ASMENS DUOMENŲ TVARKYMO UAB „SK IMPEKS MEDICINOS DIAGNOSTIKOS CENTRAS“ TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1.1. UAB „SK Impeks Medicinos diagnostikos centras“ (toliau – Centras, MDC) Asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja fizinių asmenų duomenų tvarkymą Centre, nustato asmens duomenų tvarkymo tikslus bei pagrindinius asmens duomenų tvarkymo principus, duomenų subjektų teisių įgyvendinimo tvarką, organizacines ir technines duomenų apsaugos priemones, asmens duomenų incidentų valdymo, poveikio duomenų apsaugai atlikimo tvarką, nustato Centro darbuotojų ir kitų asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis.

1.2. Taisyklės parengtos remiantis:

1.2.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau –Įstatymas);

1.2.2. Tarybos Reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva Nr. 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas, BDAR);

1.2.3. Lietuvos Respublikos Sveikatos sistemos įstatymu;

1.2.4. Lietuvos Respublikos Sveikatos priežiūros įstaigų įstatymu;

1.2.5. 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“;

1.2.6. 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“;

1.2.7. 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“;

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

1.3. Taisyklės taikomos tvarkant fizinių asmenų duomenis automatiniu būdu, taip pat ir neautomatiniu būdu tvarkant Asmens duomenų susistemintas rinkmenas (pacientų ligos istorijas ir (arba) kitus susijusius dokumentus, sąrašus, bylas, sąvadus ir kt.).

1.4. Taisyklių privalo laikytis visi Centro darbuotojai (toliau – Darbuotojai), kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino ir tretieji asmenys (sutartiniu su MDC pasirašytų sutarčių ar susitarimų pagrindu) turintys prieigą prie Centre tvarkomų asmens duomenų ar gaunantys asmens duomenis sutartiniais pagrindais (duomenų tvarkytojai, Centro informacinių sistemų priežiūrą vykdantys rangovai ir pan.).

1.5. Šiose Taisyklėse vartojamos sąvokos:

1.5.1. Duomenų valdytojas – UAB „SK Impeks Medicinos diagnostikos centras“;

1.5.2. Duomenų tvarkytojas – UAB „SK Impeks Medicinos diagnostikos centras“ ir (arba) fizinis ar juridinis asmuo Centro vardu sutartiniais pagrindais pagal valdytojo nurodymus tvarkantis Centro valdomus asmens duomenis;

1.5.3. Duomenų naudotojas – duomenų valdytojo padaliniai ir (arba) darbuotojai, fiziniai ar juridiniai asmenys, kurie turi teisę naudoti asmens duomenis numatytoms funkcijoms atlikti;

1.5.4. Duomenų subjektas – Darbuotojai, kandidatai į Darbuotojus, pacientai, kiti fiziniai asmenys kurių asmens duomenis tvarko duomenų valdytojas;

1.5.5. Priežiūros institucija – Valstybinė duomenų apsaugos inspekcija arba kita Lietuvos Respublikos įsteigta institucija, atsakinga už Reglamento taikymo stebėseną.

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

1.5.7. Kitos šiose Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Įstatyme ir (arba) Reglamente.

II. ASMENS DUOMENŲ TVARKYMAS

2.1. Centre asmens duomenys tvarkomi laikantis reikalavimų, numatytų Įstatyme / Reglamente ir poįstatyminiuose teisės aktuose bei šiose Taisyklėse numatytos tvarkos nuostatų, tiek, kiek ji neprieštarauja teisės aktams.

2.2. Visa informacija apie paciento buvimą Centre, jo gydymą, sveikatos būklę, diagnozę, prognozes ir gydymą, taip pat visa kita asmeninio pobūdžio informacija apie pacientą yra konfidenciali ir gali būti teikiama tik įgaliotiems asmenims, esant paciento sutikimui, ar institucijoms be sutikimo, jei tokį teikimą nustato galiojantys teisės aktai.

2.3. Centro įgalioti Darbuotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jei šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja taip pat ir pasibaigus darbo santykiams. Tvarkyti asmens duomenis Darbuotojai gali tik susipažinę su šiomis taisyklėmis bei pasirašę konfidencialumo pasižadėjimą (Taisyklių priedas Nr. 1).

2.4. Centras užtikrina, kad MDC darbuotojai ir tretieji asmenys vykdydami savo funkcijas ir tvarkydami asmens duomenis, laikytųsi šių duomenų tvarkymo principų:

2.4.1. asmens duomenys yra tvarkomi teisėtu, skaidriu ir sąžiningu būdu;

2.4.2. asmens duomenys renkami ir tvarkomi aiškiai apibrėžtais bei teisėtais tikslais,

2.4.3. tvarkomi asmens duomenys yra adekvatūs, tinkami ir tik tokie, kokių reikia siekiant tų tikslų, dėl kurių jie yra tvarkomi. Renkant ir tvarkant Asmens duomenis būtina laikytis tikslingumo, proporcingumo ir duomenų kiekio mažinimo principų, nereikalauti iš pacientų, kitų asmenų pateikti tų duomenų, kurie nėra reikalingi konkrečiam tikslui, nekaupti ir netvarkyti perteklinių duomenų;

2.4.4. asmens duomenys yra tikslūs ir esant būtinybei atnaujinami. Netikslūs ar neišsamūs duomenys turi būti ištaisomi, papildomi, sunaikinami arba sustabdomas jų tvarkymas;

2.4.5. asmens duomenys yra saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi;

2.4.6. asmens duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ir 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.

