PATVIRTINTA
Telšių rajono pirminės sveikatos priežiūros centro
direktoriaus 2026 m. lapkričio 6 d.
įsakymu Nr. V-179

TELŠIŲ RAJONO PIRMINĖS SVEIKATOS PRIEŽIŪROS CENTRO ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Telšių rajono pirminės sveikatos priežiūros centro (toliau – Centras) asmens duomenų saugumo priemonių aprašas (toliau – Aprašas) nustato Centre taikomas organizacines ir technines asmens duomenų saugumo priemones, jų įgyvendinimo, priežiūros, dokumentavimo ir peržiūros tvarką, atsižvelgiant į Centro naudojamas kitų organizacijų valdomas ar administruojamas informacines sistemas.

2. Aprašas parengtas įgyvendinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas, toliau – BDAR) 5 straipsnio 1 dalies f punktą, 24, 25 ir 32 straipsnius, Centro asmens duomenų tvarkymo politikos (toliau – Politika) 62 punktą ir 86.8 papunktį. Taikomos ir kibernetinio saugumo teisės aktų nuostatos tiek, kiek jos Centrui privalomos.

3. Taikydamas Aprašą, Centras atsižvelgia į Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) „Asmens duomenų, tvarkomų sveikatos priežiūros įstaigose, saugumo užtikrinimo gaires“ (2024 m.), „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires duomenų valdytojams ir duomenų tvarkytojams“ (4 versija, 2024 m.) ir „Rekomendaciją sveikatos priežiūros įstaigoms dėl saugumo priemonių“ (2026 m.). Rekomendacijos taikomos atsižvelgiant į Centro vykdomą duomenų tvarkymą, rizikos vertinimą ir pagal kompetenciją valdomas technines priemones.

4. Aprašas taikomas Centro darbuotojams, praktikantams ir kitiems Centro įgaliotiems asmenims, kurie tvarko asmens duomenis elektroniniu ar popieriniu būdu. Centras, nustatydamas sveikatos priežiūros ir kitus savo veiklos duomenų tvarkymo tikslus bei priemones, veikia kaip duomenų valdytojas, net jei naudojasi kitų organizacijų informacinėmis sistemomis. Centro vaidmuo konkrečiose kitų valdytojų sistemose nustatomas pagal atitinkamus teisės aktus ir susitarimus.

5. Apraše vartojamos sąvokos:

5.1. išorinės informacinės sistemos valdytojas arba administratorius – subjektas, pagal teisės aktus ar sutartį atsakingas už naudojamos sistemos veikimą, administravimą ir jam priskirtas saugumo priemones;

5.2. IT administratorius – Centro įgaliotas darbuotojas arba pagal sutartį pasitelktas paslaugų teikėjas, pagal jam pavestas funkcijas prižiūrintis Centro darbo vietų įrangą, vietinį tinklą ir kitus jam priskirtus;

5.3. kibernetinio saugumo vadovas – Centro paskirtas arba pagal sutartį funkcijas vykdantis asmuo, organizuojantis ir prižiūrintis kibernetinio saugumo reikalavimų įgyvendinimą savo įgaliojimų ribose;

5.4. duomenų apsaugos pareigūnas (toliau – DAP) – Centro direktoriaus įsakymu pagal BDAR 37 straipsnį paskirtas Centro darbuotojas, atsakingas už asmens duomenų apsaugos organizavimą Centre ir vykdantis BDAR 39 straipsnyje nustatytas funkcijas;

5.5. kitos sąvokos suprantamos taip, kaip apibrėžtos BDAR, Politikoje ir kibernetinio saugumo teisės aktuose.

6. Centro naudojamų išorinių informacinių sistemų infrastruktūros, jų serverių, atsarginių kopijų ir sisteminių žurnalų techninį administravimą pagal priskirtą kompetenciją vykdo atitinkami sistemų valdytojai ar paslaugų teikėjai. Centras įgyvendina ir tikrina tas priemones, kurios priklauso jo kompetencijai, o dėl kitų priemonių siekia gauti pagrįstą patvirtinimą ar kontrolės įrodymus.

