Lietuvos sveikatos mokslų universiteto Kauno ligoninė

VIEŠOSIOS ĮSTAIGOS LIETUVOS SVEIKATOS MOKSLŲ UNIVERSITETO KAUNO LIGONINĖS GENERALINIS DIREKTORIUS

ĮSAKYMAS DĖL VIEŠOSIOS ĮSTAIGOS LIETUVOS SVEIKATOS MOKSLŲ UNIVERSITETO KAUNO LIGONINĖS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO

2022 m. spalio 11 d. Nr. 1V-527

Kaunas

Vadovaudamasis Lietuvos Respublikos viešųjų įstaigų įstatymo 9 straipsnio 4 dalimi, viešosios įstaigos Lietuvos sveikatos mokslų universiteto Kauno ligoninės (toliau – Ligoninė) mokslų universiteto Kauno ligoninės įstatų 37.2. ir 37.3. punktais, 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) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu:

1. T v i r t i n u viešosios įstaigos Lietuvos sveikatos mokslų universiteto Kauno ligoninės asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą (toliau – Aprašas) (pridedama).

2. Į p a r e i g o j u:

2.1. Dokumentų valdymo skyriaus vyriausiąją specialistę Teresą Gutovskają su šiuo įsakymu pasirašytinai supažindinti Ligoninės direktorius, direktorių pavaduotojus, vadovą intervencinei medicinai, struktūrinių padalinių vadovus/vedėjus, filialo P. Mažylio gimdymo namai vadovą, vyr. slaugos administratorius, vyresniuosius slaugytojus-administratorius, vyr. koordinatorius, vyr. slaugytojus, vyr. akušerius, vyr. technologus, Vidaus audito ir Juridinio skyriaus darbuotojus;

2.2. visus struktūrinių padalinių vadovus/vedėjus, vadovą intervencinei medicinai, filialo P. Mažylio gimdymo namai vadovą, vyr. slaugos administratorius, vyresniuosius slaugytojus-administratorius, vyr. koordinatorius, vyr. slaugytojus, vyr. akušerius, vyr. technologus patvirtintu tvarkos aprašu pasirašytinai supažindinti dokumentų valdymo sistemos priemonėmis pavaldžius esamus ir būsimus darbuotojus;

3. P a v e d u įsakymo vykdymo kontrolę sau.

4. Šis įsakymas gali būti skundžiamas Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka.

Generalinis direktorius Albinas Naudžiūnas

Parengė
V. Bučinskaitė
2022-10-11

VIEŠOSIOS ĮSTAIGOS LIETUVOS SVEIKATOS MOKSLŲ UNIVERSITETO KAUNO LIGONINĖS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO TVARKOS APRAŠAS

Parengė: Viktorija Bučinskaitė Juridinio skyriaus vadovė 2022-10- 11	Suderinta: Darius Petraitis Vidaus audito skyriaus vadovas 2022-10-11 Evaldas Bačiulis Informacinių technologijų skyriaus vadovas 2022-10- 11

TURINYS

1. PASKIRTIS

1.1. Viešosios įstaigos Lietuvos sveikatos mokslų universiteto Kauno ligoninės Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas (toliau – Aprašas) nustato asmens duomenų saugumo pažeidimų (toliau – pažeidimas) ir jų priežasčių klasifikavimą, pranešimo apie pažeidimus viešajai įstaigai Lietuvos sveikatos mokslų universiteto Kauno ligoninei (toliau – Ligoninė), Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) ir duomenų subjektams, pažeidimų tyrimo, jų ir jų pasekmių pašalinimo ir mažinimo, pažeidimų prevencijos ir dokumentavimo tvarką.

1.2. Aprašas parengtas atsižvelgiant į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (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) (toliau – Reglamentas).

1.3. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme bei Ligoninės generalinio direktoriaus 2021 m. balandžio 14 d. įsakymu Nr. IV-240 „Viešosios įstaigos Lietuvos sveikatos mokslų universiteto Kauno ligoninės kibernetinių incidentų valdymo planas" patvirtintame Kibernetinių incidentų valdymo plane.

