PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2013 m. 2013 m. 021 d.
įsakymu Nr. V - 70

ŽMOGAUS AUDINIŲ, LĄSTELIŲ IR ORGANŲ DONORŲ BEI RECIPIENTŲ REGISTRO SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato saugų Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro (toliau – Registras) elektroninės informacijos tvarkymą, reikalavimus saugos priemonėms ir Registro funkcionavimui reikalingoms paslaugoms vykdyti ir yra privalomos visiems Registro naudotojams.

2. Taisyklės parengtos vadovaujantis šiais teisės aktais:

2.1. Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891);

2.2. Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070);

2.3. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866);

2.4. Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro duomenų saugos nuostatais, patvirtintais Lietuvos Respublikos sveikatos ministro 2012 m. rugsėjo 28 d. įsakymu Nr. V-920 (Žin., 2012, Nr. 116-5888);

2.5. kitais teisės aktais, reglamentuojančiais saugų duomenų tvarkymą.

3. Taisyklėse vartojamos sąvokos atitinka Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, Saugos dokumentų turinio gairėse, kituose elektroninės informacijos tvarkymą reglamentuojančiuose teisės aktuose, Lietuvos standartuose LST ISO/IEC 27002:2009 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas“ ir LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ apibrėžtas sąvokas.

4. Elektroninės informacijos savybės:

4.1. konfidencialumas – su Registre tvarkoma elektronine informacija gali susipažinti tik tam įgalioti asmenys;

4.2. vientisumas – elektroninė informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta;

4.3. prieinamumas – elektroninė informacija gali būti tvarkoma reikiamu metu.

5. Registre saugomi ir apdorojami Žmogaus audinių, ląstelių ir organų donorų bei recipientų duomenys.

6. Registre esanti elektroninė informacija skirstoma į kategorijas:

6.1. duomenys apie asmenis, pareiškusius sutikimą (nesutikimą), kad jų audiniai ir (ar) organai po jų mirties būtų panaudoti transplantacijai;

6.2. duomenys apie gyvus donorus;

6.3. duomenys apie mirusius donorus;

6.4. duomenys apie recipientus;

6.5. duomenys ir informacija apie audinių, ląstelių, organų paėmimą, transplantaciją ir šalinimą;

6.6. Registro objekto registravimo Registre duomenys ir informacija;

6.7. duomenų ir informacijos įrašymo bei keitimo datos;

6.8. duomenų teikėjo, pateikusio duomenis ir informaciją, duomenys;

6.9. už duomenų ir informacijos teisingumą atsakingo asmens identifikavimo duomenys – vardas, pavardė.

7. Taisyklės yra privalomos visiems Registro naudotojams.

8. Už Taisyklių įgyvendinimą ir jų laikymosi kontrolę atsakingas Registro duomenų valdymo įgaliotinis.

9. Už Registro elektroninės informacijos tvarkymą atsakingi:

9.1. Nacionalinio transplantacijos biuro prie Sveikatos apsaugos ministerijos (toliau – Biuras) Registro administratorius;

9.2. registruoti Registro naudotojai.

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

10. Registro kompiuterinės įrangos saugos priemonės:

10.1. siekiant užtikrinti Registro patikimumą bei jame saugomų ir apdorojamų duomenų konfidencialumą, vientisumą ir prieinamumą, turi būti įdiegti duomenų bazių ir rinkmenų tarnybinių stočių klasteriai, viena kitą dubliuojančios užkardos, keli interneto prieigos serveriai, dubliuoti tinklo komutatoriai, patikima duomenų saugykla ir rezervinio kopijavimo įranga;

10.2. visa Registro kompiuterių aparatinė įranga privalo turėti šios įrangos gamintojų garantinį arba pratęstą pogarantinį aptarnavimą;

10.3. Registro kompiuterių aparatinė įranga gali būti keičiama tik gavus Biuro direktoriaus leidimą;

10.4. visi Registro kompiuterių aparatinės įrangos gedimai ir keitimai turi būti registruojami žurnale;

10.5. Registro programinė sistema turi perspėti Registro administratorius, kai tarnybinėse stotyse sumažėja iki nustatytos pavojingos ribos laisvos operatyviosios atminties ar vietos diske (diskuose) ar duomenų saugykloje, ilgą laiką stipriai apkraunamas centrinis procesorius ar tinklo sąsaja.