II SKYRIUS
ATSAKOMYBĖ IR FUNKCIJŲ ATSKYRIMAS

7. Centro direktorius užtikrina Centro, kaip duomenų valdytojo, pareigų įgyvendinimą: tvirtina Aprašą, rizikos valdymo sprendimus ir taisomųjų priemonių planus, paskiria atsakingus vykdytojus, užtikrina išteklius, nustatyta tvarka sprendžia dėl prieigos teisių bei dėl reikšmingų neatitikčių ir priima kitus Centrui priskirtus sprendimus.

8. Kibernetinio saugumo vadovas pagal savo paskyrimą ar paslaugų sutartį:

8.1. organizuoja su Centro darbo vietomis, vietiniu tinklu, išorinių sistemų naudojimu ir tiekėjais susijusių kibernetinių rizikų vertinimą ir periodinę saugumo priemonių peržiūrą;

8.2. koordinuoja kibernetinio saugumo reikalavimų įgyvendinimo stebėseną, vertina tiekėjų pateiktą saugumo informaciją ir siūlo riziką mažinančias priemones;

8.3. koordinuoja kibernetinių incidentų valdymo veiksmus pagal atskirus Centro kibernetinio saugumo dokumentus; jei incidentas susijęs su asmens duomenimis, nedelsdamas informuoja DAP;

8.4. stebi nustatytų neatitikčių šalinimą, teikia rekomendacijas direktoriui ir bendradarbiauja su DAP, neperimdamas BDAR 39 straipsnyje nurodytų DAP funkcijų;

8.5. neatlieka nesuderinamų tinklų ar informacinių sistemų techninio administravimo funkcijų, kai tai draudžia Centrui taikomi kibernetinio saugumo reikalavimai.

9. IT administratorius pagal sutartį ar pavestas funkcijas techniškai prižiūri Centro galinius įrenginius, programinę įrangą ir vietinį tinklą, įgyvendina jiems taikomas patvirtintas apsaugos priemones, padeda kreiptis į išorinių sistemų administratorius ir pateikia Centrui atliktų darbų patvirtinimus.

10. Struktūrinių padalinių vadovai nustato darbuotojams reikalingų prieigos teisių poreikį, teikia motyvuotus prašymus direktoriui ar jo įgaliotam asmeniui, nedelsdami praneša apie pasikeitusias darbuotojų funkcijas ir užtikrina, kad darbuotojai laikytųsi saugaus duomenų tvarkymo taisyklių.

11. DAP organizuoja asmens duomenų apsaugos atitikties priežiūrą Centre: konsultuoja dėl rizikos, prieigos, saugumo priemonių, pažeidimų ir duomenų tvarkymo teisėtumo; koordinuoja asmens duomenų saugumo priemonių dokumentų tarpusavio atitikties peržiūrą; stebi, ar taikomos organizacinės kontrolės priemonės, ir teikia rekomendacijas direktoriui.

12. Kiekvienas personalo narys atsako už jam suteiktų individualių prisijungimo priemonių saugumą, asmens duomenų konfidencialumą ir teisėtą prieigą tik pavestoms funkcijoms vykdyti. Apie pastebėtą ar įtariamą asmens duomenų saugumo pažeidimą nedelsiant, ne vėliau kaip per 24 valandas nuo pastebėjimo, pranešama DAP, nelaukiant papildomo patvirtinimo. Jeigu įvykis susijęs su kibernetiniu saugumu, informuojamas ir kibernetinio saugumo vadovas arba kitas nustatytas kontaktinis asmuo. Pranešama Centro asmens duomenų saugumo pažeidimų valdymo tvarkos apraše nustatyta tvarka.

III SKYRIUS
RIZIKOS VERTINIMAS IR NEATITIKČIŲ VALDYMAS

13. Saugumo rizika vertinama ne rečiau kaip kartą per metus, taip pat prieš pradedant naudoti naują išorinę informacinę sistemą, keičiant naudojimosi ja sąlygas, diegiant naują Centro techninę priemonę arba po reikšmingo incidento. Kibernetinio saugumo vadovas koordinuoja techninių ir kibernetinių rizikų vertinimą, DAP konsultuoja dėl poveikio asmens duomenų saugumui, o padalinių vadovai pateikia informaciją apie darbo procesus.

14. Vertinamos darbuotojų prieigos ir jų atsekamumas, galinių įrenginių ir tinklo saugumas, popierinių dokumentų apsauga, nuotolinis darbas, tiekėjų saugumo užtikrinimo galimybės, išorinių sistemų prieinamumas, veiklos tęstinumas, incidentai ir kitos Centrui aktualios rizikos. Išorinių sistemų infrastruktūros rizikos vertinamos remiantis prieinama tiekėjo ar sistemos valdytojo informacija.

