PATVIRTINTA
VšĮ Kėdainių ligoninės
direktoriaus 2024 m. gegužės 13d.
įsakymu D1-112

VIEŠOSIOS ĮSTAIGOS KĖDAINIŲ LIGONINĖS ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Viešosios įstaigos Kėdainių ligoninė (toliau – Ligoninė arba Duomenų valdytojas) asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reguliuoja fizinių asmenų (toliau – Duomenų subjektas) asmens duomenų tvarkymo tikslus, nustato Duomenų subjekto teisių įgyvendinimo tvarką, įtvirtina organizacines ir technines duomenų apsaugos priemones, reguliuoja asmens duomenų tvarkytojo pasitelkimo atvejus.

2. Šios Taisyklės parengtos remiantis:

2.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ);

2.2. Lietuvos Respublikos sveikatos sistemos įstatymu;

2.3. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymu;

2.4. Lietuvos Respublikos Vyriausybės 2001 m. vasario 28 d. nutarimu Nr. 228 „Dėl duomenų teikimo duomenų subjektui atlyginimo tvarkos ir duomenų surinkimo ir registruotų duomenų valdytojų atlyginimo tvarkos patvirtinimo“;

2.5. Lietuvos Respublikos Vyriausybės 2002 m. vasario 20 d. nutarimu „Dėl asmens duomenų valdytojų valstybės registro reorganizavimo, registro nuostatų ir asmens duomenų valdytojų pranešimo apie duomenų tvarkymą automatiniu būdu tvarkos patvirtinimo“;

2.6. Lietuvos Respublikos sveikatos apsaugos ministro 2017 m. lapkričio 30 d. įsakymu Nr. V-1371 „Dėl sveikatos priežiūros įstaigos asmens duomenų tvarkymo pavyzdinių taisyklių patvirtinimo“;

2.7. 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 – BDAR).

2.8. kitais teisės aktais, susijusiais su asmens duomenų tvarkymu ir apsauga.

3. Taisyklėse vartojamos sąvokos atitinka ADTAĮ vartojamas sąvokas. Taisyklių nuostatos negali plėsti ar siaurinti ADTAĮ taikymo srities bei prieštarauti ADTAĮ nustatytiems asmens duomenų tvarkymo reikalavimams ir kitiems asmens duomenų tvarkymą reglamentuojantiems teisės aktams.

4. Šios Taisyklės taikomos tvarkant Duomenų subjekto duomenis automatiniu būdu, taip pat ir neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: pacientų ligos istorijas, ambulatorines korteles, kartotekas, bylas, sąvadus ir kita. Šios Taisyklės taip pat nustato Duomenų valdytojo darbuotojų teises, pareigas ir atsakomybę tvarkant asmens duomenis.

5. Šių Taisyklių reikalavimai privalomi visiems Duomenų valdytojo darbuotojams (toliau - Darbuotojai), kurie tvarko Ligoninėje esančius asmens duomenis arba eidami savo pareigas juos sužino. Šių Taisyklių taip pat privalo laikytis duomenų tvarkytojai, kurie teikdami Ligoninei duomenų tvarkymo paslaugas, sužino ir tvarko asmens duomenis.

6. Duomenų valdytojas – VšĮ Kėdainių ligoninė, įstaigos kodas: 191045561, adresas: Budrio g. 5, LT–57164, Kėdainiai, el. paštas: administracija@kedligonine.lt.

II. ASMENS DUOMENŲ TVARKYMO PRINCIPAI IR TIKSLAI

7. Tvarkant asmens duomenis laikomasi asmens duomenų tvarkymo reikalavimų:

7.1. asmens duomenys renkami apibrėžtais ir teisėtais tikslais ir toliau negali būti tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis;

7.2. asmens duomenys tvarkomi tiksliai, sąžiningai ir teisėtai;

7.3. asmens duomenys turi būti tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas;

7.4. asmens duomenys turi būti tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti;

7.5. 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;

7.6. asmens duomenys tvarkomi pagal ADTAĮ, BDAR ir kituose atitinkamą veiklą reglamentuojančiuose įstatymuose nustatytus aiškius ir skaidrius asmens duomenų tvarkymo reikalavimus.

8. Ligoninėje Duomenų subjektų asmens duomenys tvarkomi vidaus administravimo, asmens sveikatos priežiūros paslaugų teikimo tikslais ir pacientų, lankytojų, darbuotojų bei turto saugumo užtikrinimo tikslais (vaizdo stebėjimas):

8.1. Ligoninei tvarkant duomenis vidaus administravimo tikslu, iš duomenų subjektų renkami ir tvarkomi tokie jų duomenys, kurie yra būtini darbo sutarties su jais sudarymo, vykdymo ir nutraukimo tikslu. Asmens duomenys gaunami tiesiogiai iš Duomenų subjektų (darbuotojų). Šių duomenų Ligoninė neperduoda jokiems duomenų gavėjams, išskyrus įstatymo numatytus atvejus.

8.2. Ligoninei tvarkant duomenis asmens sveikatos priežiūros teikimo tikslu, iš Duomenų subjektų (pacientų) yra renkami ir tvarkomi Duomenų subjektų (pacientų) asmens duomenys.

