**LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS**

# 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

2014 m. rugsėjo 22 d. Nr. V-975

Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. gruodžio 16 d. įsakymą Nr. V-1071 „Dėl Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro duomenų saugos nuostatų patvirtinimo“ ir išdėstau jį nauja redakcija:

„**LIETUVOS REPSUBLIKOS SVEIKATOS APSAUGOS MINISTRAS**

## ĮSAKYMAS DĖL SVEIKATOS PRIEŽIŪROS IR FARMACIJOS SPECIALISTŲ PRAKTIKOS LICENCIJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

Vadovaudamasi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu:

1. T v i r t i n u Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro duomenų saugos nuostatus (pridedama).

2. P a v e d u:

2.1. Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos direktoriui:

2.1.1. per 1 mėnesį nuo Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro duomenų saugos nuostatų patvirtinimo dienos paskirti Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro saugos įgaliotinį, administratorių ir duomenų valdymo įgaliotinį;

2.1.2. per 3 mėnesius nuo Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro duomenų saugos nuostatų patvirtinimo dienos parengti ir pateikti Lietuvos Respublikos sveikatos apsaugos ministerijai tvirtinti:

2.1.2.1. Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.1.2.2. Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro veiklos tęstinumo valdymo plano projektą;

2.1.2.3. Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro naudotojų administravimo taisyklių projektą;

2.2. įsakymo vykdymo kontrolę viceministrui pagal veiklos sritį.“

Sveikatos apsaugos ministrė Rimantė Šalaševičiūtė

PATVIRTINTA
Lietuvos Respublikos sveikatos
apsaugos ministro 2011 m.
gruodžio 16 d. įsakymu Nr. V-1071
(Lietuvos Respublikos sveikatos
apsaugos ministro 2014 m.
rugsėjo 22 d. įsakymo Nr. V-975
redakcija)

# SVEIKATOS PRIEŽIŪROS IR FARMACIJOS SPECIALISTŲ PRAKTIKOS LICENCIJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Sveikatos priežiūros ir farmacijos specialistų praktikos licencijų registro (toliau – Registras) duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Registre tvarkomos elektroninės informacijos saugos tikslus, duomenų saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus, apibrėžia duomenų saugos politiką.

2. Šiuose Saugos nuostatuose vartojamos sąvokos atitinka teisės aktuose, nurodytuose šių Saugos nuostatų 13 punkte, vartojamas sąvokas.

3. Šiais Saugos nuostatais turi vadovautis Registro valdytojas, Registro tvarkytojai, Registro saugos įgaliotinis (toliau – saugos įgaliotinis), Registro administratorius (toliau – administratorius) ir Registro naudotojai (toliau – naudotojai).

4. Informacijos saugos tikslai:

4.1. informacijos vientisumo, konfidencialumo, prieinamumo užtikrinimas;

4.2. kompiuterizuotų darbo vietų pakankamo saugos lygio įdiegimas ir palaikymas;

4.3. tinkamo kompiuterinės, programinės ir ryšių įrangos funkcionavimo užtikrinimas;

4.4. kompiuterinio ryšio, priimant ir perduodant informaciją elektroniniu paštu, patikimumo ir saugos užtikrinimas.

5. Informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. Registro duomenims tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

5.2. Registro duomenų tvarkymo kontrolė;

5.3. veiklos tęstinumo užtikrinimas;

5.4. asmens duomenų apsauga.

6. Registro valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija (Vilniaus g. 33, LT-01506 Vilnius).

7. Registro tvarkytojai yra Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos (Jeruzalės g. 21, LT-08420 Vilnius), Valstybinė vaistų kontrolės tarnyba prie Lietuvos Respublikos sveikatos apsaugos ministerijos (Žirmūnų g. 139A, LT-09120 Vilnius), Lietuvos Respublikos odontologų rūmai (J. Jasinskio g. 16, LT-01112 Vilnius).

8. Registro valdytojas atlieka šias funkcijas:

8.1. organizuoja Registro veiklą ir jai vadovauja;

8.2. priima sprendimus dėl Registro techninių ir programinių priemonių įsigijimo, įdiegimo ir modernizavimo;

8.3. priima sprendimą dėl Registro informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

8.4. atsako už elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugą;

8.5. tvirtina Saugaus elektroninės informacijos tvarkymo taisykles, Informacinės sistemos veiklos tęstinumo valdymo planą bei Informacinės sistemos naudotojų administravimo taisykles;

8.6. prižiūri saugos dokumentų reikalavimų įgyvendinimą;

8.7. skiria saugos įgaliotinį ir administratorių;

8.8. kontroliuoja, kad Registras būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais, šiais Saugos nuostatais ir kitais teisės aktais.

9. Šių Saugos nuostatų 8.3, 8.6 ir 8.7 papunkčiuose nurodytas funkcijas Registro valdytojas gali perduoti vykdyti vienam iš Registro tvarkytojų.

10. Registro tvarkytojai užtikrina, kad naudotojai laikytųsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose nurodytų reikalavimų.

11. Saugos įgaliotinio funkcijos ir atsakomybė:

11.1. teikia Registro valdytojui (arba jos paskirtam Registro tvarkytojui) siūlymus dėl:

11.1.1. administratoriaus paskyrimo (saugos įgaliotinis negali atlikti administratoriaus funkcijų);

11.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

11.1.3. Registro saugos atitikties vertinimo atlikimo;

11.2. koordinuoja Registro saugos incidentų tyrimą;

11.3. teikia administratoriui privalomus vykdyti nurodymus bei pavedimus;

11.4. konsultuoja naudotojus Registro saugos klausimais;

11.5. atsako už Registro saugos politikos įgyvendinimo organizavimą.

12. Administratoriaus funkcijos ir atsakomybė:

12.1. įvertina, ar naudotojai yra pasirengę darbui;

12.2. suteikia teisę naudotojams naudotis elektronine informacija paskirtoms funkcijoms atlikti;

12.3. administruoja ir užtikrina tinkamą Registrą sudarančių komponentų (kompiuteriai, operacinės sistemos, duomenų bazių valdymo sistemos, taikomųjų programų sistemos, ugniasienės) veikimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

12.4. informuoja saugos įgaliotinį apie saugos incidentus ir teikia pasiūlymus dėl saugos užtikrinimo;

12.5. atsako už kompiuterių tinklo funkcionavimą;

12.6. atsako už Registro atsarginių duomenų kopijų darymą.

13. Registro sauga užtikrinama vadovaujantis:

13.1. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

13.2. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

13.3. Interneto tarnybinių stočių apsaugos rekomendacijomis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 21 d. įsakymu Nr. 1V-176 „Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo“;

13.4. Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“.

## II SKYRIUS
## ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.2 papunkčiu, Registre tvarkoma informacija priskiriama svarbios elektroninės informacijos kategorijai.

15. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.2 papunkčiu, Registras priskiriamas antrai informacinių sistemų kategorijai.

16. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais 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“, Registro duomenų tvarkymas automatiniu būdu priskiriamas antram saugumo lygiui.

17. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, ne rečiau kaip kartą per metus organizuoja Registro rizikos įvertinimą. Minėtą rizikos įvertinimą gali atlikti ir pats saugos įgaliotinis. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą.

18. Registro rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama Registro valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

18.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

18.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

19. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Registro valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

20. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

21. Saugos užtikrinimo priemonės parenkamos, siekiant užtikrinti Registro veiklos tęstinumą, patiriant kuo mažiau išlaidų ir užtikrinant saugų informacinės sistemos darbą.

22. Registro saugos atitikties vertinimas atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų

ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

23. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Registro valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Registro valdytojo vadovas.

24. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

## III SKYRIUS
## ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

25. Programinės įrangos, skirtos informacinei sistemai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

25.1. kompiuterinėse darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos automatiniu būdu;

25.2. turi būti naudojamos priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą, veikiančią sisteminiuose kataloguose esančiose rinkmenose tarnybinėje stotyje ir visuose kompiuterių tinklo kompiuteriuose;

25.3. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų;

25.4. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 24 valandas.

26. Naudotojams draudžiama patiems diegti bet kokią programinę įrangą. Draudimą kontroliuoja tarnybinės stoties operacinė sistema. Programinę įrangą, reikalingą naudotojo funkcijoms vykdyti, diegia ir prižiūri administratorius.

27. Neteisėtų programų įdiegimo (apeinant operacinės sistemos apsaugos mechanizmus) paiešką bent kartą per mėnesį atlieka administratorius. Nuolat turi būti stebimas interneto srautas, siekiant aptikti ir išaiškinti galimus neleistinus, ne su naudotojų funkcijomis susijusius didelius duomenų srautus, apkraunančius ne mažiau kaip 20 proc. interneto ryšio resurso.

28. Kompiuterių tinklo tarnybinės stotys bei kiekvienas kompiuterių tinklui priklausantis kompiuteris privalo turėti užkardą, ribojančią priėjimą iš išorės bei duomenų srautus į išorę. Turi būti draudžiama naudoti interneto ryšį visoms programoms, kurios gali visiškai atlikti savo funkcijas ir be internetinio ryšio su išore. Visi nenaudojami prievadai turi būti užblokuoti.

29. Turi būti galimybė reguliuoti atskirų interneto sričių pasiekiamumą tiek pagal interneto sričių vardus, tiek pagal fizinius adresus. Reguliavimą kontroliuoja administratorius, blokuodamas potencialiai pavojingas interneto sritis.

30. Nešiojamuosius Registro naudotojų kompiuterius, skirtus Registro elektroninei informacijai tvarkyti, išnešti iš Registro tvarkytojų patalpų yra griežtai draudžiama.

31. Registro atsarginės duomenų kopijos daromos automatiniu būdu kiekvieną dieną esant aktyviai registro duomenų bazei. Kopijos įrašomos į keičiamus informacijos kaupiklius (kompaktinius diskus, magnetines juostas ar kitas duomenų kopijų saugojimo laikmenas) ir saugomos seife, prieinamame tik administratoriui, jo nesant – administratorių pavaduojančiam asmeniui. Prireikus jas atkurti turi teisę tik administratorius ar jį pavaduojantis asmuo. Kopijų, iš

kurių būtų galima atkurti Registro duomenis, darymo ir saugojimo tvarka detaliai aprašyta Registro saugaus informacijos tvarkymo taisyklėse.

32. Naudotojai prie Registro prisijungia nuotoliniu būdu naudodami interneto naršyklę.

## IV SKYRIUS
## REIKALAVIMAI PERSONALUI

33. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

34. Saugos įgaliotinis turi išmanyti saugos užtikrinimo principus, darbą su kompiuterių tinklais, turėti darbo su operacinėmis sistemomis, taikomosiomis programomis patirties. Savo darbe turi vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

35. Administratorius turi išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

36. Naudotojai privalo turėti pagrindinius darbo kompiuteriu įgūdžius, būti susipažinę su šiais Saugos nuostatais bei kitais saugos politiką reglamentuojančiais dokumentais.

37. Naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui.

38. Saugos įgaliotinis ne rečiau kaip kartą per metus inicijuoja naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką.

## V SKYRIUS
## INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

39. Naudotojų supažindinimą su šiais Saugos nuostatais bei kitais saugos politiką reglamentuojančiais dokumentais vykdo saugos įgaliotinis. Su minėtais dokumentais naudotojai supažindinami pasirašytinai.

## VI SKYRIUS
## BAIGIAMOSIOS NUOSTATOS

40. Saugos įgaliotinis, administratorius ir naudotojai, pažeidę šių Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

_____