PATVIRTINTA
Lietuvos, JAV ir Izraelio UAB „VAISINGUMO KLINIKA“ direktoriaus
2018 m. gegužės 18 d. įsakymu Nr.2-10 V

Lietuvos, JAV ir Izraelio UAB „VAISINGUMO KLINIKA“

ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Lietuvos, JAV ir Izraelio UAB „VAISINGUMO KLINIKA“ (toliau – Klinika) Asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja duomenų subjektų teisių, įtvirtintų 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 – BDAR), įgyvendinimo tvarką Klinikoje, reguliuoja fizinių asmenų, kurių duomenis tvarko Klinika, Asmens duomenų tvarkymo tikslus, nustato jų teisių įgyvendinimo tvarką, įtvirtina organizacines ir technines duomenų apsaugos priemones, Asmens duomenų incidentų valdymo, poveikio duomenų apsaugai atlikimo tvarką, reguliuoja Asmens duomenų tvarkytojo pasitelkimo atvejus.

2. Šios Taisyklės parengtos remiantis:

2.1. Bendruoju Asmens duomenų apsaugos reglamentu;

2.2. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymu;

2.3. Lietuvos Respublikos sveikatos sistemos įstatymu;

2.4. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymu;

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

2.6. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2016 m. birželio 23 d. įsakymu Nr. 1T-25(1.12E) „Dėl pranešimų dėl išankstinės patikros formų patvirtinimo“;

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

2.8. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“;

2.9. Kitais teisės aktais, susijusiais su Asmens duomenų tvarkymu ir apsauga.

3. Šios Taisyklės taikomos tvarkant fizinių asmenų duomenis automatiniu būdu, taip pat ir neautomatiniu būdu tvarkant Asmens duomenų susistemintas rinkmenas: pacientų ligos istorijas, pacientų korteles, sąrašus, kartotekas, bylas, sąvadus ir kita. Šios Taisyklės taip pat nustato Klinikos darbuotojų teises, pareigas ir atsakomybę tvarkant Asmens duomenis.

4. Šių Taisyklių reikalavimai privalomi visiems Klinikos darbuotojams (toliau – Darbuotojai), kurie tvarko Klinikoje esančius Asmens duomenis arba eidami savo pareigas juos sužino. Šių Taisyklių taip pat privalo laikytis Duomenų tvarkytojai, kurie teikdami Klinikai duomenų tvarkymo paslaugas, sužino ir tvarko Asmens duomenis.

II SKYRIUS

PAGRINDINĖS SĄVOKOS

5. Asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai arba netiesiogiai nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens kodą, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to

fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

6. 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.

7. Duomenų valdytojas – Klinika, kuri tvarkydama pacientų, kitų fizinių asmenų ir Darbuotojų duomenis nustato tų duomenų naudojimo būdus ir priemones.

8. Duomenų subjektas – Darbuotojai, pacientai ir kiti fiziniai asmenys, kurių duomenis tvarko Klinika.

9. Duomenų tvarkytojas – subjektai, kurie tvarko Klinikos valdomus Asmens duomenis pagal Klinikos nurodymus ir vadovaujantis sudarytomis paslaugų teikimo sutartimis.

10. Duomenų teikimas – Asmens duomenų atskleidimas perduodant ar kitu būdu padarant juos prieinamus (išskyrus paskelbimą visuomenės informavimo priemonėse).

11. Vidaus administravimas – veikla, kuria užtikrinamas duomenų valdytojo savarankiškas funkcionavimas (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, raštvedybos tvarkymas).

12. Kitos Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR.

III SKYRIUS

ASMENS DUOMENŲ TVARKYMO PRINCIPAI IR TIKSLAI

13. Darbuotojai, atlikdami savo pareigas ir tvarkydami Asmens duomenis, privalo:

13.1. Asmens duomenis tvarkyti teisėtai, sąžiningai ir skaidriai;

13.2. Rinkti nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkyti su tais tikslais nesuderinamu būdu;

13.3. Renkant ir tvarkant Asmens duomenis laikytis tikslingumo, proporcingumo ir duomenų kiekio mažinimo principų, nereikalauti iš pacientų, kitų interesantų pateikti tų duomenų, kurie nėra reikalingi, nekaupiami ir netvarkyti perteklinių duomenų;

13.4. Užtikrinti Asmens duomenų tikslumą ir, jei reikia dėl Asmens duomenų tvarkymo, juos atnaujinti; netikslius ar neišsamius duomenis ištaisyti, papildyti, sunaikinti arba jų tvarkymą sustabdyti;

13.5. Asmens duomenis saugoti teisės aktų ir šių Taisyklių nustatyta tvarka;

13.6. Asmens duomenis tvarkyti 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 tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

14. Visa informacija apie paciento buvimą sveikatos priežiūros įstaigoje, 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.

