LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTERIJOS VALDOMŲ IR VALSTYBĖS ĮMONĖS REGISTRŲ CENTRO TVARKOMŲ ELEKTRONINĖS SVEIKATOS SISTEMOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ IR DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMO IŠANKSTINĖS PACIENTŲ REGISTRACIJOS INFORMACINĖJE SISTEMOJE TVARKOS APRAŠO PATVIRTINIMO

2019 m. liepos 3 d. Nr. V-777
Vilnius

Vadovaudamasis 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, 12, 19, 26, 31 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, 6 punktu ir 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrojo duomenų apsaugos reglamento) 24 straipsnio 1 dalimi ir atsižvelgdamas į Europos Komisijos 2018 m. sausio 24 d. komunikatą Europos Parlamentui ir Tarybai „Didesnė apsauga, naujos galimybės. Komisijos gairės dėl tiesioginio Bendrojo duomenų apsaugos reglamento taikymo nuo 2018 m. gegužės 25 d.“:

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

1.1. Lietuvos Respublikos sveikatos apsaugos ministerijos valdomų ir Valstybės įmonės Registrų centro tvarkomų elektroninės sveikatos sistemos informacinių sistemų duomenų saugos nuostatus;

1.2. Duomenų subjektų teisių įgyvendinimo Išankstinės pacientų registracijos informacinėje sistemoje tvarkos aprašą.

2. P a v e d u:

2.1. Lietuvos Respublikos sveikatos apsaugos ministerijos valdomų ir Valstybės įmonės Registrų centro tvarkomų elektroninės sveikatos sistemos informacinių sistemų – Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos ir Išankstinės pacientų registracijos informacinės sistemos (toliau – informacinės sistemos) – pagrindiniam tvarkytojui valstybės įmonei Registrų centrui:

2.1.1. paskirti informacinių sistemų koordinuojantįjį saugos įgaliotinį ir informacinių sistemų administratorius;

2.1.2. per 6 mėnesius nuo šio įsakymo įsigaliojimo parengti ir pateikti Lietuvos Respublikos sveikatos apsaugos ministerijai informacinių sistemų elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką įgyvendinančių dokumentų projektus;

2.2. informacinių sistemų tvarkytojams – sveikatinimo veiklą vykdančioms įstaigoms, užsiimančioms asmens sveikatos priežiūros, visuomenės sveikatos priežiūros, farmacine ar kita sveikatinimo veikla, – savo įstaigose paskirti informacinių sistemų saugos įgaliotinius ir administratorius.

2.3. Įsakymo vykdymą kontroliuoti viceministrui pagal veiklos sritį.

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

3.1. Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. kovo 17 d. įsakymą Nr. V-360 „Dėl Išankstinės pacientų registracijos informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

3.2. Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. spalio 7 d. įsakymą Nr. V-889 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais.

Sveikatos apsaugos ministras Aurelijus Veryga

SUDERINTA:
Nacionalinio kibernetinio saugumo centro
2019-01-22 raštu Nr. (4.2)6K-53

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2019 m. liepos 3 d. įsakymu Nr. V-777

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTERIJOS VALDOMŲ IR VALSTYBĖS ĮMONĖS REGISTRŲ CENTRO TVARKOMŲ ELEKTRONINĖS SVEIKATOS SISTEMOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos sveikatos apsaugos ministerijos valdomų ir Valstybės įmonės Registrų centro tvarkomų elektroninės sveikatos sistemos informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos ir Išankstinės pacientų registracijos informacinės sistemos (toliau – informacinės sistemos) elektroninės informacijos saugos (kibernetinio saugumo) politiką.

2. 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 Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai).

3. Saugos dokumentų taikymas ir naudojimas:

3.1. Saugos dokumentai taikomi:

3.1.1. Lietuvos Respublikos sveikatos apsaugos ministerijai (Vilniaus g. 33, 01506 Vilnius) – informacinių sistemų valdytojui;

3.1.2. valstybės įmonei Registrų centrui (toliau – Registrų centras) (Lvovo g. 25-101, 09320 Vilnius) – pagrindiniam informacinių sistemų tvarkytojui;

3.1.3. sveikatinimo veiklą vykdančioms įstaigoms, užsiimančioms asmens sveikatos priežiūros, visuomenės sveikatos priežiūros, farmacine ar kita sveikatinimo veikla, kurios rūšis ir reikalavimus ją vykdantiems subjektams nustato Lietuvos Respublikos sveikatos apsaugos ministerija (toliau – sveikatinimo įstaigos), – informacinių sistemų tvarkytojams;

3.1.4. saugos įgaliotiniui, informacinių sistemų administratoriams, informacinių sistemų naudotojams, informacinėms sistemoms funkcionuoti reikalingų paslaugų teikėjams;

3.2. saugos nuostatai yra vieši ir skelbiami Lietuvos Respublikos teisės aktų registre. Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių, informacinių sistemų veiklos tęstinumo valdymo plano, informacinių sistemų naudotojų administravimo taisyklių naudojimas yra ribojamas – informacinių sistemų naudotojams, informacinėms sistemoms funkcionuoti reikalingų paslaugų teikėjams ir kitiems tretiesiems asmenims suteikiama teisė susipažinti tik su saugos dokumentų santrauka Saugos nuostatų V skyriuje nustatyta tvarka.