2.5. Tvarkyti asmens duomenis Centras turi teisę tik jei duomenų subjektas davė sutikimą tvarkyti savo asmens duomenis arba yra kitas tvarkymo teisėtumą pagrindžiantis pagrindas.

2.6. Asmens duomenys turi būti saugomi ne ilgiau nei to reikalauja duomenų tvarkymo tikslai. Kai asmens duomenys nebereikalingi jų tvarkymo tikslais, jie yra sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti išsaugoti archyvavimo tikslais viešojo intereso

labui, mokslinių ar istorinių tyrimų arba statistiniais tikslais, arba kaip nurodyta programoje INV2 „Įrašų, duomenų, informacijos, dokumentų saugojimo laiko nustatymo procedūra“.

2.7. Teisės aktų nustatytais atvejais ir tvarka arba gavus duomenų subjekto sutikimą Centras gali teikti tvarkomus asmens duomenis tretiesiems asmenims.

2.8. Už tinkamą šių Taisyklių įgyvendinimą, asmens duomenų tvarkymo principų laikymąsi ir reikiamų duomenų apsaugos priemonių taikymą atsakingas MDC direktoriaus įgaliotas asmuo.

2.9. Centras, sudarydamas rašytinę asmens duomenų tvarkymo sutartį, gali asmens duomenų tvarkymui valdytojo vardu pasitelkti Duomenų tvarkytoją ar tvarkytojus.

2.10. Sprendimą pasitelkti Duomenų tvarkytoją ir perduoti jam Duomenų tvarkymą priima Centro direktorius;

2.11. Pasitelkiant duomenų tvarkytoją ir perduodant jam Centro vardu tvarkyti asmens duomenis, turi būti užtikrinama, kad pasitelkiamas Duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, užtikrinančias tvarkomų asmens duomenų saugumą bei duomenų subjektų teisių apsaugą, įskaitant bet neapsiribojant šiose Taisyklėse nurodytas duomenų saugumo užtikrinimo priemones.

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

2.13. Centras, pasitelkdamas Duomenų tvarkytoją, sutartyje turi nurodyti, kad Asmens duomenys būtų tvarkomi atsižvelgiant į Asmens duomenų tvarkymą reglamentuojančius teisės aktus, Centro nurodymus, taip pat nurodant, kokius Asmens duomenų tvarkymo veiksmus privalo atlikti Duomenų tvarkytojas Centro vardu, Duomenų tvarkytojo įsipareigojimai, įskaitant, bet neapsiribojant įsipareigojimą laikytis Reglamente įtvirtintų reikalavimų, Duomenų tvarkytojo pareiga ištrinti arba grąžinti Centrui Asmens duomenis, jų kopijas pasibaigus ar nutraukus sutartį ir baigus teikti paslaugas. Šios Taisyklės gali būti pridedamos kaip priedas prie sudaromos sutarties su Duomenų tvarkytoju ir tampa neatskiriama sutarties dalimi.

2.14. Asmens duomenys Centre tvarkomi šiais tikslais:

2.14.1. Darbuotojų asmens duomenys – vidaus administravimo tikslu;

2.14.2. Pacientų asmens duomenys – sveikatos priežiūros paslaugų teikimo tikslu;

2.14.3. Pacientų asmens duomenys – tiesioginės rinkodaros tikslu;

2.14.4. Pacientų, lankytojų, darbuotojų, kitų asmenų asmens duomenys – turto saugumo ir viešosios tvarkos užtikrinimo tikslu (vaizdo stebėjimas).

2.14.5. Kandidatų į Darbuotojus asmens duomenys – Vidaus administravimo tikslu.

2.15. Tvarkant duomenis Taisyklių 2.14.1 p. nurodytu tikslu, yra renkami ir tvarkomi šie Darbuotojų asmens duomenys, kurie yra būtini darbo sutarties su jais sudarymo, vykdymo ir nutraukimo tikslais (šie duomenys yra gaunami tiesiogiai iš Darbuotojų):

2.15.1. vardas, pavardė;

2.15.2. asmens kodas ir gimimo data;

2.15.3. gyvenamoji vieta;

2.15.4. asmeninis telefono numeris ir elektroninio pašto adresas;

2.15.5. banko sąskaitos numeris;

2.15.6. socialinio draudimo numeris;

2.15.7. išsilavinimas;

2.15.8. medikų licencijų Nr. ir turinys;

2.15.9. informacija apie darbuotojo pensijų fondą, kita draudimo informacija (gyvybės draudimas);

2.15.10. automobilio valstybinis numeris;

2.15.11. asmens dokumento numeris;

2.15.12. duomenys apie šeimos narius, kiek tai susiję su darbinių funkcijų, interesų deklaravimo vykdymu, mokesčių mokėjimu, renginių organizavimu.

