

PATVIRTINTA
VšĮ Ukmergės ligoninės
vyriausiojo gydytojo 2020-11-11
įsakymu Nr. V-164

VIEŠOSIOS ĮSTAIGOS UKMERGĖS LIGONINĖS INFORMACIJOS SAUGUMO POLITIKA

SAVOKOS

BDAR	reiškia 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).
Darbuotojas	reiškia Ligoninės darbuotoją.
Ligoninė	reiškia Viešąją įstaigą Ukmergės ligoninę, juridinio asmens kodas: 182935350, adresas: Vytauto g. 105, LT-20184 Ukmergė, Lietuvos Respublika, įregistruotą Lietuvos Respublikos juridinių asmenų registre.
Ligoninės vadovas	reiškia Ligoninės vienasmenį valdymo organą.
Įrenginys	reiškia bet kokią Darbuotojui suteiktą techninę įrangą ar įrenginį.
Politika	reiškia šią Informacijos saugumo politiką.

I TIKSLAS IR APIMTIS

1. Šia Politika yra siekiama nustatyti bendruosius saugumo reikalavimus Ligoninės pasitelkiamoms informacinėms technologijoms bei jų panaudojimo būdams, siekiant užtikrinti maksimalų Ligoninės ir jos pacientų, pacientų atstovų, taip pat darbuotojų, kontrahentų bei kitų asmenų informacijos saugumą, ir apsaugoti juos nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, tyčinių ar atsitiktinių asmenų veiksmų tvarkant jiems prieinamus asmens ar kitus duomenis, taip pat naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.
2. Politikos tikslas yra apsaugoti Ligoninės pacientus, pacientų atstovus, darbuotojus, kontrahentus nuo neteisėtų ir žalą sukeliančių tiesioginių ar netiesioginių, tyčinių ar atsitiktinių asmenų veiksmų tvarkant jiems prieinamus asmens ar kitus duomenis, taip pat naudojant atitinkamą įrangą savo darbo funkcijoms atlikti.
3. Ši Politika yra taikoma tvarkant bet kuriose informacinėse sistemose esančią ir bet kurioje laikmenoje saugomą Ligoninės informaciją, nepriklausomai nuo to, ar šios informacijos tvarkymas yra susijęs su Ligoninės vidaus procesais, ar su Ligoninės išorės santykiais su bet kuriais trečiaisiais asmenimis.
4. Ši Politika taip pat yra taikoma Ligoninės darbuotojams jų darbo funkcijų vykdymo metu ir (ar) naudojant jiems Ligoninės suteiktą įrangą ir įrankius.
5. Ši Politika gali būti taikoma kartu su kitomis politikomis, taisyklėmis, procedūromis ar kitais Ligoninės vidaus dokumentais.

6. Ši Politika yra taikoma ir Ligoninės vardu informaciją tvarkantiems paslaugų teikėjams (įskaitant duomenų tvarkytojus) tiek, kiek Politikos nuostatos neprieštarauja sudarytai paslaugų teikimo, duomenų tvarkymo ar kitai sutarčiai.

II INFORMACIJAI TVARKYTI NAUDOJAMOS SISTEMOS

7. Bet kokios informacinės sistemos, įskaitant, bet neapsiribojant, kompiuterine, serverių įranga, bet kokia programine įranga, operacinėmis sistemomis, bet kokiomis duomenų laikmenomis, tinklo paskyromis, elektroninio pašto paskyromis, paieškos sistemomis ir bet kokia kita Ligoninės veikloje naudojama techninė įranga ir įrankiais, yra laikomos Ligoninės nuosavybe.
8. Kiekvienas darbuotojas jam Ligoninės suteiktus įrenginius ir įrangą privalo naudoti atsakingai bei atidžiai, ir tik su Ligoninės veikla susijusiems tikslams. Vienintelė šios taisyklės išimtis yra atvejai, kai Ligoninė, suteikdama darbuotojui įrenginį (pavyzdžiui, mobilųjį telefoną), leidžia jį naudoti ir asmeniniais tikslais.
9. Kiekvienas darbuotojui suteikiamas įrenginys yra registruojamas.