IV SKYRIUS

DUOMENŲ TVARKYMO TIKSLAS, ŠALTINIAI, TEIKIMAS IR SAUGOJIMAS

15. Klinikos Duomenų subjektų Asmens duomenys tvarkomi:

15.1. Darbuotojų asmens duomenys – vidaus administravimo tikslu;

15.2. Pacientų – sveikatos priežiūros paslaugų teikimo tikslu;

16. Klinikai tvarkant duomenis Taisyklių 15.1. p. nurodytu tikslu, iš darbuotojų yra renkami ir tvarkomi tokie jų Asmens duomenys, kurie yra būtini darbo sutarties su jais sudarymo, vykdymo ir nutraukimo tikslu

(vardas, pavardė, asmens kodas, gimimo data, gyvenamosios vietos adresas, elektroninio pašto adresas, telefono numeris, spaudo numeris, duomenys apie išsilavinimą, profesinę patirtį, kvalifikaciją, pareigas, darbo užmokestis, banko sąskaitos numeris, dirbtas laikas, sukauptos, panaudotos atostogos, šeiminė padėtis, pilietybė, pareigos, duomenys apie priėmimą / perkėlimą / atleidimą iš pareigų, duomenys apie mokymą, duomenys apie darbo užmokestį, išeitines išmokas, kompensacijas, pašalpas, informacija apie dirbtą darbo laiką, informacija apie skatinimus ir nuobaudas, informacija apie atliktus darbus ir užduotis).

16.1. Klinikai tvarkant duomenis Taisyklių 15.1. p. tikslu, Asmens duomenys yra gaunami tiesiogiai iš Darbuotojų. Šių duomenų Klinika neperduoda jokiems duomenų gavėjams, išskyrus įstatymo numatytus atvejus, kai toks perdavimas būtų sąlygotas teisės aktų ar teismo, kitos institucijos privalomo sprendimo. Darbuotojų duomenys yra saugomi sutinkamai su teisės aktų nustatytais reikalavimais (Lietuvos vyriausiojo archyvaro patvirtinta bendrųjų dokumentų saugojimo terminų rodyklė).

17. Klinikai tvarkant duomenis Taisyklių 15.2 p. tikslu, iš pacientų yra renkami ir tvarkomi pacientų Asmens duomenys: vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, telefonas, elektroninio pašto adresas, šeimyninė padėtis, lytis, adresas, elektroninio pašto adresas, mobilaus telefono numeris, telefono numeris, valstybinio socialinio draudimo numeris ir asmens vidinis informacinės sistemos identifikatorius, gydytojų konsultacinės komisijos (toliau – GKK) išvados; naujai suformuoti ir jau anksčiau išduoti, bet galiojantys (neuždaryti) nedarbingumo bei nėštumo ir gimdymo atostogų pažymėjimai; nedarbingumo priežastis, gydymo tipas, diagnozės kodas, nedarbingumo laikotarpis (pradžia ir pabaiga), gimdymo data, profesinė liga (pradžios data, ligos patvirtinimo akto numeris), nelaimingas atsitikimas (data, aprašymas), gydymas stacionare (pradžios data, pabaigos data), reabilitacija (pradžios data, pabaigos data); GKK išvada (data, išvada, GKK pirmininkas (vardas, pavardė, gydytojo spaudo numeris)), neįgalumo ir darbingumo nustatymo tarnybos (toliau – NDNT) sprendimas; paciento šeimos nariai/atstovai (sutuoktinis, tėvas/įtėvis, motina/įmotė, vaikas/įvaikis, globėjas, rūpintojas), kai veikiama įgaliojimo pagrindu – asmens tapatybę patvirtinančio dokumento rūšis, serija, numeris bei pateikto įgaliojimo dokumento numeris, išdavimo data, galiojimo pradžia bei pabaiga; šeimos nario/atstovo vardas, pavardė, asmens kodas (jeigu tokio nėra – gimimo data), darbovietė (juridinio asmens kodas, pavadinimas, darbo laikotarpis (pradžia ir pabaiga), išduoti nedarbingumo pažymėjimai (galiojantys ir neuždaryti), išduoti nėštumo ir gimdymo atostogų pažymėjimai (galiojantys ir neuždaryti); suteiktos paslaugos, intervencijos, diagnozė (ligos kodas), ligos tipas (ūminė, nauja lėtinė, sena lėtinė); paslaugos kodas ir pavadinimas, traumos priežastis, paslaugos tipas, atlikęs specialistas (spaudo serija ir numeris, vardas, pavardė), gydymo rezultatas (baigtas, tęsiamas, siuntimas ir pan.). Taip pat visi kiti duomenys, kurie turi būti nurodomi Ambulatorinėje asmens sveikatos istorijoje, atsižvelgiant į teisės aktų nustatyta tvarka patvirtintą formą.

17.1. Klinikai tvarkant duomenis šių Taisyklių 15.2. p. tikslu, šie duomenys gaunami iš pacientų, Sveikatos apsaugos ministerijos, Valstybinės ligonių kasos, Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos („Sodros“), Neįgalumo ir nedarbingumo nustatymo tarnybos, draudimo bendrovių ir kitų asmenų. Klinika duomenis apie pacientus gali teikti pagal sudarytas sutartis ar vienkartinius prašymus. Duomenys taip pat gali būti teikiami valstybės, savivaldybės institucijoms, kurioms tokie duomenys yra būtini jų funkcijoms vykdyti. Pacientų duomenis Klinika saugo sutinkamai su teisės aktų reikalavimais (Sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymu Nr. 515 patvirtinta Sveikatos priežiūros įstaigų veiklos apskaitos ir atskaitomybės tvarka).