2.16. Tvarkant duomenis Taisyklių 2.14.2 p. nurodytu tikslu, yra renkami ir tvarkomi šie pacientų asmens duomenys, kurie yra būtini jiems suteiktų gydymo paslaugų administravimo; informacijos apie gydymo eigą suteikimo, apmokėjimo už suteiktas paslaugas tikslais (šie duomenys yra gaunami tiesiogiai iš pacientų, iš 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):

2.16.1. vardas, pavardė;

2.16.2. asmens kodas, demografiniai duomenys (gimimo data, lytis);

2.16.3. gyvenamoji vieta;

2.16.4. telefono numeris, elektroninio pašto adresas;

2.16.5. mokėjimo už suteiktas paslaugas duomenys;

2.16.6. su sveikatos būkle susijusi informacija (ligos ir gyvenimo anamnezė, sveikatos būklės pokyčiai, vaistų naudojimas, fizinės apžiūros duomenys (organizmo būklės požymiai, kūno svoris, ūgis, kraujo spaudimas, pulsas, temperatūra; praeityje persirgtos ligos bei operacijos, praeityje buvusios operacijos bei skirtas gydymas bei kita medicininė anamnezė, alergijos, infekcinių ligų patikra, laboratoriniai organizmo skysčių ir audinių tyrimai, instrumentiniai organų ir sistemų tyrimai, ligų kodai, skaitmeninių tyrimų DICOM vaizdai ir pan.);

2.16.7. išsilavinimas, profesija, darbovietė, jei tai gali būti susiję su paciento ligomis, nedarbingumo pažymėjimais, įvairiomis pažymomis.

2.17. Tvarkant duomenis Taisyklių 2.14.3 p. nurodytu tikslu, yra renkami ir tvarkomi šie pacientų asmens duomenys, kurie yra būtini naujienų sveikatos klausimais ir pasiūlymų teikimo, pacientų apklausų organizavimo tikslais (šie duomenys gaunami tiesiogiai iš pacientų):

2.17.1. vardas, pavardė;

2.17.2. gyvenamoji vietovė;

2.17.3. telefono numeris ir elektroninio pašto adresas

2.17.4. gimimo data ir amžius;

2.17.5. lytis;

2.17.6. šeimyninė padėtis.

2.18. Tvarkant duomenis Taisyklių 2.14.4 p. nurodytu tikslu, siekiant užtikrinti Darbuotojų, pacientų bei lankytojų turto saugumą ir užtikrinti viešąją tvarką, yra renkami ir tvarkomi šie asmens duomenys:

2.18.1. į vaizdo kamerų stebėjimo lauką patenkančių asmenų vaizdas (be garso) – Centro įėjimai, ir teritorija prie jų, automobilių stovėjimo aikštelė registratūra, koridoriai, laiptinės, Centro patalpų perimetras).

2.19. Tvarkant duomenis Taisyklių 2.14.5 p. nurodytu tikslu, yra renkami ir tvarkomi šie kandidatų į Darbuotojus asmens duomenys, kurie yra būtini siekiant įvertinti asmenų, pretenduojančių užimti konkrečias pareigas Centre, tinkamumą tikslu (šie duomenys gaunami tiesiogiai iš kandidatų į Darbuotojus ir įdarbinimo agentūrų):

2.19.1. vardas, pavardė;

2.19.2. asmens kodas ir (arba) gimimo data;

2.19.3. gyvenamoji vieta;

2.19.4. asmeninis telefono numeris ir elektroninio pašto adresas;

2.19.5. išsilavinimas ir papildomi kursai;

2.19.6. buvusios ir esamos darbovietės;

2.19.7. rekomendacijos.

2.20. Medicininės įrangos generuojami vaizdiniai asmens duomenys yra įrangoje ir saugomi DICOM serveriuose arba pačioje įrangoje.

III. DUOMENŲ SUBJEKTŲ TEISĖS

3.1. Duomenų subjektas turi teisę:

3.1.1. žinoti (būti informuotas) apie savo asmens duomenų tvarkymą;

3.1.2. susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi;

3.1.3. reikalauti ištaisyti netikslius duomenis;

3.1.4. reikalauti ištrinti duomenis („teisė būti pamirštam“); dėl asmens sveikatos duomenų ši teisė yra specialiai reglamentuojama, remiantis asmens sveikatos sritį reglamentuojančių įstatymų bei kitų specialiųjų teisės aktų nustatytais tikslais ir tvarka;

3.1.5. reikalauti apriboti asmens duomenų tvarkymą, išskyrus saugojimą, kai duomenys tvarkomi nesilaikant teisės aktų reikalavimų;

3.1.6. gauti susijusius duomenų subjekto pateiktus asmens duomenis susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu (rtf, arba word, arba pdf, arba dicom, arba html);

3.1.7. nesutikti, kad būtų tvarkomi jo asmens duomenys ir atšaukti savo sutikimą tvarkyti asmens duomenis (kai duomenų tvarkymas grindžiamas duomenų subjekto sutikimu);

3.1.8. pateikti skundą priežiūros institucijai.

