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)