8.3. Ligoninei tvarkant duomenis pacientų, lankytojų, darbuotojų bei turto saugumo užtikrinimo tikslu (vaizdo stebėjimas), tvarkomas tik vaizdas (be garso) iš vaizdo stebėjimo kamerų, patenkantis į stebėjimo lauką. Šiuos duomenis valdo ir tvarko pati Ligoninė. Vaizdo stebėjimo duomenys yra saugomi iki 30 kalendorinių dienų, po kurių yra automatiškai ištrinami. Vaizdo stebėjimo duomenys gali būti pateikti teisėsaugos institucijoms bei Duomenų subjektams, pateikus pagrįstą prašymą dėl duomenų pateikimo. Pacientai, darbuotojai, lankytojai apie vykdomą vaizdo stebėjimą (konkrečią teritoriją) yra informuojami matomoje vietoje patalpintais informaciniais pranešimais. Darbuotojai pasirašytinai supažindinami su šiomis Taisyklėmis ir „Vaizdo asmens duomenų tvarkymo VšĮ Kėdainių ligoninėje taisyklėmis“

9. Už Duomenų subjektų duomenų atnaujinimą ir tvarkymą atsakingi Ligoninės direktorius.

10. Visa informacija apie paciento buvimą VšĮ Kėdainių ligoninėje, gydymą, sveikatos būklę, diagnozę, prognozes ir gydymą, taip pat visa kita asmeninio pobūdžio informacija apie pacientą yra konfidenciali, taip pat ir po paciento mirties. Informacija apie pacientą turi būti teikiama, jeigu tai yra privaloma pagal įstatymus. Paciento duomenys nėra teikiami pakartotiniam naudojimui komerciniais tikslais.

III. DUOMENŲ VALDYTOJO IR TVARKYTOJO FUNKCIJOS, TEISĖS IR PAREIGOS

11. Duomenų valdytojas – VšĮ Kėdainių ligoninė, įstaigos kodas: 191045561, adresas: Budrio g. 5, LT–57164, Kėdainiai, el. paštas: administracija@kedligonine.lt. Duomenų valdytojas nustato asmens

duomenų tvarkymo tikslus ir priemones, vykdo funkcijas, numatytas Ligoninės informacinės sistemos nuostatuose.

12. Duomenų valdytojas turi šias teises:

12.1. rengti ir priimti vidinius teisės aktus, reglamentuojančius asmens duomenų tvarkymą;

12.2. spręsti dėl tvarkomų asmens duomenų teikimo;

12.3. paskirti už asmens duomenų apsaugą atsakingą asmenį ar skyrių;

12.4. įgalioti duomenų tvarkytojus tvarkyti asmens duomenis;

12.5. sudaryti sutartis su paslaugų teikėju dėl duomenų tvarkymo įrangos priežiūros;

12.6. sudaryti sutartis su paslaugų teikėju dėl duomenų apsaugos pareigūno paslaugų;

12.7. tvarkyti asmens duomenis.

13. Duomenų valdytojas turi šias pareigas:

13.1. užtikrinti, kad būtų laikomasi ADTAĮ, BDAR ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą;

13.2. įgyvendinti duomenų subjekto teises ADTAI, BDAR ir šiose Taisyklėse nustatyta tvarka;

13.3. užtikrinti asmens duomenų saugumą įgyvendinant technines ir organizacines asmens duomenų saugumo priemones;

13.4. tvarkyti duomenų tvarkymo veiklos įrašus;

13.5. vertinti poveikį duomenų apsaugai;

13.6. konsultuotis su Valstybine duomenų apsaugos inspekcija;

13.7. skirti duomenų apsaugos pareigūną arba sudaryti sutartį su paslaugų teikėju dėl duomenų apsaugos pareigūno funkcijų įgyvendinimo;

13.8. pranešti apie duomenų saugumo pažeidimą;

13.9. parinkti tik tokius asmens duomenų tvarkymo įrangos priežiūros paslaugų teikėjus, kurie garantuotų reikiamas technines ir organizacines asmens duomenų apsaugos priemones.

13.10. vykdyti stebėseną ir kontrolę, kad būtų laikomasi bendrųjų reikalavimų organizacinėms ir techninėms saugumo priemonėms;

13.11. kontroliuoti patekimą į patalpas, kuriose saugomi dokumentai ir jų archyvai;

13.12. užtikrinti bendrųjų reikalavimų organizacinėms ir techninėms priemonėms laikymąsi.

14. Duomenų valdytojas atlieka šias funkcijas:

14.1. nustato asmens duomenų tvarkymo tikslą ir apimtį;

14.2. organizuoja asmens duomenų tvarkymą;

14.3. analizuoja technologines, metodologines ir organizacines asmens duomenų tvarkymo problemas ir priima sprendimus, reikalingus tinkamam asmens duomenų saugumo užtikrinimui;

14.4. teikia metodinę pagalbą darbuotojams ir duomenų tvarkytojams asmens duomenų tvarkymo tikslais;

14.5. organizuoja darbuotojų mokymus asmens duomenų teisinės apsaugos klausimais;

14.6. vykdo kitas funkcijas, reikalingas Duomenų valdytojo teisėms ir pareigoms įgyvendinti.