18. Klinikos asmens duomenų apsaugos pareigūnas (toliau – Pareigūnas) privalo tvarkyti bei saugoti su Asmens duomenų apsauga susijusios veiklos duomenis (toliau – Veiklos įrašus), kurie nurodytų bent šią minimalią ir aktualią informaciją:

18.1. Klinikos rekvizitus ir Pareigūno rekvizitus;

18.2. Duomenų subjektų kategorijas ir jų trumpus aprašymus;

18.3. Duomenų gavėjų kontaktus;

18.4. Duomenų tvarkytojų kontaktus;

18.5. Asmens duomenų saugojimo, ištrynimo terminus ir/arba kriterijus, pagal kuriuos Asmens duomenys yra saugomi Klinikoje;

18.6. Techninių, organizacinių saugumo priemonių aprašymą.

19. Už šių Taisyklių 18 punkte nurodytų Veiklos įrašų pateikimą Valstybinei duomenų apsaugos inspekcijai (esant jos prašymui/reikalavimui) atsako Pareigūnas.

V SKYRIUS

DUOMENŲ SUBJEKTŲ TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

Duomenų subjektų teisės ir informuotumo užtikrinimas

20. Duomenų subjektai turi teisę:

20.1. Žinoti (būti informuoti) apie savo Asmens duomenų tvarkymą;

20.2. Pateikę Klinikai asmens tapatybės dokumentą arba elektroninio ryšio priemonėmis, kurios leidžia tinkamai identifikuoti asmenį, susipažinti su savo Asmens duomenimis ir jų tvarkymu, gauti informaciją, iš kokių šaltinių ir kokie jo Asmens duomenys surinkti, kokiu tikslu jie tvarkomi, kokiems duomenų gavėjams teikiami ir buvo teikti bent per paskutinius 3 metus, taip pat gauti dokumentų, kuriame yra jų Asmens duomenys, kopiją (medicinos dokumentų pateikimas pacientui gali būti ribojamas įstatymo nustatyta tvarka, jeigu juose esanti informacija pakenktų paciento sveikatai ar sukeltų pavojų jo gyvybei);

20.3. Reikalauti ištaisyti, ištrinti savo Asmens duomenis arba apriboti Duomenų tvarkymą, išskyrus saugojimą, kai duomenys tvarkomi nesilaikant teisės aktų reikalavimų;

20.4. Nesutikti, kad būtų tvarkomi jo Asmens duomenys;

20.5. Reikalauti perkelti duomenis kitam duomenų valdytojui arba pateikti tiesiogiai Duomenų subjektui patogia forma (tuos duomenis, kuriuos Klinikai pateikė pats Duomenų subjektas);

20.6. Pateikti skundą priežiūros institucijai;

20.7. Atšaukti duotą sutikimą (jei Asmens duomenys tvarkomi sutikimo pagrindu).

21. Visais atvejais, Klinika privalo suteikti Duomenų subjektui informaciją (išskyrus atvejus, kai Duomenų subjektas tokią informaciją jau turi) apie:

21.1. savo pavadinimą, juridinio asmens kodą ir buveinę;

21.2. pareigūno kontaktinius duomenis, jei toks yra;

21.3. kokiais tikslais ir teisiniu pagrindu tvarkomi Duomenų subjekto Asmens duomenys;

21.4. duomenų gavėjus, jų kategorijas;

21.5. duomenų saugojimo laikotarpį arba kriterijus, taikomus tam laikotarpiui nusakyti;

21.6. kitą papildomą informaciją (duomenų gavimo šaltinus, kokius savo Asmens duomenis Duomenų subjektas privalo pateikti ir kokios yra duomenų 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 Asmens duomenų tvarkymas nepažeidžiant Duomenų subjekto teisių.

22. Klinika užtikrina, kad Duomenų subjektams įgyvendinant savo teisę į duomenų perkeliamumą, perkeliami tik tie duomenys, kurie tvarkomi sutarties arba sutikimo pagrindu ir yra tvarkomi automatizuotomis priemonėmis. Tokiu atveju Asmens duomenys Duomenų subjektui būtų pateikiami susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu.

