PATVIRTINTA
VšĮ Regioninės Mažeikių ligoninės
direktoriaus 2023 m. gegužės 2 d.
įsakymu Nr. V1- 47

VŠĮ REGIONINĖS MAŽEIKIŲ LIGONINĖS TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO VALDYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šios VšĮ Regioninės Mažeikių ligoninės tvarkomų asmens duomenų saugumo pažeidimo valdymo taisyklės (toliau – Taisyklės) reglamentuoja asmens duomenų saugojimo principus, nustato asmens duomenų saugumo galimus pažeidmus, rizikas bei priemones, kurių privalo imtis tai identifikavęs asmuo.

2. Su Taisyklėmis elektroninėmis priemonėmis supažindinami visi VšĮ Regioninės Mažeikių ligoninės (toliau – Ligoninė) darbuotojai. Taisyklės taip pat skelbiamos Ligoninės internetinėje svetainėje.

3. Taisyklėse vartojamos sąvokos:

3.1. ***Atsakingas asmuo*** – fizinis ar juridinis asmuo, Ligoninės paskirtas tvarkyti asmens duomenis;

3.2. ***Asmens duomenys*** – vardas, pavardė, asmens kodas, gyvenamoji vieta, gyvenimo būdas, šeiminė padėtis, gyvenamoji aplinka, santykiai su kitais žmonėmis, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas, lytinis, dvasinis, religinis gyvenimas, privatus susirašinėjimas, pokalbiai, privati užrašuose ar elektroninėse laikmenose saugoma informacija;

3.3. ***Asmens duomenų apsaugos pažeidimas*** – bet koks veiksmas, situacija, informacija, iš kurios gali asmuo identifikuoti, jog saugomiems asmens duomenims iškilo realus pavojus, t.y. užfiksuotas įsilaužimas, vagystė, kibernetinės atakos ar kiti panašūs veiksmai, kurių dėka, saugomi duomenys iš Ligoninės yra nutekinami.

3.4. ***Asmens duomenų praradimas*** – atvejai, kai asmens duomenys yra išsaugoti, tačiau duomenų valdytojas yra praradęs šių duomenų valdymą ir kontrolę arba prieigą prie jų;

3.5. ***Asmens duomenų sugadinimas*** – atvejai, kai asmens duomenys buvo pakeisti, sugadinti arba yra išnykęs jų vientisumas;

3.6. ***Asmens duomenų sunaikinimas*** – atvejai, kai asmens duomenų nebėra arba jie tokios formos, kuri gali būti skirta bet kokiam duomenų valdytojo naudojimui;

3.7. ***Asmens duomenų tvarkymas*** – bet koks automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekamas veiksmas ar jų seka, pvz. duomenų rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;

3.8. ***Duomenų apsaugos pareigūnas*** – Ligoninės direktoriaus įsakymu paskirtas asmuo, atsakingas už asmens duomenų apsaugą Ligoninėje;

3.9. ***Duomenų subjektas*** – fizinis asmuo, kurio tapatybė yra nustatyta (gali būti nustatyta) ir kurio duomenis tvarko (valdo) Ligoninė;

3.10. ***Duomenų tvarkytojas*** – fizinis arba juridinis asmuo, valdžios institucija, ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.

3.11. ***Priežiūros institucija*** – Lietuvos Respublikos valstybinė duomenų apsaugos inspekcija;

3.12. ***Saugumo pažeidimo pranešimas*** – informacinis pranešimas, skirtas Priežiūros institucijai, o tam tikrais atvejais – ir duomenų subjektams, kuriame pateikta su saugumo pažeidimu susijusi informacija.

3.13. Taisyklėse vartojamos sąvokos turi būti suprantamos taip, kaip yra apibrėžtos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 2016/679 (Bendrajame duomenų apsaugos

reglamente, toliau – BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau – ADTAĮ) ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose.

