PATVIRTINTA
VšĮ Jonavos ligoninės direktoriaus
2019-02-04 įsakymu Nr. V-26

VIEŠOSIOS ĮSTAIGOS JONAVOS LIGONINĖS DUOMENŲ SAUGOS IR KONFIDENCIALUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS IR SĄVOKOS

1. Viešosios įstaigos Jonavos ligoninės (toliau – Ligoninė) duomenų saugos ir konfidencialumo politika (toliau – Politika) reglamentuoja pagrindinius asmens duomenų tvarkymo ir konfidencialumo užtikrinimo principus ir priemones.
2. Šia Politika siekiama:
   2.1. Užtikrinti, kad Ligoninės darbuotojai asmens duomenis tvarkytų saugiai ir asmens duomenų tvarkymas atitiktų teisės normų, susijusių su duomenų apsauga ir konfidencialumu, reikalavimus ir gerą praktiką;
   2.2. Išlaikyti aukščiausią visos pacientų informacijos, susijusios su sveikata, konfidencialumo ir paciento privataus gyvenimo neliečiamumo laipsnį.
3. Politikos privalo laikytis visi Ligoninės darbuotojai, kurie tvarko pacientų ar darbuotojų asmens duomenis arba eidami savo pareigas juos sužino.
4. Ligoninėje tvarkomi pacientų ir darbuotojų asmens duomenys. Ligoninėje gali būti tvarkomi ir kitų duomenų subjektų kategorijų asmens duomenys ir jų tvarkymui taikomi Politikoje nustatyti asmens duomenų tvarkymo principai.
5. Pagrindinės sąvokos:
   5.1. Asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti.
   5.2. Sveikatos duomenys – asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę.
   5.3. Duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.
   5.4. Duomenų tvarkymas automatiniu būdu – duomenų tvarkymo veiksmai, visiškai ar iš dalies atliekami automatinėmis priemonėmis.
   5.5. Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.
6. Kitos Politikoje vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau - Bendrasis duomenų apsaugos reglamentas) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme.

II SKYRIUS
ASMENS DUOMENŲ TVARKYMO PRINCIPAI

7. Ligoninėje asmens duomenys tvarkomi laikantis šių principų:
   7.1. Duomenų subjekto asmens duomenys tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas).
   7.2. Duomenų subjekto asmens duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu; tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais nėra laikomas nesuderinamu su pirminiais tikslais (tikslo apribojimo principas).
   7.3. Tvarkomi asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas).
   7.4. Tvarkomi asmens duomenys turi būti tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi (tikslumo principas).
   7.5. Tvarkomi asmens duomenys laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves (saugojimo trukmės apribojimo principas).
   7.6. Asmens duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų.
8. Tvarkant pacientų asmens duomenis taip pat turi būti laikomasi šių principų:
   8.1. Darbuotojas tvarkantis pacientų asmens duomenis asmuo privalo žinoti duomenų tvarkymo tikslą ir teisinį pagrindą;
   8.2. Kur įmanoma taikyti pseudonimus ir naudoti anoniminę informaciją;
   8.3. Naudoti minimalų reikalingą asmens duomenų kiekį;
   8.4. Asmens duomenų naudojimui taikomas „reikia žinoti“ principas t. y. konfidencialia informacija gali naudotis tik tie darbuotojai, kuriems ji reikalinga pagal atliekamas pareigas ir atsakomybes;
   8.5. Teikti pacientų asmens duomenis tretiesiems asmenims galima tik teisės normų nustatyta tvarka.
9. Kiekvienas darbuotojas privalo saugoti asmens duomenis, kuriuos sužino atlikdamas savo pareigas. Darbuotojų konfidencialumo pareigos detalizuojamos Susitarimuose dėl konfidencialios informacijos apsaugos.

III SKYRIUS
DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI

10. Asmens duomenys Ligoninėje gali būti tvarkomi šiais pagrindais:
   10.1. tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė;
   10.2. tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas;
   10.3. tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį;

10.4. tvarkyti duomenis būtina siekiant teisėtų Ligoninės arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas;

10.5. duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais.