15. Duomenų tvarkytojas turi teises ir pareigas bei vykdo funkcijas, numatytas duomenų tvarkymo sutartyje.

16. Duomenų tvarkytojas turi šias teises:

16.1. teikti duomenų valdytojui pasiūlymus dėl duomenų tvarkymo techninių ir programinių priemonių gerinimo;

16.2. tvarkyti asmens duomenis, kiek tam yra įgaliotas duomenų valdytojo.

17. Duomenų tvarkytojas turi šias pareigas:

17.1. įgyvendinti tinkamas organizacines ir technines duomenų saugumo priemones, skirtas asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo apsaugoti;

17.2. supažindinti naujai priimtus darbuotojus su Taisyklėmis;

17.3. užtikrinti, kad prieiga prie asmens duomenų būtų suteikta tik Taisyklėse nustatyta tvarka įgaliotiems asmenims;

17.4. užtikrinti, kad asmens duomenys būtu saugomi Taisyklėse nustatytais terminais;

17.5. užtikrinti, kad asmens duomenys būtų tvarkomi vadovaujantis Taisyklėmis, ADTAI, BDAR ir kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais;

17.6. saugoti asmens duomenų paslaptį, neatskleisti, neperduoti tvarkomos informacijos ir nesudaryti sąlygų jokiomis priemonėmis su ja susipažinti nei vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija, tiek įstaigoje, tiek už jos ribų;

17.7. tvarkyti duomenų tvarkymo veiklos įrašus;

17.8. padėti duomenų valdytojui užtikrinti jam numatytas prievoles;

17.9. įsivertinus ir nusprendus, kad reikalingas duomenų apsaugos pareigūnas, skirti duomenų apsaugos pareigūną;

17.10. pranešti duomenų valdytojui apie duomenų saugumo pažeidimą;

18. Duomenų tvarkytojas atlieka šias funkcijas:

18.1. įgyvendina asmens duomenų saugumo priemones;

18.2. tvarko asmens duomenis pagal Duomenų valdytojo nurodymus.

IV. DUOMENŲ SUBJEKTO TEISIŲ ĮGYVENDINIMO TVARKA

19. Duomenų subjektai turi teisę:

19.1. sužinoti (būti informuotas) apie savo asmens duomenų tvarkymą;

19.2. susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi:

19.3. reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti, išskyrus saugojimą, savo asmens duomenų tvarkymo veiksmus, kai duomenys tvarkomi nesilaikant įstatymo nuostatų;

19.4. nesutikti, kad būtų tvarkomi jo Asmens duomenys;

19.5. savo, kaip duomenų subjekto, teises įgyvendinti per atstovą (atstovą pagal įstatymą arba atstovą pagal notaro patvirtintą įgaliojimą).

20. Duomenų subjekto teisių įgyvendinimo tvarka:

20.1. Ligoninė, kurioje renkami ir tvarkomi Duomenų subjekto duomenys, privalo sudaryti sąlygas Duomenų subjektui įgyvendinti pirmiau nurodytas Duomenų subjekto teises, išskyrus įstatymų nustatytus atvejus, kai reikia užtikrinti valstybės saugumą ar gynybą, viešąją tvarką, nusikalstamų veiklų prevenciją, tyrimą, nustatymą ar baudžiamąjį persekiojimą, svarbius valstybės ekonominius ar finansinius interesus, tarnybinės ar profesinės etikos pažeidimų prevenciją, tyrimą ir nustatymą, Duomenų subjekto ar kitu asmenų teisių ir laisvių apsaugą;

20.2. Duomenų subjekto informavimo tvarka apie asmens duomenų tvarkymą ir sutikimas dėl asmens duomenų tvarkymo:

20.2.1. Duomenų subjektas gali susipažinti su asmens duomenų tvarkymo taisyklėmis Ligoninės interneto svetainėje arba atvykęs į Ligoninę;

20.2.2. prieš pateikdamas asmens duomenis, turi patvirtinti, kad sutinka su asmens duomenų tvarkymo taisyklėmis:

20.2.2.1. raštu, jei atvyko į Ligoninę, ir raštiško sutikimo dar nėra pateikęs;

20.2.2.2. jei registruojasi internetu, patvirtina sutikimą interneto svetainėje;

20.2.2.3. jei registruojasi telefonu, patvirtina sutikimą telefonu;

20.3. Duomenų subjektas, norėdamas susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi:

20.3.1. atvykęs į Ligoninę, turi pateikti asmens tapatybės dokumentą bei raštišką prašymą lietuvių kalba;

20.3.2. el. paštu administracija@kedligonine.lt. atsiųsti prašymą lietuvių kalba, kuris būtų patvirtintas asmens elektroniniu parašu arba kitais būdais, leidžiančiais tinkamai identifikuoti duomenų subjektą;

20.3.3. paštu arba per kurjerį atsiųsti prašymą lietuvių kalba ir asmens tapatybę patvirtinančio dokumento kopiją, patvirtintą notaro.