4. Taisyklės taikomos valdant asmens duomenis, tvarkomus automatizuotomis priemonėmis (elektroniniu būdu), ir asmens duomenis, saugomus neelektronine (popierine) forma.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO PRINCIPAI

5. Ligoninė, tvarkydama asmens duomenis, vadovaujasi šiais principais:

5.1. Asmens duomenis Ligoninė tvarko tik teisėtiems tikslams pasiekti;

5.2. Asmens duomenys yra tvarkomi tiksliai, sąžiningai ir teisėtai, laikantis teisės aktų reikalavimų;

5.3. Ligoninė asmens duomenis tvarko taip, kad jie būtų tikslūs ir esant jų pasikeitimui nuolat atnaujinami;

5.4. Asmens duomenys saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi;

5.5. Renkamų duomenų apsaugai pasitelkiamos priemonės, t.y. slaptažodžiai, užraktai ir kitos būtinos priemonės.

III SKYRIUS
ASMENS DUOMENŲ SAUGUMO UŽTIKRINIMO PRIEMONĖS

6. Ligoninė, saugodama asmens duomenis, įgyvendina ir užtikrina tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

7. Ligoninė užtikrina tinkamą dokumentų bei duomenų rinkmenų saugojimą, imasi priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui. Dokumentų kopijos, kuriose nurodomi asmens duomenys, turi būti sunaikintos taip, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

8. Ligoninėje su asmens duomenimis turi teisę susipažinti tik tie asmenys, kurie yra įgalioti susipažinti su tokiais duomenimis, ir tik tuomet, kai tai yra būtina šiose Taisyklėse numatytiems tikslams pasiekti.

9. Ligoninė užtikrina patalpų, kuriose laikomi asmens duomenys, saugumą, tinkamą techninės įrangos išdėstymą ir peržiūrą, tinkamą tinklo valdymą, informacinių sistemų priežiūrą bei kitų techninių priemonių, būtinų asmens duomenų apsaugai užtikrinti, įgyvendinimą.

10. Ligoninė imasi priemonių, kad būtų užkirstas kelias atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugodama jai patikėtus dokumentus bei duomenų rinkmenas tinkamai ir saugiai.

IV SKYRIUS
ASMENŲ VEIKSMAI, ĮTARUS, JOG YRA AR GALĖJO BŪTI PAŽEISTAS ASMENS DUOMENŲ SAUGUMAS

11. Jei Ligoninės darbuotojas ar kitas atsakingas asmuo abejoja įdiegtų saugumo priemonių patikimumu, jis turi kreiptis į tiesioginį savo vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

12. Darbuotojai ar kiti atsakingi asmenys, kurie automatiniu būdu tvarko asmens duomenis arba iš kurių kompiuterių galima patekti į vietinio tinklo sritis, kuriose yra saugomi asmens duomenys, naudoja

slaptažodžius. Slaptažodžiai yra keičiami periodiškai, ne rečiau kaip kartą per tris mėnesius, taip pat susidarius tam tikroms aplinkybėms (pvz., pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims ir pan.), asmuo privalo apie tai pranešti Ligoninės duomenų apsaugos pareigūnui, o pats, jei įmanoma, imtis visų saugumo priemonių, t.y. pakeisti slaptažodį, apriboti prieigą ir pan.

13. Darbuotojas, dirbantis konkrečiu kompiuteriu, gali žinoti tik savo slaptažodį. Paaiškėjus, jog kažkas slaptažodį sužinojo, kažkur duomenys galimai nutekėjo, kažkas įsilaužė ar be asmens nurodymo pakeitė slaptažodį, nedelsiant privalu pranešti Ligoninės duomenų apsaugos pareigūnui.

14. Fiziniai veiksmai, kuriuos pastebėjus, asmuo privalo pranešti Ligoninės duomenų apsaugos pareigūnui ir/ar Ligoninės vadovui:

14.1. duomenų kontrolės praradimas.

14.2. dokumentų suklastojimas.

14.3. prarastas konfidencialumas.

14.4. įsilaužimas

14.5. vagystė

15. Nustačius asmens duomenų saugumo pažeidimą, Ligoninė imasi neatidėliotinų priemonių užkertant kelią neteisėtam asmens duomenų tvarkymui, t.y. pagal pažeidimo sudėtingumą, arba tvarkosi Ligoninės viduje, arba apie pažeidimą praneša Asmens duomenų inspekcijai per 72 valandas, užpildant Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. gegužės 24 d. įsakymu Nr. 1T-53 (1.12.) patvirtintą formą (Pridedama). Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus asmenų teisėms ir laisvėms, Ligoninė nedelsdama praneša apie tai ir patiems asmenims kurių duomenys galimai nutekėjo.