III DARBUOTOJŲ PAREIGOS

10. Bet kokia informacija, prieinama darbuotojui jo darbo funkcijų vykdymo metu, bus laikoma konfidencialia ir saugoma laikantis šios Politikos nuostatų. Informacija negali būti atskleidžiama jokiems kokioms tretiesiems asmenims, išskyrus atvejus, kai toks atskleidimas yra būtinas su Ligoninės veikla susijusiems tikslams ir ją gaunantys tretieji asmenys įsipareigoja užtikrinti tokios informacijos konfidencialumą. Darbuotojai, dirbantys su tokia informacija, turi laikytis konfidencialumo principo ir laikyti ją paslapyje. Šios pareigos lieka galioti ir perėjus dirbti į kitas pareigas Ligoninėje, taip pat pasibaigus darbo ar kitiems sutartiniais santykiams su Ligonine.
11. Visi fizinių asmenų prašymai, susiję su asmens duomenimis ir (ar) jų tvarkymu, kuriuos Ligoninės darbuotojas gauna vykdydamas savo darbo funkcijas, turi būti nedelsiant perduodami Ligoninės Duomenų subjektų prašymų nagrinėjimo tvarkoje numatytiems asmenims.
12. Tais atvejais, kai jungdamiesi prie Ligoninės informacinių sistemų ar prieigai kitų išteklių (pvz., jungdamiesi prie darbinio elektroninio pašto, Ligoninei priklausančių ar jos naudojamų duomenų bazių), darbuotojai naudoja asmeninius įrenginius ar įrangą, jie privalo laikytis šios Politikos nuostatų taip pat, kaip ir naudodamiesi Ligoninės suteiktais įrenginiais ar įranga. Atitinkamai draudžiama yra saugoti bet kokius su Ligoninės veikla susijusius duomenis ir informaciją savo asmeniniame įrenginyje ar įrangoje; bet koks Ligoninės duomenų tvarkymas ir saugojimas yra galimas tik per Ligoninei priklausančiose ar jos naudojamose informacinėse sistemose ir saugyklose.
13. Kiekvienas darbuotojas privalo laikytis šios Politikos, taikytinų teisės aktų bei Ligoninės vidaus dokumentų ar lokalinių teisės aktų, kurie nustato informacijos tvarkymo ir saugumo reikalavimus.

IV PRIEIGŲ VALDYMAS IR INFORMACIJOS APSAUGA

14. Bet kokie įrenginiai bei informacija darbuotojams yra pasiekiami priklausomai nuo jų darbo funkcijų pobūdžio, turimų atsakomybių ir griežtai vadovaujantis principu „būtina žinoti“. Prieiga prie konkrečios Ligoninės informacinės sistemos nereikia, kad darbuotojas yra įgaliotas peržiūrėti ir naudoti visą ir bet kurią toje sistemoje esančią informaciją.
15. Darbuotojai, kurių kompiuteriuose saugomi pacientų, kitų asmenų duomenys, arba iš kurių kompiuterių galima prisijungti prie Ligoninės informacinių sistemų, kuriose yra saugomi pacientų, kitų asmenų duomenys, savo kompiuterius turi apsaugoti slaptažodžiais; „svečio“ (angl. *guest*) tipo, t. y. neapsaugotos slaptažodžiais, vartotojų paskyros yra draudžiamos.

Šiuose kompiuteriuose taip pat turi būti nustatytas sesijos laikas (t. y. naudotojui esant neaktyviam tam tikrą laiką (pavyzdžiui, 15 min.), jo sesija turi būti nutraukta).