Duomenų subjekto teisių įgyvendinimo tvarka

23. Klinika, privalo:

23.1. Sudaryti sąlygas Duomenų subjektui įgyvendinti šių Taisyklių V skyriuje nurodytas Duomenų subjekto teises, išskyrus įstatymų nustatytus atvejus, kai reikia užtikrinti valstybės saugumą ar gynybą, viešąją tvarką, nusikalstamų veikų prevenciją, tyrimą, nustatymą ar baudžiamąjį persekiojimą, svarbius valstybės ekonominius ar finansinius interesus, tarnybinės ar profesinės etikos pažeidimų prevenciją, tyrimą ir nustatymą, Duomenų subjekto ar kitų asmenų teisių ir laisvių apsaugą;

23.2. Duomenų subjektai dėl šių Taisyklių V skyriuje nurodytų teisių įgyvendinimo, privalo kreiptis į Klinikos direktorių;

23.3. Klinika privalo užtikrinti, kad visa reikalinga informacija Duomenų subjektui būtų pateikiama aiškiai ir suprantamai;

23.4. Duomenų subjektui atsakymas privalo būti pateiktas ne vėliau kaip per 20 (dvidešimt) darbo dienų nuo prašymo gavimo dienos. Jei duomenis teikti Duomenų subjektui atsisakoma, jam turi būti pateiktas motyvuotas ir pagrįstas atsakymas dėl jo prašymo nevykdymo.

24. Klinika privalo ne vėliau kaip per 5 dienas 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.

25. Klinika duomenis Duomenų subjektui teikia neatlygintinai.

26. Tam tikrais atvejais (kai Duomenų subjektas akivaizdžiai piktnaudžiauja savo teisėmis, nepagrįstai pakartotinai teikia prašymus pateikti informaciją, išrašus, dokumentus), toks informacijos ir duomenų teikimas Duomenų subjektui gali būti apmokestintas sutinkamai su Klinikos nustatytais įkainiais.

Duomenų teikimas duomenų gavėjams

27. Klinika Duomenų subjektų duomenis duomenų gavėjams teikia tik nepažeidžiant teisės aktuose įtvirtintų reikalavimų ir Asmens duomenų konfidencialumo užtikrinimo pagal sudarytą sutartį arba vienkartinį duomenų gavėjo prašymą.

28. Vienkartinio duomenų teikimo atveju, Klinika, teikdama Asmens duomenis pagal duomenų gavėjo prašymą, prioritetą teikia duomenų teikimui elektroninių ryšių priemonėmis.

29. Asmens duomenų teikimas valstybės ir savivaldybės institucijoms ir įstaigoms, kai šios institucijos ir įstaigos pagal konkretų paklausimą gauna Asmens duomenis įstatymų nustatytoms kontrolės funkcijoms atlikti, nelaikytinas duomenų teikimu duomenų gavėjams.

VI SKYRIUS

ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS

30. Klinika tvarko ypatingus pacientų duomenis, be ko būtų neįmanomas tinkamas Klinikos funkcionavimas ir sveikatos priežiūros paslaugų teikimas.

31. Klinikos direktoriaus įsakymu, Pareigūnu gali būti paskirtas vienas iš esamų Klinikos darbuotojų, naujas darbuotojas arba asmuo, su kuriuo būtų sudaroma paslaugų teikimo sutartis.

32. Skirdamas Pareigūną, Klinikos direktorius privalo įvertinti ir įgyvendinti tai, kad:

32.1. Pareigūnas turėtų tinkamų Asmens duomenų teisinės apsaugos praktinių ir ekspertinių žinių;

32.2. Pareigūnas būtų įtraukiamas į visų su Asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Klinikoje;

32.3. Pareigūnas būtų tiesiogiai pavaldus Klinikos direktoriui;

33. Pareigūnas privalo:

33.1. Užtikrinti, kad Klinikoje vykdomas Asmens duomenų tvarkymas atitiktų BDAR, kitų, asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimus, tinkamai įvertinant duomenų tvarkymo operacijas, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, potencialų pavojų;

33.2. Stebėti, kaip laikomasi BDAR, kitų, Asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimų, šių Taisyklių, kitų vidinių dokumentų, susijusių su Asmens duomenų apsauga;

33.3. Konsultuoti ir stebėti, kaip atliekamas poveikio duomenų apsaugai vertinimas, aptariamas šių Taisyklių VII skyriuje.

33.4. Informuoti Klinikos direktorių ir kitus darbuotojus apie jų pareigas pagal BDAR ir kitus, asmens duomenų teisinę apsaugą reglamentuojančius, teisės aktus ir juos konsultuoti dėl konkrečių pareigų vykdymo;

33.5. Informuoti Klinikos direktorių apie bet kokius neatitikimus, pažeidimus asmens duomenų apsaugos srityje, kuriuos Pareigūnas nustato, vykdydamas savo funkcijas;

33.6. Mokyti Klinikos darbuotojus, dirbančius su Asmens duomenimis, asmens duomenų teisinės apsaugos klausimais;

33.7. Bendradarbiauti, būti kontaktiniu asmeniu santykiuose su Valstybine duomenų apsaugos inspekcija.

34. Klinikos direktorius paskyręs arba sudaręs su Pareigūnu paslaugų teikimo sutartį, privalo užtikrinti, kad Pareigūno kontaktiniai duomenys per protingą terminą nuo jo paskyrimo / paslaugų sutarties sudarymo būtų tinkamai paskelbti Duomenų subjektams bei pranešti Valstybinei duomenų apsaugos inspekcijai.