2. TAIKYMO SRITIS

Aprašas taikomas visiems Ligoninės darbuotojams, tvarkantiems (renkantiems, įrašantiems, sisteminantiems, saugojantiems, keičiantiems, gaunantiems, susipažinusiems, naudojantiems ir t.t.), asmens duomenis, ir Ligoninės pasitelktiems juridiniams ir fiziniams asmenims, tvarkantiems asmens duomenis Ligoninės vardu ir pagal jos nurodymus (toliau – duomenų tvarkytojai), kuriems pagal Reglamento 33 straipsnio 2 dalį yra nustatyta prievolė pranešti Ligoninei apie pažeidimą.

3. ATSAKOMYBĖ

3.1. Ligoninės generalinis direktorius paskiria darbuotojus, atsakingus už asmens duomenų pažeidimų valdymą;

3.2. Informacinių technologijų skyriaus vadovas arba jo įgaliotas asmuo atsakingas dėl asmens duomenų, tvarkomų Ligoninės informacinėje sistemoje ir (ar) apdorojamų kitomis Ligoninės informacinių technologijų priemonėmis, pažeidimų valdymo;

3.3. Ligoninės generalinio direktoriaus paskirtas darbuotojas, vykdantis Asmens duomenų pareigūno funkcijas (toliau – Asmens duomenų apsaugos pareigūnas), atsakingas dėl asmens duomenų, nenurodytų šio Aprašo 3.2. papunktyje, pažeidimų valdymo bei už šio Aprašo įgyvendinimo priežiūrą.

3.4. Visi Ligoninės darbuotojai, pasirašytinai susipažinę su šiuo Aprašu, įsipareigoja laikytis jame įtvirtintų nuostatų ir pranešti Asmens duomenų apsaugos pareigūnui apie bet kokius galimus asmens duomenų saugos pažeidimus. Ligoninės darbuotojai privalo išsaugoti esamos situacijos, susijusios su galimu pažeidimu, įrodymus, kad vėliau būtų galima tirti pažeidimą. Už Aprašo nesilaikymą taikoma atsakomybė teisės aktų nustatyta tvarka.

4. APRAŠYMAS

4.1. PAŽEIDIMŲ IR JŲ PRIEŽASČIŲ KLASIFIKAVIMAS

4.1.1. Pažeidimai pagal pobūdį (tipą) yra:

4.1.1.1. konfidencialumo pažeidimas – netyčinis arba neteisėtas asmens duomenų laikinas ar nuolatinis atskleidimas ar prieigos prie asmens duomenų suteikimas asmenims, kurie neturi teisės susipažinti su asmens duomenimis;

4.1.1.2. prieinamumo pažeidimas – neteisėtas, laikinas ar nuolatinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas;

4.1.1.3. vientisumo pažeidimas – neteisėtas asmens duomenų laikinas ar nuolatinis pakeitimas;

4.1.1.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių Aprašo 4.1.1.1- 4.1.1.3. papunkčiuose nurodytų pažeidimų derinys.

4.1.2. Pažeidimai gali būti nulemti šių priežasčių:

4.1.2.1. netyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas neturint tikslo tai padaryti (dėl duomenų tvarkymo klaidos, informacijos laikmenų, duomenų įrašų klaidingo įvedimo, ištrynimo, sunaikinimo ar sistemų sutrikimų dėl elektros tiekimo nutrūkimo, įvykusio dėl asmens veiklos, kompiuterinio viruso, paskleisto dėl asmens veiklos, vidaus taisyklių pažeidimo, sistemos priežiūros trūkumo, programinės įrangos testų atlikimo, netinkamos duomenų laikmenų priežiūros, netinkamo ryšio linijų pajėgumo ir apsaugos nustatymo, kompiuterių integravimo į tinklą, netinkamos kompiuterinių programų apsaugos parinkimo ir kt.);

4.1.2.2. tyčiniai veiksmai, kai asmens duomenų saugumas pažeidžiamas sąmoningai turint tikslą tai padaryti (neteisėtas įsibrovimas į asmens duomenų tvarkytojo patalpas, asmens duomenų laikmenų saugyklas, informacines sistemas, kompiuterių tinklą, tyčinis nustatytų taisyklių tvarkant asmens duomenis pažeidimas, sąmoningas kompiuterinio viruso platinimas, asmens duomenų vagystė, neteisėtas naudojimasis kito Ligoninės darbuotojo teisėmis ir kt.);

4.1.2.3. *force majeure* ir kiti netikėti įvykiai, kurių negalima kontroliuoti, numatyti ir užkirsti kelio jų atsiradimui (žaibas, gaisras, potvynis, užliejimas, audros, elektros instaliacijos degimas, temperatūros ir (ar) drėgmės pakitimų poveikis, purvo, dulkių ir magnetinių laukų įtaka, techninės avarijos, išskyrus nurodytas Aprašo 4.1.2.1. papunktyje, ir kt.).