4. Saugos dokumentų santrauka rengiama vadovaujantis būtinumo žinoti principu. Saugos dokumentų santrauką tvirtina informacinių sistemų valdytojas.

5. Elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetinės kryptys:

5.1. elektroninės informacijos saugos – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo – užtikrinimas;

5.2. informacinių sistemų kibernetinio saugumo užtikrinimas;

5.3. asmens duomenų apsauga;

5.4. informacinių sistemų naudotojų mokymas.

6. Elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo tikslai:

6.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

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

6.3. 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.

7. Informacinių sistemų valdytojo – Sveikatos apsaugos ministerijos – funkcijos:

7.1. organizuoti ir vadovauti informacinių sistemų veiklai;

7.2. rengti ir tvirtinti teisės aktus, susijusius su duomenų sauga, ir prižiūrėti, kaip jų laikomasi;

7.3. kontroliuoti, kad informacinės sistemos būtų tvarkomos vadovaujantis Lietuvos Respublikos valstybės įstatymais, informacinių sistemų duomenų saugos nuostatais ir kitais teisės aktais;

7.4. tvirtinti Saugos nuostatus ir saugos politiką įgyvendinančius dokumentus (toliau – saugos dokumentai) ir kitus teisės aktus, susijusius su informacinių sistemų elektroninės informacijos sauga (kibernetiniu saugumu);

7.5. nagrinėti informacinių sistemų tvarkytojų pasiūlymus dėl informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;

7.6. skirti informacinių sistemų saugos įgaliotinius ir informacinių sistemų administratorius arba pavesti juos paskirti savo organizacijose informacinių sistemų tvarkytojams;

7.7. atlikti kitas informacinių sistemų nuostatuose ir Saugos nuostatuose nustatytas funkcijas.

8. Pagrindinio informacinių sistemų tvarkytojo – Registrų centro – funkcijos:

8.1. atlikti informacinių sistemų nuostatuose nustatytas funkcijas;

8.2. užtikrinti informacinių sistemų nepertraukiamą veiklą;

8.3. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

8.4. pagal kompetenciją prižiūrėti informacinių sistemų duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus ir kitus informacinių sistemų komponentus, užtikrinti jų veikimą;

8.5. užtikrinti saugos dokumentų ir kitų informacinių sistemų valdytojo priimtų teisės aktų, susijusių su informacinių sistemų elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

8.6. pagal kompetenciją įgyvendinti informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

8.7. pagal kompetenciją užtikrinti informacinių sistemų elektroninės informacijos saugą (kibernetinį saugumą);

8.8. teikti informacinių sistemų valdytojui pasiūlymus dėl informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

8.9. informacinių sistemų valdytojui pavedus, skirti koordinuojantįjį saugos įgaliotinį ir informacinių sistemų administratorius;

8.10. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrėjimą (persvarstymą);

8.11. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 20 punkte nurodytuose teisės aktuose nustatytas informacinių sistemų tvarkytojo funkcijas savo organizacijose.

9. Informacinių sistemų tvarkytojų – sveikatinimo įstaigų – funkcijos:

9.1. pagal kompetenciją prižiūrėti kompiuterius, operacines sistemas ir kitus informacinių sistemų komponentus savo sveikatinimo įstaigose, užtikrinti jų veikimą;

9.2. užtikrinti administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą informacinių sistemų naudotojų kompiuteriuose ir kituose informacinių sistemų komponentuose savo sveikatinimo įstaigose;

9.3. užtikrinti organizacinėmis, techninėmis, technologinėmis ir metodinėmis priemonėmis saugų informacinių sistemų elektroninės informacijos tvarkymą savo sveikatinimo įstaigose;

9.4. valdyti elektroninės informacijos saugos (kibernetinius) incidentus savo sveikatinimo įstaigose ir juos šalinti;

9.5. užtikrinti saugos dokumentų ir kitų informacinių sistemų valdytojo priimtų teisės aktų, susijusių su informacinių sistemų elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

9.6. pagal kompetenciją įgyvendinti informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus savo sveikatinimo įstaigose;

9.7. pagal kompetenciją užtikrinti informacinių sistemų elektroninės informacijos saugą (kibernetinį saugumą) savo sveikatinimo įstaigose.

10. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako informacinių sistemų valdytojas ir informacinių sistemų tvarkytojai.

11. Informacinių sistemų valdytojas atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

12. Informacinių sistemų tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą saugos dokumentuose nustatyta tvarka.

13. Saugos įgaliotinių funkcijos:

13.1. Koordinuojančiojo saugos įgaliotinio funkcijos:

13.1.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą Saugos dokumentuose nustatyta tvarka;

13.1.2. teikti informacinės sistemos valdytojo vadovui pasiūlymus dėl:

13.1.2.1.saugos dokumentų priėmimo, keitimo;

13.1.2.2.informacinių technologijų saugos atitikties vertinimo atlikimo pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos krašto apsaugos ministro;

13.1.3. organizuoti rizikos ir informacinių technologijų saugos atitikties įvertinimą;

13.1.4. koordinuoti informacinės sistemos tvarkytojų paskirtų saugos įgaliotinių veiklą ir teikti paskirtiems saugos įgaliotiniams konsultacijas elektroninės informacijos saugos klausimais;

13.1.5. atlikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

13.1.6. koordinuojantis saugos įgaliotinis, atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus saugos įgaliotiniams, administratoriams ir kitiems informacinių sistemų valdytojo ir informacinių sistemų tvarkytojų darbuotojams, jeigu tai būtina elektroninės informacijos saugos (kibernetinio saugumo) politikai įgyvendinti;

13.1.7. atlikti kitas saugos dokumentuose ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše saugos įgaliotiniui priskirtas funkcijas.