11. Sveikatos duomenys ir kiti specialių kategorijų asmens duomenys Ligoninėje gali būti tvarkomi šiais pagrindais:

11.1. tvarkyti duomenis būtina profilaktinės arba darbo medicinos tikslais, siekiant įvertinti darbuotojo darbingumą, nustatyti medicininę diagnozę, teikti sveikatos priežiūros arba socialinės rūpybos paslaugas ar gydymą arba valdyti sveikatos priežiūros ar socialinės rūpybos sistemas ir paslaugas remiantis Sąjungos arba valstybės narės teise arba pagal sutartį su sveikatos priežiūros specialistu, taikant 3 dalyje nurodytas sąlygas ir apsaugos priemones;

11.2. tvarkyti duomenis būtina, kad duomenų valdytojas arba duomenų subjektas galėtų įvykdyti prievoles ir naudotis specialiomis teisėmis darbo ir socialinės apsaugos teisės srityje, kiek tai leidžiama Sąjungos arba valstybės narės teisėje arba pagal valstybės narės teisę sudaryta kolektyvine sutartimi, kuriuose nustatytos tinkamos duomenų subjekto pagrindinių teisių ir interesų apsaugos priemonės.

12. Ligoninės personalas turi būti atsargus jeigu asmens duomenis reikia rinkti ar jais dalintis ne sveikatos priežiūros paslaugų teikimo tikslais. Tokiu atveju kiekvienas darbuotojas privalo įvertinti ar duomenų tvarkymas bus teisėtas. Esant neaiškumas darbuotojams visada rekomenduojama kreiptis į Ligoninės duomenų apsaugos pareigūną ar Ligoninės administraciją.

IV SKYRIUS
PACIENTŲ ASMENS DUOMENŲ TVARKYMAS

13. Informacija apie paciento gyvenimo faktus renkama tik su paciento sutikimu ir tuo atveju, kai tai yra būtina ligai diagnozuoti, gydyti ar pacientui slaugyti.
14. Gydytojai privalo rinkti tik tą sveikatos informaciją, kuri reikalinga teikti pacientui sveikatos priežiūros paslaugas, tuo pačiu užtikrinant, kad būtų surinkta visa informacija, reikalinga kokybiškų paslaugų teikimui.
15. Paciento sveikatos informacija gali būti renkama iš paciento artimųjų, tačiau tik paciento sutikimu. Paciento sveikatos informacija gali būti gaunama iš kitų sveikatos priežiūros įstaigų teisės aktų nustatyta tvarka.
16. Konfidencialia laikoma visa žodinė, rašytinė ar vaizdinė paciento informacija, sukurta Ligoninėje ar gauta iš kitų sveikatos priežiūros teikėjų, leidžianti identifikuoti konkretų pacientą. Konfidencialia informacija laikoma informacija nurodyta paciento medicinos dokumentuose, kituose dokumentuose (raštuose, pažymose ir pan.) ir bet kokiose kitose laikmenose (įskaitant elektronines) ir duomenų bazes, kuriose yra saugoma informacija apie pacientą. Ši informacija laikoma konfidencialia ir po paciento mirties.
17. Darbuotojai dokumentus, kompiuterines rinkmenas (failus), duomenų bazes, kuriose yra konfidencialios informacijos apie pacientus, turi teisę naudoti tik savo darbo funkcijų vykdymui.
18. Duomenų laikmenos (popierinės ar elektroninės), kuriose yra paciento asmens duomenų gali būti naudojamos tik darbo vietoje. Duomenų laikmenų išnešimas iš darbo vietos galimas tik su informacinių technologijų specialisto sutikimu.
19. USB raktai gali būti naudojami tik trumpalaikiam duomenų saugojimui. USB raktuose ir kituose išimamuose duomenų laikmenose asmens duomenys gali būti saugomi tik užšifruoti.
20. Kopijuoti konfidencialią informaciją apie pacientus (įskaitant kopijavimą į išorines duomenų laikmenas) galima tik darbo funkcijų vykdymo tikslu.