4.2. PRANEŠIMAS APIE GALIMĄ PAŽEIDIMĄ IR JO NAGRINĖJIMAS

4.2.1. Ligoninės darbuotojas, sužinojęs ar pats nustatęs galimą pažeidimą arba kai informacija apie galimą pažeidimą gaunama iš kito šaltinio (toliau – galimo pažeidimo paaiškėjimas), privalo:

4.2.1.1. tą pačią darbo dieną, ne vėliau kaip per 1 (vieną) darbo valandą nuo galimo pažeidimo paaiškėjimo momento, informuoti žodžiu, raštu ar elektroninėmis priemonėmis savo tiesioginį vadovą, Ligoninės duomenų apsaugos pareigūną;

4.2.1.2. užpildyti Aprašo 1 priede nustatytos formos pranešimą apie galimą asmens duomenų saugumo pažeidimą ir nedelsiant, bet ne vėliau kaip per 2 (dvi) darbo valandas nuo galimo pažeidimo paaiškėjimo momento perduoti jį Ligoninės duomenų apsaugos pareigūnui;

4.2.1.3. jei įmanoma, turimų kompetencijų ribose, imtis priemonių užkirsti kelią tolimesniam pažeidimo vykdymui ar išplitimui.

4.2.2. Asmens duomenų apsaugos pareigūnas, šio Aprašo 4.2.1.1 ir 4.2.1.2 papunkčiuose nurodyta tvarka gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą, privalo:

4.2.2.1. informaciją apie galimą pažeidimą fiksuoti Asmens duomenų saugumo pažeidimų registracijos žurnale (Aprašo 2 priedas) (toliau – Žurnalas);

4.2.2.2. atlikti pažeidimo tyrimą Aprašo 4.3. punkte nustatyta tvarka;

4.2.2.3. pasitelkti Ligoninės darbuotojus pagal kompetenciją, jei pažeidimas yra susijęs su elektroninės informacijos saugumu ir (ar) kibernetiniu incidentu;

4.2.2.4. kuo greičiau imtis priemonių pašalinti pažeidimus ir (ar) sumažinti ar pašalinti jų pasekmes, siekiant atkurti padėtį, kuri buvo prieš pažeidimą;

4.2.2.5. esant poreikiui, konsultuotis ir bendradarbiauti su Valstybine duomenų apsaugos inspekcija (toliau – Inspekcija) dėl pažeidimų;

4.2.2.6. įvertinti, ar padarytas asmens duomenų saugumo pažeidimas;

4.2.2.7. nustatyti, ar apie asmens duomenų saugumo pažeidimą būtina pranešti Inspekcijai ir (ar) duomenų subjektui.

4.2.3. Jei asmens duomenų galimas pažeidimas įvyksta Ligoninės informacinėje sistemoje (toliau - ESIS) ir su asmens duomenų pažeidimu susiję duomenys perduodami į Elektroninės

sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinę sistemą (toliau - ESPBI IS), Asmens duomenų apsaugos pareigūnas nedelsdamas, bet ne vėliau kaip per 24 valandas nuo galimo pažeidimo paaiškėjimo momento, apie tai privalo pranešti Lietuvos sveikatos apsaugos ministerijai (toliau – Ministerija). Pranešime turi būti nurodyta Reglamento (ES) 2016/679 33 straipsnio 3 dalyje nustatyta informacija, kiek tos informacijos įmanoma pateikti tuo metu. Jei visos informacijos pranešime, nustačius pažeidimą, nurodyti negalima, informacija turi būti pateikta nedelsiant po jos paaiškėjimo.

4.2.4. Kai asmens duomenų galimas saugumo pažeidimas yra susijęs su kibernetiniu incidentu, turi nusikalstamos veikos požymių, vadovaujamasi Kibernetinių incidentų valdymo planu, informaciją apie galimą pažeidimą kartu su informacija apie kibernetinį incidentą pateikiama Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytoms valstybės institucijoms plane nustatyta tvarka ir atvejais.

