DIAGNOSTIKOS IR GYDYMO ĮSTAIGŲ ASOCIACIJA

ASOCIACIJOS DIGA
ASMENS DUOMENŲ TVARKYMO DIAGNOSTIKOS IR GYDYMO ĮSTAIGOSE ELGESIO KODEKSAS

2019

ASMENS DUOMENŲ TVARKYMO ČIOSE DIAGNOSTIKOS IR GYDYMO ĮSTAIGOSE ELGESIO KODEKSĄ PASIRAŠIUSIOS ĮSTAIGOS IR PRISIJUNGIMAS PRIE ŠIO KODEKSO

Diagnostikos ir gydymo įstaigų asociacija DIGA, atstovaudama jos narių bendriems veiklos interesams, siekdama gerinti sveikatos priežiūros paslaugų sektoriaus veiklos aplinką ir tinkamai taikyti Europos Parlamento ir Tarybos reglamento (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***) 40 straipsnyje nustatytus reikalavimus bei taikydama savireguliacijos mechanizmą, susitarė dėl Asmens duomenų tvarkymo Diagnostikos ir gydymo įstaigose elgesio kodekso (toliau – DIGA kodeksas) išleidimo.

Šiam kodeksui pritarė ir tai patvirtino parašais įstaigos, DIGA narės, kurių sąrašas pateikiamas 1 priede.

DIGA kodeksas yra priimtas siekiant užtikrinti vienodo lygio šių įstaigų pacientų, lankytojų ir personalo apsaugą tvarkant asmens duomenis sveikatos priežiūros sektoriuje visoje Lietuvoje.

DIGA kodeksas, užtikrinantis atitikimą Reglamento 2016/679 nuostatoms, yra priemonė, kuri turi nustatyti privalomas elgesio taisykles, kurių privalo laikytis pasirašiusių šį kodeksą sveikatos priežiūros įstaigų (jie ir duomenų valdytojai) gydytojai, slaugytojos, vadovybė ir kiti sveikatos priežiūros įstaigų darbuotojai, savanoriai, atliekantys praktiką medicinos studentai, partneriai (asmenys sudarę sutartis su šiomis įstaigomis dėl paslaugų ir (arba) medicinos įrenginių, įrankių, medikamentų ar kitų prekių tiekimo ir pan.), ar kitais pagrindais sveikatos priežiūros įstaigos pavedimu ar jos įgalioti atliekantys funkcijas subjektai tam, kad visose Asociacijos DIGA narėse būtų užtikrintos vienodo lygio teisiškai įgyvendinamos duomenų subjekto teisės, o diagnostikos ir gydymo įstaigoms būtų nustatytos vienodo lygio prievolės bei atsakomybė, būtų užtikrintas teisinis tikrumas ir skaidrumas.

Asociacijos DIGA yra atvira visoms diagnostikos ir gydymo bei kitoms sveikatos priežiūros įstaigoms, šių įstaigų partneriams ir profesinėms medicinos įstaigų ir pacientų organizacijoms siekiančioms prisijungti prie šio kodekso.

Dėl prisijungimo prie šio kodekso kreiptis į Asociacijos DIGA

_____

(Asociacijos DIGA kontaktinio asmens vardas, pavardė, telefono Nr., el. paštas)

TURINYS

I. BENDROSIOS NUOSTATOS

1. Asmens duomenų tvarkymo diagnostikos ir gydymo įstaigose elgesio kodeksas nustato Diagnostikos ir gydymo įstaigų asociacijos DIGA narių vykdomų asmens duomenų tvarkymo ir apsaugos principus ir reikalavimus, asmens duomenų tvarkymo tikslus, duomenų subjektų teises ir jų įgyvendinimo tvarką, duomenų apsaugos priemones.

2. Šis DIGA kodeksas taikomas ir yra privalomas asmens duomenų valdytojams ir tvarkytojams – 1 priede išvardytoms diagnostikos ir gydymo įstaigų asociacijos DIGA narėms, taip pat prie šio kodekso prisijungusioms įstaigoms (toliau – DIGA įstaigos) ir visiems šiose įstaigose dirbantiems asmenims, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužinojo.

3. DIGA kodeksas taikomos tvarkant fizinių asmenų duomenis automatiniu būdu, taip pat ir neautomatiniu būdu tvarkant susistemintas rinkmenas: pacientų ligos istorijas, pacientų korteles, sąrašus, kartotekas, bylas, sąvadus ir kita.

4. DIGA įstaigos, jie ir duomenų valdytojai ir (arba) tvarkytojai, tvarko savo pacientų ir lankytojų, visų šių įstaigų esamų ir buvusių darbuotojų – administracijos, gydytojų, medicinos personalo ir kitų darbuotojų, taip pat medicinos studentų bei rezidentų, ir kitų asmenų, jie ir duomenų subjektai, įstatymų nustatyta tvarka sutartinių ir kitų teisinių santykių pagrindu pateikusių informaciją apie save, asmens duomenis, o taip pat šiuos duomenis, gautus iš trečiųjų šalių.

5. Šis kodeksas taip pat nustato DIGA įstaigų darbuotojų teises, pareigas ir atsakomybę tvarkant asmens duomenis.

6. DIGA kodeksas parengtas vadovaujantis 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 94/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – ***Reglamentas 2016/679***), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ), Lietuvos Respublikos darbo kodeksu, Lietuvos Respublikos biomedicininių tyrimų etikos įstatymu (toliau – BTEĮ),, Lietuvos Respublikos pacientų teisių ir žalos atlyginimo įstatymu (toliau – PTĮ), kitais, 2 priede išvardytais, teisės aktais.

7. DIGA įstaigos siekia bendradarbiauti ir suderintais veiksmais tvarkyti asmens duomenis bei įgyvendinti priemones, kurios užtikrintų vienodą *Reglamento 2016/679* taikymą, tačiau turi teisę pasirinkti individualius, tik tai įstaigai būdingus sprendimus, jeigu šie sprendimai neprieštarauja šio Kodekso nuostatoms.

II. SĄVOKOS IR SANTRUMPOS

1. DIGA kodekse vartojamos sąvokos:

1.1. Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.

1.2. Atsakymas – žodžiu, raštu ar elektroniniu būdu pateiktas atsakymas teisės aktų nustatyta tvarka prašymą pateikusiems asmenims, pateikta informacinėse sistemose, popierinėse, elektroninių ryšių priemonėmis gautose laikmenose tvarkoma informacija, įteikta prašomų DIGA įstaigose tvarkomų asmens duomenų kopija, nuorašas ar išrašas, medicininių tyrimų, medicinos įrenginių ir įrangos automatiškai renkami sveikatos, sveikatos priežiūros, medicininių ir medicininių mokslinių tyrimų tikslais surinkti duomenys, išdėstyta DIGA nuomonė, pasiūlymai ir skundai ar pageidavimai arba kt. informacija.

1.3. Asmens sveikatos duomenys – duomenys apie asmens sveikatą, ligas ir sveikatos sutrikimus, jų priežastis, išorės veiksnius, diagnozę, eigą, prognozę, gydymą, išeitis, mirtį, paveldimumą ar bet kuri kita su asmens sveikata susijusi informacija.

1.4. Duomenų tvarkymo principai – DIGA kodekse ir (arba) ***Reglamente 2016/679,*** ir (arba) ADTAĮ bei kituose teisės aktuose įtvirtinti, su elgesio ir patirties aspektais suderinti principai.

1.5. Duomenų apsaugos pareigūnas – Asociacijos DIGA ar DIGA įstaigos vadovo paskirtas darbuotojas arba pasitelktas išorės paslaugų teikėjas, valdomų ir (ar) tvarkomų Asociacijos DIGA ar DIGA įstaigos atstovas, atliekantis ***Reglamente 2016/679*** ir ADTAĮ bei kituose teisės aktuose nustatytas, duomenų apsaugos pareigūno funkcijas.

1.6. Duomenų gavėjas – juridinis ar fizinis asmuo, kuriam teikiami asmens duomenys.

1.7. Duomenų subjektas – fizinis asmuo, kurio asmens duomenis tvarko duomenų valdytojas ir tvarkytojai.

1.8. Incidentas – tai įvykis ar veika elektroninėje erdvėje, galintys sukelti duomenų saugumo pažeidimą.

1.9. 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, arba incidentas, dėl kurio kyla grėsmė arba neigiamas poveikis automatizuotomis priemonėmis tvarkomų

asmens duomenų prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys paslaugų teikimą.

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

1.11. Duomenų tvarkymas – bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (ar) aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitas veiksmas arba veiksmų rinkinys.

1.12. Duomenų tvarkymas automatiniu būdu – duomenų tvarkymo veiksmai, visiškai ar iš dalies atliekami automatinėmis priemonėmis.

1.13. Duomenų tvarkymas neautomatiniu būdu – duomenų tvarkymo veiksmai, atliekami neautomatinėmis priemonėmis (informaciją tvarkant popierinėse laikmenose).

1.14. Duomenų tvarkymas statistikos tikslais – statistinių tyrimų vykdymas, jų rezultatų teikimas ir saugojimas.

1.15. Duomenų tvarkymas sveikatos priežiūros tikslais – sveikatos priežiūros ir diagnostikos įstaigose atliekamas fizinio asmens sveikatos ir su sveikata susijusių duomenų, duomenų apie sveikatos sutrikimus, diagnostinių tyrimų, duomenų apie šeimos gyvenimą, žalingus įpročius tvarkymas.

1.16. Duomenų subjekto sutikimas (toliau – Sutikimas) – savanoriškas rašytinis duomenų subjekto arba jo atstovo valios pareiškimas tvarkyti jo asmens duomenis jam žinomu tikslu.

1.17. Lankytojas – fizinis asmuo, išskyrus įstaigos darbuotojus, kuris lankosi DIGA įstaigoje su sveikatos priežiūros paslaugomis susijusiais tikslais (pvz., yra paciento atstovas, klausia informacijos apie teikiamas paslaugas, dalyvauja moksliniuose biomedicininiuose tyrimuose ir kt.).

1.18. Pacientas – fizinis asmuo, kuris naudojasi įstaigos teikiamomis sveikatos priežiūros paslaugomis.

1.19. Prašymas – su asmens duomenų apsaugos teisių ar teisėtų interesų pažeidimu nesusijęs asmens kreipimasis į Asociaciją DIGA ar DIGA įstaigą (įstaigas) prašant pagal šiame kodekse ir (arba) teisės aktuose nustatytą tvarką įgyvendinti duomenų subjekto teises ar suteikti informaciją apie Asociacijos DIGA ar DIGA įstaigos (įstaigų) tvarkomus jo asmens duomenis arba, išskirtinais atvejais, gauti jų kopiją.

1.20. Prašymo nagrinėjimas – Asociacijos DIGA ar DIGA įstaigos (įstaigų) veikla, apimanti asmens prašymo priėmimą, įregistravimą, esmės nustatymą, atsakymo parengimą ir siuntimą (įteikimą) asmeniui.

1.21. Profiliavimas – bet kokios formos automatinis asmens duomenų tvarkymas, kai asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti arba numatyti aspektus, susijusius su to fizinio asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu.

1.22. Pseudonimų suteikimas – asmens duomenų tvarkymas taip, kad šie duomenys nebegalėtų būti priskiriami konkrečiam fiziniam asmeniui, jis ir duomenų subjektas, nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jai taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti.