20.4. Duomenų valdytojas, gavęs iš duomenų subjekto prašymą ir kitus dokumentus 20.3. straipsnyje numatyta tvarka, ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo prašymo pateikimo dienos turi suteikti duomenų subjektui šią informaciją (išskyrus atvejus, kai šią informaciją duomenų subjektas jau turi):

20.4.1. savo pavadinimą, juridinio asmens kodą, buveinės adresą;

20.4.2. kokiais tikslais ir kokie tvarkomi duomenų subjekto asmens duomenys;

20.4.3. kokiems duomenų gavėjams asmens duomenys buvo teikiami per paskutinius 1 metus;

20.4.4. kitą papildomą informaciją (kam ir kokiais tikslais teikiami duomenų subjekto duomenys, kokius asmens duomenis duomenų subjektas privalo pateikti ir kokios nepateikimo pasekmės, apie duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis), kiek jos reikia, kad būtų užtikrintas teisingas duomenų tvarkymas nepažeidžiant duomenų subjekto teisių.

20.5. Duomenų valdytojas, kuris asmens duomenis gauna ne iš duomenų subjekto, privalo apie tai informuoti duomenų subjektą pradėdamas tvarkyti asmens duomenis arba, jei ketina duomenis teikti tretiesiems asmenims, privalo apie tai informuoti duomenų subjektą ne vėliau kaip iki to momento, kai duomenys teikiami pirmą kartą, išskyrus atvejus, kai įstatymai ar kiti teisės aktai apibrėžia tokių duomenų rinkimo ir teikimo tvarką bei duomenų gavėjus. Šiuo atveju duomenų valdytojas privalo duomenų subjektui suteikti šią informaciją (išskyrus atvejus, kai duomenų subjektas tokią informaciją jau turi):

20.5.1 savo pavadinimą, juridinio asmens kodą, buveinės adresą;

20.5.2 kokiais tikslais tvarkomi ar ketinami tvarkyti duomenų subjekto asmens duomenys;

20.5.3. kitą papildomą informaciją (iš kokių šaltinių ir kokie duomenų subjekto asmens duomenys renkami ar ketinami rinkti; kam ir kokiais tikslais teikiami duomenų subjekto asmens duomenys; apie duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis), kiek jos reikia, kad būtų užtikrintas teisingas asmens duomenų tvarkymas nepažeidžiant duomenų subjekto teisių.

20.6. Duomenų subjekto prašymu, Duomenų valdytojas 20.4. straipsnyje numatytą informaciją pateikia raštu:

20.6.1. registruotu paštu, jei prašymas buvo pateiktas atvykus, paštu ar per kurjerį;

20.6.2. siunčiant šifruotą informaciją el. paštu, jei prašymas buvo pateiktas el. paštu.

20.7. Duomenų valdytojas 20.4. straipsnyje numatytą informaciją duomenų subjektui teikia neatlygintinai vieną kartą per metus. Jei duomenų subjektas pateikia prašymus pagal 20.3. straipsnį keletą kartų per metus, informacija pagal antrąjį ir kitus prašymus bus teikiama atlygintinai pagal Ligoninės direktoriaus nustatytus duomenų teikimo atlyginimo įkainius

20.8. Duomenų subjektai gali prašyti ištaisyti neteisingus, neišsamius, netikslius asmens duomenis:

20.8.1. atvykus į Ligoninę ir pateikus prašymą lietuvių kalba su asmens tapatybės dokumentu;

20.8.2. paštu arba per kurjerį atsiuntus prašymą lietuvių kalba kartu su asmens tapatybės dokumento kopija, patvirtinta notaro;

20.8.3. el. paštu administracija@kedligonine.lt atsiųsti prašymą lietuvių kalba, kuris būtų patvirtintas asmens elektroniniu parašu arba arba kitais būdais, leidžiančiais tinkamai identifikuoti duomenų subjektą;

20.9. Duomenų valdytojas, gavęs iš duomenų subjekto rašytinį prašymą ir kitus dokumentus 20.8. straipsnyje numatyta tvarka, turi nedelsiant neatlygintinai patikrinti asmens duomenis ir ištaisyti neteisingus, neišsamius, netikslius asmens duomenis ir (arba) sustabdyti tokių asmens duomenų tvarkymo veiksmus, išskyrus saugojimą.

20.10. Jeigu duomenų subjektas, susipažinęs su savo asmens duomenimis, nustato, kad jo asmens duomenys yra tvarkomi neteisėtai, nesąžiningai, jis turi apie tai pranešti Duomenų valdytojui:

20.10.1. atvykus į Ligoninę, pateikti raštą lietuvių kalba ir patvirtinti savo tapatybę asmens tapatybės dokumentu;

20.10.2. paštu arba per kurjerį atsiųsti raštą kartu su asmens tapatybės dokumento kopija, patvirtinta notaro;

20.10.3. el. paštu administracija@kedligonine.lt atsiųsti raštą lietuvių kalba, kuris būtų patvirtintas asmens elektroniniu parašu arba arba kitais būdais, leidžiančiais tinkamai identifikuoti duomenų subjektą;

20.11. Duomenų valdytojas, gavęs iš duomenų subjekto rašytinį prašymą ir kitus dokumentus 20.10. straipsnyje numatyta tvarka, turi patikrinti asmens duomenis ir nedelsiant neatlygintinai patikrinti asmens duomenų tvarkymo teisėtumą, sąžiningumą ir duomenų subjekto prašymu (išreikštu rašytine forma) nedelsdamas sunaikinti neteisėtai ir nesąžiningai sukauptus asmens duomenis ar sustabdyti tokių asmens duomenų tvarkymo veiksmus, išskyrus saugojimą.