13.2. Informacinių sistemų tvarkytojų paskirtų saugos įgaliotinių funkcijos:

13.2.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą savo organizacijose Saugos dokumentuose nustatyta tvarka;

13.2.2. teikti informacinių sistemų tvarkytojo vadovui pasiūlymus dėl informacinių sistemų administratorių savo organizacijose paskyrimo ir reikalavimų jiems nustatymo;

13.2.3. teikti koordinuojančiajam saugos įgaliotiniui pasiūlymus dėl saugos dokumentų priėmimo ir keitimo;

13.2.4. pagal kompetenciją dalyvauti atliekant informacinių sistemų rizikos vertinimą ir informacinių sistemų informacinių technologijų saugos atitikties vertinimą;

13.2.5. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą savo organizacijose ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos (kibernetinio saugumo) darbo grupės;

13.2.6. informuoti koordinuojantįjį saugos įgaliotinį apie elektroninės informacijos saugos (kibernetiniais) incidentus, įvykusius informacinėse sistemose;

13.2.7. teikti informacinių sistemų administratoriams ir informacinių sistemų naudotojams privalomus savo organizacijose vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimo;

13.2.8. atlikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d.

nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

13.2.9. informacinių sistemų tvarkytojų paskirti saugos įgaliotiniai, atlikdami savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus kitiems darbuotojams savo organizacijose, jeigu tai būtina elektroninės informacijos saugos (kibernetinio saugumo) politikai įgyvendinti.

14. Saugos įgaliotiniai negali atlikti informacinių sistemų administratoriaus funkcijų.

15. Informacinių sistemų administratorių grupės:

15.1. koordinuojantysis administratorius, prižiūrintis informacinių sistemų administratorių veiklą, siekdamas užtikrinti tinkamą informacinių sistemų administratorių funkcijų vykdymą;

15.2. informacinių sistemų naudotojų administratoriai, atliekantys funkcijas, susijusias su informacinių sistemų naudotojų teisių valdymu savo organizacijoje;

15.3. informacinių sistemų komponentų administratoriai, atliekantys funkcijas, susijusias su informacinių sistemų komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazėmis ir jų valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo ir prevencijos sistemomis, elektroninės informacijos perdavimo tinklais, duomenų saugyklomis, bylų serveriais ir kita technine ir programine įranga, kurios pagrindu funkcionuoja informacinės sistemos ir užtikrinama jose tvarkomos elektroninės informacijos sauga (kibernetinis saugumas) ir šių informacinių sistemų komponentų sąranka savo organizacijoje;

15.4. saugos administratoriai, atliekantys funkcijas, susijusias su informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena savo organizacijoje.

16. Informacinių sistemų administratoriai yra atsakingi už tinkamą saugos dokumentuose nustatytų funkcijų vykdymą.

17. Informacinių sistemų administratoriai privalo vykdyti visus saugos įgaliotinių nurodymus ir pavedimus dėl informacinių sistemų saugos (kibernetinio saugumo) užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

18. Atlikdami informacinių sistemų sąrankos pakeitimus, informacinių sistemų komponentų administratoriai turi laikytis informacinių sistemų pokyčių valdymo tvarkos, nustatytos informacinių sistemų valdytojo tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse.

19. Informacinių sistemų komponentų administratoriai informacinių sistemų sąranką ir informacinių sistemų būsenos rodiklius privalo tikrinti (peržiūrėti) reguliariai – ne rečiau kaip kartą per metus ir (arba) po informacinių sistemų pokyčio.

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

20.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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) (OL 2016 L 119, p. 1);

20.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

20.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

20.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

20.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

20.6. 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 – Klasifikavimo gairių aprašas);

20.7. Techniniai elektroninės informacijos saugos reikalavimai;

20.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

20.9. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

21. Informacinėse sistemose tvarkomos elektroninės informacijos svarbos kategorijos:

21.1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinėje sistemoje tvarkoma elektroninė informacija priskiriama ypatingos svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 7.1–7.3 papunkčių nuostatomis;

21.2. Išankstinės pacientų registracijos informacinėje sistemoje tvarkoma elektroninė informacija priskiriama vidutinės svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 9.1 ir 9.2 papunkčių nuostatomis.

22. Informacinių sistemų svarbos kategorijos:

22.1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema pagal joje tvarkomos informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.1 papunkčiu, priskiriama pirmajai kategorijai;

22.2. Išankstinės pacientų registracijos informacinė sistema pagal joje tvarkomos informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčiu, priskiriama trečiajai kategorijai.