VII SKYRIUS

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

35. Klinikai pradėjus vykdyti naują (-as) duomenų tvarkymo operaciją (-as), ji privalo atlikti poveikio duomenų apsaugai vertinimą, jei Duomenų tvarkymas:

35.1. Keltų didelį pavojų Duomenų subjektų teisėms ir laisvėms (pavyzdžiui, atvejai, kai Duomenų subjektas neturi galimybės nesutikti su Duomenų tvarkymu, duomenys perduodami už ES ribų, būtų pradėti tvarkyti duomenys, kurie gauti juos sujungus su duomenimis iš kitų šaltinių, būtų tvarkomi jautrūs duomenys tokie kaip sveikata, būtų pradėti naudoti nauji technologiniai sprendimai, pavyzdžiui, veido atpažinimo sistemos, kt.);

35.2. Automatizuotai būtų tvarkomi asmeniniai aspektai, vykdomas profiliavimas ir priimami teisiniai ar kiti didelio poveikio (pavyzdžiui, asmenų suskirstymas į grupes, kuris gali turėti jiems įtakos) sprendimai;

35.3. Būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;

35.4. Būtų pradėti tvarkyti ypatingi Asmens duomenys dideliu mastu.

36. Jei Klinika, atlikdama poveikio duomenų apsaugai vertinimą nustatytų, kad Duomenų subjektų teisėms ir laisvėms gali kilti didelis pavojus (žr. Taisyklių 37.1 p.), ji privalo konsultuotis su Valstybine duomenų apsaugos inspekcija dėl tinkamų saugumo ir kitų priemonių įgyvendinimo.

37. Atliekant poveikio duomenų apsaugai vertinimą, Klinika privalo nustatyti:

37.1. Kokia bus atliekama duomenų tvarkymo operacija (-os);

37.2. Kiek konkreti duomenų tvarkymo operacija yra reikalinga ir proporcinga;

37.3. Koks gali būti poveikis Duomenų subjektams;

37.4. Kokios yra galimos potencialių pavojų šalinimo, saugumo užtikrinimo priemonės.

38. Klinika privalo užtikrinti, kad šiame skyriuje aprašytas ir Klinikos numatytais atvejais atliekamas poveikio duomenų apsaugai vertinimas, būtų tinkamai dokumentuotas ir saugomas.

39. Poveikio duomenų apsaugai vertinimas gali būti atliekamas ir esamoms duomenų tvarkymo operacijoms (t. y. vykdomoms iki BDAR įsigaliojimo), jei tose operacijose atsirastų reikšmingų pokyčių, pavyzdžiui, būtų pradėtos naudoti naujos technologijos, duomenys būtų pradėti tvarkyti kitu tikslu nei iki tol, atsirastų naujos rizikos, susijusios su įvykdytomis kibernetinėmis, atakomis, įsilaužimais į Klinikos sistemą, duomenys būtų pradėti teikti naujiems duomenų gavėjams, tvarkytojams už ES ribų, kt.

40. Poveikio duomenų apsaugai vertinimas taip pat gali būti atliekamas ir šiame skyriuje neaptartais atvejais, bet esant Klinikos direktoriaus, Pareigūno ar Valstybinės duomenų apsaugos inspekcijos rekomendacijai tai atlikti.

VIII SKYRIUS

ASMENS DUOMENŲ INCIDENTAI

41. Asmens duomenų incidentu yra laikomas toks pažeidimas, dėl kurio netyčia arba neteisėtais veiksmais būtų:

41.1. sunaikinami, prarandami, pakeičiami Asmens duomenys;

41.2. be leidimo atskleidžiami Asmens duomenys;

41.3. be leidimo asmenys, neturintys tam teisės, gautų prieigą prie Asmens duomenų.

42. Jei dėl įvykdyto asmens duomenų incidento kyla pavojus Duomenų subjektų teisėms ir laisvėms, Pareigūnas ar kitas direktoriaus paskirtas darbuotojas privalo nedelsiant, bet ne vėliau nei kaip per 72 val. pranešti Valstybinei duomenų apsaugos inspekcijai apie įvykusį incidentą. Kilus ypatingai dideliam pavojui Duomenų subjektų teisėms ir laisvėms, informacija apie įvykusį incidentą nedelsiant taip pat turi būti pateikta Duomenų subjektams.

43. Šių Taisyklių 42 p. numatytame pranešime dėl įvykusio Asmens duomenų incidento Valstybinei duomenų apsaugos inspekcijai, Duomenų subjektams privalo būti trumpai aprašytas asmens duomenų incidento pobūdis, nurodant apytikslį Duomenų subjektų skaičių, kurių asmens teisės ir laisvės galėjo būti pažeistos, Pareigūno ar kito atsakingo darbuotojo kontaktai, trumpai aprašytos tikėtinos incidento pasekmės bei priemonės, kurių Klinika imasi/imsis, kad būtų pašalintos neigiamos pasekmės, susijusios su įvykusiu incidentu.