15. Kai dėl numatomo asmens duomenų tvarkymo pagal BDAR 35 straipsnį reikalingas poveikio duomenų apsaugai vertinimas (PDAV), sprendimą dėl jo atlikimo priima Centras, atsižvelgdamas į DAP rekomendaciją. Techninių priemonių dalyje dalyvauja kibernetinio saugumo vadovas ir, pagal poreikį, atitinkamas paslaugų teikėjas.

16. Saugumo priemonių įgyvendinimo, kontrolės įrodymų, atsakingų vykdytojų ir nustatytų trūkumų suvestinė tvarkoma 2 priede arba jau turimuose Centro kibernetinio saugumo rizikos ir priemonių registruose, jeigu juose fiksuojami tie patys duomenys. Dvigubo registro pildyti nereikia.

17. Jeigu nustatyta saugumo priemonė dėl objektyvių priežasčių neįgyvendinta arba išorinė sistema jos techniškai nepalaiko, kibernetinio saugumo vadovas įvertina techninę ir kibernetinę riziką bei siūlo ją mažinančias priemones, o DAP konsultuoja dėl poveikio asmens duomenų saugumui ir duomenų subjektų teisėms bei laisvėms. Prireikus kreipiamasi į išorinės sistemos valdytoją ar paslaugų teikėją.

IV SKYRIUS
ORGANIZACINĖS SAUGUMO PRIEMONĖS

18. Prieš suteikiant prieigą prie asmens duomenų personalas pasirašytinai arba elektroniniu būdu supažindinamas su Politika, jam aktualiais Aprašo reikalavimais, konfidencialumo pareiga ir pranešimo apie pažeidimus tvarka bei pasirašo konfidencialumo pasižadėjimą. Supažindinimą pagal Politikos 15.4 ir 81 punktus organizuoja DAP, bendradarbiaudamas su struktūrinių padalinių vadovais ir už personalo dokumentus atsakingais darbuotojais. Supažindinimo faktas dokumentuojamas.

19. Asmens duomenų apsaugos mokymus pagal Politikos 15.4 ir 82 punktus organizuoja DAP, užtikrindamas jų turinio pritaikymą personalo funkcijoms. Kibernetinio saugumo vadovas organizuoja arba koordinuoja kibernetinio saugumo mokymus pagal Centro nustatytą periodiškumą. Mokymų data, tema ir dalyviai dokumentuojami pagal Politikos 83 punktą; naudojamas bendras Centro mokymų registras.

20. Prieigos teisių suteikimas, pakeitimas ir panaikinimas pagrindžiamas struktūrinio padalinio vadovo motyvuotu prašymu ir Centro direktoriaus arba jo įgalioto asmens sprendimu, jeigu teisės aktai ar išorinės sistemos naudojimo taisyklės nenustato kitos privalomos procedūros. Pagal Politikos 55 punktą DAP koordinuoja šių procesų atitikties asmens duomenų apsaugos reikalavimams užtikrinimą, prašymų ir sprendimų dokumentavimo kontrolę bei prieigos teisių peržiūrą. Techninius veiksmus atlieka įgaliotas atitinkamos sistemos administratorius pagal jai taikomą tvarką. Prašymas, sprendimas, įvykdymo data ir patvirtinimas dokumentuojami 1 priede arba lygiaverčiame elektroniniame registre.

21. Darbuotojai asmens duomenis gali peržiūrėti, keisti, siųsti ar kitaip naudoti tik tiek, kiek būtina pavestoms funkcijoms. Techninė galimybė atverti paciento įrašą nesuteikia teisės susipažinti su jo duomenimis ne darbo tikslu.

22. Popieriniai dokumentai ir laikmenos saugomi užrakintose vietose. Darbo vietose laikomasi švaraus stalo ir užrakinto ekrano principo; pasitraukiant iš darbo vietos atviri pacientų duomenys negali būti matomi kitiems asmenims. Pacientų duomenys neskelbiami ir neaptariami taip, kad juos galėtų išgirsti pašaliniai asmenys.