4.3. PAŽEIDIMO TYRIMAS

4.3.1. Asmens duomenų apsaugos pareigūnas nedelsiant, bet ne vėliau kaip per 24 valandas nuo pranešimo gavimo momento, išnagrinėja pranešime nurodytas aplinkybes, įvertina, ar padarytas pažeidimas, jei pažeidimas padarytas, nustato, kokio pobūdžio (tipo) pažeidimas padarytas, asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis, pažeidimo priežastis, pažeidimo apimtis (duomenų subjektų kategorijos ir jų skaičius), esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (-ams), įvertina pavojų duomenų subjekto teisėms ir laisvėms (toliau – rizika), kuris gali atsirasti dėl galimo pažeidimo.

4.3.2. Ligoninės darbuotojai, susiję su galimu asmens duomenų saugos pažeidimu, pateikia Asmens duomenų apsaugo pareigūnui visą jo prašomą informaciją, susijusią su asmens duomenų saugumo pažeidimu ir tyrimu, per jo nurodytą terminą.

4.3.3. Jei asmens duomenų saugumo pažeidimas nustatomas, Asmens duomenų apsaugos pareigūnas papildomai įvertina pažeidimo keliamos rizikos duomenų subjektų teisėms ir laisvėms lygį.

4.3.4. Rizika vertinama objektyviai įvertinus pažeidimo aplinkybes ir atsižvelgiant į:

4.3.4.1. pažeidimo pobūdį (tipą);

4.3.4.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

4.3.4.3. galimybę identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

4.3.4.4. padarinių duomenų subjektui sunkumą. Vertinant riziką turi būti laikoma, kad pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, kyla grėsmė duomenų subjektų sveikatai ir (ar) gyvybei ar grėsmė patirti materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją ir pan. Preziumuojama, kad pažeidimas kelia riziką, kai pažeidimas yra susijęs su specialių kategorijų asmens duomenimis. Taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis;

4.3.4.5. duomenų subjekto savybes – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

4.3.4.6. duomenų subjektų, kurių asmens duomenų saugumas buvo pažeistas, skaičių - kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus.

4.3.5. Įvertinus riziką, nustatomas vienas iš trijų rizikos tikimybių lygių:

4.3.5.1. maža rizika, kai nustatoma, kad pavojaus duomenų subjekto teisėms ir laisvėms nėra;

4.3.5.2. vidutinė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra / gali kilti nedidelis pavojus duomenų subjektų teisėms ir laisvėms;

4.3.5.3. didelė rizika, kai nustatoma, kad dėl asmens duomenų saugumo pažeidimo yra / gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms.

4.3.6. Asmens duomenų apsaugos pareigūnas, atlikęs asmens duomenų saugumo pažeidimo tyrimą, užpildo Asmens duomenų saugumo pažeidimo tyrimo ataskaitą (Aprašo 3 priedas).

4.3.7. Asmens duomenų saugumo pažeidimo tyrimo ataskaita yra teikiama Ligoninės generaliniam direktoriui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais. Atsižvelgęs į ataskaitą Ligoninės generalinis direktorius, prireikus, tvirtina priemonių planą, kuriame numatomos būtinos techninės, organizacinės, administracinės ir kitos priemonės, reikalingos užkirsti kelią pažeidimams, jų pasekmėms pašalinti ar sumažinti, atsakingi priemonių vykdytojai ir įgyvendinimo terminai.

4.4. PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ VALSTYBINEI DUOMENŲ APSAUGOS INSPEKCIJAI

4.4.1. Tyrimo metu nustačius, kad asmens duomenų saugumo pažeidimas buvo, Asmens duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jam tapo žinoma apie pažeidimą, apie tai raštu informuoja Inspekciją, išskyrus atvejus, kai saugumo pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

4.4.2. Inspekcija informuojama Inspekcijos nustatyta tvarka ir sąlygomis, užpildant pranešimo apie asmens duomenų saugumo pažeidimo formą (toliau – Pranešimas).

4.4.3. Jeigu įvertinus riziką abejojama, ar asmens duomenų saugumo pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama Inspekcijai.