44. Nustatant, ar būtina vykdyti informavimo pareigą, aptartą šių Taisyklių 43 p., Pareigūnas ar kitas Klinikos direktoriaus paskirtas atsakingas darbuotojas privalo įvertinti, ar dėl įvykusio incidento:

44.1. Įvyko konfidencialumo pažeidimas (pavyzdžiui, atskleisti duomenys ir jie tapo prieinami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant, kt.);

44.2. Įvyko duomenų pasiekiamumo pažeidimas (pavyzdžiui, prarasti duomenys ir neturima atsarginių kopijų);

44.3. Įvyko duomenų vientisumo pažeidimas (pavyzdžiui, prarastos pacientų ligos istorijos, turima tik dalis atsarginių kopijų, dėl ko neįmanoma „atkurti“ visos paciento ligos istorijos).

45. Jei Pareigūnas ar kitas Klinikos direktoriaus paskirtas atsakingas darbuotojas nustato, kad yra bent vienas iš šių Taisyklių 44.1. p., 44.2. p., 44.3. p. numatytų pažeidimų, nedelsiant vykdo informavimo pareigą, kaip tai aptarta Taisyklių 42 p. Informavimas gali vykti ir esant kitiems pagrindams, jei tokius nustato Klinika ir/ar Pareigūnas.

46. Pareigūnas ar kitas Klinikos direktoriaus paskirtas atsakingas darbuotojas privalo užtikrinti, kad visi asmens duomenų apsaugos incidentai, įskaitant ir tuos, dėl kurių nevykdoma informavimo pareiga kaip aptarta šiame Taisyklių skyriuje, būtų tinkamai dokumentuoti ir saugomi.

47. Įvykus asmens duomenų incidentui, aptartam šiame Taisyklių skyriuje, Pareigūnas ar kitas direktoriaus paskirtas atsakingas darbuotojas, informuoja Klinikos darbuotojus ir duoda atitinkamas instrukcijas konkretiems darbuotojams dėl jų pareigų, funkcijų atlikimo, susijusio su asmens duomenų incidento valdymu.

48. Įvykus asmens duomenų incidentui, aptartam šiame Taisyklių skyriuje, Pareigūnas, be kitų šiame skyriuje aptartų pareigų, taip pat sudaro veiksmų planą su prevenciniais veiksmais, kuriais būtų siekiama ateityje užkirsti kelią pasikartoti analogiškam ar panašiam incidentui ir pateikia jį Klinikos direktoriui.

IX SKYRIUS

ORGANIZACINĖS IR TECHNINĖS ASMENS DUOMENŲ APSAUGOS PRIEMONĖS

49. Klinikos organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti trečiąjį automatiniu būdu tvarkomų Asmens duomenų saugumo lygį. Siekiant apsaugoti Asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo turi būti taikomos tokios infrastruktūrinės, administracinės ir telekomunikacinės (elektroninės) priemonės:

49.1. Tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių sistemų priežiūra, tinklo valdymas, naudojimosi internetu saugumo užtikrinimas ir kitos informacinių technologijų priemonės:

49.1.1. Griežtas priešgaisrinės apsaugos tarnybos nustatytų normų laikymasis;

49.1.2. Tinkamas darbo organizavimas ir kitos administracinės priemonės;

49.1.3. Informacinių sistemų duomenų tvarkymo keliamos rizikos vertinimas, kuris būtų atliekamas kartą per 1 (vienerius) metus;

49.1.4. Įgyvendintų organizacinių ir techninių duomenų saugumo priemonių įvertinimo auditas, kuris būtų atliekamas kartą per 2 (dvejus) metus;

49.1.5. Diegiamos reikiamos duomenų saugumo priemonės, atsižvelgiant į rizikos vertinimo rezultatus;

49.1.6. Atliekami praktiniai bandymai dėl avarinio Asmens duomenų atkūrimo;

49.1.7. Duomenų atsarginių kopijų darymas ir atkūrimas, kuris būtų atliekamas ne rečiau kaip vieną kartą per mėnesį;

49.1.8. Atsarginių duomenų kopijų laikmenos, kurios būtų saugomos atsarginių kopijų saugykloje arba rakinamoje nedegančioje spintoje;

49.1.9. Užtikrinamas duomenų atkūrimas iš paskutinių turimų atsarginių duomenų kopijų, praradus duomenis dėl aparatinės kompiuterių įrangos gedimo, programinės įrangos klaidos ar kitaip pažeidus duomenų vientisumą;

49.1.10. Informacinės sistemos funkcionalumo ir duomenų vientisumo bei parengtumo testavimų atlikimas;

49.1.11. Bandomasis duomenų atkūrimas, kuris būtų vykdomas bent kartą per metus.

50. Už šiame skyriuje numatytų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimą, kontrolę, užtikrinimą yra atsakingas Klinikos direktoriaus paskirtas atsakingas Darbuotojas.

51. Darbuotojai, kurie tvarko pacientų, kitų fizinių asmenų duomenis, turi laikytis konfidencialumo principo ir laikyti paslaptyje bet kokią su pacientais, kitais interesantais susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas. Ši pareiga išlieka galioti perėjus dirbti į kitas pareigas Klinikoje arba pasibaigus darbo ar sutartiniams santykiams su Ligonine.