20.12. Duomenų subjekto prašymu sustabdžius jo asmens duomenų tvarkymo veiksmus, Duomenų valdytojas asmens duomenis, kurių tvarkymo veiksmai sustabdyti, saugo tol, kol bus ištaisyti ar sunaikinti (duomenų subjekto prašymu arba pasibaigus duomenų saugojimo terminui). Kitus tvarkymo veiksmus su tokiais asmens duomenimis Duomenų valdytojas atlieka tik:

20.12.1. siekiant įrodyti aplinkybes, dėl kurių duomenų tvarkymo veiksmai buvo sustabdyti;

20.12.2. jei duomenų subjektas duoda sutikimą toliau tvarkyti savo asmens duomenis;

20.12.3. jei reikia apsaugoti trečiųjų asmenų teises ar teisėtus interesus.

20.13. Duomenų valdytojas turi nedelsdamas pranešti duomenų subjektui apie jo prašymu atliktą ar neatliktą asmens duomenų ištaisymą, sunaikinimą ar asmens duomenų tvarkymo veiksmų sustabdymą.

20.14. Jeigu Duomenų valdytojas abejoja duomenų subjekto pateiktų asmens duomenų teisingumu, jis privalo sustabdyti tokių duomenų tvarkymo veiksmus, duomenis patikrinti ir patikslinti. Tokie asmens duomenys gali būti naudojami tik jų teisingumui patikrinti.

20.15. Duomenų valdytojas privalo nedelsdamas informuoti duomenų gavėjus apie duomenų subjekto prašymu ištaisytus ar sunaikintus asmens duomenis, sustabdytus asmens duomenų tvarkymo veiksmus, išskyrus atvejus, kai pateikti tokią informaciją būtų neįmanoma arba pernelyg sunku (dėl didelio duomenų subjektų skaičiaus, duomenų laikotarpio, nepagrįstai didelių sąnaudų). Tokiu atveju turi būti nedelsiant pranešama Valstybinei duomenų apsaugos inspekcijai.

20.16. Duomenų subjekto teisė nesutikti, kad butų tvarkomi jo asmens duomenys įgyvendinama tuo atveju, kai asmens duomenys tvarkomi vadovaujantis ADTAĮ 5 straipsnio 1 dalies 5 ir 6 punktuose nurodytais atvejais prieš atliekant asmens duomenų tvarkymo veiksmus:

20.16.1. Duomenų valdytojas, įgyvendindamas šių Taisyklių 20.5. punkte nurodytą pareigą, per 3 (tris) darbo dienas nuo asmens duomenų gavimo ar ketinimo juos teikti tretiesiems asmenims, be

minėtame punkte nurodytos informacijos, kartu informuoja Duomenų subjektą ir apie jo teisę išreikšti savo nesutikimą per 3 (tris) darbo dienas nuo Duomenų valdytojui atsiųsto rašto gavimo dienos.

20.16.2. Duomenų subjektas, įgyvendindamas savo teisę nesutikti, kad būtų tvarkomi jo asmens duomenys, pateikia Duomenų valdytojui pranešimą apie nesutikimą dė1 jo asmens duomenų tvarkymo:

20.16.2.1. atvykus į Ligoninę, pateikia rašytinį pranešimą lietuvių kalba ir patvirtina savo tapatybę asmens tapatybės dokumentu;

20.16.2.2. paštu arba per kurjerį atsiuntus rašytinį pranešimą lietuvių kalba kartu su asmens tapatybės dokumento kopija, patvirtinta notaro;

20.16.2.3. el. paštu administracija@kedligonine.lt atsiuntus rašytinį pranešimą lietuvių kalba, kuris būtų patvirtintas asmens elektroniniu parašu arba arba kitais būdais, leidžiančiais tinkamai identifikuoti duomenų subjektą;

20.16.3. Jeigu duomenų subjekto nesutikimas yra teisiškai pagrįstas, Duomenų valdytojas nedelsdamas neatlygintinai nutraukia asmens duomenų tvarkymo veiksmus, išskyrus įstatymų nustatytus atvejus, ir informuoja duomenų gavėjus.

20.16.4. Duomenų valdytojas praneša Duomenų subjektui apie jo asmens duomenų tvarkymo veiksmų nutraukimą ar atsisakymą nutraukti duomenų tvarkymo veiksmus.