V SKYRIUS
PRIEIGŲ VALDYMAS IR TAPATYBĖS PATVIRTINIMAS

23. Centras užtikrina, kad darbuotojai išorinėmis informacinėmis sistemomis naudotųsi individualiomis paskyromis pagal suteiktas teises. Jei sistema leidžia tik bendrinį identifikatorių, vertinama rizika ir iš sistemos valdytojo prašoma užtikrinti individualių veiksmų atsekamumą arba kitą tinkamą saugumo sprendimą.

24. Išorinių informacinių sistemų privilegijuotų paskyrų valdymas ir techninė jų kontrolė priklauso tų sistemų valdytojams ar administratoriams. Centro IT administratoriaus privilegijuotos prieigos prie Centro įrenginių ir tinklo suteikiamos tik pagal patvirtintą būtinybę; jų naudojimas ir peržiūra dokumentuojami pagal Centro kibernetinio saugumo dokumentus.

25. Kelių veiksnių autentifikavimas (MFA) naudojamas Centro kontroliuojamoms nuotolinėms ir privilegijuotoms prieigoms, kai tai techniškai įmanoma ir būtina pagal riziką ar teisės aktus. Naudojantis išorinėmis sistemomis taikomos jų nustatytos tapatybės patvirtinimo priemonės. Jei jautrius duomenis tvarkančioje sistemoje MFA nėra, kibernetinio saugumo vadovas ir DAP įvertina riziką, dokumentuoja papildomas priemones ir prireikus kreipiasi į sistemos valdytoją. Autentifikavimo priemonių naudojimui taip pat taikomi šie reikalavimai:

25.1. darbuotojas privalo naudoti jam skirtas autentifikavimo priemones ir neperduoti jų kitiems asmenims;

25.2. Centro techninėms prieigoms taikomos Centro patvirtintos autentifikavimo taisyklės, o išorinių sistemų paskyroms – jų valdytojų taisyklės, nepažeidžiant privalomų teisės aktų reikalavimų.

26. Darbuotojų naudojami slaptažodžiai ar kitos prisijungimo priemonės negali būti perduodami kitiems. Centro valdomų įrenginių ir paslaugų slaptažodžiams, kai tokį metodą galima nustatyti, taikomas ne trumpesnis kaip 12 simbolių reikalavimas arba lygiavertė riziką mažinanti autentifikavimo priemonė. Išorinėse sistemose laikomasi jų patvirtintų autentifikavimo reikalavimų.

27. Centro darbo vietos užrakinamos automatiškai ne vėliau kaip po 15 minučių neveikimo, kai technologijos leidžia. Išorinių informacinių sistemų sesijų apribojimus nustato jų administratoriai; Centras praneša apie nustatytus trūkumus ir, esant poreikiui, taiko papildomas darbo vietos apsaugos priemones.

28. Pasikeitus darbuotojo funkcijoms ar pasibaigus darbo arba kitiems santykiams su Centru, padalinio vadovas nedelsdamas inicijuoja nebereikalingų prieigos teisių pakeitimą ar panaikinimą. Politikos 56 punkte nustatyta, kad pasikeitus funkcijoms nereikalingos teisės panaikinamos ne vėliau kaip kitą darbo dieną, o pasibaigus santykiams – ne vėliau kaip paskutinę jų dieną. Centro įgaliotas asmuo laiku pateikia prašymą išorinės sistemos administratoriui ir kontroliuoja įvykdymo patvirtinimo gavimą; jei išorinės sistemos taisyklės ar techninės aplinkybės neleidžia užtikrinti nustatyto termino, nedelsiant kreipiamasi dėl prieigos apribojimo ir informuojamas direktorius bei DAP.

29. Ne rečiau kaip kartą per metus DAP koordinuoja Centro darbuotojams suteiktų prieigų poreikio peržiūrą kartu su padalinių vadovais. Kibernetinio saugumo vadovas koordinuoja Centro kontroliuojamų privilegijuotų prieigų prie įrenginių ir tinklo peržiūrą pagal riziką, paprastai ne rečiau kaip kas šešis mėnesius. Išorinių sistemų privilegijuotų paskyrų auditas yra jų valdytojų atsakomybė, išskyrus Centrui suteiktas administravimo teises.