3.2. Centras privalo visais atvejais, kai iš duomenų subjekto renkami asmens duomenys (išskyrus, kai Duomenų subjektas tokią informaciją jau turi) suteikti Duomenų subjektui šią informaciją:

3.2.1. savo pavadinimą, juridinio asmens kodą ir buveinę;

3.2.2. Duomenų apsaugos pareigūno kontaktinius duomenis, jei toks MDC yra paskirtas;

3.2.3. Asmens duomenų tvarkymo tikslus ir tvarkymo teisinį pagrindą;

3.2.4. Duomenų gavėjus ir jų kategorijas;

3.2.5. Duomenų saugojimo laikotarpį arba kriterijus, taikomus tam laikotarpiui nustatyti;

3.2.6. Duomenų subjektų teises, kuriomis gali pasinaudoti (teisę susipažinti su savo asmens duomenimis ir teisę reikalauti ištaisyti neteisingus, neišsamius, netikslius savo Asmens duomenis, teisę reikalauti juos ištrinti, teisę į duomenų perkeliamumą);

3.2.7. Kitą papildomą informaciją kuri reikalinga, kad būtų užtikrintas teisingas Asmens duomenų tvarkymas nepažeidžiant Duomenų subjekto teisių (duomenų gavimo šaltinus jei duomenys gauti ne iš Duomenų subjekto, kokius savo Asmens duomenis Duomenų subjektas privalo pateikti ir kokios yra duomenų nepateikimo pasekmės).

3.3. Centras užtikrina, kad įgyvendinant savo teisę į duomenų perkeliamumą, Duomenų subjektui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu pateikiami tik tie duomenys, kurie tvarkomi sutarties arba sutikimo pagrindu, jei jie tvarkomi automatizuotomis priemonėmis.

3.4. Centras, privalo sudaryti sąlygas Duomenų subjektui įgyvendinti Taisyklėse 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.

3.5. Duomenų subjektai, norėdami įgyvendinti savo teises, privalo kreiptis į Centrą tiesiogiai el. paštu adresu *kokybe@medcentras.lt*.

3.5.1. Duomenų subjektas, norėdamas susipažinti su Centre tvarkomais jo 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), privalo kreiptis į nurodytą padalinį/darbuotoją tiesiogiai ir pateikti asmens tapatybės dokumentą arba pateikti prašymą elektroniniu būdu, leidžiančiu identifikuoti asmenį;

3.5.2. Centras, gavęs duomenų subjekto prašymą dėl subjekto teisių įgyvendinimo privalo ne vėliau kaip per 20 (dvidešimt) darbo dienų nuo prašymo gavimo dienos pateikti atsakymą. Jei Centras dėl tam tikrų priežasčių atsisako vykdyti gautą prašymą, Duomenų subjektui turi būti pateiktas motyvuotas ir pagrįstas atsakymas dėl jo prašymo nevykdymo;

3.5.3. Prašoma informacija Duomenų subjektui turi būti pateikiama raštu, elektroniniu paštu aiškia ir suprantama forma.

3.6. Jeigu duomenų subjektas, susipažinęs su savo asmens duomenimis, nustato, kad duomenys yra neteisingi, neišsamūs ar netikslūs, gali kreiptis į Centrą, kuris privalo ne vėliau kaip per 5 (penkias) darbo dienas nuo kreipimosi gavimo dienos patikrinti ir ne vėliau kaip per 5 (penkias) darbo dienas nuo nustatymo, kad duomenys neteisingi, neišsamūs, netikslūs nedelsiant ištaisyti neteisingus, neišsamius, netikslius asmens duomenis bei informuoti duomenų gavėjus apie Duomenų subjekto prašymu ištaisytus Asmens duomenis.

3.7. Jeigu duomenų subjektas, susipažinęs su savo duomenimis, nustato, kad jie yra tvarkomi neteisėtai, nesąžiningai ir kreipiasi į Centrą, šis nedelsdamas per protingą laikotarpį privalo patikrinti duomenų tvarkymo teisėtumą, sąžiningumą ir duomenų subjekto rašytiniu prašymu sustabdyti tokių duomenų tvarkymo veiksmus, išskyrus saugojimą. Sustabdžius duomenų tvarkymo veiksmus, atitinkami duomenys saugomi tol, kol bus ištaisyti ar sunaikinti (duomenų

subjekto prašymu arba pasibaigus duomenų saugojimo terminui). Kiti tvarkymo veiksmai su tokiais duomenimis gali būti atliekami tik:

3.7.1. turint tikslą įrodyti aplinkybes, dėl kurių duomenų tvarkymo veiksmai buvo sustabdyti;

3.7.2. jei duomenų subjektas duoda sutikimą toliau tvarkyti savo duomenis;

3.7.3. jei reikia apsaugoti trečiųjų asmenų teises ar teisėtus interesus

3.8. Duomenų subjektui pagal jo prašymą Centras kartą per kalendorinius metus duomenis teikia neatlygintinai. Duomenų subjektui nepagrįstai pakartotinai teikiant prašymus pateikti informaciją, išrašus, dokumentus dažniau nei kartą per kalendorinius metus, Centras gali atsisakyti teikti informaciją, jei ji jau buvo pateikta, arba informacijos teikimas gali būti apmokestintas atsižvelgiant į Centro nustatytus dokumentų, duomenų pateikimo, kopijavimo ir pan. įkainius.

IV. ASMENS DUOMENŲ APSAUGOS PAREIGŪNAS

4.1. Centras vykdydamas savo funkcijas, tvarko specialiųjų kategorijų asmens duomenis – pacientų sveikatos duomenis dideliu mastu, be ko būtų neįmanomas tinkamas Centro, kaip medicinos įstaigos, funkcionavimas ir sveikatos priežiūros paslaugų teikimas.