20.16.5. Duomenų valdytojas, per 20.16.1. punkte nurodytą terminą negavęs duomenų subjekto rašytinio pranešimo apie nesutikimą dėl jo asmens duomenų tvarkymo, atlieka jų tvarkymo veiksmus teisės aktų nustatyta tvarka.

20.17. Atstovai pagal pavedimą, veikdami duomenų subjekto vardu, Duomenų valdytojui privalo pateikti atstovavimą patvirtinantį dokumentą. Šis atstovavimas įforminamas ir patvirtinamas notaro arba duomenų subjektas apie savo pasirinktą atstovą pasirašytinai nurodė savo medicinos dokumentuose.

20.18. Nepilnamečiam Duomenų subjektui iki 16 (šešiolikos) metų atstovauja jo atstovai pagal įstatymą: vienas iš tėvų (įtėvių), globėjas, rūpintojas. Nepilnamečiam pacientui iki 16 (šešiolikos) metų, kuriam nustatyta institucinė globa (rūpyba), atstovauja šių įstaigų paskirti asmenys, pateikę atstovavimą patvirtinantį dokumentą. Duomenų subjekto nuo 16 (šešiolikos) metų sutuoktinis, sugyventinis (partneris), o kai jų nėra - vienas iš duomenų subjekto tėvų (įtėvių) arba vienas iš pilnamečių vaikų yra duomenų subjekto, kuris negali būti laikomas gebančiu protingai vertinti savo interesų, atstovu pagal įstatymą; nurodyti asmenys nelaikomi paciento nuo 16 (šešiolikos) metų atstovais pagal įstatymą, jeigu jie atsisako būti atstovais, duomenų subjektas yra paskyręs atstovą pagal pavedimą arba duomenų subjektui nustatyta globa (rūpyba).

V. ORGANIZACINĖS IR TECHNINĖS ASMENS DUOMENŲ APSAUGOS PRIEMONĖS

21. Ligoninės organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti trečiąjį automatiniu būdu tvarkomų asmens duomenų saugumo lygį.

22. Siekiant apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo turi būti taikomos šios infrastruktūrinės, administracinės ir telekomunikacinės (elektroninės) priemonės:

22.1. Ligoninės direktoriaus įsakymu paskirtas duomenų valdymo įgaliotinis ir informacinės sistemos administratorius;

22.2. tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių sistemų priežiūra, tinklo valdymas, naudojimosi internetu saugumo užtikrinimas ir kitos informacinių technologijų priemonės. Už priemonių įgyvendinimą ir priežiūrą atsako Ligoninės, direktoriaus įsakymu, paskirtas darbuotojas arba IT paslaugas, pagal paslaugų sutartį, teikianti įmonė;

22.3. griežtas priešgaisrinės apsaugos tarnybos nustatytų normų laikymasis. Už priemonės įgyvendinimą ir priežiūrą atsako Ligoninės direktoriaus įsakymu paskirtas darbuotojas;

22.4. tinkamas darbo organizavimas ir kitos administracinės priemonės. Už priemonių įgyvendinimą ir priežiūrą atsako Ligoninės direktorius arba kitas direktoriaus įsakymų patvirtintas įstaigos darbuotojas.

23. Ligoninė privalo užtikrinti šias organizacines ir technines asmens duomenų saugumo priemones:

23.1. užtikrinti prieigos prie asmens duomenų apsaugą, valdymą ir kontrolę;

23.2. prieigą prie asmens duomenų suteikti tik tiems darbuotojams, kuriems asmens duomenys yra reikalingi jų funkcijoms vykdyti. Darbo santykiams pasibaigus, prieigas buvusiam darbuotojui panaikinti;

23.3. užtikrinti, kad su asmens duomenimis būtų galima atlikti tik tuos veiksmus, kuriems atlikti naudotojui yra suteiktos teisės;

23.4. užtikrinti, kad prieigos prie asmens duomenų slaptažodžiai:

23.4.1. suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą;

23.4.2. unikalūs, sudaryti iš ne mažiau kaip 8 (aštuonių) simbolių, nenaudojant asmeninio pobūdžio informacijos;

23.4.3. keičiami ne rečiau kaip kartą per 2 (du) mėnesius;

23.4.4. pirmojo prisijungimo metu naudotojo privalomai keičiami;

23.5. užtikrinti asmens duomenų apsaugą nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis;

23.6. užtikrinti patalpų, kuriose saugomi asmens duomenys, saugumą (užtikrinamas tik įgaliotų asmenų patekimas į atitinkamas patalpas ir pan.);

23.7. užtikrinti kompiuterinės įrangos apsaugą nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.).