16. Darbuotojas yra atsakingas už visus veiksmus, atliekamus naudojantis jam priskirta paskyra. Kiekvienas darbuotojas privalo užtikrinti, kad jo paskyrų duomenys (slaptažodžiai) nebūtų prieinami jokiems tretiesiems asmenims, įskaitant kitus Ligoninės darbuotojus.
17. Prieigas prie informacinių sistemų apsaugantys slaptažodžiai turi būti sudaromi atsakingai (jie negali būti lengvai atspėjami) ir reguliariai keičiami (ne rečiau kaip kartą per 3 mėnesius). Kiekvienas darbuotojas yra asmeniškai atsakingas už savo naudojamų slaptažodžių atitiktį šios Politikos nuostatomis ir bet kokioms kitoms Ligoninės taisyklėms. Slaptažodžiams keliami šie reikalavimai:
 - 17.1. slaptažodis turi būti sudarytas iš mažiausiai 8 simbolių, iš kurių bent vienas turi būti skaičius ir bent vienas turi būti raidė;
 - 17.2. slaptažodis negali sutapti su darbuotojo ar jo šeimos narių asmeniniais duomenimis;
 - 17.3. slaptažodį saugo ir jį gali žinoti tik darbuotojai, dirbantys su konkrečių kompiuterių ar sistema;
 - 17.4. slaptažodžiai negali būti pasiekiami kitiems asmenims (pvz., užrašomi ant lapelių ir paliekami darbo vietoje).
18. Darbuotojas gali susipažinti su konfidencialia informacija tik tuo atveju, jeigu jis turi atitinkamus įgaliojimus pagal darbo sutartį ir (ar) jam tokius įgaliojimus suteikė Ligoninė.
19. Darbuotojai, atliekantys asmens duomenų tvarkymą, turi užkirsti kelią bet kokiam atsitiktiniam ar neteisėtam duomenų tvarkymui, tinkamai bei atsakingai saugoti dokumentus (vengti nereikalingų dokumentų kopijų su asmens duomenimis laikymo ir kt.). Dokumentų, kuriuose yra asmens duomenų, kopijos turi būti sunaikinamos tokiu būdu, kad šių dokumentų ir jų turinio nebūtų galima atkurti.
20. Nesant būtinybės, rinkmenos su pacientų, kitų asmenų duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. neturi būti daromos rinkmenų kopijos, saugomos kompiuterių kietuosiuose diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir kt.
21. Ligoninės darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma būtų apribota galimybė kitiems asmenims (kitiems Ligoninės darbuotojams, paslaugų teikėjams ir kitiems tretiesiems asmenims) susipažinti su jų tvarkomais asmens duomenimis. Tai įgyvendinama:
 - 21.1. nepaliekant dokumentų su asmens duomenimis ir įrenginių, kuriais naudojantis galima susipažinti su asmens duomenimis, be priežiūros tokiu būdu, kad juose esančią informaciją galėtų perskaityti darbuotojai, neturintys teisės dirbti su konkrečiais asmens duomenimis, ir kiti tretieji asmenys;
 - 21.2. dokumentus laikant taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai tretieji asmenys;
 - 21.3. jeigu dokumentai, kuriuose yra asmens duomenų, jų gavėjams perduodami per asmenis, neturinčius teisės tvarkyti tokius asmens duomenis, arba paštu ar per kurjerį, jie turi būti siunčiami užklijuotame nepermatomame voke.
22. Darbuotojai gali perduoti dokumentus, kuriuose yra asmens duomenų, tik tiems darbuotojams, kurie pagal savo pareigas ar atskirus pavedimus turi teisę susipažinti su tais asmens duomenimis.
23. Darbuotojo prieigos teisės prie Ligoninės informacinės sistemos ar kitų išteklių turi būti nedelsiant panaikinamos, kai išnyksta pagrindas ar poreikis naudotis ta sistema ir (ar) tvarkyti joje esančius duomenis (pvz., pasibaigus darbo santykiams arba pasikeitus darbuotojo pareigoms ar darbo funkcijoms):

V TECHNINĖS SAUGUMO PRIEMONĖS

24. Visiems bet kokių būdu surinktiems ir tvarkomiems bet kokios formos (popierinės, elektroninės, kt.) duomenims ir informacijai yra taikomi šios Politikos ir atitinkamų teisės aktų reikalavimai dėl informacijos rinkimo, tvarkymo, apsaugos ir tolesnio saugojimo; tokie

duomenys ir informacija saugiai laikomi Ligoninės nustatytose vietose, laikantis taikytinuose teisės aktuose ir Ligoninės vidaus dokumentuose nustatytų terminų.

25. Asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugumo kontrolė ir jų savalaikis ištyrinimas užtikrinami perkeltant juos į atitinkamas informacines sistemas.
26. Visi duomenų pakeitimai Ligoninės informacinėse sistemose yra stebimi ir registruojami paskirto atsakingo asmens (juo gali būti ir Ligoninę aptarnaujantis paslaugų teikėjas (jo įgaliotas asmuo)).
27. Kiekvienos informacinės sistemos, naudojamos asmens duomenų tvarkymui, atžvilgiu yra įgyvendinama tokia kontrolė bei stebėseną:
 - 27.1. Fiksuojami šie techninių žurnalų įrašai apie prieigą prie asmens duomenų: asmens duomenys, prie kurių buvo prieita, su asmens duomenimis atlikti veiksmai (įvedimas, peržiūra, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai). Šie įrašai turi būti saugomi ne trumpiau kaip 1 (vienėrius) metus.
 - 27.2. Techninių žurnalų įrašai periodiškai (taip pat iškilus poreikiui) peržiūrimi ir (ar) teikiamos jų peržiūros ataskaitos Ligoninės vadovui.
28. Ligoninės įrenginiai bei informacinės sistemos yra tinkamai apsaugoti techninėmis bei organizacinėmis priemonėmis, siekiant išvengti neleistinos prieigos.
29. Kai prie Ligoninės informacinių sistemų yra jungiamasi internetu (prie nuotolį), yra naudojami saugūs, šifruoti komunikacijos kanalai. Perduodant asmens duomenis išoriniais duomenų perdavimo tinklais, yra užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas.
30. Darbuotojų kompiuteriai, kuriuose saugomos rinkmenos su pacientų, kitų fizinių asmenų duomenimis, negali būti laisvai prieinami iš kitų tinklo kompiuterių.
31. Jeigu Ligoninės duomenims pasiekti yra naudojami įvairūs nuotoliniai įrenginiai, darbuotojas privalo įsitikinti, kad naudojamas interneto ryšys yra saugus ir patikimas. Ligoninės duomenims pasiekti negali būti naudojamas viešas, neapsaugotas interneto ryšys. Mobiliosiuose įrenginiuose (nešiojamuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne Ligoninės vidiniame kompiuterių tinkle, esantys specialių kategorijų asmens duomenys ir prisijungimo prie Ligoninės informacinių sistemų duomenys turi būti šifruojami arba apsaugomi kitomis priemonėmis, kurios atitiktų esamas rizikas.
32. Į Ligoninės įrenginius bei įrangą gali būti diegiamos ir juose naudojamos tik Ligoninės leidžiamos informacinės sistemos ir tinkamai licencijuota programinė įranga.
33. Ligoninės įrenginiai bei įranga yra tinkamai apsaugoti antivirusine ir (ar) kitokia programine įranga, skirta apsaugoti nuo kenkėjiškos programinės įrangos.
34. Ligoninės naudojama programinė įranga, įskaitant operacines sistemas, yra nuolat atnaujinama pagal tiekėjų rekomendacijas.
35. Siekiant užtikrinti Ligoninės duomenų atkuriamumą, nuolat daromos informacijos atsarginės kopijos, laikantis gerųjų rinkos praktikų:
 - 35.1. atsarginės duomenų kopijos, jei jos daromos, saugomos kitoje geografinėje vietoje, negu aktyviai naudojamos informacinės sistemos duomenys;
 - 35.2. atsarginės kopijos, archyvuose ir išorinėse duomenų laikmenose saugomi duomenys yra šifruojami.
36. Elektroniniu paštu perduodami asmens duomenys turi būti šifruojami.
37. Kai Ligoninės saugoma informacija tampa nebereikalinga vykdant Ligoninės veiklą, tokia informacija ištrinama, visos jos kopijos sunaikinamos, o su šios informacijos tvarkymu susiję darbuotojai atitinkamai informuojami apie jų pareigą ištrinti, sunaikinti ir (ar) grąžinti Ligoninei visą informaciją, kurios jiems nebereikia vykdant darbo funkcijas (visų pirma, grąžinti Ligoninei, ištrinti arba sunaikinti duomenų kopijas tuo atveju, kai nutrūksta darbo santykiai su darbuotoju).