4.2. Duomenų valdytojas skiria Duomenų apsaugos pareigūną (toliau – DAP), kuriuo gali būti paskirtas vienas iš esamų Centro darbuotojų, naujas darbuotojas arba asmuo, su kuriuo būtų sudaroma paslaugų teikimo sutartis.

4.3. Skiriant DAP turi būti atsižvelgta ir įvertinta tai, kad:

4.3.1. asmuo turėtų tinkamų duomenų apsaugos teisės ir praktikos ekspertinių žinių bei reikiamų gebėjimų atlikti DAP užduotis;

4.3.2. DAP būtų įtraukiamas į visų su asmens duomenų apsauga ir privatumu susijusių klausimų nagrinėjimą Centre;

4.3.3. DAP, vykdydamas užduotis veiktų nepriklausomai ir būtų tiesiogiai pavaldus Centro vadovybei (direktoriui arba vienam iš direktoriaus pavaduotojų) arba būtų kokybės ir medicininio audito skyriaus darbuotojas;

4.3.4. DAP neturėtų jokių kitų pareigų ar neatliktų funkcijų, kurios galėtų sukelti interesų konfliktą su jo atliekamomis DAP funkcijomis;

4.3.5. būtų užtikrinta, kad Centras skiria DAP pakankamus resursus (finansinius ir žmogiškuosius) jo funkcijų tinkamam atlikimui.

4.4. Vykdydamas savo funkcijas DAP privalo:

4.4.1. informuoti duomenų valdytoją ir Darbuotojus apie jų prievoles ir pareigas pagal Reglamentą ir kitus asmens duomenų teisinę apsaugą reglamentuojančius teisės aktus bei užtikrinti, kad Centre vykdomas Asmens duomenų tvarkymas atitiktų šių teisės aktų reikalavimus, tinkamai įvertinant duomenų tvarkymo operacijas, duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, potencialų pavojų;

4.4.2. konsultuoti duomenų valdytoją ir Darbuotojus asmens duomenų tvarkymo klausimais, didinti darbuotojų informuotumą ir supratimą organizuojant mokymus asmens duomenų apsaugos klausimais;

4.4.3. stebėti, kaip laikomasi Reglamento ir kitų, asmens duomenų teisinę apsaugą reglamentuojančių teisės aktų reikalavimų, šių Taisyklių, kitų vidinių dokumentų, susijusių su Asmens duomenų apsauga;

4.4.4. konsultuoti ir stebėti, kaip atliekamas poveikio duomenų apsaugai vertinimas;

4.4.5. Informuoti Centro vadovybę apie bet kokius nustatytus asmens duomenų apsaugos neatitikimus ir (arba) pažeidimus;

4.4.6. būti kontaktiniu asmeniu asmens duomenų apsaugos klausimais ir bendradarbiauti su Priežiūros institucija;

4.5. DAP privalo tvarkyti bei saugoti su Asmens duomenų tvarkymu susijusios veiklos duomenis (toliau – Veiklos įrašus), kurie nurodytų bent šią minimalią ir aktualią informaciją:

4.5.1. Centro rekvizitus ir DAP kontaktinius duomenis;

4.5.2. Duomenų subjektų kategorijas ir jų trumpus aprašymus;

4.5.3. Duomenų gavėjų kontaktus;

4.5.4. Duomenų tvarkytojų kontaktus;

4.5.5. Asmens duomenų tvarkymo, saugojimo, sunaikinimo terminus ir/arba kriterijus, pagal kuriuos Asmens duomenys yra saugomi Centre;

4.5.6. Techninių, organizacinių saugumo priemonių aprašymą.

4.6. Už šių Taisyklių 5.5 punkte nurodytų Veiklos įrašų pateikimą priežiūros institucijai (esant jos prašymui / reikalavimui) atsako DAP.

4.7. Duomenų valdytojas, paskyręs DAP arba sudaręs su juo paslaugų teikimo sutartį, privalo per protingą terminą nuo jo paskyrimo ar paslaugų sutarties sudarymo tinkamai paskelbti Duomenų subjektams bei pranešti Priežiūros institucijai.

V. POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

5.1. Centrui vykdant ar planuojant pradėti vykdyti naują duomenų tvarkymo operaciją, jei dėl duomenų tvarkymo rūšies, kai naudojamos naujos technologijos, taip pat atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus duomenų subjektų teisėms bei laisvėms gali kilti didelis pavojus, privaloma atlikti poveikio duomenų apsaugai vertinimą. Poveikio duomenų apsaugai vertinimas gali būti atliekamas ir esamoms duomenų tvarkymo operacijoms, jei dėl vykdomo duomenų tvarkymo ar reikšmingų pokyčių gali kilti didelis pavojus duomenų subjektų teisėms bei laisvėms.

5.2. Poveikio duomenų apsaugai vertinimas turi būti atliekamas jei:

5.2.1. vykdomas ar planuojamas duomenų tvarkymas keltų didelį pavojų duomenų subjektų teisėms ir laisvėms (pvz., jei 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 specialiųjų kategorijų duomenys, būtų pradėti naudoti nauji technologiniai sprendimai (veido atpažinimo sistemos ir pan.);

5.2.2. 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;

5.2.3. būtų pradėtas vykdyti sistemingas vaizdo stebėjimas dideliu mastu;

5.2.4. būtų pradėti tvarkyti ypatingi Asmens duomenys dideliu mastu.