1.23. Skundas – Asociacijai DIGA ar DIGA įstaigai adresuotas rašytinis kreipimasis siekiant apginti pažeistas, ***Reglamente 2016/679*** ir ADTAĮ bei kituose teisės aktuose įtvirtintas, duomenų subjekto teises į asmens duomenų apsaugą ar teisėti interesai.

1.24. Susisteminta rinkmena – bet kuris sistemingai sutvarkytas pagal nustatytus kriterijus, leidžiančius lengviau surasti arba pateikti reikiamą informaciją, asmens duomenų rinkinys.

1.25. Trečiasis asmuo – fizinis ar juridinis asmuo, ar kita bet kurios teisinės formos organizacija, išskyrus duomenų subjektą, duomenų valdytoją, duomenų tvarkytoją ir asmenis, kurie yra tiesiogiai duomenų valdytojo ar duomenų tvarkytojo įgalioti tvarkyti asmens duomenis.

1.26. Vidaus administravimas – veikla, kuria užtikrinamas duomenų valdytojo ar tvarkytojo funkcionavimas (struktūros tvarkymas, personalo valdymas, turimų materialinių ir finansinių išteklių valdymas ir naudojimas, dokumentų valdymas).

1.27. Kitos vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos *Reglamente 2016/679,* ADTAĮ, BTEĮ, PTĮ ir kituose teisės aktuose.

2. DIGA kodekse vartojamos santrumpos:

2.1. ADTAĮ – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

2.2. BTEĮ – Lietuvos Respublikos biomedicininių tyrimų elgesio įstatymas;

2.3. DIGA kodeksas – Asmens duomenų tvarkymo diagnostikos ir gydymo įstaigose elgesio kodeksas

2.4. DK – Lietuvos Respublikos darbo kodeksas;

2.5. IS – informacinė sistema;

2.6. PTĮ – Lietuvos Respublikos pacientų teisių ir žalos atlyginimo įstatymas.

III. ASMENS DUOMENŲ TVARKYMO PRINCIPAI

3. ***Reglamente 2016/679*** apsaugos principai taikomi Asociacijos DIGA ir DIGA įstaigose tvarkomiems bet kokiems duomenims ar informacijai apie fizinį asmenį, kurių pagrindu tiesiogiai ar netiesiogiai nustatyta asmens tapatybė.

4. Anonimiškos informacijos, t. y. duomenų, kurie nėra susiję su konkrečiu fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali arba nebegali būti nustatyta, įskaitant statistinius ar mokslinių tyrimų duomenis, šio Kodekso nuostatos netaikomos.

5. DIGA kodeksas netaikomas mirusių asmenų duomenims. Pacientų duomenys yra saugojami 3 (trejus) metus po jų mirties arba pacientų duomenys, susijusieji su mirusių asmenų duomenimis teikiami tik kompetentingoms institucijoms įstatymų nustatyta tvarka.

6. DIGA įstaigose asmens duomenų tvarkymas vykdomas:

6.1. taikant skaidrumo principą, šiame Kodekse įtvirtintos taisyklės, kurių laikomasi tvarkant pacientų ir lankytojų, visų esamų ir buvusių darbuotojų – administracijos, gydytojų, medicinos personalo ir kitų darbuotojų, taip pat medicinos studentų bei rezidentų, ir kitų su jais susijusių asmenų duomenis. Pagal skaidrumo principą šis Kodeksas ir visa informacija bei pranešimai, susiję su asmens duomenų tvarkymo taisyklėmis, duomenų subjektų informavimu apie duomenų tvarkymo teisinį pagrindą, tvarkomų duomenų apimtį, duomenų valdytojo tapatybę ir duomenų tvarkymo tikslus bei duomenų subjekto teisių įgyvendinimu ir teise tuos duomenis gauti, informacija apie su asmens duomenų tvarkymu susijusius pavojus, taisykles, apsaugos priemones yra vieša, arba lengvai prieinama. Tvarkomų asmens duomenų elementai, jų šaltiniai, teikimo ir saugojimo tvarka išdėstyta pagal šių duomenų tvarkymo tikslus pateikiama DIGA kodekso 3 priede.

6.2. Taikant teisėtumo principą duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais, ir toliau tvarkomi su tais tikslais suderinamu būdu. DIGA įstaigose tvarkomi:

6.2.1. pacientų duomenys – sveikatos priežiūros paslaugų teikimo tikslais;

6.2.2. DIGA įstaigų darbuotojų – vidaus administravimo tikslais;

6.2.3. buvusių darbuotojų – saugojami ir teikiami Lietuvos Respublikos teisės aktuose nustatytais tikslais ir apimtimi;

6.2.4. sveikatos mokslų specialistus ruošiančių formaliojo švietimo mokyklų, pvz., Vilniaus universiteto ir Lietuvos sveikatos mokslų universiteto studentų bei rezidentų, ir kitų su

jais susijusių asmenų duomenys, kuriuos teikia vienos kitoms DIGA įstaigos ir šios įstaigos – mokymo ir mokslinio tyrimo tikslais;

6.2.5. visų šiame punkte išvardytų asmenų duomenys (vaizdo stebėjimo duomenys) – turto ir asmenų saugumo užtikrinimo tikslais.

6.3. Taikant tikslingumo, proporcingumo ir duomenų kiekio mažinimo principus DIGA įstaigos įsipareigoja nereikalauti iš pacientų, kitų lankytojų ar darbuotojų pateikti tų duomenų, kurie nėra reikalingi teisėtiems tikslams pasiekti, nekaupti ir netvarkyti perteklinių duomenų.

6.4. Taikant tikslumo principą, patikslinti pacientų, kitų lankytojų duomenis kaskart jiems apsilankius ir paprašius bei pateikus įrodymus, kad duomenys netikslūs, darbuotojų – esant poreikiui ar jiems paprašius. Jeigu reikia duomenys atnaujinami, netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba jų tvarkymas sustabdomas.

6.5. Taikant duomenų vientisumo principą DIGA įstaigos užtikrina atitinkamų techninių ir organizacinių priemonių naudojimą tam, kad būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba kitokio neteisėto tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo su asmens duomenimis ar asmens duomenų rinkiniais. Duomenų tvarkymas – tai operacija ar operacijų seka, pvz., šių duomenų rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę šiais duomenimis naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas. Minimalūs reikalavimai organizacinėms ir techninėms nurodyti DIGA kodekso 4 priede.

6.6. Kiekviena DIGA įstaiga ir (arba) kita prisijungusi prie šio kodekso įstaiga ar organizacija savarankiškai rūpinasi ir užtikrina, kad asmens duomenys būtų tvarkomi laikantis organizacinių ir techninių duomenų saugumo priemonių, nurodytų tvarkomų IS dokumentuose (nuostatuose, duomenų saugos nuostatuose, IS administravimo taisyklėse, ar kt.).

6.7. Taikant konfidencialumo principą visa informacija apie paciento buvimą DIGA įstaigoje sveikatos, 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 teikiama tik pagal įstatymus ir turintiems teisę šią informaciją gauti asmenims.

7. Kiekviena DIGA įstaiga ir (arba) prisijungusi prie šio kodekso įstaiga ar organizacija turi teisę taikyti pačios pasirinktas, atitikimą ***Reglamento 2016/679*** reikalavimams užtikrinančias, organizacines ir (arba) technines priemones.

IV. STANDARTINIAI ASMENS DUOMENŲ TVARKYMO REIKALAVIMAI

8. Kiekviena DIGA įstaiga ir (arba) prisijungusi prie šio Kodekso įstaiga ar organizacija savarankiškai rūpinasi, kad asmens duomenys šioje įstaigoje būtų tvarkomi:

8.1. automatiniu būdu arba susistemintuose rinkiniuose naudojant turimas asmens duomenų tvarkymo priemones bei laikantis teisės aktų reikalavimų ir šio kodekso nuostatų;

8.2. renkami teisės aktų nustatyta tvarka, juos gaunant tiesiogiai iš duomenų subjekto, oficialiai užklausiant reikalingą informaciją tvarkančių ir turinčių teisę ją teikti subjektų ar sutarčių pagrindu, o taip pat įstatymų nustatytais atvejais – gavus duomenų subjekto sutikimą.

8.3. Tiesiogiai renkant duomenis iš duomenų subjekto privaloma suteikti šią informaciją (išskyrus atvejus, kai duomenų subjektas tokią informaciją jau turi):

8.3.1. DIGA įstaigos, ji ir duomenų valdytojas, adresas, telefonas, elektroninio pašto adresas;

8.3.2. kokiais tikslais tvarkomi (ketinama tvarkyti) duomenų subjekto asmens duomenys;

8.3.3. kokios yra asmens duomenų nepateikimo pasekmės;

8.3.4. kam ir kokiais tikslais bus teikiami jo asmens duomenys;

8.3.5. apie duomenų subjekto teisę susipažinti su savo asmens duomenimis;

8.3.6. teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo asmens duomenis.

8.4. Kai asmens duomenys gaunami netiesiogiai iš duomenų subjekto arba ketinant asmens duomenis teikti tretiesiems asmenims, privaloma apie tai informuoti duomenų subjektą ne vėliau kaip iki to momento, kai duomenys teikiami pirmą kartą, išskyrus atvejus, kai duomenų subjektas tokią informaciją jau turi arba duomenų perdavimą nustato teisės aktai. Duomenų subjektui turi būti pateikta ši informacija:

8.4.1. DIGA įstaigos, ji ir duomenų valdytojas, ir duomenų gavėjo adresas, telefonas, elektroninio pašto adresas;

8.4.2. kokiais tikslais tvarkomi ar ketinami tvarkyti duomenų subjekto duomenys;

8.4.3. iš kokių šaltinių ir kokie duomenų subjekto duomenys yra surinkti ar ketinami rinkti;

8.4.4. kam ir kokiais tikslais duomenys teikiami;

8.4.5. apie duomenų subjekto teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo duomenis.

9. Asmens duomenų tvarkymo DIGA įstaigose sveikatos priežiūros tikslais teisiniai pagrindai yra šie:

9.1. vadovaujantis teisės aktų reikalavimais duomenis tvarkyti būtina sveikatos priežiūros paslaugų teikimo tikslais;

9.2. administruoti ir naudotis sveikatos priežiūros IS, remiantis taikytinais teisės aktais;

9.3. remiantis taikytinais teisės aktais ir standartų reikalavimais tvarkyti duomenis būtina, kad būtų apsaugoti gyvybiniai duomenų subjekto (paciento) interesai;

9.4. tvarkyti duomenis būtina, siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;

9.5. pacientas sutinka, kad būtų tvarkomi jo asmens duomenys.

10. Duomenų subjektas turi būti informuotas kokiais atvejais ir kokie duomenys yra tvarkomi jo sutikimu, šio sutikimo atšaukimo tvarką bei galimas pasekmes sutikimo nedavus ar sutikimą atšaukus. DIGA kodekso 6 priede pateikiamas Paciento valios pareiškimo ir informuoto sutikimo administravimo tvarkos aprašas ir rekomenduojamos sutikimo formos, jeigu šios formos nenustato Lietuvos Respublikos teisės aktai.