23. Rizikos vertinimo organizavimas:

23.1. Koordinuojantysis saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet arba po esminių organizacinių ar sisteminių pokyčių organizuoja informacinių sistemų rizikos įvertinimą savo organizacijoje. Informacinių sistemų rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

23.2. Prireikus, koordinuojantysis saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą. Informacinių sistemų tvarkytojo rašytiniu pavedimu informacinių sistemų rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Organizuojant rizikos vertinimą, rekomenduojama

informacinių sistemų rizikos vertinimą įtraukti į informacinių sistemų tvarkytojų veiklos rizikos vertinimo procesus.

23.3. 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 informacinių sistemų pagrindinio informacinių sistemų tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

23.4. Rizikos vertinimo metu turi būti:

23.4.1. nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos informacinių sistemų saugai (kibernetiniam saugumui);

23.4.2. nustatomos galimos grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritys;

23.4.3. įvertinama informacinių sistemų pažeidimo grėsmių tikimybė ir galimos pasekmės;

23.4.4. nustatomas rizikos lygis ir įvertinamos identifikuotos galimos grėsmės, kurios išdėstomos prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą.

23.5. Informacinių sistemų rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama informacinių sistemų valdytojo vadovui ir informacinių sistemų tvarkytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

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

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

23.5.3. 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.

23.6. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

23.7. Atsižvelgdamas į rizikos vertinimo ataskaitą, informacinių sistemų valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

23.8. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

23.9. Atsižvelgiant į atlikto rizikos vertinimo rezultatus, taip pat jeigu Saugos nuostatų 24 punkte nustatyta tvarka atliekamo informacinių technologijų saugos atitikties vertinimo metu

nustatoma kibernetinių incidentų valdymo ir šalinimo, organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinamas informacinių sistemų veiklos tęstinumo valdymo planas ir (arba) kibernetinių incidentų valdymo planas. Šių planų veiksmingumo išbandymo rezultatai išdėstomi šių planų veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitose, kurių kopijos ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

24. Informacinių technologijų saugos atitikties vertinimo organizavimas:

24.1. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų įgyvendinimo savo organizacijoje organizavimą ir kontrolę, ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip, turi būti organizuojamas Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos informacinių technologijų saugos atitikties vertinimas. Išankstinės pacientų registracijos informacinės sistemos informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas ne rečiau kaip kartą per dvejus metus, jei kituose teisės aktuose nenustatyta kitaip.

24.2. Ne rečiau kaip kartą per trejus metus Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos informacinių technologijų saugos atitikties vertinimą turi atlikti nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai. Nepriklausomą informacinių technologijų saugos atitikties vertinimą organizuoja informacinių sistemų valdytojas arba informacinių sistemų valdytojas šį vertinimą paveda organizuoti pagrindiniam informacinių sistemų tvarkytojui.

24.3. Informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka.

24.4. Informacinių sistemų 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.

24.5. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos vertinimo ataskaita, kuri pateikiama informacinių sistemų valdytojo vadovui ir informacinių sistemų tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinių sistemų valdytojo vadovas.

24.6. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

25. Elektroninės informacijos saugos (kibernetinio saugumo) būklės gerinimas:

25.1. Techninės, programinės, organizacinės ir kitos informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonės pasirenkamos atsižvelgiant į informacinių sistemų valdytojo turimus išteklius, vadovaujantis šiais principais:

25.1.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

25.1.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei.

25.2. Atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 22 punkte nustatytas informacinių sistemų svarbos kategorijas vadovaujantis Saugos nuostatų 20 punkte nurodytais teisės aktais ir standartais.

27. 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 gerąja saugumo praktikos rekomendacija.

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

29. Pagrindinės organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų nuostatos:

29.1. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami informacinių sistemų saugos (kibernetinio saugumo) politiką įgyvendinančiuose dokumentuose.

29.2. Turi būti naudojama ir operatyviai atnaujinama programinė įranga, skirta informacinėms sistemoms nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.) apsaugoti. Detalios šios programinės įrangos naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas neatnaujinimo laikas ir kt.) nustatomi informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse.

29.3. Informacinių sistemų techninėje įrangoje ir informacinių sistemų naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga. Detalios programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos, atnaujinimo ir kt. reikalavimai nustatomi informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse.

29.4. Turi būti naudojama kompiuterių tinklo filtravimo įranga (užkardos, turinio kontrolės sistemos, įgaliotieji serveriai (angl. *proxy*) ir kt.). Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse.

29.5. Užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojamas šifravimas, virtualus privatus tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodų, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie informacinių sistemų būdai, protokolai, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimai teikti ir (ar) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir pan.), aprašymai pateikiami informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse.

29.6. Stacionarius kompiuterius leidžiama naudoti tik informacinių sistemų valdytojo ir informacinių sistemų tvarkytojų patalpose. Nešiojamiesiems kompiuteriams, išnešamiems iš informacinių sistemų valdytojo ar informacinių sistemų tvarkytojų patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir pan.).

30. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

30.1. Atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. *recovery point objetive*) ir priimtiną informacinių sistemų neveikimo laikotarpį (angl. *recovery time objective*).

30.2. Atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokia apimtimi, kad informacinių sistemų veiklos sutrikimo, elektroninės informacijos saugos (kibernetinio) incidento ar elektroninės informacijos vientisumo praradimo atvejais informacinių sistemų neveikimo laikotarpis nebūtų ilgesnis, nei nustatyta konkrečioms informacinių sistemų svarbos kategorijoms, nurodytoms Saugos nuostatų 22 punkte, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus.