5.3. Jei poveikio duomenų apsaugai vertinimo metu nustatoma, kad Duomenų subjektų teisėms ir laisvėms gali kilti didelis pavojus, Centras privalo konsultuotis su Priežiūros institucija dėl tinkamų asmens duomenų saugumo priemonių taikymo.

5.4. Poveikio duomenų apsaugai vertinimo metu turi būti nustatoma:

5.4.1. Kokia duomenų tvarkymo operacija vykdoma/planuojama vykdyti, jos tikslas;

5.4.2. Vykdomos ar planuojamos duomenų tvarkymo operacijos reikalingumas ir proporcingumas lyginant su tikslais;

5.4.3. Koks gali būti poveikis Duomenų subjektams;

5.4.4. Kokios taikomos ar planuojamos saugumo užtikrinimo priemonės.

5.5. Poveikio duomenų apsaugai vertinimas gali būti atliekamas ir kitais šiame skyriuje neaptartais atvejais, duomenų valdytojo sprendimu ar esant DAP priežiūros institucijos rekomendacijoms.

5.6. Poveikio duomenų apsaugai vertinimas, būtų tinkamai dokumentuotas ir saugomas Centre bei, esant reikalui, pateikiamas priežiūros institucijai.

VI. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI

6.1. Asmens duomenų saugumo pažeidimais laikomi incidentai, kai dėl neatsargumo ar tyčia yra:

6.1.1. Pažeidžiamas tvarkomų asmens duomenų konfidencialumas (asmens duomenys atskleidžiami tokios teisės neturintiems asmenims, pvz., asmens duomenys buvo atskleisti ir jie tapo prieinami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant, kt.);

6.1.2. Pažeidžiamas tvarkomų asmens duomenų vientisumas (asmens duomenys yra pakeičiami ar prarandami ir negalima jų atkurti, pvz., prarastos pacientų sveikatos kortelės, turima tik dalis atsarginių kopijų, dėl ko neįmanoma jos pilnai „atkurti“);

6.1.3. Pažeidžiamas tvarkomų asmens duomenų prieinamumas (asmens duomenys yra sunaikinami, pvz., asmens duomenys prarasti ir neturima atsarginių kopijų).

6.1.4. Atvejai, kai dėl neteisėtų ar neatsargių Asmens duomenų saugumo incidentu yra laikomas pažeidimas, dėl kurio tyčia ar dėl neatsargumo Centro tvarkomi asmens duomenys.

6.2. Darbuotojai ir kiti asmenys, teisėtai tvarkantys asmens duomenis, pastebėję šiose Taisyklėse ir kituose teisės aktuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias asmens duomenų saugos užtikrinimo priemones, privalo nedelsdami informuoti DAP arba bet kurį direktoriaus pavaduotoją, kurio pavaldume šiame punkte paminėti darbuotojai yra pagal centro struktūrinę schemą.

6.3. Jei dėl įvykusio incidento kyla pavojus Duomenų subjektų teisėms ir laisvėms, DAP ar kitas Centro direktoriaus paskirtas darbuotojas privalo nedelsiant, bet ne vėliau kaip per 72 val. nuo asmens duomenų saugumo pažeidimo nustatymo ar sužinojimo momento, pranešti Priežiūros institucijai apie įvykusį incidentą.

6.4. Jei dėl incidento gali kilti didelis pavojus Duomenų subjektų teisėms ir laisvėms, informacija apie įvykusį incidentą nedelsiant taip pat turi būti pateikta Duomenų subjektams. Nesant galimybės informuoti visus Duomenų subjektus dėl jų didelio kiekio ar kitų priežasčių, DAP kartu su Centro direktoriumi apsvarsto ir priima sprendimą šią informaciją pateikti per Centro internetinį tinklalapį ir (arba) visuomenės informavimo kanalus (spauda, televizija, radijas ir kt.).

6.5. Pranešime apie asmens duomenų saugumo pažeidimą Priežiūros institucijai ir Duomenų subjektams turi būti:

6.5.1. aprašytas asmens duomenų incidento pobūdis, nurodant Duomenų subjektų kategorijas ir apytikslį skaičių, kurių asmens teisės ir laisvės galėjo būti pažeistos;

6.5.2. DAP ar kito atsakingo darbuotojo, galinčio suteikti informaciją, kontaktai;

6.5.3. aprašytos tikėtinos incidento pasekmės bei priemonės, kurių ėmėsi ar rekomenduoja imtis Centras, kad būtų pašalintas asmens duomenų saugumo pažeidimas ir neigiamos pasekmės, susijusios su įvykusiu incidentu.

6.6. Įvykus asmens duomenų saugumo pažeidimui ar incidentui, DAP ar kitas atsakingas darbuotojas, informuoja Darbuotojus ir kitus asmenis apie įvykusį pažeidimą ir teikia atitinkamas instrukcijas ar rekomendacijas konkretiems Darbuotojams dėl jų pareigų, funkcijų atlikimo, susijusio su asmens duomenų incidento valdymu.