VI SKYRIUS
FIZINĖS SAUGUMO PRIEMONĖS

30. Centro patalpos, kuriose tvarkomi ar saugomi asmens duomenys, taip pat Centre esanti kompiuterinė ir tinklo įranga apsaugomi nuo neteisėtos prieigos, vagystės, sugadinimo, gaisro ir kitų aktualių rizikų. Priemones pagal kompetenciją įgyvendina už ūkį atsakingi asmenys, IT administratorius ir struktūrinių padalinių vadovai.

31. Centras netaiko išorinių informacinių sistemų serverinių apsaugos procedūrų toms patalpoms, kurių nevaldo. Jeigu Centras turi vietinio tinklo įrangos ar duomenų laikmenų saugojimo vietas, į jas įleidžiami tik įgalioti asmenys; išorinių sistemų infrastruktūros fizinę saugą užtikrina jų valdytojai.

32. Popieriniai dokumentai, išorinės laikmenos, mobilieji ir nešiojamieji įrenginiai, kuriuose gali būti asmens duomenų, nepaliekami be priežiūros viešose ar pašaliniams prieinamose vietose.

33. Prieš perduodant nebenaudojamą Centro įrangą ar laikmenas tretiesiems asmenims, joje saugoti asmens duomenys saugiai ištrinami arba laikmenos sunaikinamos.

VII SKYRIUS
TECHNINĖS IR NUOTOLINIO DARBO PRIEMONĖS

34. Centro valdomuose kompiuteriuose ir vietiniame tinkle pagal riziką įdiegiamos ugniasienės, kenkėjiškos programinės įrangos apsauga, sistemos saugos atnaujinimai ir kitos reikalingos priemonės. Techninį įgyvendinimą vykdo IT administratorius; kibernetinio saugumo vadovas prižiūri kontrolės vykdymą. Išorinių sistemų infrastruktūros apsaugos priemonės priklauso jų valdytojų kompetencijai.

35. Centro darbo vietose naudojama palaikoma, saugos atnaujinimus gaunanti programinė įranga. Kai jos pakeisti nedelsiant neįmanoma, dokumentuojamas rizikos vertinimas ir tvirtinamos laikinos saugumo priemonės pagal 17 punktą.

36. Pacientų sveikatos duomenys iš Centro darbo vietų perduodami tik patvirtintais saugiais kanalais. Nešiojamuose įrenginiuose ir leidžiamose išorinėse laikmenose esantys asmens duomenys saugomi šifruojant, kai tai techniškai įmanoma ir būtina pagal riziką. Išorinių sistemų serverių, duomenų saugyklų ir šifravimo raktų valdymą užtikrina jų valdytojai pagal jiems taikomus reikalavimus.

37. Centras savo informacinių sistemų kūrimo ar testavimo aplinkų pagal šį Aprašą neadministruoja.

38. Nuotolinis darbas su asmens duomenimis leidžiamas tik Centro patvirtintomis priemonėmis ir pagal naudojamos išorinės sistemos taisykles. Privalomos individualios prisijungimo priemonės, saugus ryšys ir kitos pagal riziką nustatytos kontrolės. Draudžiama naudoti nepatvirtintas privačias elektroninio pašto paskyras ir duomenų saugyklas.

39. IT administratorius pagal paskirtas funkcijas tvarko Centro darbui patvirtintų įrenginių ir, kai aktualu, išorinių laikmenų sąrašą. Asmens duomenys kopijuojami į išorines laikmenas tik turint darbo būtinybę ir Centro leidimą.

40. Nešiojamuose ir mobiliuosiuose Centro darbo įrenginiuose pagal riziką taikomas ekrano užrakinimas, tapatybės patvirtinimas, šifravimas ir pametus įrenginį taikomos reagavimo priemonės.

VIII SKYRIUS
ATSARGINĖS KOPIJOS IR VEIKLOS TĘSTINUMAS

41. Centras neadministruoja naudojamų išorinių sveikatos informacinių sistemų atsarginių kopijų; jų kūrimą, saugojimą ir atkūrimą vykdo atitinkami sistemų valdytojai ar paslaugų teikėjai pagal jiems taikomus teisės aktus ir susitarimus. Centro valdomų vietinių dokumentų bei kitų duomenų atsarginių kopijų poreikį, vykdytoją ir periodiškumą nustato kibernetinio saugumo vadovas kartu su IT administratoriumi, atsižvelgdami į riziką.