11. Teisės aktų nustatytais atvejais ir tvarka DIGA įstaiga (įstaigos) pagal prašymus (vienkartinio asmens duomenų rinkimo atveju) arba pagal duomenų teikimo sutartį (daugkartinio duomenų rinkimo atveju). teikia šios įstaigos (įstaigų) tvarkomus asmens duomenis:

11.1. kitoms sveikatos priežiūros įstaigoms, kuriose gydomas, slaugomas pacientas arba atliekama jo sveikatos ekspertizė;

11.2. Lietuvos Respublikos sveikatos apsaugos ministerijai, Valstybinėms ligonių kasoms prie Lietuvos Respublikos sveikatos apsaugos ministerijos, kitoms institucijoms, kontroliuojančioms sveikatos priežiūros paslaugas;

11.3. Lietuvos Respublikos valstybinei mokesčių inspekcijai;

11.4. savivaldybių administracijoms;

11.5. prokuratūroms, ikiteisminio tyrimo įstaigoms, Lietuvos Respublikos specialiųjų tyrimų tarnybai, Lietuvos Respublikos valstybės saugumo departamentui;

11.6. Valstybinio socialinio draudimo fondo valdybai;

11.7. Lietuvos Respublikos nacionaliniam kibernetinio saugumo centrui;

11.8. ir kitiems tretiesiems asmenims, kuriems tokią teisę suteikia Lietuvos Respublikos įstatymai.

12. Asmens duomenys, kurie duomenų subjekto prašymu perduodami arba kuriuos ketinama perduoti į trečiąją valstybę arba tarptautinei organizacijai, perduodami tik tuo atveju, jeigu trečiosios valstybės duomenų valdytojas ir duomenų tvarkytojas, jeigu jis yra, laikosi *Reglamento 2016/679* nuostatų.

13. DIGA įstaigos tvarko duomenis ne ilgiau nei to reikalauja duomenų tvarkymo tikslai.

14. Laikydamosi teisės aktų reikalavimų kiekviena DIGA įstaiga ir (arba) prisijungusi prie šio kodekso įstaiga ar organizacija savarankiškai rūpinasi, kad nebereikalingi duomenys, pvz., dokumentai, kuriuose yra asmens duomenų, ar jų kopijos, filmuota medžiaga, diagnostikos prietaisų suformuoti duomenys ar kt., įstatymų nustatyta tvarka būtų perduota archyvams, arba sunaikinti taip, kad juose esanti informacija nebūtų atpažįstama, o automatiniu būdu surinkti duomenys būtų saugojami duomenų bazių archyvuose arba ,sunaikinti ištrinant nebereikalingus duomenis iš saugojimo laikmenos taip, kad jų nebūtų galima atgaminti.

15. Konkrečios duomenų tvarkymo procedūros, duomenų tvarkymo taisyklės ir šiuos duomenis tvarkančių darbuotojų ar paslaugų teikėjų teisės ir pareigos nustatomi kiekvienoje DIGA įstaigoje atskirai.

V. DUOMENŲ SUBJEKTO TEISĖS IR JŲ ĮGYVENDINIMAS

16. Duomenų subjektas, kurio duomenys tvarkomi DIGA įstaigos veikloje, turi šias teises:

16.1. žinoti (būti informuotas) apie savo duomenų tvarkymą (teisė žinoti);

16.2. susipažinti su savo duomenimis ir kaip jie yra tvarkomi (teisė susipažinti);

16.3. reikalauti ištaisyti arba, atsižvelgiant į duomenų tvarkymo tikslus, papildyti neišsamius asmens duomenis (teisė ištaisyti);

16.4. reikalauti sunaikinti arba sustabdyti savo duomenų tvarkymo veiksmus (išskyrus saugojimą) (teisė sunaikinti ir teisė būti pamirštam);

16.5. reikalauti, kad DIGA įstaiga, ji ir duomenų valdytojas, apribotų asmens duomenų tvarkymą (teisė apriboti);

16.6. prašyti perkelti savo duomenis kitam duomenų valdytojui (teisė į duomenų perkėlimą).

17. DIGA įstaiga, ji ir duomenų valdytojas, gali nesudaryti duomenų subjektams sąlygų įgyvendinti šių teisių, kai įstatymų numatytais atvejais reikia užtikrinti sveikatos priežiūros paslaugų teikimą nepaprastomis aplinkybėmis, siekiant užtikrinti duomenų subjekto gyvybinius interesus, nusikaltimų, tarnybinės ar profesinės etikos pažeidimų prevenciją, tyrimą ir nustatymą, taip pat duomenų subjekto ar kitų asmenų teisių ir laisvių apsaugą.

18. Visais klausimais, susijusiais su duomenų subjektų asmens duomenų tvarkymu ir duomenų subjektų teisėmis, numatytomis *Reglamente 2016/679*, ADTAĮ ir kituose teisės aktuose, duomenų subjektai turi kreiptis tiesiogiai į DIGA įstaigos administraciją arba duomenų apsaugos pareigūną.

19. Duomenų subjektas turi teisę susipažinti, iš kokių šaltinių ir kokie jo asmens duomenys surinkti, kokiu tikslu tvarkomi, kokiems duomenų gavėjams teikiami ir (arba) buvo teikti bent per pastaruosius 2 (du) metus.

20. Duomenų subjektas turi teisę reikalauti, kad DIGA įstaiga nedelsdama ištrintų su juo susijusius duomenis, jei tai galima pagrįsti bent viena iš priežasčių:

20.1. duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi;

20.2. duomenys yra tvarkomi duomenų subjekto sutikimu ir jis savo sutikimą atšaukia, o taip pat nėra jokio kito teisinio pagrindo tvarkyti šiuos duomenis;

20.3. asmens duomenys buvo tvarkomi neteisėtai.

21. Atsakymo į duomenų subjekto prašymą ar skundą dėl jo asmens duomenų tvarkymo pateikimo procedūrą nustato kiekviena DIGA įstaiga ir (arba) prisijungusi prie šio kodekso įstaiga ar organizacija savarankiškai *Reglamente 2016/679*, ADTAĮ ir kituose teisės aktuose nustatytais terminais ir tvarka.

22. Duomenų subjektas turi teisę pateikti skundą Valstybinei duomenų apsaugos inspekcijai dėl DIGA įstaigos veiksmų (neveikimo).

23. Duomenų subjektas turi teisę pateikti skundą Asociacijai DIGA, jeigu Asociacijos narys neįgyvendina arba duomenų subjekto nuomone, netinkamai, pvz., nesilaikant šio kodekso nuostatų, įgyvendina duomenų subjekto teises, arba jeigu teikiant paslaugas Asociacijos narys nebendradarbiauja su kitais Asociacijos nariais; pvz., nesuteikia duomenų perkeliamumo paslaugos, nors yra techninės galimybės.

24. Duomenų subjektas turi teisę reikalauti atlyginti DIGA įstaigų jam padarytą turtinę ir neturtinę žalą dėl neteisėto asmens duomenų tvarkymo (neveikimo).

25. DIGA įstaigos turi užtikrinti, kad duomenų subjekto teisės būtų tinkamai įgyvendintos, visa informacija duomenų subjektui būtų pateikiama aiškiai, suprantamai ir priimtina forma. Šiame kodekse nustatytos duomenų subjektų teisės ir jų įgyvendinimo tvarka išsamiau išdėstyta 5 šio kodekso priede, nuostatos, susijusios su duomenų subjekto teisių įgyvendinimu konkrečioje DIGA įstaigoje įtvirtinamos DIGA įstaigų vidiniuose teisės aktuose, taip pat išdėstomos supaprastinta forma kiekvienos DIGA įstaigos privatumo politikoje, kuri skelbiama DIGA įstaigos interneto ir intraneto (jeigu yra) svetainėse.

26. Konkrečios duomenų subjekto teisių įgyvendinimo procedūros ir šias teises įgyvendinančių darbuotojų ar paslaugų teikėjų teisės ir pareigos nustatomi kiekvienoje DIGA įstaigoje atskirai.

VI. DUOMENŲ SAUGUMO PAŽEIDIMAI

27. Atsižvelgiant į tai, kad DIGA įstaigos tvarko specialių kategorijų duomenis, duomenų saugumo incidentas, kuriam įvykus kyla grėsmė, kad asmens duomenys gali būti sunaikinami, prarandami, pakeičiami ar be leidimo atskleidžiami, ar be leidimo asmenys, neturintys tam teisės, gautų prieigą prie duomenų, turi būti valdomas kad būtų išvengta žalos atsiradimo.

28. Jei dėl įvykusio asmens duomenų saugumo pažeidimo kyla pavojus duomenų subjektų teisėms ir laisvėms, DIGA įstaigos duomenų apsaugos pareigūnas ar kitas šios įstaigos vadovo paskirtas darbuotojas privalo nedelsiant, bet ne vėliau nei kaip per 72 val. pranešti Valstybinei duomenų apsaugos inspekcijai apie įvykusį incidentą. Kilus ypatingai dideliam pavojui apie duomenų saugumo pažeidimą būtina nedelsiant informuoti duomenų subjektus. Esant žalos atsiradimo rizikai DIGA įstaigos duomenų apsaugos pareigūnas kartu su įstaigos vadovu apsvarsto ir priima sprendimą dėl šios informacijos paskelbimo visuomenės informavimo priemonėmis (spaudoje, televizijos ir radijo laidose ar kt.).

29. Valstybinei duomenų apsaugos inspekcijai pranešimas teikiamas internetu per šios įstaigos svetainę, adresas – https://www.ada.lt/go.php/lit/Pranesimas-apie-duomenu-saugumo-pazeidima-bdar/4, nesant galimybės prisijungti prie interneto, pranešimas teikiamas el. paštu, telefonu ar kitomis įmanomomis priemonėmis.

30. Tiriant duomenų saugumo pažeidimą ir vertinant, ar būtina informuoti duomenų subjektus, pranešimą teikiantis asmuo patikrina ar dėl šio pažeidimo:

30.1. neužtikrinamas duomenų konfidencialumas, pvz., atskleisti diagnostinių tyrimų duomenys ir jie tapo prieinami neturintiems teisės į prieigą asmenims, pateko į internetą nešifruoti ir kt.);

30.2. prarastas duomenų pasiekiamumas (pvz., sugadinti elektroniniai duomenys ir nėra atsarginių kopijų);

30.3. prarastas duomenų vientisumas (pvz., prarastos pacientų ligos istorijos ir neįmanoma atkurti visos paciento ligos istorijos).

31. DIGA įstaigos duomenų apsaugos pareigūnas ar kitas įstaigos vadovo paskirtas atsakingas darbuotojas privalo dokumentuoti ir saugoti duomenų saugumo pažeidimų tyrimo medžiagą.

32. Ištyrus duomenų saugumo pažeidimą , DIGA įstaigos duomenų apsaugos pareigūnas ar kitas įstaigos vadovo paskirtas atsakingas darbuotojas sudaro veiksmų planą numatant veiksmus, kurie užkirstų kelią pasikartoti analogiškam ar panašiam pažeidimui.

VII. DUOMENŲ APSAUGOS PAREIGŪNAS

33. Vadovaudamasi *Reglamento 2016/679* 37 straipsnio nuostatomis ir atsižvelgdama į tai, kad DIGA įstaigos savo veikloje tvarko specialių kategorijų duomenų dideliu mastu, Asociacija DIGA skiria duomenų apsaugos pareigūną, vykdantį funkcijas visose DIGA įstaigose ir veikiantį šios asociacijos ir jos narių DIGA įstaigų vardu bei jiems atstovaujantį, tačiau tai neužkerta kelio šį pareigūną skirti atskiroje DIGA įstaigoje.