4.4.4. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą Inspekcijai pranešti nereikia, tačiau po kurio laiko situacija pasikeičia, saugumo pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turi būti vertinamas iš naujo ir, jeigu reikia, pranešama Inspekcijai (pvz., pamesta USB atmintinė, kurioje saugomi užšifruoti asmens duomenys taikant pažangų algoritmą. Jeigu yra atsarginės duomenų kopijos ir nėra pavojaus šifro saugumui, apie tokį saugumo pažeidimą pranešti Inspekcijai nereikia, tačiau jei vėliau paaiškėja, kad gali kilti pavojus šifro saugumui, pažeidimo keliamas pavojus turi būti vertinamas iš naujo ir apie tokį pažeidimą reikia pranešti Inspekcijai).

4.4.5. Tuo atveju, kai pagal pažeidimo pobūdį būtina atlikti išsamesnį tyrimą, tačiau per 72 valandas dėl objektyvių priežasčių ištirti padarytą pažeidimą nėra įmanoma, informacija Inspekcijai teikiama etapais, nurodant vėlavimo priežastis. Apie informacijos teikimą etapais Inspekcija informuojama teikiant pirminį Pranešimą.

4.4.6. Jeigu pateikus Inspekcijai Pranešimą ir atlikus tolesnį tyrimą yra nustatoma, kad saugumo incidentas buvo sustabdytas ir faktiškai nebuvo asmens duomenų saugumo pažeidimo, apie tai nedelsiant informuojama Inspekcija.

4.5. PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

4.5.1. Tyrimo metu nustačius, kad dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Asmens duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti pavojus.

4.5.2. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu arba elektroniniu paštu arba trumpąja žinute (SMS) ar kitu būdu.

4.5.3. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie

tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

4.5.3.1. asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;

4.5.3.2. priemonių, kurių ėmėsi Ligoninė, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti, aprašymas;

4.5.3.3. Asmens duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

4.5.3.4. kita reikšminga informacija, susijusi su pažeidimu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

4.5.4. Pranešimo apie asmens duomenų saugumo pažeidimą duomenų subjektams teikti nereikia, jeigu:

4.5.4.1. Ligoninė įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

4.5.4.2. iš karto po pažeidimo Ligoninė ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

4.5.4.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi.

4.5.5. Jeigu įvertinus riziką nustatoma, kad apie saugumo pažeidimą duomenų subjektui pranešti nereikia, tačiau po kurio laiko situacija pasikeitė, pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo.

4.5.6. Ligoninė, atsižvelgdama į esamas pagrįstas aplinkybes ir teisėtus teisėsaugos institucijų reikalavimus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą iki to laiko, kol tai netrukdys saugumo pažeidimo ar kitam tyrimui.

4.6. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

4.6.1. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Inspekcijai ir (ar) duomenų subjektui, registruojami Žurnale.

4.6.2. Informacija apie pažeidimą registruojama nedelsiant, kai tik nustatomas pažeidimo faktas ir įvertinama rizika, bet ne vėliau kaip per 5 darbo dienas.

4.6.3. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

4.6.3.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

4.6.3.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

4.6.3.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

4.6.3.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

4.6.3.5. informacija apie pranešimą ar nepranešimą Inspekcijai:

4.6.3.5.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta Inspekcijai, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta Inspekcijai, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

4.6.3.5.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti Inspekcijai, nurodomos tokio vėlavimo priežastys.

4.6.3.6. informacija apie pranešimą ar nepranešimą duomenų subjektui (subjektams):

4.6.3.6.1. jei apie asmens duomenų saugumo pažeidimą buvo nepranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

4.6.3.6.2. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

4.6.3.7. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

4.6.3.8.Žurnalas gali būti popierinės arba elektroninės formos. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale padarymo.

4.6.4. Už Žurnalo pildymą, tvarkymą ir saugojimą atsakingas Asmens duomenų apsaugos pareigūnas.

5. PARENGTA VADOVAUJANTIS

5.1. 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;

5.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

5.3. Ligoninės generalinio direktoriaus vidaus teisės aktai, reglamentuojantys asmens duomenų apsaugą.

6. KEITIMAI

Šis Aprašas periodiškai, bet ne rečiau kaip kartą per metus, peržiūrimas ir, esant poreikiui ir (arba) pasikeitus asmens duomenų tvarkymą reglamentuojantiems teisės aktams, atnaujinimas.

7. PASKIRSTYMAS

Šio Aprašo originalas saugomas Dokumentų valdymo skyriuje, skenuotas dokumentas patalpinamas Dokumentų valdymo sistemoje.