52. Darbuotojai automatiniu būdu tvarkyti Asmens duomenis gali tik po to, kai jiems suteikiama prieigos teisė prie atitinkamos informacinės sistemos. Prieiga prie Asmens duomenų gali būti suteikta tik tam asmeniui, kuriam Asmens duomenys yra reikalingi jo funkcijoms vykdyti. Darbo santykiams pasibaigus, Darbuotojui prieigos prie registrų ir kitų programų teisės panaikinamos.

53. Darbuotojai gali perduoti dokumentus, kuriuose nurodyti Asmens duomenys, tik tiems Darbuotojams, kurie pagal pareigas ar atskirus pavedimus turi teisę dirbti su asmens duomenimis.

54. Darbuotojai, vykdantys Duomenų subjekto duomenų tvarkymo funkcijas, turi užkirsti kelią atsitiktiniam ar neteisėtam tvarkymui, turi saugoti dokumentus tinkamai ir saugiai (vengiant nereikalingų kopijų su Duomenų subjekto duomenimis kaupimo ir kt.). Dokumentų kopijos, kuriose nurodomi Duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio.

55. Darbuotojai, kurių kompiuteriuose saugomi pacientų, kitų interesantų duomenys arba iš kurių kompiuterių galima patekti į Klinikos informacines sistemas, kuriose yra saugomi pacientų, kitų interesantų duomenys, savo kompiuteriuose turi naudoti slaptažodžius; „svečio“ („guest“) tipo, t. y. neapsaugoti slaptažodžiais, vartotojai yra draudžiami. Šiuose kompiuteriuose taip pat reikia naudoti ekrano užsklandą su slaptažodžiu. Reikalavimai slaptažodžiams:

55.1. Juos turi sudaryti ne mažiau kaip 8 simboliai, iš kurių bent vienas turi būti skaičius ir raidė;

55.2. Jie negali sutapti su Darbuotojų ar jų šeimos narių asmeniniais duomenimis;

55.3. Juos saugo ir juos gali žinoti tik Darbuotojai, dirbantys su konkrečiais kompiuteriais;

55.4. Jie negali būti saugomi viešai ir negali būti prieinami kaip visuma.

56. Slaptažodžiai esant būtinybei (pasikeitus Darbuotojui, iškilus įsilaužimo grėsmei ir pan.) turi būti keičiami.

57. Darbuotojų kompiuteriai, kuriuose saugomos rinkmenos su pacientų, kitų fizinių asmenų duomenimis, negali būti laisvai prieinami iš kitų tinklo kompiuterių. Šių kompiuterių antivirusinė programinė įranga turi būti nuolat atnaujinama.

58. Nesant būtinybės, rinkmenos su pacientų, kitų interesantų duomenimis neturi būti dauginamos skaitmeniniu būdu, t. y. kuriamos rinkmenų kopijos vietiniuose kompiuterių diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir kt.

59. Klinikoje yra užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, kai Asmens duomenys perduodami išoriniais duomenų perdavimo tinklais.

60. Asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolė ir ištrynimas po jų panaudojimo užtikrinamas perkeliant juos į duomenų bazes.

61. Klinikos informacinėse sistemose ir kompiuterių tinkluose įgyvendinamos šios saugumo priemonės:

61.1. Fiksuojami prisijungimų prie Asmens duomenų įrašai: 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 metus;

61.2. Ne rečiau kaip kartą per 1 mėnesį peržiūrimas naudotojų prisijungimų prie duomenų bazės (-ių) įrašų elektroninis žurnalas ir duomenų valdytojui teikiamos peržiūros ataskaitos;

61.3. Mobiliuosiuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne Klinikos vidiniame kompiuterių tinkle, esantys ypatingi Asmens duomenys ir prisijungimo prie Klinikos tvarkomų Asmens duomenų informacija šifruojama ar apsaugoma tokiomis priemonėmis, kurios atitiktų Asmens duomenų atskleidimo keliamą riziką;

61.4. Atsarginės Asmens duomenų kopijos, jei jos daromos, saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;

61.5. Šifruojami atsarginėse kopijose, archyvuose ir išorinėse duomenų laikmenose saugomi Asmens duomenys;

61.6. Šifruojami elektroniniu paštu perduodami Asmens duomenys;

61.7. Asmens duomenų paieškos užklausoje nurodomas Asmens duomenų naudojimo tikslas (-ai);

61.8. Klinikos generalinio direktoriaus paskirtas atsakingas Darbuotojas privalo užtikrinti:

61.8.1. Pašalinių asmenų įėjimo į serverių patalpas kontrolę, naudojant koduotą durų rakinimo sistemą bei bendrą apsaugos signalizacijos sistemą;

61.8.2. Vidinio Klinikos kompiuterių tinklo apsaugą.

62. Darbuotojai privalo taip organizuoti savo darbą, kad kiek įmanoma apribotų galimybę kitiems asmenims (kitiems Klinikos darbuotojams, praktikantams, savanorišką praktiką atliekantiems ar kitiems tretiesiems asmenims) sužinoti tvarkomus Asmens duomenis. Ši nuostata įgyvendinama:

62.1. Nepaliekant dokumentų su tvarkomais Asmens duomenimis ar kompiuterio, kuriuo naudojantis galima atidaryti rinkmenas su Asmens duomenimis, be priežiūros taip, kad juose esančią informaciją galėtų perskaityti Darbuotojai, neturintys teisės dirbti su konkrečiais Asmens duomenimis, praktikantai ar kiti asmenys;

62.2. Dokumentus laikant taip, kad jų (ar jų fragmentų) negalėtų perskaityti atsitiktiniai asmenys;

62.3. Jei dokumentai, kuriuose yra Asmens duomenų, kitiems Darbuotojams, padaliniams, įstaigoms perduodami per asmenis, kurie neturi teisės tvarkyti Asmens duomenis, arba per paštą ar kurjerį, jie privalo būti perduodami užklijuotame nepermatomame voke. Šis punktas netaikomas, jeigu minėti pranešimai įteikiami pacientams, kitiems interesantams asmeniškai ir konfidencialiai.

63. Už Asmens duomenų saugumo pažeidimų valdymą ir reagavimą į šiuos pažeidimus atsako Klinikos Pareigūnas.

64. Šiame Taisyklių skyriuje aptartos organizacinės ir techninės Asmens duomenų apsaugos priemonės taikomas kartu su Klinikos nuostatų nustatytomis taisyklėmis ir joms neprieštarauja.

X SKYRIUS

ASMENS DUOMENŲ TVARKYTOJO PASITELKIMAS

65. Tais atvejais, kai Klinika įgalioja Duomenų tvarkytoją atlikti asmens duomenų tvarkymo veiksmus, tarp Klinikos ir Duomenų tvarkytojo turi būti sudaroma rašytinė asmens duomenų tvarkymo sutartis.

66. Sprendimą perduoti Duomenų subjekto Duomenų tvarkymą asmens duomenų tvarkytojui priima Klinikos direktorius.

67. Klinika parenka Duomenų tvarkytoją, kuris užtikrina, kad būtų įgyvendintos techninės ir organizacinės duomenų apsaugos priemonės ir užtikrintas tokių priemonių laikymasis, įskaitant ir šių Taisyklių IX skyriuje aptartas technines, organizacines duomenų saugumo užtikrinimo priemones.

68. Klinika, sutartimi įgaliodama Duomenų tvarkytoją tvarkyti Asmens duomenis, nurodo, kad Asmens duomenys būtų tvarkomi atsižvelgiant į Asmens duomenų tvarkymą reglamentuojančius teisės aktus, Klinikos nurodymus, taip pat nurodant, kokius Asmens duomenų tvarkymo veiksmus privalo atlikti Duomenų tvarkytojas Klinikos vardu, Duomenų tvarkytojo įsipareigojimai Klinikai, įskaitant įsipareigojimą laikytis BDAR įtvirtintų reikalavimų, duomenų tvarkymo trukmė, pobūdis, Asmens duomenų rūšis, duomenų subjektų kategorijos, Duomenų tvarkytojo pareiga ištrinti arba grąžinti Klinikai Asmens duomenis, jų kopijas, pabaigus Klinikai teikti paslaugas.

69. Klinika, sudarydama sutartį su Duomenų tvarkytoju, be kita ko, nurodo, kad Duomenų tvarkytojas privalo užtikrinti Klinikos perduodamų tvarkyti duomenų konfidencialumą, o ketindamas tvarkymui pasitelkti trečiuosius asmenis (kitus Duomenų tvarkytojus), Duomenų tvarkytojas privalo gauti išankstinį rašytinį Klinikos pritarimą.

70. Klinikos Pareigūnas privalo saugoti, peržiūrėti, esant poreikiui inicijuoti sutarčių ir bendradarbiavimo su Duomenų tvarkytojais atnaujinimą / pakeitimą/nutraukimą.

71. Šios Taisyklės gali būti pridedamos kaip priedas prie sutarties su Duomenų tvarkytoju.

XI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

72. Su šiomis Taisyklėmis privalo susipažinti visi Klinikos Darbuotojai pasirašytinai.

73. Taisyklės, jų pakeitimai ar papildymai skelbiami Klinikos interneto tinklalapyje.

74. Klinika užtikrina darbuotojų, kuriems suteikta teisė tvarkyti Asmens duomenis, mokymus. Už atitinkamų Asmens duomenų teisinės apsaugos mokymų organizavimą, vykdymą darbuotojams, dirbantiems su asmens duomenimis, yra atsakingas Klinikos Pareigūnas.

75. Darbuotojai, pasikeitus jų Asmens duomenims, raštu informuoja apie tai Klinikos direktorių arba Pareigūną, o šis ne vėliau kaip per 3 darbo dienas patikslina ir atnaujina duomenis Darbuotojų Asmens duomenis bylose bei tam skirtose duomenų bazėse.

76. Už Taisyklių nuostatų laikymosi priežiūrą ir jose reglamentuotų nuostatų vykdymo kontrolę bei periodiškumą, ne rečiau kaip kartą per 2 metus, Taisyklių peržiūrėjimo, atnaujinimo pagal poreikį iniciavimą ir šių veiksmų atlikimo kontrolę yra atsakingas Klinikos Pareigūnas.

_____