34. Šis duomenų apsaugos pareigūnas paskiriamas per 3 (tris) mėnesius pradėjus taikyti šį kodeksą neilgesniam kaip 3 (trijų) metų terminui remiantis profesinėmis savybėmis, visų pirma duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis, taip pat gebėjimu atlikti *Reglamento 2016/679* 39 straipsnyje nurodytas užduotis. Asociacija DIGA ir DIGA įstaigos paskelbia duomenų apsaugos pareigūno kontaktinius duomenis interneto svetainėse ir praneša juos Valstybinei duomenų apsaugos inspekcijai.

35. Duomenų apsaugos pareigūnas:

35.1. stebi, kaip DIGA įstaigų darbuotojai ir kiti DIGA įstaigų valdomų asmens duomenų tvarkytojai vykdo jiems nustatytas asmens duomenų tvarkymo pareigas ir tvarko asmens duomenis;

35.2. nustatyta tvarka viešai skelbia apie duomenų valdytojo atliekamus duomenų tvarkymo veiksmus;

35.3. DIGA asociacijos ir DIGA įstaigų vadovybei teikia siūlymus ir išvadas dėl duomenų apsaugos ir duomenų tvarkymo priemonių nustatymo, stebi, kaip šios priemonės įgyvendinamos ir naudojamos;

35.4. teikia DIGA asociacijos ir DIGA įstaigų darbuotojams tiesioginius nurodymus pašalinti asmens duomenų tvarkymo pažeidimus;

35.5. supažindina DIGA asociacijos ir DIGA įstaigų darbuotojus, įgaliotus tvarkyti asmens duomenis, su teisės aktų, reglamentuojančių asmens duomenų apsaugą, nuostatomis;

35.6. stebi poveikio tvarkant asmens duomenis vertinimus DIGA įstaigose;

35.7. padeda duomenų subjektams, kurie kreipiasi į DIGA įstaigas, įgyvendinti jų teises;

35.8. konsultuoja asmens duomenų tvarkytojus asmens duomenų tvarkymo ir apsaugos klausimais;

35.9. atsako už duomenų tvarkymo veiklos įrašų parengimą;

35.10. teikia nuomonę dėl poreikio atlikti poveikio duomenų apsaugai vertinimą;

35.11. Prireikus, duomenų apsaugos pareigūnas kreipiasi į Valstybinę duomenų apsaugos inspekciją dėl išankstinių konsultacijų;

35.12. įvykus asmens duomenų saugumo pažeidimui konsultuoja dėl įmanomų priemonių, kuriomis siekiama atstatyti prarastus asmens duomenis ir (ar) sumažinti pažeidimu asmens duomenims padarytą žalą;

35.13. užtikrina informacijos slaptumą ir (arba) konfidencialumą, susijusį su jo užduočių vykdymu, laikydamasis Lietuvos Respublikos teisės aktuose nustatytų reikalavimų;

35.14. ne rečiau kaip kartą per 3 (tris) metus atlieka asmens duomenų tvarkymo rizikos vertinimą, parengia ataskaitą ir konsultuoja DIGA įstaigos vadovus dėl priemonių rizikai pašalinti arba sumažinti;

35.15. konsultuojasi su Valstybine duomenų apsaugos inspekcija, jeigu mano, kad duomenų valdytojas ar tvarkytojas asmens duomenis tvarko pažeidžiant teisės aktų, reglamentuojančių duomenų apsaugą, nuostatas, ar atsisakant pašalinti šiuos pažeidimus;

35.16. vykdo kitas duomenų apsaugos pareigūnui teisės aktuose priskirtas užduotis ir pareigas.

VIII. SUTARČIŲ DĖL DUOMENŲ TVARKYMO SUDARYMAS

36. Vadovaujantis *Reglamento 2016/679* 28 straipsnio 7 ir 8 dalies nuostatomis Europos Komisija ir (arba) Valstybinė duomenų apsaugos inspekcija turi patvirtinti standartines sutarčių su duomenų tvarkytojais sąlygas dėl duomenų tvarkymo. Kol šios sąlygos nėra patvirtintos, DIGA įstaigoms rekomenduojama pasirašant sutartis vadovautis DIGA kodekso nuostatomis.

37. DIGA įmonės su visais paslaugų teikėjais, kuriems paveda tvarkyti asmens duomenis ir (arba) šie duomenys tampa žinomi teikiant paslaugas, pvz., prižiūri kompiuterizuotas darbo vietas ar kt., pasirašo papildomus susitarimus arba įtraukia į sutartis sąlygas dėl asmens duomenų tvarkymo.

38. Rašytiniame susitarime asmens duomenų tvarkymo turi būti įtrauktos nuostatos:

38.1. dėl duomenų tvarkymo dalyko;

38.2. dėl duomenų tvarkymo būdo ir tikslo (tikslų);

38.3. tiksliai nurodyta perduotų tvarkyti duomenų elementus arba duomenų rūšys ir (arba) duomenų kategorijos;

38.4. nurodytos naudojamos asmens duomenų apdorojimo priemonės, pvz., naršyklės techninės charakteristikos, elgesio internete duomenys, IP adresas ar kt.;

38.5. nurodyta, dėl kokių duomenų tvarkymo veiksmų atlikimo yra susitariama, pvz. asmens duomenų rinkimas, perdavimas ar kt.

38.6. dėl duomenų tvarkytojo (duomenų tvarkytojų) pareigų ir atsakomybės;

38.7. dėl duomenų tvarkytojo (duomenų tvarkytojų) pareigų ir atsakomybės;

38.8. dėl sub-tvarkytojų pasitelkimo galimybės ir duomenų valdytojų teisės susipažinti su šių sub-tvarkytojų vykdomu duomenų tvarkymu.

39. Atsižvelgiant į tai, kad pagal *Reglamento 2016/679* 25, 27 ir 28 straipsnių nuostatas dėl netinkamo duomenų tvarkymo taikoma atsakomybė ir duomenų valdytojui ir duomenų tvarkytojui, rekomenduojama susitarime dėl asmens duomenų tvarkymo įtraukti rašytines nuostatas dėl duomenų tvarkytojo pareigų:

39.1. veikti tik pagal rašytinius duomenų valdytojo nurodymus;

39.2. įrašyti sąlygą, kad prieigą prie duomenų turintys duomenų tvarkytojo darbuotojai ar sub-tvarkytojai būtų pasirašę konfidencialumo įsipareigojimus;

39.3. pasitelkti tik tuos sub-tvarkytojus dėl kurių gautas rašytinis duomenų valdytojo sutikimas;

39.4. įtraukti nuostatas dėl duomenų saugojimo vietos – atsižvelgiant į tai, kad DIGA įstaigos yra specialių kategorijų duomenų valdytojai, rekomenduojama įtraukti draudimą tvarkomus duomenis saugoti už Europos ekonominės erdvės ribų;

39.5. susitarti dėl sutarties galiojimo ir sutarties nutraukimo sąlygų, pvz., kad pasibaigus sutarties galiojimo terminui visi duomenys, susiję su duomenų valdytojo pacientais, darbuotojais ar kt. turi būti ištrinti iš duomenų tvarkytojo duomenų bazių, tarnybinių stočių ar kitų laikmenų;

39.6. susitarti dėl atvejų, kurioms atsiradus bet kuri šalis – duomenų valdytojas ir (arba) duomenų tvarkytojas turi teisę nutraukti sutartį, pvz., nepranešus duomenų valdytojui apie duomenų saugumo pažeidimą, duomenų atskleidimą internete ar kt.;

39.7. turėti tinkamas organizacines ir technines priemones užtikrinančias duomenų saugumą bei patvirtinimą, kad šios priemonės pakankamos duomenų saugumui užtikrinti, pvz., atitikties *Reglamento 2016/679* nuostatoms vertinimą, informaciją apie pritaikytosios ir standartizuotosios duomenų apsaugos principų laikymąsi;

39.8. susitarti dėl pareigos nedelsiant pranešti duomenų valdytojui apie duomenų saugumo pažeidimus, kai tik jie juos sužino;

39.9. suteikti duomenų valdytojui galimybę atlikti atitikties *Reglamento 2016/679* nuostatoms auditą, susitarti kaip dažnai šį auditą galima vykdyti ir kas padengs audito išlaidas;

39.10. įpareigoti duomenų tvarkytoją registruoti visus duomenų tvarkymo veiksmus;

39.11. gavus duomenų subjekto prašymą dėl jo teisių įgyvendinimo ar Valstybinės duomenų apsaugos inspekcijos užklausą ar kt. padėti duomenų valdytojui parengti atsakymą.

40. Kai sutartį (sutartis) su tuo pačiu duomenų tvarkytoju sudaro kelios DIGA įstaigos, Asociacija DIGA turi teisę atstovauti šias įstaigas sudarant susitarimus dėl asmens duomenų tvarkymo.

IX. DIGA KODEKSO NUOSTATŲ LAIKYMOSI KONTROLĖ IR PRIEŽIŪRA

41. DIGA kodekso stebėseną vykdo Valstybinės duomenų apsaugos inspekcijos akredituota įstaiga.

42. Asociacija DIGA turi teisę veikti proaktyviai, inicijuoti vienos ar kelių DIGA įstaigų auditą siekiant įsitikinti, kad yra laikomasi DIGA kodekso nuostatų.

43. DIGA kodekso nuostatų laikymąsi prižiūri ir kontroliuoja bei šio kodekso pažeidimus tiria, vertina ir teikia Asociacijos DIGA valdybai rekomendacinio pobūdžio išvadas pagal diagnostikos ir gydymo įstaigų asociacijos etikos kodekso (toliau Etikos kodeksas) 21 punktą įsteigtas Etikos komitetas (toliau – Etikos komitetas).

44. Etikos komitetas yra Asociacijos DIGA įgaliotas nagrinėti ginčus tarp DIGA įstaigos ir duomenų subjekto dėl duomenų subjekto teisių įgyvendinimo, ar organizacinių it techninių duomenų saugumo priemonių taikymo, ginčus tarp DIGA įstaigų – duomenų valdytojų ir duomenų tvarkytojų bei analizuoja DIGA įstaigos (įstaigų) pateiktą informaciją apie duomenų saugumo pažeidimo tyrimą, nustato DIGA Kodekso pažeidimų prevencines priemones bei teikia išvadas ir pasiūlymus Asociacijos DIGA valdybai. Ginčai nagrinėjami pagal Etikos kodekse nustatytą procedūrą ir terminais.

45. Etikos komitetas nagrinėjimo procedūrą pradeda gavęs rašytinę informaciją (tarnybinį pranešimą, darbuotojo skundą, visuomenės informavimo priemonių paskelbtą ar kitokią informaciją apie DIGA įstaigos darbuotojo (darbuotojų) galimai padarytą DIGA Kodekso reikalavimų pažeidimą. Atlikdamas savo funkcijas Etikos komitetas turi teisę pasitelkti bet kurios DIGA įstaigos duomenų apsaugos pareigūną.

46. Jeigu duomenų subjekto skundas atitinka ADTAĮ 24 straipsnio reikalavimus, jis pareiškėjui sutikus persiunčiamas nagrinėti Valstybinei duomenų apsaugos inspekcijai, nesutinkant – grąžinamas pareiškėjui.