30.3. Atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau kaip nustatyta informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse, nurodytais terminais.

30.4. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos.

30.5. Atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje kitose patalpose, nei yra informacinių sistemų tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate.

30.6. Periodiškai, bet ne rečiau kaip kartą per pusmetį turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai.

30.7. Patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

31. Informacinių sistemų naudotojų, informacinių sistemų administratorių, saugos įgaliotinio kvalifikacijos ir patirties reikalavimai:

31.1. Informacinių sistemų naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose.

31.2. Visi informacinių sistemų naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos 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.

31.3. 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). Informacinių sistemų tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

31.4. 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.

31.5. Informacinių sistemų administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti informacinių sistemų komponentus (stebėti informacinių sistemų komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti informacinių sistemų komponentų nepertraukiamą funkcionavimą ir pan.). Informacinių sistemų administratoriai turi būti susipažinę su saugos dokumentais.

32. Informacinių sistemų naudotojų ir informacinių sistemų administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

32.1. Informacinių sistemų 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.).

32.2. 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, informacinių sistemų naudotojų ar informacinių sistemų administratorių poreikius.

32.3. 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.).

32.4. Mokymai informacinių sistemų naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Mokymai saugos įgaliotiniui ir informacinių sistemų administratoriams turi būti organizuojami pagal poreikį. Už mokymų savo organizacijose organizavimą pagal kompetenciją atsakingi saugos įgaliotiniai.

V SKYRIUS

INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

33. Informacinių sistemų naudotojų ir informacinių sistemų administratorių supažindinimą su saugos dokumentais ar jų santrauka, atsakomybe už saugos dokumentų nuostatų pažeidimus savo organizacijose pagal kompetenciją organizuoja saugos įgaliotiniai.

34. Informacinių sistemų naudotojų supažindinimo su saugos dokumentais ar jų santrauka būdai turi būti pasirenkami atsižvelgiant į informacinių sistemų specifiką (pvz., informacinių sistemų ir jų naudotojų lokaciją, organizacinių ar techninių priemonių, leidžiančių identifikuoti su saugos dokumentais ar jų santrauka susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir pan.). Informacinių sistemų naudotojai su saugos dokumentais ar jų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą.

35. Pakartotinai su saugos dokumentais ar jų santrauka informacinių sistemų naudotojai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba elektroninės informacijos saugą (kibernetinį saugumą) reglamentuojantiems teisės aktams.

36. Tvarkyti informacinių sistemų elektroninę informaciją gali tik informacinių sistemų naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų.

37. Informacinių sistemų naudotojai atsako už informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją. Informacinių sistemų naudotojai, informacinių sistemų 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

38. Informacinių sistemų valdytojas saugos dokumentus gali keisti savo arba koordinuojančiojo saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru. 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.

39. Informacinių sistemų saugos dokumentai peržiūrimi (persvarstomi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems informacinių sistemų valdytojo ar tvarkytojų pokyčiams. Persvarsčius (peržiūrėjus) saugos dokumentus, turi būti nustatoma, kuriuos iš juose nustatytų elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti informacinių sistemų saugą (kibernetinį saugumą).

_____

PATVIRTINTA
Lietuvos Respublikos sveikatos
apsaugos ministro
2019 m. liepos 3 d. įsakymu Nr. V-777

DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMO IŠANKSTINĖS PACIENTŲ REGISTRACIJOS INFORMACINĖJE SISTEMOJE TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Duomenų subjektų teisių įgyvendinimo Išankstinės pacientų registracijos informacinėje sistemoje tvarkos aprašo (toliau – Aprašas) tikslas – nustatyti duomenų subjektų teisių įgyvendinimo tvarką Lietuvos Respublikos sveikatos apsaugos ministerijos valdomoje Išankstinės pacientų registracijos informacinėje sistemoje (toliau – IPR informacinė sistema), siekiant įgyvendinti atskaitomybės principą.

2. Įgyvendinant duomenų subjektų teises, vadovaujamasi 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) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

3. Apraše vartojamos sąvokos atitinka Reglamente (ES) 2016/679 vartojamas sąvokas.

4. Aprašas parengtas vadovaujantis Reglamentu (ES) 2016/679 bei atsižvelgiant į Europos Komisijos 2018 m. sausio 24 d. komunikatą Europos Parlamentui ir Tarybai „Didesnė apsauga, naujos galimybės. Komisijos gairės dėl tiesioginio Bendrojo duomenų apsaugos reglamento taikymo nuo 2018 m. gegužės 25 d.“

5. Duomenų subjektų teises šio Aprašo nustatyta tvarka įgyvendina IPR informacinės sistemos asmens duomenų tvarkytojas valstybės įmonė Registrų centras (toliau – Registrų centras). Jei dėl teisių įgyvendinimo duomenų subjektas kreipiasi į Sveikatos apsaugos ministeriją, jo prašymas persiunčiamas Registrų centrui.