21. Popierinės duomenų laikmenos su pacientų asmens duomenimis turi būti saugiai sunaikinamos naudojant dokumentų naikiklį. Elektroninės duomenų laikmenos, kuriose buvo saugomi pacientų asmens duomenys gali būti išmetamos tik po Ligoninės IT specialistų patikrinimo.
22. Jokia informacija, esanti paciento medicinos dokumentuose ir/ar kitose laikmenose, nėra atskleidžiama, perduodama ar bet kokiu kitu būdu persakoma tretiesiems asmenims be paciento sutikimo, išskyrus teisės aktais nustatytus atvejus, kai leidžiama atskleisti paciento sveikatos informaciją be jo sutikimo.
23. Pacientų asmens duomenys išoriniais duomenų perdavimo įrenginiais (telefonais, faksais, internetinio ryšio priemonėmis, kitomis ryšio priemonėmis) gali būti teikiami tik teisės normų nustatyta tvarka.
24. Pacientų asmens duomenų perdavimas turi būti atliekamas saugiai, minimizuojant perduodamų duomenų nutekinimo ar praradimo riziką. Bet kokie asmens duomenys, jeigu galima identifikuoti pacientą, turi būti siunčiami tik šifruoti.

V SKYRIUS
DUOMENŲ TVARKYMAS AUTOMATINIU BŪDU

25. Ligoninės informacinę sistemą ir jos naudojimo tvarką reglamentuoja:
    25.1. Kauno regiono asmens sveikatos priežiūros įstaigų informacinės sistemos nuostatai.
    25.2. Kauno regiono asmens sveikatos priežiūros įstaigų informacinės sistemos duomenų saugos nuostatai.
    25.3. VšĮ Jonavos ligoninės informacinės sistemos naudotojų administravimo taisyklės.
    25.4. VšĮ Jonavos ligoninės informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės.
    25.5. VšĮ Jonavos ligoninės informacinės sistemos veiklos tęstinumo valdymo planas.
    25.6. Kauno regiono asmens sveikatos priežiūros įstaigų informacinės sistemos kibernetinio saugumo reikalavimų ir procedūrų aprašas.
26. Darbuotojas turi teisę naudoti informacinę sistemą tik tuo atveju, jeigu jam yra suteikta prieigos teisė.
27. Darbuotojai negali leisti kitiems darbuotojams jungtis prie informacinės sistemos su savo prisijungimo duomenimis. Prisijungimo duomenų pasidalinimas su kitais asmenimis yra laikomas šiurkščiu darbo drausmės pažeidimu.
28. Darbuotojai turi teisę peržiūrėti tik tuos pacientų ir darbuotojų duomenis, kurie reikalingi jų funkcijų vykdymui. Personalas neturi teisės peržiūrėti kitų duomenų, net jei informacinė sistema leidžia tai daryti.
29. Darbuotojai neturi teisės peržiūrėti duomenų apie savo artimuosius, draugus ar pažįstamus, jeigu jie nedalyvauja jų gydyme.

VI SKYRIUS
INFORMAVIMAS APIE DUOMENŲ TVARKYMĄ

30. Siekiant užtikrinti Bendrojo duomenų apsaugos reglamento 13 straipsnio reikalavimus Ligoninė yra raštu paskelbusi informaciją pacientams apie duomenų tvarkymą. Informacija pacientams skelbiama tinklalapyje ir informacinėse lentose visuose Ligoninės skyriuose.
31. Informacija apie darbuotojų duomenų tvarkymą yra nurodyta Asmens duomenų tvarkymo taisyklių apraše, su kuriuo darbuotojai supažindinami Ligoninėje nustatyta tvarka.