42. Kibernetinio saugumo vadovas, bendradarbiaudamas su DAP, pagal Centro turimą teisę ir galimybes inicijuoja išorinių sistemų duomenų prieinamumo, atsarginių kopijų ar paslaugų atkūrimo garantijų patikrą ir dokumentuoja gautus patvirtinimus. Centro vietinių duomenų kopijos apsaugomos nuo neteisėto naudojimo, pakeitimo ar sunaikinimo.

43. Centras nustato veiklos tęstinumo veiksmus, kai išorinė informacinė sistema laikinai neveikia: atsakingus kontaktus, incidento eskalavimo būdą, būtinuosius popierinių ar kitų teisėtų laikinųjų veiksmų procesus ir saugų duomenų suvedimą sistemai atkūrus veikimą. Techninius sistemos atkūrimo laikus nustato sistemos valdytojas ar atitinkami susitarimai.

44. Kibernetinio saugumo vadovas kasmet arba po reikšmingo sutrikimo peržiūri veiklos tęstinumo priemonių pakankamumą ir, kai prieinama, iš paslaugų teikėjų gautą kopijų bei atkūrimo testų informaciją. Centro valdomų vietinių duomenų atkūrimo bandymus organizuoja IT administratorius pagal dokumentuotą riziką. Duomenys apie patikrą įtraukiami į 2 priedo suvestinę arba bendrą kibernetinio saugumo kontrolės registrą.

IX SKYRIUS
NAUDOTOJŲ VEIKSMŲ IR SAUGUMO ĮVYKIŲ ŽURNALAI

45. Naudotojų veiksmų išorinėse informacinėse sistemose registravimo funkcijas techniškai užtikrina tų sistemų valdytojai ar administratoriai. Centras pagal teisės aktus ir naudojimosi sąlygas inicijuoja teisėtai reikalingų prieigos prie pacientų duomenų žurnalinių įrašų gavimą, jų tikrinimą ir nustatytų neatitikčių tyrimą. Centro darbo vietų bei tinklo techninių įvykių registravimą pagal kompetenciją užtikrina IT administratorius.

46. Tikrinant naudotojų prieigų teisėtumą, siekiama nustatyti darbuotoją, veiksmo laiką, prieigos pobūdį ir pakankamą nuorodą į tikrintą objektą. Jeigu informacinės sistemos žurnaliniai įrašai neleidžia nustatyti šių aplinkybių arba neregistruoja Politikos 65 punkte nurodytų duomenų, apie trūkumą sužinojęs IT administratorius arba kitas patikrą atliekantis įgaliotas asmuo nedelsdamas informuoja Centro direktorių ir DAP. DAP dokumentuoja asmens duomenų apsaugos neatitiktį ir teikia rekomendacijas, o IT administratorius pagal jam pavestas funkcijas padeda kreiptis į išorinės sistemos valdytoją dėl veiksmų atsekamumo užtikrinimo. Centro direktorius priima sprendimus dėl papildomų Centro kompetencijai priskirtų saugumo priemonių.

47. Prieiga prie išorinių sistemų žurnalinių įrašų suteikiama pagal tų sistemų valdytojų nustatytą tvarką. Centro vardu įrašus gali gauti ir analizuoti direktoriaus įgalioti asmenys tik tiek, kiek būtina jų funkcijoms vykdyti. DAP konsultuoja dėl pacientų duomenų prieigų teisėtumo, kibernetinio saugumo vadovas – dėl techninių įvykių vertinimo. Patikrų organizavimas, periodiškumas ir rezultatų dokumentavimas nustatyti 49 punkte. Žurnalų kopijos saugomos tik tiek, kiek būtina teisėtam tikrinimo ar tyrimo tikslui.

48. Išorinių informacinių sistemų žurnalinių įrašų saugojimo terminus nustato jų valdytojai pagal taikomus teisės aktus ir saugojimo taisykles; Centras šių terminų vienašališkai nenustato.

49. DAP organizuoja rizika pagrįstas darbuotojų prieigos prie pacientų duomenų teisėtumo patikras, o kibernetinio saugumo vadovas – Centro įrenginių ir tinklo techninių saugumo įvykių peržiūrą. Patikrų dažnumas ir imtys nustatomi pagal riziką ir turimas prieigos prie žurnalų galimybes; esant pagrįstam įtarimui patikra atliekama nedelsiant. Rezultatai dokumentuojami 3 priede arba lygiaverčiame Centro tyrimų ar auditų registre.