8. PRIEDAI

1 priedas. Pranešimas apie asmens duomenų saugumo pažeidimą;

2 priedas. Asmens duomenų saugumo pažeidimų registracijos žurnalas;

3 priedas. Asmens duomenų saugumo pažeidimo ataskaita.

PATVIRTINTA
VšĮ Lietuvos sveikatos mokslų universiteto
Kauno ligoninės Generalinio direktoriaus
2022 m. spalio 11 d. įsakymu Nr. 1V-527
1 priedas

(Pranešimo apie galimą asmens duomenų saugumo pažeidimą forma)

VIEŠOSIOS ĮSTAIGOS LIETUVOS SVEIKATOS MOKSLŲ UNIVERSITETO KAUNO LIGONINĖ

_____
(struktūrinio padalinio pavadinimas)

_____
(vardas, pavardė, pareigų pavadinimas)

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ
202 - - Nr. _____

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:
1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:

_____

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

_____
_____

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

_____
_____

4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., skyriaus darbuotojai, pacientai, asmenys, pateikę prašymus, skundus ir kt.) ir apytikslis jų skaičius (jei žinoma):

_____
_____

5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):
□ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.)
□ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, slaptažodžiai ir kt.)
□ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.)
□ Specialiųjų kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys, susiję su asmens lytiniu gyvenimu ir lytine orientacija, ir kt.)
□ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas
□ Kiti asmens duomenys (įrašyti):

_____

6. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

_____

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir kt.):

_____
_____

(pareigos) (vardas ir pavardė)

PATVIRTINTA
VšĮ Lietuvos sveikatos mokslų universiteto
Kauno ligoninės Generalinio direktoriaus
2022 m. spalio 11 d. įsakymu Nr. 1V-527
3 priedas

(Asmens duomenų saugumo pažeidimo ataskaitos forma)

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO ATASKAITA

_____ Nr. _____

1. Asmens duomenų saugumo pažeidimo (toliau – pažeidimas) aprašymas	
1.1. Pažeidimo nustatymo data, laikas (minučių tikslumu) ir vieta	
1.2. Asmuo, pranešęs apie pažeidimą (vardas, pavardė, struktūrinio padalinio, kuriame dirba darbuotojas, pavadinimas (jei darbuotojas), telefono Nr., elektroninio pašto adresas)	
1.3. Pažeidimo padarymo data ir vieta	
1.4. Pažeidimo pobūdis (tipas), esmė ir aplinkybės:	
1.4.1. Konfidencialumo pažeidimas	
1.4.2. Vientisumo pažeidimas	
1.4.3. Prieinamumo pažeidimas	
1.4.4. Mišraus pobūdžio (tipo) pažeidimas	
1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir jų skaičius	
1.6. Kaip ilgai tęsėsi pažeidimas?	
1.7. Asmens duomenų kategorijos, susijusios su pažeidimu:	
1.7.1. Asmens duomenys	
1.7.2. Specialių kategorijų asmens duomenys	
1.8. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius	
2. Pažeidimo rizikos įvertinimas	
2.1. Priežastys, lėmusios pažeidimą, ar įvykiai, kurie galėjo turėti įtakos padaryti pažeidimą	
2.2. Pažeidimo pasekmės:	
2.2.1. Sunaikinti asmens duomenys	
2.2.2. Prarasti asmens duomenys	
2.2.3. Pakeisti asmens duomenys	
2.2.4. Be duomenų subjekto sutikimo atskleisti asmens duomenys	
2.2.5. Sudaryta galimybė naudotis asmens duomenimis	
2.2.6. Asmens duomenys, išplitę labiau nei tai yra būtina ir prarasta duomenų subjekto kontrolė savo asmens duomenų atžvilgiu	
2.2.7. Asmens duomenų susiejimas	
2.2.8. Asmens duomenų panaudojimas neteisėtais tikslais	
2.2.9. Dėl asmens duomenų trūkumo negalima teikti paslaugų	
2.2.10. Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamų paslaugų	
2.2.11. Kita	
2.3. Dėl pažeidimo nėra pavojaus duomenų subjektų teisėms ir laisvėms (maža rizika)	