II SKYRIUS
TEISĖ GAUTI INFORMACIJĄ APIE DUOMENŲ TVARKYMĄ

6. Informacija apie atliekamą duomenų subjekto asmens duomenų tvarkymą nurodyta Reglamento (ES) 2016/679 13 straipsnyje, pateikiama asmens duomenų gavimo metu duomenų subjektui registruojantis interneto portale www.e.sveikata.lt, taip pat Registrų centro interneto svetainėje www.registrucentras.lt/asmens_duomenu_apsauga/.

7. Kai duomenų subjekto asmens duomenys renkami ne iš duomenų subjekto, informacija, nurodyta Reglamento (ES) 2016/679 14 straipsnio 1 dalyje, duomenų subjektui neteikiama, kadangi taikoma šio straipsnio 5 dalies c punkte nustatyta išimtis.

III SKYRIUS
TEISĖ SUSIPAŽINTI SU DUOMENIMIS

8. Duomenų subjektui pateikus prašymą susipažinti su savo asmens duomenimis, tvarkomais IPR informacinėje sistemoje, Registrų centras turi pateikti:

8.1. informaciją, ar duomenų subjekto asmens duomenys tvarkomi, ar ne;

8.2. su asmens duomenų tvarkymu susijusią informaciją, numatytą Reglamento (ES) 2016/679 15 straipsnio 1 ir 2 dalyse, jeigu duomenų subjekto asmens duomenys yra tvarkomi;

8.3. tvarkomų asmens duomenų kopijas.

IV SKYRIUS
TEISĖ REIKALAUTI IŠTAISYTI DUOMENIS

9. Duomenų subjektas, vadovaudamasis Reglamento (ES) 2016/679 16 straipsniu, turi teisę reikalauti, kad bet kokie jo tvarkomi netikslūs asmens duomenys būtų ištaisyti, o neišsamūs – papildyti.

10. Siekdamas įsitikinti, kad tvarkomi duomenų subjekto asmens duomenys yra netikslūs ar neišsamūs, Registrų centras gali duomenų subjekto paprašyti pateikti tai patvirtinančius įrodymus.

11. Jeigu duomenų subjekto asmens duomenys (ištaisyti pagal duomenų subjekto prašymą) buvo perduoti duomenų gavėjams, Registrų centras šiuos duomenų gavėjus apie tai informuoja, nebent tai būtų neįmanoma ar pareikalautų neproporcingų pastangų. Duomenų subjektas turi teisę prašyti, kad jam būtų pateikta informacija apie tokius duomenų gavėjus.

V SKYRIUS
TEISĖ REIKALAUTI IŠTRINTI DUOMENIS (TEISĖ BŪTI PAMIRŠTAM)

12. Duomenų subjekto teisė ištrinti jo asmens duomenis (teisė būti pamirštam), numatyta Reglamento (ES) 2016/679 17 straipsnyje, įgyvendinama tik tuo atveju, jei duomenys IPR informacinėje sistemoje tvarkomi neteisėtai.

13. Duomenų subjekto teisė reikalauti ištrinti asmens duomenis (teisė būti pamirštam) gali būti neįgyvendinta Reglamento (ES) 2016/679 17 straipsnio 3 dalyje numatytais atvejais.

14. Jeigu duomenų subjekto asmens duomenys (ištrinti pagal duomenų subjekto prašymą) buvo perduoti duomenų gavėjams, Registrų centras šiuos duomenų gavėjus apie tai informuoja, nebent tai būtų neįmanoma ar pareikalautų neproporcingų pastangų. Duomenų subjektas turi teisę prašyti, kad jam būtų pateikta informacija apie tokius duomenų gavėjus.

VI SKYRIUS
TEISĖ APRIBOTI DUOMENŲ TVARKYMĄ

15. Reglamento (ES) 2016/679 18 straipsnio 1 dalyje numatytais atvejais Registrų centras privalo įgyvendinti duomenų subjekto teisę apriboti jo asmens duomenų tvarkymą.

16. Asmens duomenys, kurių tvarkymas apribotas, yra saugomi, o prieš tokio apribojimo panaikinimą duomenų subjektas yra informuojamas tokiu būdu, kokiu pateikė prašymą dėl asmens duomenų tvarkymo apribojimo.

17. Jeigu duomenų subjekto asmens duomenys (kurių tvarkymas apribotas pagal duomenų subjekto prašymą) buvo perduoti duomenų gavėjams, Registrų centras šiuos duomenų gavėjus apie tai informuoja, nebent tai būtų neįmanoma ar pareikalautų neproporcingų pastangų. Duomenų subjektas turi teisę prašyti, kad jam būtų pateikta informacija apie tokius duomenų gavėjus.

VII SKYRIUS
TEISĖ Į DUOMENŲ PERKELIAMUMĄ

18. IPR informacinėje sistemoje neatliekamas asmens duomenų tvarkymas, grindžiamas duomenų subjekto sutikimu pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies a punktą arba 9 straipsnio 2 dalies a punktą arba sutartimi pagal 6 straipsnio 1 dalie b punktą, todėl duomenų subjektui netaikoma teisė į duomenų perkeliamumą pagal Reglamento (ES) 2016/679 20 straipsnį.