23.8. kontroliuoti prieigą prie asmens duomenų tokiomis organizacinėmis ir techninėmis asmens duomenų saugumo priemonėmis, kurios fiksuoja ir kontroliuoja registravimosi bei teisių gavimo pastangas;

23.9. nustatyti leistinų nepavykusių prisijungimų prie programinės įrangos skaičių;

23.10. fiksuoti šiuos prisijungimų prie asmens duomenų įrašus: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas (sėkmingas, nesėkmingas), bylos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai). Šie įrašai turi būti saugomi ne trumpiau kaip 1 (vienerius) metus;

23.11. asmens duomenų paieškos užklausoje turi būti nurodomas asmens duomenų naudojimo tikslas;

23.12. užtikrinti saugių protokolų ir (arba) slaptažodžių naudojimą, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais;

23.13. užtikrinti asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolę ir ištrynimą po jų panaudojimo perkeliant į duomenų bazes ir pan.;

23.14. registruoti asmens duomenų kopijavimo, jei jis daromas, ir atkūrimo jų avarinio praradimo atveju veiksmus (kada ir kas atliko šiuos veiksmus);

23.15. užtikrinti, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis, išskyrus būtinus atvejus, kurių metu būtų naudojamos organizacinės ir techninės asmens duomenų saugumo priemonės, užtikrinančios realių asmens duomenų saugumą;

23.16. ne rečiau kaip kartą per 1 mėnesį peržiūrėti naudotojų prisijungimų prie duomenų bazės (-ių) įrašų elektroninį žurnalą ir duomenų valdytojui teikiamas peržiūros ataskaitas;

23.17. mobiliuosiuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne Ligoninės vidiniame kompiuterių tinkle, esantys ypatingi asmens duomenys ir prisijungimo prie Ligoninėje tvarkomų asmens duomenų informacija turi būti šifruojama ar apsaugoma tokiomis priemonėmis, kurios atitiktų asmens duomenų atskleidimo keliamą riziką;

23.18. atsarginės asmens duomenų kopijos turi būti saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;

23.19. atsarginėse kopijose, archyvuose ir išorinėse duomenų laikmenose saugomi asmens duomenys turi būti šifruojami;

23.20. elektroniniu paštu perduodami ypatingi asmens duomenys turi būti šifruojami.

23.21. ne rečiau kaip kartą per 1(vienerius) metus atlikti asmens duomenų tvarkymo rizikos vertinimą;

23.22. ne rečiau kaip kartą per 1 (vienerius) metus patikrinti avarinio asmens duomenų atkūrimo tvarką atliekant praktinius bandymus;

23.23. šifruoti aktyvioje (veikiančioje) duomenų bazėje saugomus asmens duomenis;

23.24. naudoti organizacines ir technines asmens duomenų saugumo priemones, kontroliuojančias duomenų bazę (-es), tarnybinę (-es) stotį (-is) ir informacinę sistemą administruojančių asmenų veiksmus.

24. Darbuotojai, kurie tvarko duomenų subjektų duomenis, turi laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su duomenų subjekto duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo darbines pareigas. Ši pareiga lieka galioti perėjus dirbti į kitas pareigas Ligoninėje ir pasibaigus darbiniams santykiams su Ligonine.

25. Darbuotojai gali perduoti dokumentus, kuriuose nurodyti asmens duomenys, tik tiems darbuotojams, kurie turi teisę dirbti su asmens duomenimis pagal pareigas, kaip tai numatyta Asmens duomenų tvarkymo procedūroje arba atskirame direktoriaus įsakyme.

26. Darbuotojai, kurie tvarko duomenų subjektų duomenis, turi užkirsti kelia atsitiktiniam ar neteisėtam duomenų tvarkymui, turi saugoti dokumentus tinkamai ir saugiai. Dokumentų kopijos, kuriose nurodyti asmens duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų negalima būtų atkurti ir atpažinti jų turinio.

27. Darbuotojai privalo taip organizuoti savo darbą, kad užtikrintų, jog asmens duomenys nebus pasiekiami kitiems asmenims. Ši nuostata įgyvendinama laikantis Asmens duomenų tvarkymo procedūroje numatytų procedūrų ir tvarkos.

28. Už asmens duomenų saugumo pažeidimų valdymą ir reagavimą į šiuos pažeidimus atsakingas Ligoninės direktoriaus įsakymu paskirtas duomenų apsaugos pareigūnas arba pagal paslaugų sutartį įgaliotas duomenų apsaugos pareigūnas.

VI. ASMENS DUOMENŲ TVARKYTOJO PASITELKIMAS

29. Tais atvejais, kai Duomenų valdytojas įgalioja Duomenų tvarkytoją atlikti asmens duomenų tvarkymo veiksmus, tarp Duomenų valdytojo ir Duomenų tvarkytojo turi būti sudaroma rašytinė asmens duomenų tvarkymo sutartis.

30. Sprendimą perduoti Duomenų subjekto duomenų tvarkymą asmens duomenų tvarkytojui priima Ligoninės direktorius.

31. Duomenų valdytojas privalo parinkti toki Duomenų tvarkytoją, kuris garantuotų reikiamas technines ir organizacines duomenų apsaugos priemones ir užtikrintų, kad tokių priemonių būtų laikomasi.

32. Duomenų valdytojas, sutartyje įgaliodamas Duomenų tvarkytoją tvarkyti asmens duomenis, nurodo, kokius asmens duomenų tvarkymo veiksmus privalo atlikti duomenų tvarkytojas duomenų valdytojo vardu. Duomenų tvarkytojai, kurie tvarko duomenų subjekto duomenis, turi laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su duomenų subjekto duomenimis susijusią informaciją, su kuria jie susipažino vykdydami duomenų tvarkymo sutartį, nebent tokia informacija butų vieša pagal galiojančių įstatymų ir kitų teisės aktų nuostatas.

