PATVIRTINTA
Lietuvos Respublikos
sveikatos apsaugos ministro
2012 m. rugpjūčio 8 d. įsakymu Nr. V-761

ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Informacijos tvarkymo taisyklės) tikslas – nustatyti būtinus elektroninės informacijos techninius saugos reikalavimus Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinei sistemai.

2. Informacijos tvarkymo taisyklės privalomos Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (toliau – ESPBI IS) naudotojams ir administratoriams. Už Informacijos tvarkymo taisyklių įgyvendinimo organizavimą ir kontrolę atsako ESPBI IS vyriausiasis saugos įgaliotinis.

3. Informacijos tvarkymo taisyklėse vartojamos sąvokos:

RC ESPBI IS administratorius – valstybės įmonės Registrų centro darbuotojas, atliekantis ESPBI IS administratoriaus funkcijas;

SĮ ESPBI IS administratorius – sveikatinimo veiklą vykdančios įstaigos (toliau – sveikatinimo įstaiga) darbuotojas atliekantis ESPBI IS administratoriaus funkcijas;

Kitos Informacijos tvarkymo taisyklėse vartojamos sąvokos atitinka sąvokas, nustatytas Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniuose saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866), Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarimu Nr. 1057 (Žin., 2011, Nr. 113-5318) ir kituose Lietuvos Respublikos įstatymuose ir teisės aktuose.

4. ESPBI IS elektroninę informaciją sudaro:

4.1. asmens duomenys:

4.1.1. bendrieji pacientų duomenys;

4.1.2. ypatingieji pacientų duomenys;

4.1.3. sveikatinimo specialistų duomenys;

4.2. sveikatinimo įstaigų duomenys;

4.3. medicinos prietaisų duomenys;

4.4. medicininių vaizdų duomenys;

4.5. elektroninių receptų duomenys;

4.6. ataskaitų ir statistinės informacijos duomenys;

4.7. klasifikatorių duomenys;

4.8. saugos, audito ir administravimo posistemiuose kaupiami duomenys.

5. ESPBI IS pagal joje tvarkomą elektroninę informaciją priskirtina antrai informacinių sistemų kategorijai.

6. Už ESPBI IS elektroninės informacijos tvarkymą atsakingi:

6.1. sveikatinimo įstaigų darbuotojai – už informacijos, nurodytos Informacijos tvarkymo taisyklių 4.1.1, 4.1.2, 4.4, 4.5, 4.6 punktuose;

6.2. valstybės įmonės Registrų centro direktoriaus paskirti darbuotojai – už informacijos, nurodytos Informacijos tvarkymo taisyklių 4.1.3, 4.2, 4.3, 4.7 punktuose;

6.3. SĮ ESPBI IS administratoriai – už informacijos, nurodytos Informacijos tvarkymo taisyklių 4.1.3, 4.2, 4.3 punktuose;

6.4. institucijų, turinčių teisę atlikti medicininių duomenų analizę, darbuotojai – už informacijos, nurodytos Informacijos tvarkymo taisyklių 4.6 punkte;

6.5. RC ESPBI IS administratoriai – už informacijos, nurodytos Informacijos tvarkymo taisyklių 4.8 punkte.

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. Kompiuterinės įrangos saugos priemonės:

7.1. visose tarnybinėse stotyse ir kompiuterizuotose darbo vietose įdiegta ir reguliariai atnaujinama virusų ir kenkėjiško kodo aptikimo bei šalinimo programinė įranga, skirta tikrinti kompiuterius ir laikmenas. Kompiuterizuotose darbo vietose naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios reguliariai atnaujinamos;

7.2. pagrindinės tarnybinės stotys, svarbiausi duomenų perdavimo tinklo mazgai ir ryšio linijos yra dubliuojami ir jų techninė būklė nuolat stebima;

7.3. paslaugų tarnybinės stotys ir svarbiausi elektroninės informacijos perdavimo tinklo mazgai turi įtampos filtrą ir rezervinį elektros generatorių. Nepertraukiamos elektros energijos tiekimas svarbiausiems ESPBI IS elementams užtikrinamas dviem dyzeliniais elektros generatoriais. Rezervinis elektros energijos tiekimo šaltinis užtikrina informacinės sistemos pagrindinių tarnybinių stočių veikimą ne trumpiau kaip 8 val.

8. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

8.1. ESPBI IS tarnybinių stočių operacinės sistemos ir kitos programinės įrangos operatyviam atnaujinimui yra naudojama tarnybinė stotis WSUS (angl. Windows Server Update Services). Įdiegiami tik gamintojų rekomenduojami atnaujinimai;

8.2. ESPBI IS naudojama tik legali, patikimų gamintojų programinė įranga;

8.3. programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik ESPBI IS administratoriai;

8.4. programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

8.5. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką.

9. Duomenų perdavimo tinklais saugumo užtikrinimo priemonės:

9.1. tarnybinės stotys, kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų telekomunikacinių tinklų naudojant ugniasienes;

9.2. ESPBI IS elektroninės informacijos perdavimo tinklas yra segmentuotas pagal ESPBI IS sudedamųjų dalių atliekamas funkcijas ir turi priskirtus IP adresų intervalus:

9.2.1. paslaugų tarnybinių stočių tinklas, skirtas taikomųjų programų tarnybinėms stotims;

9.2.2. ESPBI IS kompiuterizuotų darbo vietų tinklai, skirti nutolusių ESPBI IS naudotojų kompiuterinėms darbo vietoms ir kompiuterinei įrangai;

9.2.3. ESPBI IS kūrimo, tobulinimo ir testavimo tinklas, skirtas naudojamoms tarnybinėms stotims ir duomenų bazių testavimo tarnybinėms stotims testuoti;

9.2.4. ESPBI IS administratorių tinklas, skirtas darbuotojų, turinčių ESPBI IS ir (ar) tarnybinių stočių administratoriaus teises, kompiuterizuotoms darbo vietoms;

9.2.5. elektroninės informacijos perdavimo tinklo aptarnavimo ir saugumo potinklis, skirtas tinklo stebėjimo, aptarnavimo, antivirusinių sistemų tarnybinėms stotims;

9.2.6. demilitarizuotosios zonos tinklas, skirtas tarnybinėms stotims, kurios turi ryšį su viešaisiais telekomunikacijų tinklais;

9.2.7. demilitarizuotoji zona tiek nuo išorinio, tiek nuo vidinio elektroninės informacijos perdavimo tinklo atskirta ugniasienėmis;

9.2.8. nutolę ESPBI IS naudotojai perduoda informaciją naudodami saugias ryšio linijas;

9.2.9. nutolę ESPBI IS naudotojai duomenis perduodantys ir gaunantys viešaisiais telekomunikacijų tinklais, perduodamų duomenų konfidencialumą užtikrina naudodami duomenų šifravimą arba virtualų privatų tinklą;

9.2.10. ESPBI IS taikomas elektroninės informacijos perdavimo tinklo trijų lygių saugumas – išorė, taikomosios programos, duomenų bazės, kiekvieną iš lygių atskiriant ugniasienėmis;

9.2.11. jungimasis prie ESPBI IS iš viešųjų telekomunikacijų tinklų yra griežtai kontroliuojamas ir atliekamas tik per tarpines tarnybines stotis;

9.2.12. keitimasis informacija su kitais registrais ir informacinėmis sistemomis galimas tik naudojant saugius šifruotus ryšio kanalus (VPN, SSL) ir tarpines tarnybines stotis.

10. Elektroninės informacijos perdavimo tinklai stebimi šia tvarka:

10.1. visi tinklo įrenginiai, turintys paprastojo tinklo stebėjimo protokolo (angl. Simple Network Management Protocol (SNMP) parinktį, stebimi tinklo priežiūros sistemos ir kilus nesklandumams automatiškai praneša apie problemą atsakingiems darbuotojams;

10.2. visi ryšių kanalai stebimi tinklo priežiūros sistemos ir esant sutrikimams arba didelei apkrovai automatiškai praneša apie problemą atsakingiems darbuotojams.