6.7. DAP ar kitas paskirtas atsakingas darbuotojas privalo užtikrinti, kad visi asmens duomenų saugumo pažeidimai ir incidentai, įskaitant ir tuos, dėl kurių nevykdoma informavimo pareiga kaip aptarta šiame Taisyklių skyriuje, būtų tinkamai dokumentuoti ir saugomi.

6.8. DAP ar kitas paskirtas atsakingas darbuotojas turi įvertinti ir išanalizuoti įvykusį asmens duomenų saugumo pažeidimą ar incidentą bei, esant poreikiui, imtis reikiamų papildomų priemonių, siekiant užkirsti kelią panašiems pažeidimams ar incidentams ateityje.

VII. ORGANIZACINĖS IR TECHNINĖS ASMENS DUOMENŲ APSAUGOS PRIEMONĖS

7.1. Atsižvelgiant į Centro tvarkomų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, automatiniu būdu tvarkomi asmens duomenys priskiriami trečiam saugumo lygiui, nurodytą . VDAI direktoriaus 2008-11-12 įsakyme Nr. 1T-71(1.12)

7.2. Siekiant apsaugoti Asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo turi būti taikomos organizacinės ir techninės asmens duomenų saugumo priemonės, užtikrinančios ne žemesnį nei trečiąjį asmens duomenų saugumo lygį:

7.2.1. Darbuotojai automatiniu būdu tvarkyti Asmens duomenis gali tik po to, kai jiems, vadovaujantis MDC programa INV 1 „Informacijos privatumo, konfidencialumo ir saugumo užtikrinimo procedūra“, suteikiamos prieigos teisės prie atitinkamos informacinės sistemos MedIS ir joje saugomų asmens duomenų. Prieiga prie Asmens duomenų gali būti suteikta tik tam asmeniui, kuriam Asmens duomenys yra reikalingi jo funkcijoms vykdyti. Darbo santykiams pasibaigus, Darbuotojui suteiktos prieigos teisės turi būti nedelsiant panaikinamos.

7.2.2. Darbuotojai ir kiti asmenys, kuriems suteikiama prieiga prie asmens duomenų, privalo pasirašyti Konfidencialumo pasižadėjimą (Taisyklių priedas Nr. 1) ir privalo laikyti paslaptyje bet kokius Darbuotojų, pacientų ar kitų asmenų asmens duomenis, kuriuos jie sužinojo vykdydami savo pareigas. Ši pareiga išlieka galioti ir nutraukus ar pasibaigus darbo ar sutartiniams santykiams su Centru.

7.2.3. Prieiga prie asmens duomenų turi būti užtikrinama slaptažodžiais arba kitomis priemonėmis, užtikrinančiomis tinkamą asmenų autentifikavimą.

7.2.4. Slaptažodžiams taikomi reikalavimai:

7.2.4.1. turi būti unikalūs ir sudaryti iš ne mažiau kaip 8 ženklų naudojant didžiąsias ir mažąsias raides, skaičius ir specialiuosius simbolius;

7.2.4.2. slaptažodžiams neturi būti naudojama lengvai nuspėjama informacija;

7.2.4.3. pirmo prisijungimo metu sistema turi reikalauti naudotojo pasikeisti slaptažodį, taip pat slaptažodžiai turi būti keičiami periodiškai ne rečiau kaip kartą per 120 (vienas šimtas dvidešimt) dienų arba jei kilo įtarimas, jog slaptažodį galėjo sužinoti pašaliniai asmenys.

7.2.5. Turi būti užtikrinamas patalpų, kuriose saugoma svarbiausia kompiuterinė įranga ir asmens duomenys, fizinis saugumas. Patekimas į tokias patalpas turi būti kontroliuojamas, užtikrinant, kad į patalpas patektų tik įgalioti asmenys.

7.2.6. Turi būti užtikrinama centralizuotai valdomos kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (antivirusinės programinės įrangos naudojimas), kuri turi būti periodiškai atnaujinama.

7.2.7. Kompiuterinės darbo vietose turi būti naudojamos ekrano užsklandos su slaptažodžiu, kurios automatiškai įsijungia ne vėliau kaip po 60 minučių Darbuotojui neatliekant veiksmų.

7.2.8. Darbuotojui neatliekant jokių veiksmų informacinėje sistemoje ilgiau nei 60 minučių, kurioje saugomi asmens duomenys, informacinės sistemos taikomoji programinė įranga turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartotinai patvirtinus savo tapatybę.

7.2.9. Vidinis Centro kompiuterių tinklas turi būti apsaugotas nuo neteisėto prisijungimo naudojant ugniasienę.

7.2.10. Turi būti vykdoma prieigos prie asmens duomenų kontrolė:

7.2.10.1. Fiksuojamos ir kontroliuojamos registravimosi bei prieigos teisių gavimo pastangos;

7.2.10.2. Fiksuojami prisijungimų prie asmens duomenų įrašai: bylos prie kurių jungtasi ir su asmens duomenimis atlikti veiksmai (peržiūra, įvedimas, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai), kurie turi būti saugomi ne trumpiau nei 1 metus;

7.2.10.3. Prisijungimų prie duomenų bazės žurnaliniai įrašai (angl. *Logs*) turi būti peržiūrimi ne rečiau kaip kartą per mėnesį ir duomenų valdytojui pateikiamos peržiūros ataskaitos.