X. ATSAKOMYBĖ UŽ DIGA KODEKSO PAŽEIDIMUS

47. Pažeidus DIGA kodekse įtvirtintus asmens duomenų tvarkymo ir apsaugos reikalavimus ir (arba) nustačius, kad DIGA įstaigos vadovo patvirtintos procedūros neatitinka DIGA kodekso, DIGA įstaigai taikoma Etikos kodekso VI skyriuje nustatyta nustatyta atsakomybė.

48. Konstatavus, kad DIGA įstaigos darbuotojas tvarkydamas asmens duomenis netinkamai vykdė savo pareigybės aprašyme ar kituose DIGA įstaigos vidiniuose teisės aktuose funkcijas, tyrimo medžiaga su išvada perduodama DIGA įstaigos vadovui. Sprendimą dėl poveikio priemonių darbuotojui taikymo priima DIGA įstaigos vadovas.

XI. BAIGIAMOSIOS NUOSTATOS

49. DIGA įstaigų darbuotojai tvarkydami asmens duomenis įsipareigoja vadovautis DIGA Kodeksu. Su šiuo Kodeksu pasirašytinai supažindinamas kiekvienas kiekvienos DIGA įstaigos darbuotojas. Naujai į darbą DIGA įstaigoje priimti darbuotojai su šiuo Kodeksu pasirašytinai supažindinami iškart po darbo sutarties pasirašymo.

50. DIGA kodeksas ir visi šio Kodekso pakeitimai turi būti suderinti su Valstybine duomenų apsaugos inspekcija.

51. DIGA kodeksas turi būti periodiškai, ne rečiau kaip kartą per 2 (dvejus) metus peržiūrimas ir prireikus atnaujinamas.

52. DIGA įstaigų vadovai turi užtikrinti, kad darbuotojai būtų informuoti apie DIGA kodekso atnaujinimus.

53. DIGA įstaigų darbuotojų informavimą apie DIGA kodekso atnaujinimus organizuoja kiekvienos DIGA įstaigos duomenų apsaugos pareigūnas.

54. DIGA kodeksas skelbiamas DIGA įstaigų interneto ir intraneto svetainėse.

55. DIGA kodekso nuostatas įgyvendinantys vidaus teisės aktai tvirtinami kiekvienos DIGA įstaigos vadovo arba jo įgalioto asmens įsakymu.

Asociacijos DIGA asmens duomenų tvarkymo
diagnostikos ir gydymo įstaigose
elgesio kodekso 2 priedas

TEISĖS AKTŲ SĄRAŠAS

Rengiant Asociacijos DIGA asmens duomenų tvarkymo diagnostikos ir gydymo įstaigose elgesio kodeksą vadovautasi Europos Sąjungos ir Lietuvos Respublikos teisės aktais, kurių sąrašas pateikiamas šiame priede:

1.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 94/46/EB (Bendrasis duomenų apsaugos reglamentas).

1.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Valstybės žinios, 1996-07-03, Nr. 63-1479.

1.3. Lietuvos Respublikos darbo kodeksas; TAR, 2016-09-19, Nr. 23709.

1.4. Lietuvos Respublikos biomedicininių tyrimų etikos įstatymas; TAR, 2015-09-25, Nr.14272.

1.5. Lietuvos Respublikos pacientų teisių ir žalos atlyginimo įstatymas (toliau – PTĮ); Valstybės žinios, 1996-10-23, Nr. 102-2317.

1.6. Lietuvos Respublikos dokumentų ir archyvų įstatymas; Valstybės žinios, 1995-12-30, Nr. 107-2389.

1.7. Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. liepos 4 d. Nr. V-769 įsakymas „Dėl duomenų subjektų teisių įgyvendinimo elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinėje sistemoje tvarkos aprašo patvirtinimo“; TAR, 2018-07-09, Nr. 11607.

1.8. Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. balandžio 10 d. Nr. V-405 įsakymas „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų ir Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“; TAR, 2018-04-12, Nr. 5891.

1.9. Lietuvos Respublikos sveikatos apsaugos ministro 2016 m. rugsėjo 21 d. Nr. V-1099 įsakymas „Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2008 m. sausio 14 d. įsakymo Nr. V-19 „Dėl Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos nuostatų patvirtinimo“ pakeitimo“; TAR, 2016-09-26, Nr. 24043.

1.10. Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. rugsėjo 22 d. Nr. V-975 įsakymas „Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. gruodžio 16 d. įsakymo Nr. V-1071 „Dėl Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro duomenų saugos nuostatų patvirtinimo“ pakeitimo”; TAR, 2014-09-30, Nr. 13239.

1.11. Lietuvos Respublikos sveikatos apsaugos ministro 2012 m. rugsėjo 28 d. Nr. V-920 įsakymas „Dėl Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro duomenų saugos nuostatų patvirtinimo”; Valstybės žinios, 2012-10-06, Nr. 116-5888.

1.12. 2018 m. gegužės 24 d. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas Nr. 1T-52(1.12.) „Dėl prašymo dėl leidimo perduoti asmens duomenis į trečiąsias valstybes ar tarptautinėms organizacijoms išdavimo rekomenduojamos formos patvirtinimo.“

1.13. 2018 m. gegužės 24 d. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas Nr. 1T-53(1.12.) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo.“

1.14. 2018 m. liepos 27 d. Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas Nr. 1T-72 (1.12.E) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašo patvirtinimo“, TAR, 2018-07-27, Nr.12533

1.15. Lietuvos vyriausiojo archyvaro 2011 m. liepos 4 d. įsakymas Nr. V-118 „Dėl Dokumentų tvarkymo ir apskaitos taisyklių patvirtinimo“; Valstybės žinios, 2011-07-15, Nr. 88-4230.

1.16. Lietuvos vyriausiojo archyvaro 2011 m. gruodžio 29 d. įsakymu Nr. V-158 „Dėl Elektroninių dokumentų valdymo taisyklių patvirtinimo“; Valstybės žinios, 2012-01-06, Nr. 3-104.

Asociacijos DIGA asmens duomenų tvarkymo
diagnostikos ir gydymo įstaigose
elgesio kodekso 3 priedas

ASMENS DUOMENŲ TVARKYMO DIAGNOSTIKOS IR GYDYMO ĮSTAIGOSE TVARKOS APRAŠAS

1. Asmens duomenų tvarkymo diagnostikos ir gydymo įstaigose tvarkos aprašas (toliau – Tvarkos aprašas) yra Asmens duomenų tvarkymo diagnostikos ir gydymo įstaigose elgesio kodekso 3 priedas, kuris nustato asmens duomenų tvarkymo ir apsaugos reikalavimus nurodant, kokiais tikslais ir kokie duomenys yra tvarkomi, iš kur gaunami (duomenų šaltinius), šių duomenų teikimo ir saugojimo tvarką.,

2. Šis Tvarkos aprašas taikomas ir privalomas duomenų valdytojams – Asociacijos DIGA įstaigoms ir visiems šiose įstaigose dirbantiems asmenims, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužinojo.

3. Tvarkos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Asociacijos DIGA asmens duomenų tvarkymo diagnostikos ir gydymo įstaigose elgesio kodekse, *Reglamente 2016/679,* ADTAĮ ir kituose duomenų apsaugos sritį reglamentuojančiuose teisės aktuose.

4. DIGA įstaigose neautomatiniu būdu susistemintose rinkmenose ir (arba) automatiniu būdu fizinių asmenų, jie ir duomenų subjektai, asmens duomenys tvarkomi šiais tikslais:

4.1. sveikatos priežiūros tikslais – pacientų ir kitų įstaigos lankytojų duomenys;

4.2. vidaus administravimo tikslais – esamų ir buvusių darbuotojų dirbančių (dirbusių) pagal darbo sutartis ar kitais pagrindais duomenys ir pretendentų į darbą DIGA įstaigose duomenys;

4.3. komunikacijos tikslais – fizinių asmenų, dirbančių pagal autorines, prekių, paslaugų ar kitas sutartis, bei kitų interesantų (jeigu reikia su jais susisiekti), juridinių asmenų darbuotojų, nurodytų sutartyse, kontaktiniai duomenys;

4.4. mokymų ir mokslinių tyrimų vykdymo tikslais – Sveikatos mokslų specialistus ruošiančių formaliojo šveitimo mokyklų , pvz., Vilniaus universiteto ir Lietuvos sveikatos mokslų universiteto ir kt. studentų, rezidentų ar kt. su jais susijusių asmenų duomenys;

4.5. turto ir asmenų saugumo užtikrinimo tikslais – į vaizdo kamerų stebėjimo teritoriją patekusių asmenų, pacientų ir įstaigos lankytojų, bei kt. asmenų vaizdo duomenys.

5. DIGA įstaigose sveikatos priežiūros tikslais neautomatiniu būdu susistemintose rinkmenose (paciento ligos istorijose, rašytinėse paskyrose ir kt. popieriniuose dokumentuose)

ir (arba) automatiniu būdu (IS, medicinos personalo kompiuterizuotose darbo vietose, atliekant procedūras ir tyrimus medicinine įranga ir kt.) tvarkomi šie pacientų ir kitų įstaigos lankytojų duomenys:

5.1. Bendrieji paciento duomenys – vardas, pavardė, asmens kodas, gimimo data, mirties data, deklaruotos gyvenamosios vietos adresas, faktinės gyvenamosios vietos adresas, telefono ryšio numeris, elektroninio pašto adresas, elektroninės sveikatos istorijos identifikacinis numeris, ryšys su motina (šis duomuo tvarkomas, kai pacientas yra naujagimis ir (arba) neturi asmens kodo, nuoroda į naujagimio motinos duomenis), lytis, šeiminė padėtis, asmens tapatybės identifikavimo dokumento rūšis, numeris, dokumentą išdavusi šalis, veido atvaizdas (nenustatytos asmens tapatybės paciento asmens tapatybei patvirtinti ar nustatyti).

5.2. Specialių kategorijų paciento sveikatos duomenys – valios pareiškimai, sveikatos priežiūros specialistų ir sveikatos priežiūros įstaigų pasirinkimai, ūgis, svoris, juosmens apimtis, kūno masės indeksas, kraujo grupė ir rezus faktorius, rizikos veiksniai, gyvenimo būdas (žalingi įpročiai), sveikatai kenksmingi ir pavojingi aplinkos veiksniai, neįgalumo lygis, darbingumo lygis, bendrieji pirminiai specialieji poreikiai, profilaktinių sveikatos patikrinimų duomenys, taikytų vakcinacijų duomenys, persirgtų ligų ar būklių pavadinimai ir kodai, alerginių reakcijų pavadinimai ir kodai, artimųjų giminaičių paveldimų arba genetinių ligų diagnozių kodai, paciento atvykimo į asmens sveikatos priežiūros įstaigą faktas, parengti elektroniniai medicininiai dokumentai, šių dokumentų metaduomenys, elektroninės medicininės pažymos ir jų metaduomenys, nusiskundimų ir anamnezių duomenys, duomenys apie suteiktas sveikatos priežiūros paslaugas, duomenys apie taikytą ambulatorinį gydymą, diagnozuotų ligų ar būklių pavadinimai ir kodai, taikyto gydymo būdai, atliktos procedūros ir operacijos (intervencijos), ilgalaikio stebėjimo duomenys, duomenys apie gydymą vaistiniais preparatais ir medicinos pagalbos priemonių taikymą, siuntimai konsultuoti, tirti, gydyti, duomenys apie paimtus žmogaus kūno mėginius, atliktus tyrimus.