11. Registro sisteminės ir taikomosios programinės įrangos saugos priemonės:

11.1. Registre gali būti naudojama tik legali ir įteisinta sisteminė ir taikomoji programinė įranga;

11.2. sisteminės ir taikomosios programinės įrangos apsaugai nuo virusų ir kitų kenkėjiškų programų Registre turi būti naudojama specializuota, nuolat automatiškai atnaujinama programinė įranga;

11.3. kiekvienas Registro naudotojas ir Registro administratorius turi būti unikaliai identifikuojamas, todėl visiems Registro naudotojams ir Registro administratoriams, vadovaujantis Lietuvos Respublikos sveikatos apsaugos ministro patvirtintose Žmogaus audinių, ląstelių ir organų donorų ir recipientų registro naudotojų administravimo taisyklėse nustatyta tvarka, suteikiamas Registro naudotojo ar Registro administratoriaus vardas bei nustatomi Registro naudotojo ar Registro administratoriaus tapatybę patvirtinančių slaptažodžių reikalavimai;

11.4. Registro priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą Registro administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti Registro naudotojo funkcijų;

11.5. slaptažodžiai, suteikiantys teisę administruoti Registrą ir Registro naudotojus, žinomi tik Registro administratoriui. Kad nesant Registro administratoriaus Registrą galėtų administruoti jį pavaduojantis darbuotojas, Registro administratoriaus slaptažodžiai saugomi Biuro direktoriaus seife. Perėmus Registro administravimą pagrindiniam Registro administratoriui, Registro administratoriaus slaptažodį privaloma pakeisti nauju;

11.6. Registro naudotojo teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai Registro naudotojas atostogauja, vykdomas jo veiklos tyrimas ir pan.;

11.7. Registro naudotojo teisė naudotis Registro duomenimis turi būti panaikinta pasibaigus tarnybos (darbo) santykiams;

11.8. Registro naudotojui baigus darbą, turi būti imamasi priemonių, kad su Registre saugomais duomenimis negalėtų susipažinti pašaliniai asmenys:

11.8.1. atsijungiama nuo Registro;

11.8.2. įjungiama ekrano užsklanda su slaptažodžiu;

11.8.3. dokumentai ir laikmenos padedami į pašaliniams asmenims neprieinamą vietą ir pan.;

11.9. Registro naudotojui neatliekant jokių veiksmų, Registras turi taip užsirakinti, kad toliau juo naudotis būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

11.10. Registro sisteminės ir taikomosios programinės įrangos keitimas ir atnaujinimas gali būti atliekami gavus Biuro direktoriaus leidimą, vadovaujantis Informacinės sistemos funkcijų pokyčių valdymo procedūra;

11.11. visi Registro kompiuterių sisteminės ir taikomosios programinės įrangos keitimai bei atnaujinimai turi būti registruojami žurnale.

11.12. Programinės įrangos testavimas atliekamas naudojant atskirą tam skirtą testavimo aplinką.

12. Duomenų perdavimo tinklais saugumo užtikrinimo priemonės:

12.1. siekiant užtikrinti elektroninės informacijos konfidencialumą ir vientisumą, šios informacijos teikimas bei priėmimas turi būti vykdomas naudojant Saugų valstybinį duomenų perdavimo tinklą arba kitą saugų šifruotą duomenų perdavimo kanalą;

12.2. Registro duomenys nuo grėsmių iš interneto turi būti atskirti užkardomis;

12.3. viešai prieinama Registro elektroninė informacija turi būti saugoma atskirame kompiuterių potinklyje – vadinamojoje demilitarizuotoje zonoje.

13. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

13.1. patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonių; vykdoma gaisro gesinimo patikra;

13.2. patalpos atskirtos nuo bendrojo naudojimo patalpų, asmenys, nesusiję su Registro tvarkymu, patekti į šias patalpas gali tik lydimi Registro administratoriaus;

13.3. veikia patekimo į patalpas kontrolės sistema;

13.4. techninė įranga įnešama ir išnešama iš patalpų tik Registro saugos įgaliotiniui leidus;

13.5. ryšių kabeliai apsaugoti nuo pažeidimo ir neteisėto prisijungimo prie jų;

13.6. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos;

13.7. patalpų durys šarvuotos ir apsaugotos dviem skirtingos konstrukcijos spynomis;

13.8. patalpose įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

13.9. į Registro duomenų centrą gali patekti tik tie asmenys, kuriems tai būtina atliekant darbo funkcijas;

13.10. Biuro direktorius įsakymu tvirtina darbuotojų, kuriems išduodamos kortelės, leidžiančios patekti į Registro duomenų centrą, sąrašą.

14. Registro tarnybinių stočių įvykių žurnaluose turi būti registruojami ir ne mažiau kaip 1 (vienus) metus saugomi duomenys (nurodant įvykio laiką ir Registro naudotojo identifikatorių) apie:

14.1. Registro įjungimą ir išjungimą;

14.2. sėkmingus ir nesėkmingus bandymus registruotis Registre;

14.3. bandymus prieiti prie Registro informacinių išteklių;

14.4. kitus Registro saugomų ir apdorojamų duomenų saugai svarbius įvykius.

15. Registro tarnybinių stočių įvykių žurnalai turi būti analizuojami kiekvieną darbo dieną.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

16. Registro duomenų keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

16.1 Registro duomenų keitimą, atnaujinimą, įvedimą ir naikinimą gali atlikti tik tokią teisę turintys autorizuoti Registro naudotojai;

16.2. Registre saugomi ir apdorojami duomenys įvedami, atnaujinami, keičiami ir naikinami vadovaujantis Lietuvos Respublikos žmogaus audinių, ląstelių ir organų donorų bei recipientų registro nuostatais, patvirtintais Lietuvos Respublikos Vyriausybės 2000 m. rugpjūčio 23 d. nutarimu Nr. 961 (Žin., 2000, Nr. 72-2230; 2012, 115-5834).

17. Registro naudotojų veiksmų registravimo tvarka: siekiant nustatyti neteisėtus veiksmus su Registre saugomais ir apdorojamais duomenimis bei šių duomenų vientisumo pažeidimus, Registro naudotojų veiksmai, jų darbo su Registru laikas turi būti automatiškai registruojami elektroniniuose žurnaluose.

18. Registro duomenų atsarginių kopijų darymo ir saugojimo tvarką, duomenų atkūrimo iš atsarginių duomenų kopijų metodus ir tvarką nustato, asmenis, atsakingus už atsarginių kopijų darymą, jų saugojimą, duomenų atkūrimą bei šių procesų kontrolę, skiria Biuro direktorius.

19. Duomenų perkėlimo ir teikimo kitoms informacinėms sistemoms bei duomenų gavimo iš jų tvarka: Registro duomenys kitiems registrams teikiami ir gaunami iš jų su šių registrų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, apimtimi, reguliarumu ir terminais.

20. Duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau vadinama – Neleidžiama veikla) nustatymas:

20.1. Registro administratoriai privalo naudoti visas įmanomas aparatines, programines ir administracines priemones, skirtas apsisaugoti nuo Neleidžiamos veiklos;

20.2. siekiant patikrinti, ar su Registro duomenimis nėra vykdoma Neleidžiama veikla, Registro administratoriai kiekvieną darbo dieną privalo peržiūrėti Registro programinės įrangos elektroniniuose žurnaluose sukauptus atitinkamus įrašus;

20.3. kilus įtarimui, kad su Registru ir jame saugomais ir apdorojamais duomenimis yra vykdoma Neleidžiama veikla, Registro administratoriai nedelsdami privalo apie tai informuoti Registro saugos įgaliotinį;

20.4. Registro saugos įgaliotinis, gavęs pranešimą apie Neleidžiamą veiklą, inicijuoja saugos incidentų valdymo procedūros vykdymą.

IV. REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

21. Registro priežiūros paslaugų tiekėjams suteikiami tokie prieigos prie Registro lygiai ir sąlygos, kurie reikalingi ir pakankami priežiūros paslaugoms pagal nustatytus reikalavimus atlikti.

22. Registro priežiūros paslaugų reikalavimai nurodyti Biuro direktoriaus patvirtintoje Informacinių sistemų priežiūros paslaugos techninėje specifikacijoje.

V. BAIGIAMOSIOS NUOSTATOS

23. Šios Taisyklės gali būti keičiamos teisės aktų nustatyta tvarka.

24. Asmenys, pažeidę šių Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.