7.2.11. Perduodant asmens duomenis išoriniais duomenų tinklais turi būti naudojami saugūs protokolai ir (arba) slaptažodžiai;

7.2.12. Asmens duomenys, esantys išorinėse laikmenose ir elektroniniame pašte turi būti apsaugoti naudojant tinkamas priemones (pvz., šifravimą, dvigubo kodo tapatybės nustatymą ir pan.);

7.2.13. Turi būti periodiškai atliekamas tvarkomų asmens duomenų atsarginis kopijavimas. Atsarginės duomenų kopijos turi būti saugomos kitoje patalpoje nei veikianti duomenų bazė, kurios informacija buvo išsaugota. Asmens duomenys atsarginėse kopijose ir išorinėse laikmenose turi būti šifruojami;

7.2.14. Ne rečiau kaip kartą per metus turi būti atliekami atsarginių kopijų bandymai – patikrinama avarinio asmens duomenų atkūrimo tvarka atliekant praktinius bandymus siekiant įsitikinti, kad informacija gali būti sėkmingai atkurta;

7.2.15. Informacinių sistemų testavimas turi būti vykdomas atskiroje testavimo aplinkoje, atskirtoje nuo realios. Testavimo metu neturi būti naudojami realūs asmens duomenys, išskyrus būtinus atvejus. Jei testavimui naudojami realūs asmens duomenys, turi būti naudojamos papildomos organizacinės ir techninės priemonės, užtikrinančios testavimo metu naudojamų asmens duomenų saugumą;

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

7.2.17. ne rečiau kaip kartą per 1 (vienerius) metus turi būti atliekamas asmens duomenų tvarkymo keliamos rizikos vertinimas ir, atsižvelgiant į rizikos vertinimo rezultatus, diegiamos reikiamos asmens duomenų saugumo priemonės;

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

7.2.19. Darbuotojai, vykdantys Duomenų subjekto duomenų tvarkymo funkcijas, turi užkirsti kelią atsitiktiniam ar neteisėtam asmens duomenų tvarkymui, turi tinkamai saugoti dokumentus (pvz., vengiant nereikalingų kopijų su Duomenų subjekto asmens duomenimis kaupimo ir kt.), t.y. laikytis „švaraus stalo politikos“ (2017-11-27 direktoriaus įsakymas Nr.1-1-11-93A). Dokumentų kopijos, kuriose nurodomi Duomenų subjekto duomenys, turi būti sunaikinamos tokiu būdu, kad šių dokumentų nebūtų galima atkurti;

7.2.20. Nesant būtinybės, rinkmenos su pacientų, kitų interesantų duomenimis neturi būti kopijuojamos skaitmeniniu būdu, t. y. kuriamos asmens duomenų kopijos kompiuterinėse darbo vietose, diskuose, nešiojamose laikmenose, nuotolinėse rinkmenų talpyklose ir pan.;

7.2.21. Asmens duomenų paieškos užklausoje turi būti nurodomas Asmens duomenų naudojimo tikslas;

7.2.22. Darbuotojai privalo organizuoti ir vykdyti savo darbus taip, kad kiek įmanoma apribotų galimybę kitiems asmenims (kitiems Darbuotojams, praktikantams, savanorišką praktiką atliekantiems ar kitiems tretiesiems asmenims) sužinoti tvarkomus asmens duomenis:

7.2.22.1. Darbo metu tvarkant asmens duomenis imtis reikiamų priemonių, kad su asmens duomenimis nebūtų galima susipažinti tokios teisės neturintiems asmenims (užtikrinti, kad asmenys negalėtų perskaityti informacijos iš kompiuterio monitoriaus ar popierinių dokumentų, spausdintuvuose paliktų dokumentų);

7.2.22.2. Nepaliekant dokumentų su tvarkomais Asmens duomenimis ar kompiuterio, kuriuo naudojantis galima prisijungti prie sistemų, kuriose saugomi asmens duomenys, be priežiūros taip, kad juose esančią informaciją galėtų perskaityti asmenys, neturintys teisės dirbti su konkrečiais Asmens duomenimis;

7.2.22.3. Pasitraukiant iš darbo vietos užtikrinti, kad pašaliniai asmenys neturi galimybės sužinoti asmens duomenų ar kitos informacijos (atsijungti nuo sistemų, įjungti ekrano užsklandą, dokumentus, kuriuose yra asmens duomenys, padėti į saugią vietą ir pan.).

VIII. BAIGIAMOSIOS NUOSTATOS

8.1. Su šiomis Taisyklėmis privaloma susipažinti visus Darbuotojus ir kitus asmenis, teisėtai tvarkančius asmens duomenis.

8.2. Darbuotojais ir kiti asmenys už asmens duomenų saugumo pažeidimus atsako teisės aktų nustatyta tvarka.

8.3. Taisyklės skelbiamos Centro internetiniame tinklalapyje ir (arba) Intranete.

8.4. Taisyklės turi būti peržiūrimos ne rečiau kaip kartą per metus arba įvykus asmens duomenų saugumo pažeidimui ar reikšmingiems pokyčiams Centro struktūroje ir, esant būtinybei, atnaujinamos. Už Taisyklių peržiūrą atsakingas IT padalinio vadovas ir DAP.