VIII SKYRIUS
TEISĖ NESUTIKTI SU DUOMENŲ TVARKYMU

19. IPR informacinėje sistemoje neatliekamas asmens duomenų tvarkymas pagal Reglamento (ES) 2016/679 6 straipsnio 1 dalies e arba f punktus, įskaitant profiliavimą, todėl duomenų subjektui netaikoma teisė nesutikti su duomenų tvarkymu pagal Reglamento (ES) 2016/679 21 straipsnį.

IX SKYRIUS
TEISĖ REIKALAUTI, KAD NEBŪTŲ TAIKOMAS TIK AUTOMATIZUOTU DUOMENŲ TVARKYMU, ĮSKAITANT PROFILIAVIMĄ, GRINDŽIAMAS SPRENDIMAS

20. Duomenų subjekto teisė reikalauti, kad nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas pagal Reglamento (ES) 2016/679 22 straipsnį, nėra įgyvendinama tvarkomų asmens duomenų tvarkymo atžvilgiu, nes Registrų centras, tvarkydamas asmens duomenis IPR informacinėje sistemoje, nepriima tik automatizuotu duomenų tvarkymu grindžiamų sprendimų.

X SKYRIUS
PRAŠYMO ĮGYVENDINTI DUOMENŲ SUBJEKTO TEISES PATEIKIMAS

21. Kreiptis dėl duomenų subjekto teisių įgyvendinimo duomenų subjektas turi teisę žodžiu arba raštu, pateikdamas prašymą asmeniškai, paštu ar elektroninėmis priemonėmis:

21.1. siųsdamas prašymą adresu: Vinco Kudirkos g. 18-3, 03105 Vilnius;

21.2. siųsdamas prašymą elektroniniu paštu info@registrucentras.lt.

22. Jeigu dėl duomenų subjekto teisių įgyvendinimo kreipiamasi žodžiu ar prašymas pateiktas raštu asmeniškai, duomenų subjektas turi patvirtinti savo tapatybę pateikdamas asmens tapatybę

patvirtinantį dokumentą. To nepadarius, duomenų subjekto teisės nėra įgyvendinamos. Ši nuostata netaikoma, jeigu duomenų subjektas kreipiasi dėl informavimo apie asmens duomenų tvarkymą pagal Reglamento (ES) 2016/679 13 ir 14 straipsnius.

23. Jeigu dėl duomenų subjekto teisių įgyvendinimo kreipiamasi raštu, pateikiant prašymą paštu, kartu su prašymu turi būti pateikta notaro patvirtinta asmens tapatybę patvirtinančio dokumento kopija. Teikiant prašymą elektroninėmis priemonėmis, prašymas turi būti pasirašytas kvalifikuotu elektroniniu parašu arba turi būti suformuotas elektroninėmis priemonėmis, kurios leidžia užtikrinti teksto vientisumą ir nepakeičiamumą. Ši nuostata netaikoma, jeigu duomenų subjektas kreipiasi dėl informavimo apie asmens duomenų tvarkymą pagal Reglamento (ES) 2016/679 13 ir 14 straipsnius.

24. Prašymas įgyvendinti duomenų subjekto teises turi būti įskaitomas, asmens pasirašytas, jame turi būti nurodyta duomenų subjekto vardas, pavardė, asmens kodas, adresas ir (ar) kiti kontaktiniai duomenys ryšiui palaikyti ar kuriais pageidaujama gauti atsakymą dėl duomenų subjekto teisių įgyvendinimo.

25. Savo teises duomenų subjektas gali įgyvendinti pats arba per atstovą.

26. Asmens atstovas prašyme turi nurodyti savo vardą, pavardę, adresą ir (ar) kitus kontaktinius duomenis ryšiui palaikyti, kuriais asmens atstovas pageidauja gauti atsakymą, taip pat atstovaujamo asmens vardą, pavardę asmens kodą bei pateikti atstovavimą patvirtinantį dokumentą ar jo kopiją.

27. Esant abejonių dėl duomenų subjekto tapatybės, duomenų valdytojas prašo papildomos ją patvirtinančios informacijos.

28. Kreipiantis raštu dėl duomenų subjekto teisių įgyvendinimo, rekomenduojama pateikti Aprašo priede nurodytos formos prašymą.

29. Visais klausimais, susijusiais su duomenų subjekto asmens duomenų tvarkymu ir naudojimusi savo teisėmis, duomenų subjektas turi teisę kreiptis į duomenų apsaugos pareigūną telefono numeriu
(8 5) 268 8233, el. paštu duomenusauga@registrucentras.lt arba siųsdamas prašymą paštu adresu: Vinco Kudirkos g. 18-3, 03105 Vilnius. Siekiant užtikrinti Reglamento (ES) 2016/679 38 straipsnio 5 dalyje įtvirtintą konfidencialumą, kreipiantis į duomenų apsaugos pareigūną paštu, ant voko užrašoma, kad korespondencija yra skirta duomenų apsaugos pareigūnui.

XI SKYRIUS
PRAŠYMO ĮGYVENDINTI DUOMENŲ SUBJEKTO TEISES NAGRINĖJIMAS

30. Gavus duomenų subjekto prašymą, ne vėliau kaip per vieną mėnesį nuo prašymo gavimo jam pateikiama informacija apie tai, kokių veiksmų buvo imtasi pagal gautą prašymą. Jeigu bus vėluojama pateikti informaciją per nurodytą terminą, duomenų subjektas apie tai ir apie galimybę pateikti skundą Valstybinei duomenų apsaugos inspekcijai informuojamas, nurodant vėlavimo priežastis.