VII SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

32. Ligoninėje yra paskirtas duomenų apsaugos pareigūnas.
33. Duomenų subjektai gali kreiptis į duomenų apsaugos pareigūną visais klausimais, susijusiais jų asmeninių duomenų tvarkymu ir naudojimusi savo teisėmis pagal Bendrąjį duomenų apsaugos reglamentą.
34. Duomenų apsaugos pareigūnas:
    34.1. informuoja Ligoninę ir asmens duomenis tvarkančius darbuotojus apie jų prievoles pagal Bendrąjį duomenų apsaugos reglamentą ir kitus teisės aktus ir konsultuoja juos šiais klausimais;
    34.2. stebi, kaip laikomasi pagal Bendrojo duomenų apsaugos reglamento, kitų teisės aktų ir Ligoninės politikos asmens duomenų apsaugos srityje, įskaitant pareigų pavedimą, duomenų tvarkymo operacijose dalyvaujančių darbuotojų informuotumo didinimą bei mokymą ir susijusius auditus;
    34.3. paprašius konsultuoja dėl poveikio duomenų apsaugai vertinimo ir stebi jo atlikimą;
    34.4. bendradarbiauja su priežiūros institucija;
    34.5. atlieka kontaktinio asmens funkcijas priežiūros institucijai kreipiantis su duomenų tvarkymu susijusiais klausimais ir prireikus konsultuoja visais kitais klausimais.

VIII SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

35. Poveikio duomenų apsaugai vertinimas turi būti atliekamas tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus.
36. Atliekant poveikio duomenų apsaugai vertinimą konsultuojamasi su duomenų apsaugos pareigūnu.

X SKYRIUS
PRANEŠIMAI APIE INCIDENTUS

37. Ligoninė dokumentuoja visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi.
38. Asmens duomenų saugumo pažeidimo atveju Ligoninė nedelsdama ir, jei įmanoma, praėjus ne daugiau kaip 72 valandas nuo tada, kai sužinojo apie asmens duomenų saugumo pažeidimą, apie tai praneša Valstybinei asmens duomenų apsaugos inspekcijai, nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms.
39. Kai dėl duomenų saugumo pažeidimo gali kilti didelis pavojus duomenų fizinių asmenų teisėms ir laisvėms, Ligoninė nedelsdama praneša apie asmens duomenų saugumo pažeidimą duomenų subjektui. Pranešimas gali būti nesiunčiamas, jeigu yra įvykdytos visos Bendrojo duomenų apsaugos reglamento 34 straipsnio 3 dalyje nurodytos sąlygos.

XI SKYRIUS
PERSONALO ŠVIETIMAS IR MOKYMAS

40. Darbuotojas, kurio darbo funkcijos yra susijusios su asmens duomenų tvarkymu, privalo būti apmokytas asmens duomenų apsaugos klausimais prieš pradedant vykdyti darbines funkcijas.
41. Darbuotojai reguliariai supažindinami su visais teisės aktų pasikeitimais, susijusiais su duomenų apsauga ir konfidencialumu.

42. Ligoninės personalui reguliariai, bet ne rečiau kaip kartą per metus organizuojami mokymai dėl duomenų apsaugos ir konfidencialumo.

XII SKYRIUS
INVENTORIZAVIMAS IR RIZIKOS VERTINIMAS

43. Ligoninėje tvarkomų asmens duomenų inventorizavimas ir rizikos vertinimas atliekamas kas 3 metai. Duomenų inventorizavimas ir rizikos vertinimas atliekamas dažniau, esant veiklos pasikeitimams.
44. Informacinės sistemos rizikos vertinimas ir Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimas atliekamas Šiaulių regiono asmens sveikatos priežiūros įstaigų informacinės sistemos saugos nuostatų nustatyta tvarka ir terminais.

XIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

45. Ligoninės darbuotojai, tvarkantys asmens duomenis už konfidencialumo ir asmens duomenų tvarkymo pažeidimus atsako teisės aktų nustatyta tvarka.
46. Už Politikos nuostatų laikymosi priežiūrą ir joje reglamentuotų nuostatų vykdymo kontrolę bei periodišką, ne rečiau kaip kartą per 2 metus, Politikos peržiūrėjimą atsakingas Ligoninės direktoriaus paskirtas darbuotojas, kuris, įvertinęs Politikos taikymo praktiką, esant poreikiui, inicijuoja Politikos atnaujinimą.