VII. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMO IR REAGAVIMO Į ŠIUOS PAŽEIDIMUS TVARKA

33. Ligoninės darbuotojai, turintys prieigos prie asmens duomenų teisę, pastebėję duomenų saugumo pažeidimus (veiksmus ar neveikimą, galinčius sukelti ar sukeliančius grėsmę asmens duomenų saugumui), turi informuoti Ligoninės direktorių ir duomenų apsaugos pareigūną.

34. Įvertinus duomenų apsaugos pažeidimo rizikos veiksnius, pažeidimo poveikio laipsnį, žalą ir padarinius, kiekvienu konkrečiu atveju Ligoninės direktorius priima sprendimus dėl priemonių, reikiamų duomenų apsaugos pažeidimui ir jo padariniams pašalinti.

VIII. ASMENS DUOMENŲ TEIKIMAS TRETIESIEMS ASMENIMS

35. Duomenų teikimas tretiesiems asmenims:

35.1. neįgaliotų trečiųjų asmenų elektroninius ar kitokia forma (išskyrus telefonu) pateiktus prašymus suteikti jiems informaciją apie Duomenų subjektus turi būti atsakoma tik jeigu Rašytiniame prašyme yra nurodytas Duomenų subjekto duomenų naudojimo tikslas, tinkamas teikimo bei gavimo teisinis pagrindas ir prašomų pateikti Duomenų subjektų duomenų apimtis. Informacija (asmens duomenys) apie pacientą telefonu neteikiama.

35.2. Vienkartinio duomenų teikimo atveju Duomenų valdytojas, teikdamas asmens duomenis pagal duomenų gavėjo rašytinį prašymą, prioritetą teikia duomenų teikimui elektroninių ryšių priemonėmis.

36. Konfidencialumo reikalavimas netaikomas ir informacija (asmens duomenys) gali būti suteikta tik tarnybiniais tikslais, neturint raštiško paciento sutikimo:

36.1. sveikatos priežiūros įstaigoms, kuriose yra/buvo gydomas, slaugomas pacientas Duomenų subjektas) arba atliekama jo sveikatos ekspertizė;

36.2. teismui, prokuratūrai, ikiteisminio tyrimo įstaigoms, savivaldybių vaiko teisių apsaugos skyriams bei kitoms institucijoms, kurioms tokį teisinį pagrindą suteikia Lietuvos Respublikos įstatymai;

36.3. institucijoms, kontroliuojančioms sveikatos priežiūros paslaugas.

37. Vadovaudamasi Lietuvos Respublikos įstatymais ir kitais teisės aktais, Ligoninė asmens duomenis apie pacientą (duomenų subjektą) pateikia savo iniciatyva ir be paciento sutikimo šiais atvejais:

37.1. kai reikia pranešti apie nusikaltimą;

37.2. savivaldybių vaiko teisių apsaugos skyriams pagal vaiko gyvenamą vietą nedelsiant, esant pagrįstų įtarimų dėl vaiko teisių pažeidimo:

37.2.1. kai įtaria vaiko nepriežiūra;

37.2.2. įtarus emocinį, fizinį ar seksualinį smurtą vaiko atžvilgiu;

37.2.3. kai vaiko atstovai pagal įstatymą neužtikrina sveikatos priežiūros paslaugų vaikui teikimo;

37.2.4. kai įtaria, kad vaiko atstovai pagal įstatymą dėl sveikatos būklės negali tinkamai vykdyti savo pareigų vaiko atžvilgiu;

37.2.5.kitais atvejais.

IX. BAIGIAMOSIOS NUOSTATOS

38. Už šių Taisyklių vykdymo kontrolę atsako Ligoninės direktorius.

39. Už darbuotojų supažindinimą su šiomis Taisyklėmis pasirašytinai atsako Žmogiškųjų išteklių ir administravimo skyrius, vyr. slaugytoja, skyrių vedėjai savo kompetencijų ribose.

40. Už Taisyklių nuostatų laikymosi priežiūrą pagal nustatytus teisės aktus atsakingas Ligoninės direktoriaus įsakymu paskirtas arba pagal paslaugų sutartį įgaliotas duomenų apsaugos pareigūnas, kuris, įvertinęs Taisyklių taikymo praktiką, esant poreikiui, inicijuoja Taisyklių atnaujinimą.

41. Ligoninė privalo užtikrinti darbuotojų, kuriems suteikta teisė tvarkyti asmens duomenis, mokymus.

42. Darbuotojai, kurie yra įgalioti tvarkyti asmens duomenis arba eidami savo pareigas juos sužino, privalo laikytis šių Taisyklių, Asmens duomenų tvarkymo procedūros, pagrindinių asmens duomenų tvarkymo reikalavimų bei konfidencialumo ir saugumo reikalavimų, įtvirtintų ADTAĮ, BDAR ir šiose Taisyklėse.

43. Šias Taisykles pažeidę asmenys atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____