2.4. Dėl pažeidimo yra / gali kilti pavojus duomenų subjektų teisėms ir laisvėms (būtina pranešti Valstybinei duomenų apsaugos inspekcijai (toliau – Inspekcija) (vidutinė rizika)	
2.5. Dėl pažeidimo yra / gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms (būtina pranešti Inspekcijai ir duomenų subjektams) (didelė rizika)	
2.6. Kas turėjo prieigą prie pažeistų asmens duomenų iki asmens duomenų saugumo pažeidimo padarymo?	
2.7. Kas gavo prieigą prie pažeistų asmens duomenų (jei pažeidimas yra, ar apima asmens duomenų prieinamumo pažeidimą)?	
2.8. Ar iki pažeidimo asmens duomenys buvo tinkamai užkoduoti, anonimizuoti ar kitaip lengvai neprieinami?	
2.9. Informacinės sistemos, įrenginiai, įranga, įrašai, susiję su pažeidimu	
2.10. Ar pažeidimas yra sisteminė klaida, ar vienetinis incidentas?	
2.11. Kokia žala buvo padaryta duomenų subjektams, kurių asmens duomenų saugumas pažeistas?	
2.12. Kokių veiksmų / priemonių buvo imtasi sužinojus apie padarytą pažeidimą?	
2.13. Kokios taikytos priemonės, siekiant sumažinti ir (ar) pašalinti pažeidimo pasekmes duomenų subjektams?	
2.14. Kokios techninės ir (ar) organizacinės priemonės buvo taikomos pažeidimo paveiktiems asmens duomenims, užtikrinant, kad asmens duomenys nebūtų prieinami neįgaliotiems asmenims?	
2.15. Techninės ir (ar) organizacinės priemonės, kurios įgyvendintos dėl pažeidimo, siekiant, kad pažeidimas nepasikartotų	
2.16. Techninės ir (ar) organizacinės priemonės, kurios ketinamos įgyvendinti dėl pažeidimo, įskaitant ir priemones sumažinti pažeidimo pasekmes	
3. Pranešimų pateikimas	
3.1. Ar pranešta duomenų subjektui apie pažeidimą:	
3.1.1. Taip	(Pranešimo turinys ir data)
3.1.2. Ne	
3.2. Jei buvo teikiamas pranešimas duomenų subjektams:	
3.2.1. Pranešimo duomenų subjektui būdas (paštu, elektroninio pašto pranešimu ar SMS pranešimu ir kt.)	
3.2.2. Informuotų duomenų subjektų skaičius	
3.2.3. Vėlavimo pranešti duomenų subjektui apie pažeidimą priežastys	
3.3.Nepranešimo apie pažeidimą duomenų subjektui priežastys:	
3.3.1. Nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos priežastys)	
3.3.2. duomenų tvarkytojas įgyvendino tinkamas technines ir organizacines asmens duomenų apsaugos priemones, kurios užtikrino, kad įvykus pažeidimui nekils rizika, ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio (nurodoma, kokios)	
3.3.3. iš karto po pažeidimo duomenų tvarkytojas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti rizika (nurodoma, kokios)	
3.3.4. Reikėtų neproporcingai daug pastangų susisiekti su duomenų subjektais. Informacija apie pažeidimą buvo paskelbta viešai arba taikyta panaši priemonė, kuria	

duomenų subjektai buvo informuoti taip pat efektyviai (nurodoma, kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma, kokia ir kada taikyta)	
3.3.5. Dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas	
3.4. Ar pranešta Inspekcijai apie asmens duomenų saugumo pažeidimą:	
3.4.1. Taip	(rašto data ir numeris)
3.4.2. Ne	
3.5. Vėlavimo pranešti Inspekcijai apie pažeidimą priežastys	
3.6. Nepranešimo apie pažeidimą Inspekcijai priežastys	
3.7. Ar pranešta valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą, apie pažeidimą, galimai turintį nusikalstamos veikos požymių:	
3.7.1. Taip	(rašto data ir numeris, adresatas)
3.7.2. Ne	
3.8. Ar pranešta valstybės institucijoms, nurodytoms Lietuvos Respublikos kibernetinio saugumo įstatyme, apie kibernetinį incidentą, susijusį su pažeidimu:	
3.8.1. Taip	(rašto data ir numeris, adresatas)
3.8.2. Ne	
Asmens duomenų apsaugos pareigūnas	(vardas, pavardė, parašas)