5.3. Specialių kategorijų paciento administravimo duomenys – duomenys apie paciento draustumą, duomenys apie apmokėjimą, jeigu paslaugos mokamos, ir kiti teikiant sveikatos priežiūros paslaugas surinkti duomenys, duomenys apie išduotus elektroninius nedarbingumo pažymėjimus bei elektroninius nėštumo ir gimdymo atostogų pažymėjimus (šiuose dokumentuose esantys duomenų elementai – asmens kodas, vardas, pavardė, nedarbingumo priežastis, nedarbingumo, nėštumo ir gimdymo atostogų laikotarpis, gimdymo data), duomenys apie išduotus leidimus dėl nedarbingumo bei nėštumo ir gimdymo atostogų pažymėjimų išdavimo Elektroninių nedarbingumo pažymėjimų bei elektroninių nėštumo ir gimdymo atostogų pažymėjimų išdavimo taisyklių nenumatytais atvejais (šiuose dokumentuose esantys

duomenų elementai – asmens kodas, vardas, pavardė, sveikatos priežiūros įstaiga, kuriai skirtas leidimas, nedarbingumo laikotarpis). Draudimo sveikatos draudimu duomenys gaunami registravimo sveikatos priežiūros paslaugoms gauti metu.

5.4. Su pacientu susijusių kontaktinių asmenų duomenys – vardas, pavardė, ryšio su pacientu tipas (asmuo, kuris turi teisę gauti duomenis paciento sutikimu, giminaitis, atstovas pagal įstatymą ar sutartį, ar kt.) kontaktiniai duomenys – telefono ryšio numeris, elektroninio pašto adresas.

6. DIGA įstaigose sveikatos priežiūros tikslais neautomatiniu būdu susistemintose rinkmenose ir (arba) automatiniu būdu (IS, medicinos personalo kompiuterizuotose darbo vietose ir kt.) tvarkomi pacientų ir kitų įstaigos lankytojų duomenys yra gaunami (duomenų šaltiniai) iš paties paciento, su pacientu susijusių kontaktinių asmenų (lankytojų), Valstybinės ligonių kasos, teritorinių ligonių kasų, Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos, Neįgalumo ir darbingumo nustatymo tarnybos prie Socialinės apsaugos ir darbo ministerijos, VĮ Registrų centro, sveikatos priežiūros įstaigų, Nacionalinio vėžio instituto, sveikatos draudimo kompanijų, Užkrečiamųjų ligų ir AIDS centro.

7. Pacientų ir kitų DIGA įstaigos lankytojų sveikatos priežiūros tikslais surinkti asmens duomenys gali būti teikiami Lietuvos Respublikos sveikatos apsaugos ministerijai ir jai pavaldžioms institucijoms, Valstybinei ligonių kasai, Teritorinėms ligonių kasoms, sveikatos priežiūros įstaigoms, Valstybinei darbo inspekcijai, Užkrečiamųjų ligų ir AIDS centrui, Teismams, ikiteisminio tyrimo institucijoms, Policijai, kitiems duomenų gavėjams turintiems teisinį pagrindą šiuos duomenis gauti.

8. Pacientų ir kitų įstaigos lankytojų duomenys DIGA įstaigose tvarkomi ir saugojami visą sveikatos priežiūros paslaugų pacientui teikimo laiką, kol pacientas naudojasi įstaigos paslaugomis arba visą paciento gyvenimą ir 3 metus po jo mirties. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti atitinkamam archyvui.

9. Atsižvelgiant į tai, kad Elektroninėje sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinėje sistemoje, kurios duomenų valdytojas yra Lietuvos Respublikos sveikatos apsaugos ministerija, pacientų asmens duomenys tvarkomi visą paciento gyvenimą ir 3 metus po jo mirties ir šiam laikotarpiui pasibaigus, automatiškai perkeliami į sistemos duomenų archyvą, o duomenų archyve saugomi 75 metus nuo jų perkėlimo momento ir po to sunaikinami arba perduodami valstybės archyvams ar Lietuvos Respublikos dokumentų ir archyvų įstatymo taip pat kitų teisės aktų nustatyta tvarka, DIGA įstaigoms rekomenduojama

laikytis tokios pat jų valdomose IS ir elektroninėse laikmenose sukauptų duomenų saugojimo tvarkos.

10. Vidaus administravimo (personalo valdymo, raštvedybos tvarkymo, materialinių ir finansinių išteklių naudojimo, komunikacijos) tikslais esamų ir buvusių darbuotojų dirbančių (dirbusių) pagal darbo sutartis ar kitais pagrindais yra tvarkomi:

10.1. Bendrieji darbuotojo asmens duomenys – vardas, pavardė, asmens kodas, asmens socialinio draudimo numeris, pilietybė, adresas, telefono ryšio numeris, elektroninio pašto adresas, gyvenimo ir veiklos aprašymas, parašas, šeiminė padėtis, pareigos, duomenys apie priėmimą, perkėlimą, atleidimą iš pareigų, duomenys apie išsilavinimą ir kvalifikaciją, duomenys apie sveikatos priežiūros specialisto licenciją, jos galiojimo terminą, panaikinimo datą, sveikatos priežiūros specialisto spaudo numeris, duomenys apie mokymus ir kvalifikacijos kėlimą, duomenys apie atostogas, duomenys apie darbo užmokestį, išeitines išmokas, kompensacijas, pašalpas, informacija apie dirbtą darbo laiką, skatinimus ir nuobaudas, Lietuvos Respublikos piliečio paso arba asmens tapatybės kortelės numeris, išdavimo data, galiojimo data, dokumentą išdavusi įstaiga, duomenys apie išsilavinimą ir kvalifikacijas bei tai patvirtinančių dokumentų kopijos. Komunikacijos tikslu darbuotojo sutikimu tvarkomi darbuotojo ir jo nurodyto asmens nelaimės atveju vardas, pavardė, asmeninis telefono ryšio numeris, elektroninio pašto adresas.

10.2. Specialių kategorijų asmens duomenys, susiję su sveikata (pvz., periodinių sveikatos patikrinimų) ir teistumu, dokumentų registracijos data ir numeris bei kiti asmens duomenys, kuriuos tvarkyti DIGA įstaigą įpareigoja Darbo kodeksas, įstatymai ir kiti teisės aktai).

11. DIGA įstaigose tvarkomi darbuotojų duomenys yra teikiami paties darbuotojo ir (arba) kitų valstybės institucijų, viešojo administravimo ar kitų subjektų, kurie įstatymais ar kitais teisės aktais yra įpareigoti teikti darbdaviui jo darbuotojų duomenis. Komunikacijos tikslu surinkti darbuotojo ir jo nurodyto asmens duomenys nėra teikiami.

12. DIGA įstaigų darbuotojų duomenys šiose įstaigose yra tvarkomi visą darbuotojo darbo šioje įstaigoje laiką ir saugojami kol reikalingi jų tvarkymo tikslams pasiekti. Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti atitinkamam archyvui. Komunikacijos tikslu surinkti darbuotojo ir jo nurodyto asmens duomenys tvarkomi ir saugojami darbuotojo darbo šioje įstaigoje laikotarpiu arba kol darbuotojas atšauks savo sutikimą dėl šių duomenų tvarkymo. Pasibaigus nurodytam laikotarpiui šie duomenys sunaikinami.

13. Fizinių asmenų, dirbančių pagal autorines, prekių, paslaugų ar kitas sutartis, bei kitų interesantų (jeigu reikia su jais susisiekti), o juridinių asmenų – jų darbuotojų, nurodytų sutartyse, kontaktiniai duomenys – vardas, pavardė, asmens kodas (jeigu sudaryta sutartis), telefono ryšio numeris, elektroninio pašto adresas, yra tvarkomi aktyvaus bendravimo laikotarpiu ir saugojami įstatymų ir kitų teisės aktų nustatyta tvarka.

14. Pretendentų į darbą duomenys – vardas, pavardė, asmens kodas, duomenys apie išsilavinimą ir kvalifikaciją bei tai patvirtinančių dokumentų numeriai, juos išdavusios mokymo įstaigos pavadinimas ir rekvizitai, išdavimo data ir galiojimo terminas, gyvenimo aprašymas, jame pateikti duomenys ir veido atvaizdas (nuotrauka), telefono ryšio numeris, elektroninio pašto adresas, yra gaunami iš paties pretendento ir tvarkomi aktyvaus bendravimo (darbuotojų atrankos vykdymo) laikotarpiu. Pretendentą priėmus į pareigas jo duomenys toliau tvarkomi kaip darbuotojo duomenys. Kitų, neįdarbintų asmenų duomenys ištrinami (sunaikinami), jeigu įstatymais nėra numatyta kitokia jų saugojimo tvarka. Šie duomenys tretiesiems asmenims nėra teikiami.

15. Sveikatos mokslų specialistus ruošiančių formaliojo švietimo mokyklų, pvz., Vilniaus universiteto ir Lietuvos sveikatos mokslų universiteto ir kt. studentų, rezidentų ar kt. su jais susijusių asmenų duomenys – vardas, pavardė, asmens kodas, mokymo ir (arba) mokslo įstaigos pavadinimas ir rekvizitai, studento ar rezidento buvimo DIGA įstaigoje tikslas ir tai patvirtinantys, dokumentai, telefono ryšio numeris, elektroninio pašto adresas, yra gaunami iš paties studento ar rezidento ir tvarkomi aktyvaus bendravimo (studento praktikos, tiriamojo darbo ar kt. veiklos DIGA įstaigoje laikotarpiu. Jeigu studentas ar rezidentas yra įdarbinamas, jo duomenys toliau tvarkomi kaip darbuotojo duomenys. Kitų, neįdarbintų asmenų duomenys pasibaigus jų veiklos DIGA įstaigoje laikotarpiui, sunaikinami (popieriniai sudeginami, elektroniniai ištrinami ar saugojami duomenų bazių archyvuose), jeigu įstatymais nėra numatyta kitokia jų saugojimo tvarka. Šie duomenys teikiami mokymo ar mokslo įstaigai duomenų subjekto prašymu.

16. Vaizdo duomenys – į vaizdo kamerų stebėjimo lauką (DIGA įstaigai priklausančiose automobilių parkavimo aikštelėse, kiemuose ar kt.) patekusių pacientų, darbuotojų ir kitų asmenų, kurie lankosi DIGA įstaigoje, asmenų vaizdo duomenys yra tvarkomi laikantis *Reglamente 2016/679,* ADTAĮ ir kituose teisės aktuose nustatytų reikalavimų. Vaizdo duomenys DIGA įstaigoje gali būti renkami apsaugos kameromis filmuojant įstaigai priklausančią (jos naudojamą) teritoriją, kiemą, automobilių parkavimo vietas, įėjimus į DIGA įstaigos pastatą (pastatus) ir patalpas, kuriose koncentruota elektroninių ryšių tinklų, serverių, medicininės įranga, valdymo pultai ar kt., koncentracijos patalpas. Draudžiama nukreipti

kamerų stebėjimo lauką į pacientų koncentracijos ar medicininio personalo darbo vietas ar įėjimus į pacientų arba medicininio personalo lankomas patalpas.