38. Patekimas į patalpas, kuriose laikomi Ligoninės įrenginiai bei įranga, įskaitant serverių patalpas, yra kontroliuojamas fizinėmis, elektroninėmis ar kitokiomis apsaugos priemonėmis (durų rakinimo sistema, bendra apsaugos signalizacijos sistema, kt.), kurios užtikrina, kad jokie pašaliniai, neįgalinti asmenys į tas patalpas negalėtų patekti.
39. Siekiant užtikrinti šios Politikos reikalavimų laikymąsi bei įvertinti, ar naudojamos saugumo priemonės yra pakankamos, yra atliekami:
 - 39.1. informacinėse sistemose atliekamo duomenų tvarkymo keliamos rizikos vertinimas, kuris būtų atliekamas kartą per 1 (vienerius) metus;
 - 39.2. įgyvendintų organizacinių ir techninių duomenų saugumo priemonių įvertinimo auditas, kuris būtų atliekamas kartą per 2 (dvejus) metus;
 - 39.3. reguliarius atsarginių kopijų testai, siekiant užtikrinti, kad jos galėtų būti panaudotos incidento atveju;
 - 39.4. informacinės sistemos pažeidžiamumo ir atsparumo skverbimuisi testai.

VI DRAUDŽIAMAI VEIKSMAI

40. Išskyrus konkrečiai nustatytas išimtis, jokiais atvejais ir jokiais aplinkybėmis Ligoninei priklausantys įrenginiai, sistemos ir įrankiai negali būti naudojami su darbuotojų darbo funkcijomis ar Ligoninės veikla nesusijusiems tikslams.
41. Jokia šioje Politikoje nurodyta informacija negali būti siunčiama, perduodama arba bet koku kitu būdu atskleidžiama trečiajam asmeniui, nebent tai būtina darbuotojo darbo funkcijoms vykdyti ir tik tokia apimtimi, kokia reikalinga darbo funkcijų vykdymui. Duomenų perdavimo ar kitokio atskleidimo tretiesiems asmenims atveju turi būti užtikrinama, kad duomenys yra perduodami naudojant saugias priemones ir (ar) imamasi kitų reikiamų saugumo priemonių.
42. Darbuotojams neleidžiama savo įrenginiuose laikyti Ligoninės asmens duomenis (visų pirma, pacientų duomenis) ar bet kokią kitą konfidencialią informaciją.
43. Žemiau nurodyti veiksmai yra griežtai draudžiami, nenumatant jokių išimčių:
 - 43.1. Bet kokių fizinio ar juridinio asmens intelektualinės nuosavybės teisių pažeidimas, įskaitant, bet neapsiribojant, bet kokios nelegalios programinės įrangos, virtualių platformų ar kito Ligoninei nelicencijuoto skaitmeninio turinio įdiegimu, kopijavimu, platinimu ar saugojimu Ligoninės sistemose, įrangoje ar įrenginiuose.
 - 43.2. Neteisėtas autorių teisėmis saugomos medžiagos kopijavimas.
 - 43.3. Bet kurio asmens teisių pažeidimas dėl perteklinio ir nereikalingo jo asmens duomenų rinkimo ir tvarkymo.
 - 43.4. Priėjimas prie Ligoninės duomenų, serverio, sistemos, bet kokio įrenginio ar įrangos, prisijungimas ar pasinaudojimas paskyra kitais tikslais nei Ligoninės veiklos užtikrinimas ar konkretaus darbuotojo darbo funkcijų vykdymas.
 - 43.5. Ligoninei priklausančios ir (ar) kitos konfidencialios informacijos ar duomenų eksportas, jeigu toks eksportas nėra reikalingas Ligoninės veiklai užtikrinti ar darbuotojo darbo funkcijoms vykdyti, ir (ar) atliekamas pažeidžiant taikytinus teisės aktus ar Ligoninės vidaus dokumentus.
 - 43.6. Darbuotojo paskyros slaptažodžio atskleidimas kitam asmeniui ir (ar) leidimas kitam asmeniui naudotis tokia darbuotojo paskyra (įskaitant, bet neapsiribojant, darbuotojo šeimos nariais).
 - 43.7. Apgaulingi ir (ar) neteisėti produktų ar paslaugų pasiūlymai, naudojantis Ligoninės suteikta paskyra, sistema ar įrenginiais.
 - 43.8. Saugumo pažeidimai arba tinklo sutrikdymas. Tokie saugumo pažeidimai apima, bet neapsiriboja, prieiga prie duomenų, kurie nėra skirti darbuotojui, arba prisijungimu prie serverio ar paskyros, darbuotojui neturint atitinkamų įgaliojimų (nebent prieigos teisės darbuotojui būtų suteiktos dėl jo dalyvavimo konkrečiame Ligoninės projekte).
 - 43.9. Visais atvejais griežtai draudžiama naudotis viešais prieigos įrenginiais (pavyzdžiui, bibliotekose, kt.). Jeigu suteiktomis darbo priemonėmis naudojamosi viešose vietose, darbuotojai privalo dėti pastangas, kad jų įrenginio ekranas nebūtų matomas, stebimas ar

