tikrina atsarginių Informacinės sistemos elektroninės informacijos kopijų atitiktį originalams;

15.5. vykdo pranešimų apie serverių operacinių sistemų bei duomenų bazių valdymo sistemų klaidas stebėseną ir imasi visų būtinų priemonių, kad būtų išvengta galimų gedimų;

15.6. užtikrina Informacinės sistemos komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustato Informacinės sistemos pažeidžiamas vietas;

15.7. pagal kompetenciją dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

15.8. informuoja Informacinės sistemos saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

15.9. vertina Informacinės sistemos naudotojų pasirengimą darbui su Informacine sistema;

15.10. rengia pasiūlymus dėl Informacinės sistemos kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

15.11. atlieka kitas Informacinės sistemos tvarkytojo vadovo ir saugos įgaliotinio pavestas Saugos nuostatuose ir saugos dokumentuose nustatytas funkcijas.

16. Teisės aktai, kuriais vadovaujamasi tvarkant informacinių sistemų elektroninę informaciją ir užtikrinant jos saugą:

16.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

16.2. Kibernetinio saugumo įstatymas;

16.3. Valstybės informacinių išteklių valdymo įstatymas;

16.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

16.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

16.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Elektroninės informacijos svarbos nustatymo gairių aprašas);

16.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

16.8. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Informacinių technologijų saugos atitikties vertinimo metodika);

16.9. Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

16.10. Saugos nuostatai, saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 9.2 ir 9.3 papunkčiais, Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai.

18. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12 punktu, Informacinė sistema priskiriama trečiai informacinių sistemų kategorijai.

19. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kartą per metus organizuoja Informacinės sistemos rizikos vertinimą. Pasikeitus Informacinės sistemos duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) ar po esminių organizacinių ar sisteminių pokyčių nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas. Informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

20. Organizuojant rizikos vertinimą turi būti paskirtas už rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas Informacinės sistemos tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

21. Informacinės sistemos rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Informacinės sistemos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, galimi rizikos valdymo būdai. Svarbiausieji rizikos veiksniai:

21.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

21.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

21.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

22. Informacinės sistemos rizikos veiksnių vertinimas atliekamas vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu.

23. Informacinės sistemos rizikos įvertinimo rezultatai ir priemonės rizikos veiksniams išvengti išdėstomi Rizikos įvertinimo ataskaitoje, kuri pateikiama Informacinės sistemos tvarkytojo vadovui.

24. Prireikus Informacinės sistemos valdytojas, atsižvelgdamas į rizikos analizės ataskaitą, tvirtina rizikos veiksnių valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms užtikrinti. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

25. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas.

26. Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Informacinės sistemos tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus jo vykdytojus paskiria ir įgyvendinimo terminus nustato Informacinės sistemos valdytojo vadovas.

27. Informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

28. Informacinės sistemos rizikos įvertinimo ataskaitos, Informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių plano, Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitos, taip pat pastebėtų trūkumų šalinimo plano kopijas Informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

29. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais principais:

29.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

29.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

29.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

30. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 17 ir 18 punktuose nustatytas Informacinės sistemos svarbos kategorijas ir vadovaujantis Saugos nuostatų 16 punkte nurodytais teisės aktais ir standartais.

31. Kibernetinio saugumo priemonės, nurodytos Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerosios saugumo praktikos rekomendacija.

32. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Informacinės sistemos elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

33. Programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

33.1. Informacinės sistemos tarnybinių stočių ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai ir operatyviai atnaujinamos automatiniu būdu;

33.2. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų;

33.3. Informacinės sistemos administratoriaus, Informacinės sistemos naudotojų kompiuterizuotose darbo vietose naudojama tik su tarnybine veikla susijusi programinė įranga. Periodiškai, ne rečiau kaip kas 4 mėnesius, turi būti tikrinama, ar nenaudojama nelegali programinė įranga; rasta nelegali programinė įranga turi būti nedelsiant pašalinta;

33.4. Elektroninio pašto saugai užtikrinti turi būti vadovaujamasi elektroninio pašto naudojimo reikalavimais, kurie apibrėžti Informacinės sistemos tvarkytojo vadovo patvirtintame

Kompiuterių tinklo, kompiuterinės ir programinės įrangos naudojimo ir administravimo tvarkos aprašo skyriuje „Elektroninio pašto ir interneto naudojimas“.

34. Detalios programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas neatnaujinimo laikas ir kt.) nustatomi Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

35. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

35.1. turi būti naudojama tik legali Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

35.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

35.3. turi būti įdiegta prieigos prie Informacinės sistemos elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

35.4. turi būti įgyvendinta prievolė keisti slaptažodžius ne rečiau kaip kas 3 mėnesius;

35.5. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Informacinės sistemos elektroninės informacijos, atliktus veiksmus;

35.6. Informacinės sistemos programinę įrangą diegti arba atnaujinti gali tik Informacinės sistemos administratorius ar Informacinės sistemos tvarkytojo įgalioti asmenys;

35.7. Informacinės sistemos naudotojo prieigos prie Informacinės sistemos laikas ir trukmė neribojami.

36. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

36.1. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

36.2. Informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. DOS), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project* (*OWASP*)) interneto svetainėje www.owasp.org;

36.3. Informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

36.4. Apsaugai nuo kenksmingos programinės įrangos bei naudojamos techninės ir programinės įrangos sutrikimų užtikrinti nuolat atnaujinamos serverių operacinės sistemos ir taikomosios programos. Serverių operacinės sistemos ir taikomosios programos atnaujinamos pagal techninės ir programinės įrangos gamintojo rekomendacijas.

37. Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

38. Leistinos kompiuterių naudojimo ribos:

38.1. stacionarūs ir nešiojamieji Informacinės sistemos naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Informacinės sistemos duomenys ir informacija;

38.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti taikomos papildomos saugos priemonės: informacija, esanti nešiojamuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose, turi būti šifruojama, nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis, jie turi būti atskirti nuo viešojo interneto tinklo užkarda;

38.3. Informacinės sistemos naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo;

38.4. nešiojamuosiuose kompiuteriuose negali būti jokios svarbios informacijos, išskyrus Informacinės sistemos naudotojo naudojamus darbo dokumentus.

39. Metodai, kuriais užtikrinamas saugus Informacinės sistemos elektroninės informacijos teikimas ir (ar) gavimas:

39.1. elektroninė informacija iš susijusių registrų, informacinių sistemų gaunama ir teikiama susijusiems registrams, informacinėms sistemoms tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

39.2. prieigos prie Informacinės sistemos elektroninės informacijos teises gali suteikti tik Informacinės sistemos administratorius. Informacinės sistemos naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

39.3. prieiga prie Informacinės sistemos elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie Informacinės sistemos elektroninės informacijos valdymas apibrėžtas Informacinės sistemos naudotojų administravimo taisyklėse;

39.4. pasibaigus Informacinės sistemos naudotojo darbo sutarčiai, teisė naudotis Informacinės sistemos elektronine informacija turi būti panaikinta. Informacinės sistemos naudotojui prieiga prie Informacinės sistemos turi būti ribojama ar sustabdoma, kai vyksta Informacinės sistemos naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos;

39.5. Informacinės sistemos saugai užtikrinti turi būti apribota fizinė prieiga prie Informacinės sistemos tarnybinių stočių (atskiros rakinamos patalpos arba rakinama spinta), patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

39.6. konkrečios Informacinės sistemos duomenų tvarkymo, teikimo ir saugumo procedūros išdėstomos Informacinės sistemos nuostatuose, Informacinės sistemos ir Saugaus elektroninės informacijos tvarkymo taisyklėse.

40. Informacinės sistemos atsarginės duomenų bazės kopijos daromos automatiniu būdu kas 24 valandas, esant aktyviai Informacinės sistemos duomenų bazei. Kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų).

41. Prireikus atkurti kopijas tokią teisę turi tik Informacinės sistemos administratorius ar jį pavaduojantis asmuo. Periodiškai, bet ne rečiau kaip kartą per pusmetį, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai. Patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

42. Kopijų darymo ir saugojimo tvarka nustatoma Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

43. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami Informacinės sistemos saugos (kibernetinio saugumo) politiką įgyvendinančiuose dokumentuose.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

44. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės

informacijos saugą (kibernetinį saugumą). Informacinės sistemos tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

45. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

46. Informacinės sistemos administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti Informacinės sistemos komponentus (stebėti Informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti Informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.). Informacinės sistemos administratoriai turi būti susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais.

47. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

48. Informacinės sistemos naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose ar pareigybės aprašyme.

49. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

49.1. Informacinės sistemos naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams, informacinių sistemų administratoriams ir pan.);

49.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, Informacinės sistemos naudotojų ar informacinių sistemų administratorių poreikius;

49.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

49.4. mokymai Informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas Informacinės sistemos saugos įgaliotinis. Mokymai Informacinės sistemos saugos įgaliotiniui ir Informacinės sistemos administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

50. Tvarkyti Informacinės sistemos duomenis gali tik įgalioti Informacinės sistemos naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

51. Informacinės sistemos naudotojų supažindinimą su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą organizuoja Informacinės sistemos saugos įgaliotinis. Informacinės sistemos naudotojai, pažeidę Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

52. Informacinės sistemos saugos įgaliotinis pakartotinai supažindina tik su iš esmės pasikeitusiais Informacinės sistemos saugą reguliuojančiais teisės aktais. Su teisės aktais, išvardytais Nuostatuose ir kituose saugos dokumentuose, Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis (kibernetinio saugumo vadovas) ir kiti Informacinės sistemos naudotojai susipažįsta savarankiškai ir jais turi vadovautis tvarkydami Informacinę sistemą.

53. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Informacinės sistemos tvarkytojo interneto svetainėje.

54. Informacinės sistemos naudotojų supažindinimo su Saugos nuostatais ir saugos dokumentais tvarka nustatyta Informacinės sistemos naudotojų administravimo taisyklėse.

55. Tvarkyti Informacinės sistemos elektroninę informaciją gali tik Informacinės sistemos naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų. Informacinės sistemos naudotojai atsako už Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

56. Informacinės sistemos naudotojai, Informacinės sistemos administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

57. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos. Keičiami saugos dokumentai gali būti nederinami su Nacionaliniu kibernetinio saugumo centru tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos šių dokumentų kopijos.

58. Saugos nuostatai ir saugos dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

_____

Pakeitimai:

1.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-414, 2023-04-06, paskelbta TAR 2023-04-06, i. k. 2023-06654
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2021 m. birželio 7 d. įsakymo Nr. V-1343 „Dėl Lietuviškojo SNOMED CT žodyno informacinės sistemos modernizavimo ir Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos nuostatų bei Medicinos nomenklatūrų ir klasifikatorių valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo