Suvestinė redakcija nuo 2021-04-01

PATVIRTINTA
Valstybinės ligonių kasos prie
Sveikatos apsaugos ministerijos
direktoriaus 2020 m. vasario 14 d.
įsakymu Nr. 1K-45

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, užtikrinančią saugų Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) ir teritorinių ligonių kasų (toliau – TLK) (VLK ir TLK kartu toliau – ligonių kasos) informacinių sistemų, išvardytų VLK valdomų informacinių sistemų duomenų saugos nuostatų, patvirtintų VLK direktoriaus 2017 m. gruodžio 6 d. įsakymu Nr. 1K-234 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų duomenų saugos nuostatų patvirtinimo“ (toliau – Duomenų saugos nuostatai), 2 punkte, Detalios paciento lygio sąnaudų apskaitos informacinės sistemos bei vidaus administravimui skirtų informacinių sistemų tvarkymą ir šių informacinių sistemų kibernetinio saugumo politikos įgyvendinimą.

2. Taisyklės parengtos vadovaujantis:

2.1. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

2.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

2.3. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu ir Saugos dokumentų turinio gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

2.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

2.5. Duomenų saugos nuostatais,

2.6. VLK ir TLK organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu, patvirtintu VLK direktoriaus 2017 m. kovo 9 d. įsakymu Nr. 1K-52 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo patvirtinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas);

2.7. kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

2.8. LST ISO/IEC 27001 (aktualios redakcijos) „Informacijos saugumo valdymo sistemos. Reikalavimai“.

3. Taisyklėse vartojamos sąvokos:

3.1. **VLK informacinės sistemos naudotojas** – ligonių kasų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, bei išorės naudotojai, turintys teisę naudotis VLK informacinių sistemų ištekliais tam tikroms funkcijoms atlikti.

3.2. **Informacinių sistemų administratoriai** – ligonių kasų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, arba trečiųjų šalių darbuotojai pagal sutartį teikiantys

priežiūros, diegimo ar kitas paslaugas, susijusias su informacinėmis technologijomis, ir turintys teisę naudotis VLK informacinių sistemų ištekliais tam tikroms funkcijoms atlikti.

3.3. Kitos sąvokos, atitinkančios Taisyklių 2 punkte nurodytuose teisės aktuose vartojamas sąvokas.

4. Ligonių kasos, užtikrindamos elektroninės informacijos saugą, vadovaujasi Lietuvos standartais LST ISO/IEC 27002 (aktualios redakcijos) „Informacijos saugumo valdymo praktikos kodeksas“, LST ISO/IEC 27001 (aktualios redakcijos) „Informacijos saugumo valdymo sistemos. Reikalavimai “, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų elektroninės informacijos tvarkymą.

5. VLK informacinėse sistemose tvarkoma elektroninė informacija yra nurodyta šių sistemų nuostatuose.

6. VLK informacinėse sistemose tvarkoma skirtingos svarbos elektroninė informacija. Atitinkamos VLK informacinės sistemos svarbos kategorija ir priskyrimo šiai kategorijai kriterijai nurodyti Duomenų saugos nuostatų 19–22 punktuose.

Punkto pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

7. Už VLK informacinių sistemų elektroninės informacijos saugų tvarkymą atsako atitinkamų VLK informacinių sistemų naudotojai pagal jiems suteiktas informacinių sistemų duomenų tvarkymo teises.

8. VLK informacinių sistemų administratoriai atsako už atitinkamų informacinių sistemų taikomosios programinės įrangos ir duomenų bazės administravimą, prieigų prie informacinių sistemų suteikimą naudotojams, šių prieigų pakeitimą ar panaikinimą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

9. Informacinių sistemų kompiuterinės įrangos saugos priemonės:

9.1. kompiuterinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų ir užtikrinamas šios įrangos gamintojų garantinis aptarnavimas;

9.2. visose tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti įdiegta ir reguliariai atnaujinama virusų bei kitų kenkėjų kodo aptikimo ir šalinimo antivirusinė programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti. Kompiuterizuotose darbo vietose turi būti naudojamos ir reguliariai atnaujinamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės;

9.3. tarnybinės stotys turi būti apsaugotos nuo elektros srovės svyravimų ir (ar) nutrūkimo naudojant rezervinius elektros įvadus, vietinį elektros generatorių, nenutrūkstamo svarbiausios kompiuterinės įrangos maitinimo šaltinius (UPS), užtikrinančius šios įrangos veikimą ne mažiau kaip 60 min.;

9.4. tarnybinėse stotyse ir kompiuterizuotuose darbo vietose turi būti įdiegtos darbo parametrų stebėjimo ir valdymo funkcijos; turi būti siunčiami perspėjimai, kai pagrindinėje kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisvos kompiuterio atminties ar vietos diske, arba ilgą laiką labai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

9.5. pagrindinės tarnybinės stotys, svarbiausi duomenų perdavimo tinklo mazgai ir ryšio linijos esant techninių galimybių turi būti dubliuojami ir jų techninė būklė nuolat stebima;

9.6. svarbiausios kompiuterinės įrangos gedimai turi būti registruojami atsakingų administratorių;

9.7. naudotojų kompiuteriai turi būti tinkamai paruošti darbui nustatyta tvarka, turi būti įdiegti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

9.8. nuotolinis prisijungimas prie kompiuterinės įrangos turi būti vykdomas algoritmu (protokolu), skirtu duomenims šifruoti (SSL/TLS/VPN/SSH);

9.9. tiesioginė prieiga prie tarnybinių stočių suteikiama tik informacinių sistemų administratoriams;

9.10. kitos kompiuterinės įrangos saugos priemonės yra numatytos Kibernetinio saugumo reikalavimų aprašo priede.

10. Ligonių kasų informacinių sistemų sisteminės ir taikomosios programinės įrangos saugos priemonės:

10.1. VLK informacinių sistemų programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

10.2. kompiuterizuotose darbo vietose darbo funkcijoms vykdyti turi būti naudojama tik legali, patikrinta, patikimų gamintojų programinė įranga, naudojama darbo funkcijoms vykdyti įtraukta į leistinos programinės įrangos sąrašą;

10.3. programinės įrangos testavimas turi būti atliekamas naudojant atitinkamą testavimo aplinką;

10.4. programinės įrangos diegimą, konfigūravimą ir šalinimą turi vykdyti atitinkamos informacinės sistemos administratorius arba šių paslaugų teikėjų atsakingas darbuotojas pagal atitinkamų paslaugų teikimo ir priežiūros sutartį;

10.5. programinės įrangos gedimai turi būti registruojami VLK naudotojų aptarnavimo tarnybos informacinėje sistemoje;

10.6. VLK informacinių sistemų naudotojams nesinaudojant kompiuterių įranga ilgiau nei 15 minučių, kompiuteriai turi būti užrakinami automatiškai, iš naujo prie jų prisijungti turi būti galima tik pakartotinai patvirtinus savo tapatybę;

10.7. kitos priemonės yra numatytos Kibernetinio saugumo reikalavimų aprašo priede.

11. VLK informacinių sistemų elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

11.1. informacinių sistemų elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę. Ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos pagal naujausias gamintojo rekomendacijas;

11.2. informacinės sistemos programinė įranga turi būti apsaugota nuo pagrindinių per tinklą vykdomų atakų – SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*) ir kitų;

11.3. telekomunikacijos tinklais perduodamos elektroninės informacijos konfidencialumas turi būti užtikrinamas naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones;

11.4. nuotoliniu būdu prisijungiantys VLK informacinių sistemų naudotojai, kurie duomenis perduoda ir gauna viešaisiais telekomunikacijų tinklais, perduodamų duomenų konfidencialumą užtikrina naudodami duomenų šifravimą arba virtualų privatų tinklą;

11.5. kitos priemonės yra numatytos Kibernetinio saugumo reikalavimų aprašo priede.

12. Tarnybinių stočių patalpų ir aplinkos saugumo užtikrinimo priemonės (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga):

12.1. patalpose turi būti įrengtos nedegios metalinės, atsparios laužimui, savaime užsidarančios ir visada rakinamos durys;

12.2. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti gaisro gesinimo priemonės;

12.3. patalpose turi būti įrengtas šildymas, vėdinimas ir oro kondicionavimas (turi būti priežiūros sutartys);

12.4. patalpose turi būti įrengta įsilaužimo signalizacija (garsinė, judesio);

12.5. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

12.6. patekimas į patalpas, kuriose yra tarnybinės stotys, ir patalpas, kuriose saugomos atsarginės kopijos, kontroliuojamas naudojant vaizdo stebėjimo sistemą;

12.7. įėjimo į patalpas kontrolę vykdo VLK arba TLK fizinės saugos įgaliotinis;

12.8. į VLK tarnybinių stočių patalpas gali patekti tik VLK direktoriaus patvirtintame sąraše išvardyti darbuotojai. Į TLK tarnybinių stočių patalpas gali patekti tik TLK direktoriaus patvirtintame sąraše išvardyti darbuotojai. Įeinančių į patalpas asmenų tapatybė nustatoma ir

fiksuojama elektroninės tapatybės nustatymo ir praėjimo kontrolės sistemoje (naudojama elektroninės tapatybės nustatymo kortelė). Jei elektroninės tapatybės nustatymo ir praėjimo kontrolės sistemos nėra, naudojami fiziniai raktai ir įėjimo žurnalai;

12.9. tarnybinių stočių valymas, elektros tinklo priežiūra, patalpų remonto ir kiti darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į tarnybinių stočių patalpas;

12.10. kitos tarnybinių stočių patalpų ir aplinkos saugumo užtikrinimo priemonės numatytos VLK ir TLK fizinės saugos tvarkos apraše, kuris tvirtinamas VLK direktoriaus įsakymu.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

13. VLK informacinių sistemų duomenis įvesti, keisti ir atnaujinti gali tik šių informacinių sistemų naudotojai pagal jiems suteiktas prieigos teises.

14. VLK informacinių sistemų elektroninė informacija įrašoma, atnaujinama, keičiama ir naikinama vadovaujantis atitinkamos VLK informacinės sistemos nuostatais, Duomenų saugos nuostatais ir kitais teisės aktais, reglamentuojančiais informacinių sistemų elektroninės informacijos tvarkymą.

15. VLK informacinių sistemų naudotojų duomenis įvesti, keisti, atnaujinti gali tik informacinių sistemų administratoriai.

16. Duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik informacinės sistemos administratorius pagal jam suteiktas prieigos teises, gavęs konkrečią užduotį VLK naudotojų aptarnavimo informacinėje sistemoje arba Naudotojų tapatybių ir teisių valdymo sistemoje.

17. Informacinių sistemų naudotojų veiksmai turi būti registruojami toliau nurodytu būdu:

17.1. informacinių sistemų naudotojų tapatybė ir veiksmai, atliekami su informacinių sistemų duomenimis, fiksuojami programinėmis priemonėmis;

17.2. informacinių sistemų naudotojų veiksmai įrašomi automatiniu būdu ligonių kasų informacinių sistemų duomenų bazės veiksmų žurnale, apsaugotame nuo neteisėto jo duomenų panaudojimo, pakeitimo, iškraipymo ar sunaikinimo. Šio žurnalo duomenys yra prieinami informacinių sistemų administratoriams pagal jų atliekamas darbo funkcijas.

18. Atsarginės VLK informacinių sistemų elektroninės informacijos (duomenų) kopijos daromos vadovaujantis Elektroniniu būdu tvarkomų duomenų atsarginių kopijų valdymo tvarkos aprašu, patvirtintu VLK direktoriaus įsakymu.

19. Prarasti, iškraipyti ar sunaikinti informacinių sistemų duomenys atkuriami iš atsarginių duomenų kopijų.

20. Duomenų atkūrimas iš atsarginių kopijų turi būti periodiškai išbandomas – ne rečiau kaip kartą per metus, išskyrus atvejus, kai duomenų atkūrimas vyksta realiu laiku.

21. Elektroninės informacijos mainai tarp ligonių kasų informacinių sistemų ir išorinių informacinių sistemų vykdomi duomenų teikimo sutartyse su šių informacinių sistemų valdytojais numatyta apimtimi, būdais ir terminais.

22. VLK informacinių sistemų elektroninė informacija kitiems registrams ir informacinėms sistemoms perduodama vadovaujantis atitinkamos informacinės sistemos nuostatais ir kitais saugų elektroninės informacijos tvarkymą reglamentuojančiais teisės aktais.

23. Už informacinių sistemų duomenų mainus ir gaunamos elektroninės informacijos atnaujinimą atsako informacinių sistemų administratoriai.

24. Informacinių sistemų administratoriai, užtikrindami informacinių sistemų elektroninės informacijos vientisumą, turi naudoti visas įmanomas technines, programines ir

administracines priemones, skirtas informacinių sistemų elektroninei informacijai apsaugoti nuo neteisėtų veiksmų.

25. VLK informacinių sistemų naudotojai, pastebėję Duomenų saugos nuostatų, saugos politikos įgyvendinamųjų dokumentų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, turi registruoti Naudotojų aptarnavimo tarnybos informacinėje sistemoje incidentą arba pranešti apie tai atitinkamos informacinės sistemos saugos įgaliotiniui. Atsakingi darbuotojai, pasinaudoję atitinkamos duomenų bazės veiksmų žurnalo įrašais, nustato neteisėto poveikio šaltinį, laiką ir veiksmus, atliktus su VLK informacinės sistemos programine įranga ir duomenimis.

26. Jeigu atitinkamų informacinių sistemų naudotojai neinformuoja šių sistemų saugos įgaliotinių apie Taisyklių 25 punkte nurodytus pažeidimus, šių sistemų administratoriai juos informuoja apie tai elektroninėmis priemonėmis.

27. VLK informacinių sistemų kompiuterių, tarnybinių stočių techninę ir programinę įrangą diegia, keičia ir atnaujina atitinkamų informacinių sistemų administratoriai.

28. Planuodamas atitinkamos VLK informacinės sistemos techninės ir programinės įrangos keitimą, kurio metu galimi šios informacinės sistemos veikimo sutrikimai, jos administratorius privalo ne vėliau kaip prieš 4 valandas iki techninės ir programinės įrangos pakeitimo pradžios informuoti šios VLK informacinės sistemos naudotojus apie tokių darbų pradžią ir galimus sutrikimus.

29. Perduodant remontuoti sugedusią techninę įrangą, išimamos duomenų laikmenos (kietieji diskai ir kt.) arba daromos jų kopijos ir laikmenose saugomi duomenys ištrinami.

30. Atlikus programinės ir techninės įrangos keitimą turi būti organizuojami atitinkamos VLK informacinės sistemos naudotojų darbo su nauja programine ir technine įranga mokymai.

31. VLK informacinių sistemų pokyčių valdymą planuoja ir užtikrina VLK informacinių sistemų valdytojas. Šis planavimas apima pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą (svarbumas ir skubumas), pokyčių prioritetų nustatymą (eiliškumas).

32. VLK informacinių sistemų pokyčiai valdomi vadovaujantis Informacinių technologijų paslaugų gyvavimo ciklo valdymo tvarkos aprašo, patvirtinto VLK direktoriaus įsakymu, nuostatomis.