16. Šių Taisyklių nesilaikymas, atsižvelgiant į pažeidimo sunkumą, gali būti laikomas darbo drausmės pažeidimu, už kurį darbuotojams gali būti taikoma atsakomybė, numatyta Lietuvos Respublikos darbo kodekse bei prilyginama šiurkščiam darbo drausmės pažeidimui.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

17. Šios Taisyklės peržiūrimos ir esant poreikiui atnaujinamos ne rečiau kaip kartą per metus arba pasikeitus teisės aktams, kurie reglamentuoja asmens duomenų tvarkymą.

18. Darbuotojai ir kiti atsakingi asmenys su šiomis Taisyklėmis yra supažindinami elektroninėmis priemonėmis ir privalo laikytis jose nustatytų įpareigojimų bei atlikdami savo darbo funkcijas vadovautis Taisyklėse nustatytais principais ir darbo specifika.

19. Ligoninė turi teisę keisti šias Taisykles. Su pakeitimais darbuotojai ir kiti atsakingi asmenys yra supažindinami elektroninėmis priemonėmis.

20. Šios Taisyklės saugomos pas Duomenų apsaugos pareigūną.

Forma patvirtinta
Valstybinės duomenų apsaugos inspekcijos direktoriaus
2018 m. gegužės 24 d. įsakymu Nr. 1T-53(1.12.)

Pranešimo apie asmens duomenų saugumo pažeidimą forma

_____

(duomenų valdytojo (juridinio asmens) pavadinimas, duomenų valdytojo atstovo pavadinimas, duomenų valdytojo (fizinio asmens) vardas, pavardė)

_____

(juridinio asmens kodas ir buveinės adresas arba fizinio asmens kodas, gimimo data (jeigu asmuo neturi asmens kodo) ir asmens duomenų tvarkymo vieta

_____

(telefono ryšio ir (ar) elektroninio pašto adresas, ir (ar) elektroninės siuntos pristatymo dėžutės adresas)

Valstybinei duomenų apsaugos inspekcijai

PRANEŠIMAS
APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____Nr. _____
(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:

Asmens duomenų saugumo pažeidimo :

Data _____ Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:

Data _____ Laikas _____

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):

- ☐ Informacinė sistema
- ☐ Duomenų bazė
- ☐ Tarnybinė stotis
- ☐ Internetinė svetainė
- ☐ Debesų kompiuterijos paslaugos
- ☐ Nešiojami / mobilus įrenginiai
- ☐ Neautomatiniu būdu susistemintos bylos (archyvas)
- ☐ Kita _____

1.3. Asmens duomenų saugumo pažeidimo aplinkybės (pažymėti tinkamą (-us):

- ☐ Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
- ☐ Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
- ☐ Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

_____

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

_____

_____

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):

☐ Asmens tapatybę patvirtinantys asmens duomenys (vardas, pavardė, amžius, gimimo data, lytis ir kt.):

_____

_____

☐ Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):

_____

_____

_____

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:

_____

_____

☐ Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):

_____

_____

☐ Kiti:

_____

_____

☐ Nežinomi (pranešimo teikimo metu)

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

_____

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

_____

_____

_____

_____

_____

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

☐ Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)
☐ Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)
☐ Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)
☐ Kita

_____
_____
_____
_____
_____
_____

2.2. Vientisumo praradimo atveju:

☐ Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis paslaugomis
☐ Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)
☐ Kita

_____
_____
_____
_____
_____
_____

2.3. Duomenų prieinamumo praradimo atveju:

☐ Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)
☐ Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)
☐ Kita

_____
_____
_____
_____
_____
_____

2.4. Kita:

3. Priemonės, kurių imtasi siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

☐ Taip, duomenų subjektai informuoti (nurodoma data)_____
☐ Ne, bet jie bus informuoti (nurodoma data)_____
☐ Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

☐ Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)

_____

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)

_____

_____

_____

_____

☐ Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodomos kokios)

_____

_____

_____

_____

☐ Ne, nes tai pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta)

_____

_____

☐ Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

_____

_____

_____

_____

_____

_____

_____

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

☐ Paštu
☐ Elektroniniu paštu
☐ Kitu būdu _____

5.5. Informuotų duomenų subjektų skaičius _____

6. Asmuo galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė_____

6.2. Telefono ryšio numeris _____

6.3. Elektroninio pašto adresas _____

6.4. Pareigos _____

6.5. Darbovietės pavadinimas ir adresas _____

_____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

_____
_____
_____
_____
_____
_____
_____

8. Kita reikšminga informacija

_____
_____
_____
_____
_____
_____
_____
_____

_____	_____	_____
(pareigos)	(parašas)	(vardas, pavardė)

_____