17. DIGA įstaigoje draudžiama fotografuoti, filmuoti, daryti vaizdo ar garso įrašus, kuriuose būtų fiksuojama bet kokia informacija apie pacientus ir lankytojus.

18. DIGA įstaigos personalo vaizdo ir garso įrašai gali būti daromi tik esant darbuotojo (darbuotojų ir įstaigos vadovo sutikimo.

19. Vaizdo duomenys neteikiami.

20. DIGA įstaigoje rekomenduojama vaizdo duomenų neįrašyti ir nesaugoti. Jeigu šie duomenys yra įrašomi, jų saugojimo laikas turi būti kiek įmanoma trumpesnis. Šiam laikotarpiui pasibaigus vaizdo stebėjimo duomenys turi būti sunaikinami (ištrinami).

21. DIGA įstaigos gali naudoti savo pacientų, lankytojų ir kitų asmenų, kurių duomenis tvarko, tikslu tam, kad pateiktų jiems pasiūlymus ir informaciją apie savo, kitų DIGA įstaigų ir su šiomis įstaigomis susijusių asmenų ir partnerių paslaugas ar prekes, tik gavę atskirą duomenų subjekto sutikimą naudoti jo duomenis tiesioginės rinkodaros tikslais.

22. Rinkodaros tikslu tvarkomi šie asmens duomenys: vardas, pavardė, telefono ryšio numeris, elektroninio pašto adresas, lytis, amžius, informaciją apie asmens ryšius su DIGA įstaiga, pvz., pacientas prisirašęs prie DIGA įstaigos, lankytojas ar kt.

23. Visi DIGA įstaigoje rengiami ir gaunami dokumentai, kuriuose yra asmens duomenys, tvarkomi, įtraukiami į apskaitą, viešinami ir saugomi vadovaujantis Dokumentų tvarkymo ir apskaitos taisyklių, patvirtintų Lietuvos vyriausiojo archyvaro 2011 m. liepos 4 d. įsakymu Nr. V-118 „Dėl Dokumentų tvarkymo ir apskaitos taisyklių patvirtinimo“, Elektroninių dokumentų valdymo taisyklių, patvirtintų Lietuvos vyriausiojo archyvaro 2011 m. gruodžio 29 d. įsakymu Nr. V-158 „Dėl Elektroninių dokumentų valdymo taisyklių patvirtinimo“, reikalavimais ir Lietuvos vyriausiojo archyvaro tarnybos parengtomis Vaizdo ir garso dokumentų išsaugojimo rekomendacijomis.

24. Teikdama turinčią asmens duomenų informaciją žiniasklaidai DIGA įstaiga užtikrina, kad būtų laikomasi Lietuvos Respublikos visuomenės informavimo įstatyme ir kituose visuomenės informavimą reglamentuojančiuose įstatymuose bei teisės aktuose nustatytų visuomenės informavimo principų. Informacija, susijusi su pacientais ir kitais įstaigos lankytojais bei specialių kategorijų duomenys žiniasklaidai neteikiami.

25. Kitiems tretiesiems asmenims asmens duomenis DIGA įstaiga teikia tik tuomet, kai tai įpareigoja įstatymai ar kiti teisės aktai.

26. DIGA įstaiga užtikrina, kad asmens duomenys būtų tvarkomi vadovaujantis šiuo Tvarkos aprašu ir užtikrina, kad šie duomenys būtų renkami teisės aktų nustatyta tvarka juos

gaunant tiesiogiai iš duomenų subjekto, šiuos duomenis tvarkančių ir turinčių teisę juos teikti subjektų. Esant būtinybei, atskirais atvejais, asmens duomenys tvarkomi gaunant duomenų subjekto sutikimą.

27. DIGA įstaiga, kaip duomenų valdytojas:

27.1. užtikrina duomenų subjekto teisių įgyvendinimą ir vykdo *Reglamente 2016/679,* ADTAĮ ir kituose duomenų apsaugos sritį reglamentuojančiuose teisės aktuose nustatytas asmens duomenų valdytojo pareigas;

27.2. paskiria duomenų apsaugos pareigūną ir kitus asmenis, atsakingus už asmens duomenų tvarkymą DIGA įstaigoje;

27.3. užtikrina būtinus žmogiškuosius ir finansinius išteklius, kurie reikalingi teisėtam, saugiam duomenų tvarkymui ir duomenų apsaugos pareigūno užduotims vykdyti;

27.4. užtikrina, kad duomenų apsaugos pareigūnas negautų jokių nurodymų dėl teisės aktais jam pavestų asmens duomenų tvarkymo užduočių vykdymo, ir neskiria užduočių galinčių sukelti interesų konfliktą;

27.5. nustato duomenų subjekto teisių įgyvendinimo tvarką (procedūrą);

27.6. užtikrina išteklių, reikalingų darbuotojų mokymui ir kvalifikacijos tobulinimui asmens duomenų apsaugos srityje, skyrimą;

27.7. nustato ir įgyvendina technines ir organizacines duomenų saugumo priemones, reikalingas teisėtam ir saugiam duomenų tvarkymui DIGA įstaigoje;

27.8. užtikrina, kad asmens duomenys būtų tvarkomi laikantis *Reglamente 2016/679,* ADTAĮ, DIGA kodekse ir kituose duomenų apsaugos sritį reglamentuojančiuose teisės aktuose nustatytų reikalavimų;

27.9. užtikrina, kad asmens duomenys būtų tvarkomi laikantis organizacinių ir techninių duomenų saugumo priemonių, nurodytų DIGA įstaigos ir (arba) kitų įstaigų ir organizacijų valdomų ir DIGA įstaigos naudojamų informacinių sistemų dokumentuose (nuostatuose, duomenų saugos nuostatuose, saugaus elektroninės informacijos tvarkymo taisyklėse, naudotojų administravimo taisyklėse ir kt.);

27.10. DIGA įstaiga supažindina savo darbuotojus su *Reglamente 2016/679,* ADTAĮ, DIGA kodekse ir kituose duomenų apsaugos sritį reglamentuojančiuose teisės aktuose nustatytais reikalavimais būdu, kuris užtikrina susipažinimo įrodomumą.

27.11. DIGA įstaiga užtikrina, kad įstaigoje nustatytos konkrečios duomenų tvarkymo procedūros, duomenų tvarkymo taisyklės ir (arba) šiuos duomenis tvarkančių darbuotojų ar paslaugų teikėjų teisių ir pareigų turinys nepriešstarauja *Reglamente 2016/679,* ADTAĮ, DIGA

kodekse ir kituose duomenų apsaugos sritį reglamentuojančiuose teisės aktuose įtvirtintiems reikalavimams.

Asociacijos DIGA asmens duomenų tvarkymo privačiose diagnostikos ir gydymo įstaigose elgesio kodekso 4 priedas

ORGANIZACINIŲ IR TECHNINIŲ ASMENS DUOMENŲ APSAUGOS PRIEMONIŲ ĮGYVENDINIMO APRAŠAS

1. Vadovaujantis DIGA kodekso 6.5. papunkčio reikalavimais ir atsižvelgiant į Valstybinės duomenų apsaugos inspekcijos 2018-10-31 išleistą rekomendaciją „Dėl tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gairės asmens duomenų valdytojams ir tvarkytojams“ bei Valstybinės duomenų apsaugos inspekcijos 2017-08-07 išleistą rekomendaciją „Asmens duomenų, tvarkomų sveikatos priežiūros įstaigose, saugumo užtikrinimo gairės“ šiame organizacinių ir techninių asmens duomenų apsaugos priemonių įgyvendinimo privačiose diagnostikos ir gydymo įstaigose apraše (toliau – Aprašas) pateikiamos rekomendacijos dėl organizacinių ir techninių priemonių, kurias rekomenduojama įgyvendinti DIGA įstaigoje, kad apsaugotų tvarkomus asmens duomenis nuo neteisėto atskleidimo, pakeitimo ar praradimo, įgyvendinimo.

2. Šis Aprašas taikomas DIGA įstaigoms, duomenų valdytojams ir ir šiose įstaigose dirbantiems asmenims, kurie privalo taip organizuoti veiklos procesus ir priemones, kad įvykus duomenų saugumo pažeidimui, būtų sumažinta žalos atsiradimo tikimybė.

3. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Asociacijos DIGA asmens duomenų tvarkymo privačiose diagnostikos ir gydymo įstaigose elgesio kodekse, *Reglamente 2016/679,* ADTAĮ ir kituose duomenų apsaugos sritį reglamentuojančiuose teisės aktuose.

4. Aprašas yra rekomendacinio pobūdžio dokumentas. Kiekviena DIGA įstaiga, ji ir duomenų valdytojas ir (arba) tvarkytojas, įgyvendina technines ir organizacines priemones, kad būtų užtikrintas atitinkamo lygio saugumas. Atsižvelgdamas į techninių galimybių išsivystymo lygį, naudojamą medicininę įrangą ir komunikacijai skirtus įrenginius, duomenų saugumo priemonių sąnaudas bei duomenų tvarkymo pobūdį, aprėptį ir tikslus, DIGA įstaigoje įgyvendinamos priemonės, kad būtų užtikrintas tinkamo lygio duomenų saugumas, įskaitant *inter alia*, jei reikia:

4.1. pseudonimų suteikimą asmens duomenims ir jų šifravimą, ypač tuomet, kai tvarkomi specialių kategorijų duomenys;

4.2. gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;

4.3. gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento ar duomenų saugumo pažeidimo atveju;

4.4. reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą.

5. DIGA įstaigose asmens duomenys (užrašyti popieriuje ar elektroniniai) yra kaupiami:

5.1. popierinėse laikmenose – ligos istorijos, paciento valios pareiškimai, įrašai apie siuntimą konsultuoti paciento kortelėje, siuntimai konsultuoti ir kt.,

5.2. elektroniniai dokumentai – elektroninės medicininės pažymos ir jų metaduomenys, duomenys apie gydymą vaistiniais preparatais, receptai, diagnozės ir kt.;

5.3. informacinėse sistemose duomenų bazėse kaupiami duomenys – apie suteiktas sveikatos priežiūros paslaugas, duomenys apie taikytą ambulatorinį gydymą, diagnozuotų ligų ar būklių pavadinimai ir kodai, taikyto gydymo būdai, atliktos procedūros ir operacijos (intervencijos), ilgalaikio stebėjimo duomenys, duomenys apie gydymą vaistiniais preparatais ir medicinos pagalbos priemonių taikymą ir kt ,

5.4. Medicininės įrangos, analizatorių, mobiliųjų įrenginių ir kt. generuojami duomenys – diagnostinių tyrimų duomenys, registravimo vizitui pas gydytoją duomenys ir kt.

6. Popieriniai dokumentai, kuriuose yra asmens duomenys, ar jų kopijos, turi būti saugomi tam skirtose patalpose, neturi būti laikomi visiems prieinamoje matomoje vietoje, kur neturintys teisės šiuos duomenis asmenys nekliudomai galėtų su jais susipažinti.