33. VLK informacinių sistemų pokyčiai numatomi pagal atitinkamų informacinių sistemų naudotojų ir administratorių poreikius, įvertinus techninės ir programinės įrangos naudojimo problemas, gerąją praktiką.

34. Jei įtariama grėsmė elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, prieš atliekant VLK informacinių sistemų pakeitimus jie turi būti išbandomi testavimo aplinkoje, identiškoje gamybinei aplinkai.

35. Sėkmingai išbandžius VLK informacinių sistemų pakeitimus testavimo aplinkoje, atitinkami pakeitimai atliekami gamybinėje aplinkoje.

36. VLK informacinių sistemų naudotojai (tik ligonių kasų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis) nešiojamuosius kompiuterius ir kitus mobiliuosius įrenginius naudoja tik tarnybinėms funkcijoms vykdyti.

37. Techninės įrangos (įskaitant stacionarius ir nešiojamuosius kompiuterius, mobiliuosius įrenginius ir kt.) naudojimo tvarką nustato VLK informacinių sistemų valdytojas, kuris turi numatyti:

37.1. techninės ir programinės įrangos apskaitos tvarkymą;

37.2. atitinkamus draudimus VLK informacinių sistemų naudotojams dirbant su technine ir programine įranga;

37.3. techninių įrenginių skyrimo ir naudojimo tvarką;

37.4. kenksmingos programinės įrangos aptikimo priemones; techninio aptarnavimo sąlygas ir pan.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINĖMS SISTEMOMS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

38. Reikalavimai paslaugoms, užtikrinančioms tinkamą VLK informacinių sistemų funkcionavimą, ir šių paslaugų teikėjams nustatomi šių paslaugų teikimo sutartyse, kuriose turi būti nurodomas paslaugos objektas ir paslaugos apimtis, jos teikimo laikas, prieinamumo ir patikimumo reikalavimai, funkcionalumo ir vykdymo reikalavimai, prieigos prie atitinkamos VLK informacinės sistemos ir elektroninės informacijos sukūrimo reikalavimai, stebėsenos reikalavimai, taip pat reikalavimai, keliami informacinių sistemų priežiūrai, elektroninės informacijos perdavimui tinklais, saugai, įskaitant konfidencialumo ir informavimo apie elektroninės informacijos saugos incidentus, sutarties šalių veiksmų ribos ir atsakomybė, už sutarties vykdymą atsakingi sutarties šalių paskirti asmenys.

39. Informacinės sistemos administratorius atsako už programinių, techninių ir kitų prieigos prie atitinkamos VLK informacinės sistemos organizavimą, suteikimą ir panaikinimą taikomosios programinės įrangos priežiūros paslaugų teikėjui.

40. Paslaugų, užtikrinančių reikiamą atitinkamos VLK informacinės sistemos funkcionavimą, teikėjams suteikiamos tokios prieigos prie informacinės sistemos teisės, kurios yra būtinos sutartyje nustatytiems įsipareigojimams vykdyti ir neprieštarauja teisės aktų reikalavimams. Paslaugų teikėjo įgaliotam asmeniui teisės suteikiamos vadovaujantis VLK ir TLK informacinių išteklių privilegijuotųjų naudotojų veiksmų kontrolės tvarkos apraše, patvirtinto VLK direktoriaus įsakymu, nustatyta tvarka.

41. Pasibaigus paslaugų teikimo sutartyje nurodytam laikotarpiui, ligonių kasų darbuotojas, atsakingas už sutarties vykdymą, informuoja atitinkamos VLK informacinės sistemos administratorių apie paslaugų teikėjo įgalioto darbuotojo prieigos prie Privilegijuotų naudotojų veiksmų kontrolės sistemos teisės panaikinimą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. VLK informacinių sistemų naudotojai, informacinių sistemų administratoriai ir informacinių sistemų saugos įgaliotinai už Taisyklių pažeidimus atsako teisės aktų nustatyta tvarka.

_____