X SKYRIUS
PASLAUGŲ TEIKĖJAI IR DUOMENŲ NAIKINIMAS

50. Prieš sudarant ar keičiant sutartį su paslaugų teikėju, vykdančiu IT administratoriaus funkcijas, arba kitu duomenis tvarkančiu tiekėju, pagal realų jo vaidmenį įvertinamos BDAR 28 straipsnio sąlygos, konfidencialumo, prieigos, incidentų informavimo, saugumo ir veiklos tęstinumo reikalavimai.

51. Popieriniai ir Centro valdomose laikmenose esantys asmens duomenys pasibaigus taikytinam saugojimo terminui naikinami arba teisėtu būdu nuasmeninami pagal Politiką ir dokumentų valdymo teisės aktus. Išorinėse sistemose asmens duomenų saugojimas ir naikinimas vykdomas pagal tų sistemų valdytojų kompetenciją ir taikomas teisės normas.

52. Prieš reikšmingą Centro naudojamų technologijų, paslaugų teikėjų ar duomenų tvarkymo būdo pakeitimą padalinio vadovas informuoja DAP ir kibernetinio saugumo vadovą. Šie pagal kompetenciją įvertina riziką, poreikį atnaujinti veiklos įrašus, privatumo pranešimus, sutartis ir kibernetinio saugumo dokumentus.

XI SKYRIUS
KONTROLĖ IR BAIGIAMOSIOS NUOSTATOS

53. Ne rečiau kaip kartą per metus kibernetinio saugumo vadovas organizuoja Centro taikomų techninių ir organizacinių saugumo priemonių peržiūrą, o DAP – asmens duomenų apsaugos atitikties kontrolę. Peržiūra gali būti įforminama vienoje 2 priedo suvestinėje arba kituose Centro jau naudojamuose registruose, jei užtikrinamas sprendimų ir įrodymų atsekamumas.

54. Personalas, nustatęs saugumo priemonės neatitiktį ar pagrįstai įtaręs neteisėtą asmens duomenų tvarkymą, nedelsdamas informuoja DAP, o kai neatitiktis techninio ar kibernetinio pobūdžio – ir kibernetinio saugumo vadovą. DAP pagal Politikos 85 punktą organizuoja asmens duomenų apsaugos aplinkybių įvertinimą, informuoja Centro direktorių ir teikia rekomendacijas.

55. Įtarus ar nustačius asmens duomenų saugumo pažeidimą, nedelsiant taikomas Centro asmens duomenų saugumo pažeidimų valdymo tvarkos aprašas. DAP koordinuoja asmens duomenų pažeidimo vertinimą ir dokumentavimą, kibernetinio saugumo vadovas – techninių incidento aplinkybių ir kibernetinio saugumo veiksmų koordinavimą, o direktorius priima jam priskirtus sprendimus dėl pranešimų ir priemonių. Šių funkcijų vykdymas neturi uždelsti BDAR 33 ir 34 straipsnių terminų.

56. Įgyvendinimo įrodymai – prieigų prašymai, tiekėjų patvirtinimai, auditų rezultatai, rizikos vertinimai ir priimti sprendimai – saugomi Centro dokumentacijos plane nustatytais terminais, laikantis teisėto pagrindo ir būtino duomenų kiekio principo.

57. DAP ne rečiau kaip kartą per metus peržiūri Aprašo ir asmens duomenų tvarkymo veiklos įrašų, privatumo pranešimų, duomenų tvarkymo sutarčių bei kitų BDAR dokumentų tarpusavio suderinamumą. Kibernetinio saugumo vadovas vertina ryšį su Centro kibernetinio saugumo dokumentais.

58. Aprašo peržiūrą organizuoja DAP, bendradarbiaudamas su kibernetinio saugumo vadovu, ne rečiau kaip kartą per metus ir esant reikšmingiems teisiniams, technologiniams ar veiklos pokyčiams, taip pat po reikšmingo asmens duomenų saugumo pažeidimo. Pasiūlymai dėl pakeitimų teikiami Centro direktoriui.

59. Darbuotojai supažindinami su Aprašu Politikos nustatyta tvarka. Aprašo nesilaikymo pasekmės nustatomos pagal taikomus teisės aktus, Centro vidaus dokumentus ir su paslaugų teikėjais sudarytas sutartis.