31. Jeigu prašymas pateiktas nesilaikant Aprašo X skyriuje nustatytos tvarkos ir reikalavimų, jis nenagrinėjamas ir nedelsiant, bet ne vėliau kaip per 10 darbo dienų duomenų subjektas apie tai informuojamas nurodant priežastis.

32. Jeigu prašymo nagrinėjimo metu nustatoma, kad duomenų subjekto teisės yra apribotos Reglamento (ES) 2016/679 23 straipsnio 1 dalyje numatytais pagrindais, apie tai informuojamas duomenų subjektas.

33. Informacija pagal duomenų subjekto prašymą dėl jo teisių įgyvendinimo pateikiama valstybine kalba.

34. Visi veiksmai pagal duomenų subjekto prašymus įgyvendinti duomenų subjekto teises atliekami ir informacija teikiama nemokamai. Kai duomenų subjekto prašymai yra akivaizdžiai nepagrįsti arba neproporcingi, visų pirma dėl jų pasikartojančio turinio, Registrų centras gali atsisakyti imtis veiksmų pagal prašymą.

35. Registrų centro veiksmus ar neveikimą įgyvendinant duomenų subjekto teises duomenų subjektas turi teisę skųsti pats arba duomenų subjekto atstovas, taip pat jo įgaliota ne pelno įstaiga, organizacija ar asociacija, atitinkanti Reglamento (ES) 2016/679 80 straipsnio reikalavimus, Valstybinei duomenų apsaugos inspekcijai, A. Juozapavičius g. 6, Vilnius, el. paštas ada@ada.lt, interneto svetainė www.ada.lt, taip pat Vilniaus apygardos administraciniam teismui.

36. Dėl duomenų subjekto teisių pažeidimo patyrus materialinę ar nematerialinę žalą, duomenų subjektas turi teisę į kompensaciją, dėl kurios priteisimo turi teisę kreiptis į Vilniaus apygardos administracinį teismą.

_____

Duomenų subjektų teisių įgyvendinimo
Išankstinės pacientų registracijos
informacinėje sistemoje
tvarkos aprašo
priedas

(Prašymo įgyvendinti duomenų subjekto teisę (-es) rekomenduojama forma)

_____
(duomenų subjekto vardas, pavardė, asmens kodas)

_____
(adresas ir (ar) kiti kontaktiniai duomenys (telefono numeris ar el. pašto adresas (nurodoma pareiškėjui pageidaujant)

_____
(atstovas ir atstovavimo pagrindas, jeigu prašymą pateikia duomenų subjekto atstovas)

Valstybės įmonei Registrų centrui
Vinco Kudirkos g. 18-3
03105 Vilnius

PRAŠYMAS
ĮGYVENDINTI DUOMENŲ SUBJEKTO TEISĘ (-ES)
IŠANKSTINĖS PACIENTŲ REGISTRACIJOS INFORMACINĖJE SISTEMOJE

_____
(data)

_____
(vieta)

1. Prašau įgyvendinti šią (šias) duomenų subjekto teisę (-es):
(Tinkamą langelį pažymėkite kryželiu):

- ☐ Teisę susipažinti su duomenimis
- ☐ Teisę reikalauti ištaisyti duomenis
- ☐ Teisę reikalauti ištrinti duomenis (teisė būti pamirštam)
- ☐ Teisę apriboti duomenų tvarkymą.

2. Nurodykite, ko konkrečiai prašote, ir pateikite kiek įmanoma daugiau informacijos, kuri leistų tinkamai įgyvendinti Jūsų teisę (-es) *(pavyzdžiui, jeigu norite gauti asmens duomenų kopiją, nurodykite, kokių konkrečiai duomenų (pavyzdžiui, 2018 m. x mėn. x d. elektroninio pašto laiško kopiją; jeigu norite ištaisyti duomenis, nurodykite, kokie konkrečiai Jūsų asmens duomenys yra netikslūs; jeigu nesutinkate, kad būtų tvarkomi Jūsų asmens duomenys, nurodykite argumentus, kuriais grindžiate savo nesutikimą, nurodykite, dėl kokio konkrečiai duomenų tvarkymo nesutinkate)*:

_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____.

PRIDEDAMA[1]:

1. _____.
2. _____.
3. _____.
4. _____.

_____ _____

(Parašas) (Vardas, pavardė)

[1] Jeigu prašymas yra siunčiamas paštu, prie prašymo pridedama asmens tapatybę patvirtinančio dokumento kopija, patvirtinta notaro ar kita teisės aktų nustatyta tvarka.

Jeigu kreipiamasi dėl netikslių duomenų ištaisymo, pateikiamos tikslius duomenis patvirtinančių dokumentų kopijos; jeigu jos siunčiamos paštu, turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka.

Jeigu duomenų subjekto asmens duomenys, tokie kaip vardas, pavardė, yra pasikeitę, kartu pateikiamos dokumentų, patvirtinančių šių duomenų pasikeitimą, kopijos; jeigu jos siunčiamos paštu, tuomet turi būti patvirtintos notaro ar kita teisės aktų nustatyta tvarka.