11. Valstybės įmonės Registrų centro patalpų ir aplinkos saugumo užtikrinimas:

11.1. įrengta elektroninė perimetro kontrolės sistema. Tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą;

11.2. įrengta tam tikrų patalpų apsaugos signalizacija, kurios signalai pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis persiunčiami patalpas saugančiai saugos tarnybai;

11.3. kiekvienas darbuotojas turi asmeninę magnetinę kortelę ir įeidamas arba išeidamas pasižymi įėjimo punktuose;

11.4. visi darbuotojų įėjimų ir išėjimų į patalpas kartai fiksuojami ir laikomi elektronine forma;

11.5. lankytojams ir svečiams privalomai išduodamos svečio elektroninės kortelės. Už apsilankymą atsakingas darbuotojas pasirašo įėjimo punkto žurnale už kiekvieną lankytoją;

11.6. po 18 val. ir ne darbo dienomis į pastatą patekti gali tiktai specialius leidimus turintys darbuotojai.

12. Valstybės įmonės Registrų centro ESPBI IS tarnybinių stočių patalpose:

12.1. sienos sumūrytos iš plytų ar blokelių, lubos pagamintos iš gelžbetonio;

12.2. durys atsparios laužimui, nedegios, rakinamos viena cilindrine spyna ir viena plokšteline spyna;

12.3. į tarnybinių stočių patalpas gali patekti tik valstybės įmonės Registrų centro direktoriaus patvirtintame sąraše išvardyti darbuotojai. Valymas, elektros tinklo priežiūra, patalpų remonto ir kiti darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į serverių patalpas;

12.4. tarnybinių stočių patalpos turi alternatyvų elektros energijos tiekimo šaltinį;

12.5. tarnybinių stočių patalpose įrengta gaisro gesinimo halonu sistema;

12.6. tarnybinių stočių patalpų raktai saugomi seife. Atsarginiai tarnybinių stočių patalpos raktai saugomi kitame nei pagrindiniai raktai pastate.

13. Lietuvos Respublikos sveikatos apsaugos ministerijos ir sveikatinimo įstaigų patalpose:

13.1. durys rakinamos;

13.2. įrengta patalpų signalizacija arba jas saugo apsaugos darbuotojai;

13.3. patalpos atitinka priešgaisrinės saugos reikalavimus, yra gaisro gesinimo priemonės, atliekama gaisro gesinimo priemonių patikra;

13.4. patalpos, kurioje yra tarnybinės stotys, atskirtos nuo bendro naudojimo patalpų, durys rakinamos.

14. Nešiojamųjų kompiuterių naudojimo tvarka:

14.1. išvežti iš patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros viešose vietose. Kelionės metu nešiojamieji kompiuteriai turi būti saugomi;

14.2. visi nešiojamieji kompiuteriai turi būti apsaugoti saugiais slaptažodžiais, vadovaujantis prieigos valdymo procedūra. Jei įmanoma, turi būti aktyvuotas BIOS slaptažodis. Kompiuterio išdavimo metu naudotojas turi nedelsdamas pakeisti standartinį ar prieš tai nustatytą slaptažodį;

14.3. prieš perduodant nešiojamąjį kompiuterį ESPBI IS naudotojui, jis turi būti patikrinamas antivirusine programine įranga;

14.4. nešiojamojo kompiuterio grąžinimas ir antivirusinės programos tikrinimo rezultatai turi būti dokumentuojami;

14.5. siekiant apsaugoti nešiojamuosiuose kompiuteriuose sukauptus ESPBI IS duomenis, atsarginės duomenų kopijos turi būti daromos į atskirus diskus ar duomenų laikmenas.

15. Kitos priemonės, naudojamos užtikrinti ESPBI IS elektroninės informacijos saugą:

15.1. ESPBI IS registruoja duomenų bazių informacijos ir tarnybinių stočių operacinės sistemos pakeitimus. ESPBI IS fiksuoja visus elektroninės informacijos pakeitimus, pakeitimą atlikusius ESPBI IS naudotojus bei atliktų pakeitimų datą ir laiką;

15.2. ESPBI IS priežiūros funkcijos atliekamos naudojant tam skirtą RC ESPBI IS administratoriaus identifikatorių, kuriuo naudojantis negalima atlikti kitų ESPBI IS naudotojų funkcijų;

15.3. kiekvienas ESPBI IS naudotojas unikaliai identifikuojamas – ESPBI IS naudotojas patvirtina savo tapatybę ESPBI IS naudotojo vardu ir slaptažodžiu arba skaitmeniniu kvalifikuotu sertifikatu;

15.4. baigus darbą, būtina užtikrinti, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo ESPBI IS, atjungti saugią sertifikato laikmeną nuo kompiuterinės įrangos, uždaryti programinę įrangą, įjungti ekrano užsklandą su slaptažodžiu, dokumentus padėti į pašaliniams asmenims neprieinamą vietą;

15.5. ESPBI IS naudotojui neatliekant jokių veiksmų 60 min., visos kompiuterizuotos darbo vietos ir tarnybinės stotys automatiškai užsirakina ir naudotis ESPBI IS galima tik pakartojus vartotojo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus. ESPBI IS turi perspėti RC ESPBI IS administratorių, kai pagrindinėse tarnybinėse stotyse laisvos operatyviosios atminties ar laisvos vietos diske sumažėja iki nustatytos pavojingos ribos, taip pat, kai ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

15.6. ESPBI IS yra įdiegtos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemonės (filtrai);

15.7. pagrindinių tarnybinių stočių įvykių žurnaluose (angl. event log) registruojami ir ne trumpiau nei 36 mėnesius saugomi duomenys apie: ESPBI IS įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis ir prieiti prie informacinių išteklių, kitus svarbius saugai įvykius, nurodant ESPBI IS naudotojo identifikatorių ir įvykio laiką. Ši informacija analizuojama įvykus saugos incidentui;

15.8. ESPBI IS veikla atkuriama vadovaujantis Elektroninės sveikatos paslaugų ir bendradarbiavimo informacinės sistemos veiklos tęstinumo valdymo planu.

16. Darbo apskaitos priemonės:

16.1. ESPBI IS naudotojams suteikiama prieigos teisė atlikti veiksmus tik su jiems priskirtais ESPBI IS duomenimis Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudotojų administravimo taisyklėse nustatyta tvarka;

16.2. elektroniniuose žurnaluose registruojami ESPBI IS naudotojo veiksmai su ESPBI IS duomenimis.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

17. Duomenų įvedimo, keitimo, atnaujinimo ir naikinimo tvarka:

17.1. pacientų duomenų bazėje tvarkomus bendruosius pacientų duomenis, elektroninių sveikatos istorijų (toliau – ESI) duomenų bazėje tvarkomus ypatinguosius pacientų duomenis, medicininių vaizdų duomenų bazėje ir e. receptų duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik sveikatinimo specialistas pagal nustatytą prieigos teisių lygmenį;

17.2. ESI duomenų bazėje tvarkomus sveikatinimo specialistų ir sveikatinimo įstaigų duomenis, medicinos prietaisų duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik valstybės įmonės Registrų centro direktoriaus paskirti darbuotojai ir SĮ ESPBI IS administratoriai pagal nustatytą prieigos teisių lygmenį;

17.3. klasifikatorių duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik valstybės įmonės Registrų centro direktoriaus paskirti darbuotojai pagal nustatytą prieigos teisių lygmenį;

17.4. ataskaitų ir statistinės informacijos duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik institucijų, turinčių teisę atlikti medicininių duomenų analizę, darbuotojai pagal nustatytą prieigos teisių lygmenį;

17.5. duomenys į ESPBI IS duomenų bazes gali būti įvesti, pakeisti, atnaujinti tik turint teisėtą pagrindą;

17.6. duomenų įvedimas, pakeitimas, atnaujinimas registruojami elektroniniuose žurnaluose, nurodant ESPBI IS naudotoją, darbo laiką, prisijungimo datą, laiką ir atliktus veiksmus;

17.7. duomenys ESPBI IS nėra naikinami. Duomenys, perkelti į ESPBI IS archyvą, naikinami Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų VII skyriuje nustatyta tvarka.

18. Atsargines duomenų bazių kopijas daro RC ESPBI IS administratoriai. Atsarginių duomenų bazių kopijų darymo tvarką reglamentuoja Duomenų rezervinio kopijavimo ir laikmenų saugojimo tvarka, patvirtinta valstybės įmonės Registrų centro direktoriaus 2008 m. birželio 20 d. įsakymu Nr. v-148 (2011 m. lapkričio 18 d. įsakymo Nr. v-221 redakcija).

19. Duomenys kitiems registrams ir informacinėms sistemoms teikiami ir gaunami iš jų tik pasirašius duomenų teikimo sutartis, laikantis šių reikalavimų:

19.1. ESPBI IS duomenys kitai informacinei sistemai perduodami vadovaujantis Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatais, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatais, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugumo politiką įgyvendinančiais dokumentais bei kitais, duomenų saugą užtikrinančiais ir reglamentuojančiais, teisės aktais;

19.2. duomenų teikėjai į ESPBI IS duomenis turi teikti teisės aktų nustatytais būdais, apimtimi, reguliarumu ir terminais;

19.3. visi faktai apie apsikeitimus duomenimis fiksuojami ir laikomi elektroninėje duomenų bazėje.

20. Neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

20.1. ESPBI IS naudotojai, pastebėję saugos dokumentų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai ESPBI IS administratoriui;

20.2. ESPBI IS administratorius apie saugos pažeidimus informuoja ESPBI IS saugos įgaliotinį ir imasi visų įmanomų prevencinių veiksmų, susijusių su neteisėtu duomenų naudojimu.

21. ESPBI IS funkcijų pakeitimo (toliau – pakeitimas) tvarka:

21.1. visi pakeitimai (projektavimas, kūrimas, testavimas, diegimas) atliekami tik ESPBI IS valdytojo iniciatyva;

21.2. pakeitimo projektavimą ir kūrimą atlieka valstybės įmonės Registrų centro darbuotojai tam skirtoje kūrimo aplinkoje. Atlikdamas pakeitimo projektavimą ir kūrimą, valstybės įmonė Registrų centras gali pasitelkti trečiąsias šalis;

21.3. prieš atliekant pakeitimus, kurių metu gali iškilti grėsmė elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pakeitimai turi būti išbandomi testavimo aplinkoje, kuri yra identiška gamybinei aplinkai;

21.4. įgyvendinant pakeitimus, kurių metu galimi ESPBI IS veikimo sutrikimai, RC ESPBI IS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų pakeitimų pradžios (elektroniniu paštu, faksu ar kitomis priemonėmis) informuoti ESPBI IS naudotojus apie tokių darbų pradžią ir galimus sutrikimus;

21.5. atlikęs pakeitimų testavimą, jei ir testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, RC ESPBI IS administratorius gali pradėti eksploatuoti pakeitimus;

21.6. jeigu testavimas sėkmingas, pakeitimai perkeliami į gamybinę aplinką;

21.7. visi pakeitimai registruojami ir apie tai informuojami ESPBI IS naudotojai;

21.8. RC ESPBI IS administratorius SĮ ESPBI IS administratoriams ir ESPBI IS naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi ESPBI IS pakitimus, kurių atsiradimas susijęs su atliktais arba atliekamais pakeitimais.

IV. REIKALAVIMAI, KELIAMI ESPBI IS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

22. RC ESPBI IS administratorius atsako už programinių, techninių ir kitų prieigos prie ESPBI IS resursų organizavimą, suteikimą ir panaikinimą techninės ir (ar) programinės paslaugos teikėjui.

23. RC ESPBI IS administratorius suteikia paslaugos teikėjui tik tokią prieigą prie ESPBI IS resursų, kuri yra būtina norint atlikti arba vykdyti sutartyje nustatytus įsipareigojimus, kurie neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

24. RC ESPBI IS administratorius privalo supažindinti paslaugos teikėjus su suteiktos prieigos prie informacinės sistemos reikalavimais ir sąlygomis.

25. Pasibaigus sutarties su paslaugos teikėjais galiojimo terminui ar atsiradus kitoms sutartyje ar saugos politiką įgyvendinančiuose dokumentuose įvardytoms sąlygoms, RC ESPBI IS administratorius nedelsdamas privalo panaikinti suteiktą prieigą.

26. Reikalavimai, keliami patalpoms, įrangai, informacinės sistemos priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms, turi atitikti šiose Informacijos tvarkymo taisyklėse nustatytus reikalavimus.

V. BAIGIAMOSIOS NUOSTATOS

27. Asmenys, pažeidę šių Informacijos tvarkymo taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

28. Šios Informacijos tvarkymo taisyklės skelbiamos valstybės įmonės Registrų centro tinklalapyje www.registrucentras.lt ir Lietuvos Respublikos sveikatos apsaugos ministerijos tinklalapyje www.sam.lt.

_____