60. Aprašas ir jo pakeitimai tvirtinami Centro direktoriaus įsakymu.

Telšių rajono pirminės sveikatos priežiūros centro
asmens duomenų saugumo priemonių aprašo
1 priedas

(Naudotojų prieigos suteikimo, keitimo ir panaikinimo registravimo forma)

Sistemos valdytojo patvirtintas prašymas ar elektroninis įrašas gali pakeisti šią formą, jei užfiksuoti analogiški duomenys. Prieigos poreikį nustato padalinio vadovas; sprendimą priima direktorius arba jo įgaliotas asmuo; techninį veiksmą atlieka išorinės sistemos administratorius. Atsakingas asmuo organizuoja dokumentavimą, DAP atlieka atitikties priežiūrą.

Eil. Nr.	Darbuotojas, padalinys	Išorinė sistema ir reikalinga prieigos apimtis	Veiksmas (suteikti / keisti / panaikinti), motyvas	Padalinio vadovo prašymo data	Sprendimas, data, patvirtinęs	Sistemos administratoriaus įvykdymas, data	DAP atitikties kontrolės pastaba
1.							
2.							
3.							
4.							

Pastaba. Prieigos panaikinimo užklausos ir įvykdymo patvirtinimai saugomi kartu su šiuo registru arba kitame atsekamame dokumentų valdymo kanale.

Telšių rajono pirminės sveikatos priežiūros centro
asmens duomenų saugumo priemonių aprašo
2 priedas

(Asmens duomenų saugumo priemonių kontrolės ir neatitikčių suvestinė)

Pildoma metinės peržiūros, rizikos vertinimo ar reikšmingo neatitikimo metu. Jeigu tos pačios sritys užregistruotos galiojančiame Centro kibernetinio saugumo priemonių registre, papildoma forma nepildoma.

Eil. Nr.	Sritis / patikros objektas	Atsakingas vykdytojas ar sistemos valdytojas	Vertinimo įrodymas (dokumento / atsakymo nuoroda)	Būklė ir nustatytas trūkumas	Siūloma priemonė, vykdytojas, terminas	DAP / kibernetinio saugumo vadovo išvada
1.	Prieigos teisių poreikio peržiūra					
2.	Išorinių sistemų autentifikavimas ir MFA					
3.	Centro darbo vietų ir tinklo saugumas					
4.	Popierinių dokumentų ir patalpų apsauga					
5.	Išorinių sistemų paslaugų saugumas ir prieinamumas					
6.	Atsarginių kopijų / atkūrimo patvirtinimai, jei prieinami					
7.	Darbuotojų prieigų žurnalų peržiūra					
8.	Saugumo incidentai, pažeidimai, taisomieji veiksmai					
9.	Mokymai, supažindinimas, konfidencialumas					
10.	Veiklos tęstinumo procedūros					
11.	Saugumo priemonės neįgyvendinimas / likutinė rizika					
12.	BDAR ir kibernetinio saugumo dokumentų sąsajos					

Peržiūros data: _____ DAP: _____ Kibernetinio saugumo vadovas: _____

Direktoriaus sprendimas dėl reikšmingų neatitikčių: _____

_____

Telšių rajono pirminės sveikatos priežiūros centro
asmens duomenų saugumo priemonių aprašo
3 priedas

(Naudotojų veiksmų ir saugumo įvykių žurnalų peržiūros forma)

Pildoma gavus iš išorinės sistemos valdytojo atitinkamus išrašus arba atliekant Centro kontroliuojamų įrenginių / tinklo žurnalų patikrą. Pacientų identifikavimo duomenų čia nedubliuoti; naudoti tyrimo ar registracijos numerį.

Eil. Nr.	Patikros data	Sistema ir žurnalo šaltinis	Patikros pagrindas ir apimtis	Nustatytos aplinkybės (be perteklinių asmens duomenų)	Tolesnis veiksmas, terminas	Patikrą atliko	DAP / kibernetinio saugumo vadovo pastaba
1.							
2.							
3.							
4.							

Pastaba. Prireikus detalesni žurnalų išrašai saugomi prie konkretaus patikros ar pažeidimo tyrimo bylos, taikant ribotą prieigą.