įrašinėjamas pašalinių asmenų, taip pat nebūtų jungiamasi, naudojamosi viešu, nesaugiu, belaidžiu interneto ryšiu (*Wi-Fi*).

VII PRANEŠIMAS APIE SAUGUMO INCIDENTUS

44. Apie visus informacijos saugumo incidentus turi būti nedelsiant pranešta atsakingiems darbuotojams ir (ar) Ligoninės vadovui, kurie atitinkamai imasi priemonių galimai žalai išvengti, kilusiai žalai pašalinti ir buvusiai saugumo būklei atkurti.
45. Visi su asmens duomenimis susiję saugumo incidentai yra valdomi vadovaujantis kitais Ligoninės vidaus dokumentais.
46. Kai tai yra būtina, Ligoninės vadovas privalo užtikrinti, kad apie informacijos saugumo pažeidimus būtų pranešta kompetentingoms valdžios institucijoms ir (ar) kitiems asmenims, kaip tai numatyta taikytinuose teisės aktuose ir (ar) Ligoninės vidaus dokumentuose.
47. Už visų šioje Politikoje nurodytų saugumo priemonių įgyvendinimą yra atsakinga Ligoninė ir (ar), kai taikytina, jos pasitelkti paslaugų teikėjai.

VIII KITOS NUOSTATOS

48. Ligoninė organizuoja darbuotojų, kuriems suteikti įgaliojimai tvarkyti asmens duomenis, mokymus. Už tokių mokymų organizavimą, vykdymą darbuotojams, dirbantiems su asmens duomenimis, yra atsakingas Ligoninės vadovas.
49. Už šioje Politikoje numatytų organizacinių ir techninių saugumo priemonių įgyvendinimą, kontrolę, užtikrinimą yra atsakinga(-s) Ligoninės informacinės sistemas aptarnaujanti įmonė pagal sudarytą paslaugų pirkimo – pardavimo sutartį.
50. Už Politikos laikymosi priežiūrą ir jos nuostatų įgyvendinimo kontrolę, Politikos nuostatų peržiūrą ne rečiau kaip kartą per 2 metus, taip pat, esant poreikiui, Politikos atnaujinimą yra atsakinga(-s) Ligoninės duomenų apsaugos pareigūnas.