7. Teikiant popieriniuose dokumentuose esančius duomenis būtina įsitikinti, kad duomenų gavėjas turi teisę šiuos duomenis gauti, ar turi tesėtą tikslą (tikslus), ar prašomų duomenų apimtis atitinka šiuos tikslus, ir ar gavėjas užtikrins šių duomenų saugumą. Teikiant popierinius dokumentus, kuriuose yra asmens duomenys, ar šių dokumentų kopijas, būtina įsitikinti, kad neteikiami kitų asmenų duomenys, ir ar teikiamų duomenų apimtis nėra didesnė, nei reikia gavėjo teisėtam tikslui pasiekti. Perteklinius duomenis privalu padaryti nepasiekiamais, pvz., darant išrašus, naudojant pseudonimus, anoniminius duomenis, ar kt.

8. Keičiantis popierinius duomenis (dokumentus) tvarkantiems darbuotojams ar jų įgaliojimams, asmens duomenys (dokumentai, kuriuose yra asmens duomenys, ar jų kopijos) perduodami naujai priimtiems ir (arba) asmens duomenis tvarkyti paskirtiems darbuotojams perdavimo–priėmimo aktu.

9. Elektroniniai asmens duomenys, ar jų kopijos – dokumentai, įskaitant metaduomenis, duomenų bazės, informacinėmis sistemomis, medicininės įrangos tvarkomi asmens duomenys, turi būti saugomi tam skirtose elektroniniams duomenims saugoti skirtose laikmenose, organizuota saugi ir ribota prieiga prie šių duomenų.

10. Saugi prieiga prie elektroninių duomenų reiškia, kad su elektroniniais dokumentais turi teisę dirbti ir susipažinti DIGA įstaigos vadovo paskirti darbuotojai bei informacines sistemas ar duomenų tinklus administruojantys asmenys (DIGA įstaigos darbuotojai ar išorės paslaugų teikėjai), teisę susipažinti su šiais duomenimis turintys asmenys (pacientai ar jų atstovai, paciento šeimos gydytojas ar kt.). Teisė jungtis prie IS ar duomenų tinklų turi būti ribota laike, pvz., einant pareigas, vykdant funkciją, atliekant užduotį, vykdant įsipareigojimus pagal sutartį ar kt., ir ribotos apimties, pvz., įvesti duomenis į IS ar juos keisti, ar naikinti, matyti duomenis, administruoti IS ir tinklus, ar atlikti duomenų tvarkymo veiksmus, kuriuos atlikti šie asmenys yra paskirti.

11. Kiekviena DIGA įstaiga įsipareigoja užtikrinti pacientų ir kitų įstaigos interneto svetainės ir jose esančio turinio naudotojų asmeninės informacijos saugumą ir jų teisės į asmens duomenų apsaugą įgyvendinimą.

12. Vadovaudamasi teisės aktų reikalavimais ir atsižvelgdama interneto svetainės technines galimybes DIGA įstaiga nustato ir šioje svetainėje pateikia informaciją visuomenei kokius duomenis renka apie svetainės naudotoją, kokiais tikslais juos naudoja, kiek laiko duomenis saugo, kokius duomenis perduoda tretiesiems asmenims, kokius slapukus renka, naudoja ir saugoja.

13. Esant techninėms galimybėms rekomenduotina informuoti, kokie duomenys apie interneto svetainės naudotojus yra renkami automatiškai kiekvieną kartą lankantis interneto svetainėje, kokius duomenis įstaiga gauna naudotojams jungiantis prie svetainės ir kokie duomenys yra gaunami iš kitų svetainių ir portalų.

14. Šie reikalavimai netaikomi DIGA įstaigos svetainėje pateikiamoms nuorodoms į kitų asmenų interneto svetaines.

15. Tvarkant elektroninius duomenis būtina įsitikinti, kad yra užtikrintos šio aprašo 7 punkte nurodytos sąlygos ir laikomasi šių taisyklių:

15.1. Specialių kategorijų duomenys teikiami šifruoti arba pseudonimai.

15.2. valdoma prieigos prie duomenų kontrolė;

15.3. fiksuojami prisijungimai prie IS ir kitos įrangos;

15.4. vykdoma fizinė ir loginė prieigos kontrolė;

15.5. vykdoma duomenų integralumo stebėsena ir kontrolė;

15.6. įdiegta apsauga nuo virusų ir kitų kibernetinių atakų ar incidentų;

15.7. užtikrinta interneto svetainės sauga;

15.8. užtikrinta tinklų sauga ir vykdoma stebėsena;

15.9. vykdoma asmens duomenų saugumo pažeidimų stebėsena ir valdymas;

15.10. saugios kompiuterinės darbo vietos, atnaujinama programinė įranga, pvz., antivirusinės programos, ugniasienės ir kt.;

15.11. užtikrinta apsauga nuo neteisėtos fizinės prieigos prie asmens duomenų – išeinant rakinamos patalpos, kuriose įrengtos kompiuterinės darbo vietos, medicininė ar kt. įranga, įrengta gaisro signalizacija ir apribotas asmenų patekimas į šias patalpas ar įgyvendintos kitos duomenų praradimo, atskleidimo, sugadinimo ir pakeitimo riziką atitinkančios ar mažinančios priemonės.

15.12. nuolat vykdomi personalo mokymai.

16. Keičiantis elektroninius duomenis (dokumentus) tvarkantiems darbuotojams ar jų įgaliojimams, prieiga prie duomenų turi būti valdoma – DIGA įstaigoje turi būti naudotojų ir kitų turinčių prieigas prie duomenų asmenų teisių valdymo tvarka.

17. DIGA įstaigos darbuotojas, tvarkantis asmens duomenis, privalo:

17.1. susipažinti su šiuo Aprašu susipažinimo įrodomumą užtikrinančiu būdu, pvz., pažymint dokumentų valdymo IS, pasirašant popieriniame dokumente ar kt.

17.2. pasirašyti įsipareigojimą saugoti asmens duomenų paslaptį, (tokio įsipareigojimo formos pavyzdys pateiktas šio Aprašo priede;

17.3. laikytis šio Aprašo ir įsipareigojimo saugoti asmens duomenų paslaptį nuostatų;

17.4. laikytis konfidencialumo reikalavimų ir neatskleisti tretiesiems asmenims bet kokios su asmens duomenimis susijusios informacijos, su kuria jis susipažino vykdydamas savo funkcijas, nebent tokią informaciją teikti įpareigoja įstatymai arba tokia informacija būtų vieša pagal teisės aktų nuostatas, konfidencialumo pareiga galioja ir pasibaigus darbo santykiams ar kitos sutarties (sutarčių) galiojimui;

17.5. nedelsiant pakeisti slaptažodį (slaptažodžius), jeigu iškilo įsilaužimo į kompiuterinę darbo vietą, ar IS, ar kitą laikmeną grėsmė ar kilo įtarimas, kad slaptažodis (slaptažodžiai) ar kita asmens autentifikavimo arba identifikavimo priemonė tapo žinomas (žinomi) tretiesiems asmenims ir kt.;

17.6. netvarkyti perteklinių duomenų ir nesant būtinumo nedaryti dokumentų su asmens duomenimis kopijų;

17.7. nelaikyti atviros prieigos prie IS, laikmenų su elektroniniais duomenimis ir popierinių dokumentų visiems prieinamoje matomoje vietoje, juos saugoti ir perduoti archyvams teisės aktuose nustatyta tvarka;

17.8. įvykus incidentui, ar įtarus, kad duomenų saugumas nėra užtikrintas ar organizacinės ar techninės priemonės, skirtos asmens duomenų apsaugai, yra nepatikimos, pranešti savo tiesioginiam vadovui ir (arba) arba DIGA įstaigos vadovui bei duomenų apsaugos

pareigūnui, kuris įvertina ir nustato, ar patikimos yra asmens duomenų apsaugai skirtos organizacinės ir techninės priemonės.

18. Įsipareigojimas saugiai tvarkyti asmens duomenis DIGA įstaigos valdomose kompiuterinėse darbo vietose, medicininėje įrangoje ir kt. įrenginiuose užtikrinamas vadovaujantis įstaigos vadovo patvirtintais Europos Sąjungos, Lietuvos Respublikos teisės aktų reikalavimų ir saugos politiką įgyvendinamaisiais dokumentais, pvz., duomenų saugos nuostatais, saugaus elektroninės informacijos tvarkymo taisyklėmis, veiklos tęstinumo valdymo planu, prieigos prie IS teisų suteikimo ir naudotojų administravimo taisyklėmis ir kt.

19. Duomenų apsaugos pareigūnas ne rečiau kaip kartą per 3 (tris) metus atlieka asmens duomenų tvarkymo organizacinių ir techninių apsaugos priemonių auditą (atitikties teisės aktų reikalavimams vertinimą).

20. Šis Aprašas peržiūrimas ne rečiau kaip kartą per 2 (du) metus arba įvykus esminiams asmens duomenų tvarkymo reglamentavimo pokyčiams.

Organizacinių ir techninių asmens duomenų apsaugos priemonių įgyvendinimo aprašo Priedas

ĮSIPAREIGOJIMAS SAUGOTI ASMENS DUOMENŲ PASLAPTĮ

(Rekomenduojama forma)

_____ _____
(sudarymo data) ir (vieta)

Aš, _____,
(vardas, pavardė)

_____,
(įstaigos ir pareigų pavadinimas)

patvirtinu, kad esu susipažinęs su 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentų (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), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, Asociacijos DIGA asmens duomenų tvarkymo privačiose diagnostikos ir gydymo įstaigose elgesio kodeksu, kitais teisės aktais, reglamentuojančiais asmens duomenų apsaugą, ir pasižadu:

1. Saugoti asmens duomenų paslaptį visą darbo/sutarties galiojimo (reikalingą pabraukti) laiką ir pasibaigus darbo santykiams/sutarties galiojimo laikui (reikalingą pabraukti), jeigu šie asmens duomenys nėra paskelbti viešai.

2. Asmens duomenis tvarkyti tik teisėtais tikslais.

3. Asmens duomenis tvarkyti tikslius ir prireikus nuolat atnaujinti, ištaisyti ar papildyti netikslius ar neišsamius duomenis ir (ar) sustabdyti tokių asmens duomenų tvarkymą.

4. Asmens duomenis tvarkyti tik tokios apimties, kuri būtina jiems tvarkyti ir vykdomai funkcijai atlikti, nedaryti tvarkytų duomenų kopijų, jeigu to imperatyviai nenustato teisės aktai.

5. (įskaitant ir nepasilikimą tvarkytų duomenų kopijų, nebent to reikalauja galiojantys teisės aktai).

6. Asmens duomenis tvarkyti taip, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei to reikia tiems tikslams, dėl kurių šie duomenys buvo tvarkomi, įgyvendinti.

7. įgyvendinti teisės aktų, reglamentuojančių asmens duomenų apsaugą, nuostatas, numatančias, kaip asmens duomenis apsaugoti nuo neteisėto tvarkymo ar atskleidimo.

8. Neatskleisti, neperduoti tvarkomų asmens duomenų ir nesudaryti sąlygų jokiomis priemonėmis su jais susipažinti asmenims, neturintiems teisės ar įgaliojimų su jais susipažinti.

9. Pranešti savo tiesioginiam vadovui apie kiekvieną incidentą, dėl kurio gali kilti grėsmė duomenų saugumui.

10. Teisės aktų nustatyta tvarka užtikrinti duomenų subjekto teisių įgyvendinimą.

Pasirašydamas šį įsipareigojimą, patvirtinu, kad suprantu, kad už jo nesilaikymą taikoma atsakomybė.

_____
(parašas ir pasirašymo data)