APSTIPRINĀTS
ar SIA "Rīgas Austrumu klīniskā universitātes slimnīca"
valdes 2026. gada 06. augusta
lēmumu Nr.V1/01-01/26/192

SIA "Rīgas Austrumu klīniskā universitātes slimnīca"

Fizisko personu datu apstrādes noteikumi

Satura rādītājs

I. Lietotie termini ... 3

II. Noteikumu mērķis un piemērošanas joma ... 6

III. Galvenie datu aizsardzības principi ... 8

IV. Personas datu apstrādes organizēšana ... 8

V. Pacientu datu konfidencialitāte ... 11

VI. Personas datu apstrādes tiesiskais pamats un datu subjektu informēšana ... 12

VII. Piekļuves tiesības un piekļuves kontrole ... 13

VIII. Lietotāju konti, paroles, autentifikācija un darba vietas drošība ... 14

IX. Personas datu izmantošana, glabāšana, labošana ... 15

X. Medicīniskās dokumentācijas apstrāde ... 16

XI. Personas datu izpaušana ... 16

XII. Datu subjektu pieprasījumu izskatīšana ... 17

XIII. Personas datu apstrādes darbību reģistrs ... 18

XIV. Personas datu dzēšana un iznīcināšana ... 19

XV. Slimnīcas personāla pienākumi, tiesības un atbildība personas datu apstrādē ... 19

XVI. Personāla rīcība drošības incidentu un personas datu aizsardzības pārkāpumu gadījumā ... 22

XVII. Personāla apmācības un konfidencialitātes apliecinājumi ... 24

XVIII. Vadības, apstrādes procesa īpašnieku, struktūrvienību un datu aizsardzības speciālista atbildība ... 24

XIX. Iekšējā kontrole, audits un auditācijas pieraksti ... 25

XX. Noslēguma noteikumi ... 26

I. Lietotie termini

1. Iekšējā normatīvajā aktā "Fizisko personu datu apstrādes noteikumi" lietotie termini un saīsinājumi (alfabētiskā secībā):

1.1. **anonimizācija** – personas datu neatgriezeniska pārveidošana tādā veidā, ka datu subjektu vairs nav iespējams identificēt ne tieši, ne netieši, izmantojot saprātīgi pieejamus līdzekļus. Anonimizēti dati vairs nav uzskatāmi par personas datiem, ja anonimizācija ir veikta neatgriezeniski un nav iespējama personas atkārtota identificēšana;

1.2. **atbildīgā struktūrvienība** – Slimnīcas struktūrvienība, kuras kompetencē ir konkrētā personas datu apstrādes procesa īstenošana un kuras vadītājs vai cita Slimnīcas noteikta atbildīgā persona ir attiecīgās personas datu apstrādes procesa īpašnieks.

1.3. **apstrādātājs** – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus;

1.4. **apstrādes darbību reģistrs** – Slimnīcas uzturēts reģistrs, kurā tiek dokumentētas personas datu apstrādes darbības, tostarp apstrādes nolūki, tiesiskie pamati, datu subjekti un datu kategorijas, saņēmēji, glabāšanas termiņi un drošības pasākumi;

1.5. **apstrādes procesa īpašnieks** – Slimnīcas noteikts struktūrvienības vadītājs vai cita atbildīgā persona, kura savā darbības jomā atbild par konkrētās personas datu apstrādes nepieciešamību, nolūku, organizēšanu, tiesiskumu, dokumentēšanu, risku identificēšanu un izvērtēšanu, atbilstošu tehnisko un organizatorisko pasākumu ieviešanu, kā arī personas datu apstrādes atbilstības uzraudzību;

1.6. **autentifikācija –** process, kura laikā tiek pārbaudīta lietotāja identitāte pirms piekļuves piešķiršanas informācijas sistēmai vai personas datiem;

1.7. **autorizācija** – process, kura laikā pēc lietotāja autentifikācijas tiek noteikts tam piešķirto piekļuves tiesību apjoms;

1.8. **biometriskie dati** – personas dati, kas iegūti pēc specifiskas tehniskas apstrādes un attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprināt minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli;

1.9. **darba vieta** – vieta, kurā darbinieks, personāls vai cita pilnvarota persona veic personas datu apstrādi, tostarp telpa, kabinets, reģistratūras zona, nodaļas postenis, arhīvs, informācijas sistēma, attālinātā darba vieta vai cita vieta, kur tiek apstrādāti personas dati;

1.10. **darbinieks** – fiziska persona, ar kuru Slimnīca ir nodibinājusi darba tiesiskās attiecības un kura amata pienākumu izpildes ietvaros var apstrādāt personas datus;

1.11. **datu aizsardzības speciālists -** Slimnīcas iecelta persona, kura neatkarīgi veic VDAR un piemērojamajos normatīvajos aktos noteiktos datu aizsardzības speciālista uzdevumus, tostarp informē, konsultē, uzrauga atbilstību, sniedz atzinumus par NIDA un sadarbojas ar Datu valsts inspekciju kā uzraudzības iestādi;

1.12. **datu subjekta piekrišana** – datu subjekta brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru datu subjekts paziņojumā vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei;

1.13. **datu subjekts** – fiziskā persona, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem (piemēram, pacients, kandidāts, pacienta likumiskais pārstāvis);

1.14. **daudzfaktoru autentifikācija** – lietotāja identitātes apstiprināšana, izmantojot vismaz divus neatkarīgus autentifikācijas faktorus (piemēram, paroli un vienreizējo kodu vai viedierīces apstiprinājumu);

1.15. **drošības incidents** – notikums vai notikumu kopums, kas rada vai var radīt apdraudējumu informācijas drošībai vai personas datu aizsardzībai;

1.16. **ģenētiskie dati** – personas dati, kas attiecas uz fiziskas personas mantotām vai iegūtām ģenētiskajām pazīmēm un kas izriet no attiecīgās fiziskās personas bioloģiskā parauga analīzes, jo īpaši hromosomu, dezoksiribonukleīnskābes (DNS) vai ribonukleīnskābes (RNS) analīzes, vai no cita elementa analīzes, kas ļauj iegūt līdzvērtīgu informāciju;

1.17. **informācijas sistēma** – elektroniska sistēma vai programmatūras risinājums, kurā tiek uzglabāti, apstrādāti vai pārvaldīti personas dati vai cita Slimnīcas informācija;

1.18. **īpašo kategoriju personas dati** – personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, kā arī ģenētiskie dati, biometriskie dati, ja tos apstrādā fiziskas personas unikālas identifikācijas nolūkā, veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju;

1.19. **glabāšanas ierobežojums** – princips, saskaņā ar kuru personas dati tiek glabāti tikai tik ilgi, cik nepieciešams personas datu apstrādes nolūka sasniegšanai vai piemērojamo normatīvo aktu prasību izpildei;

1.20. **konfidenciāla informācija** – informācija, kurai Slimnīcā ir noteikta ierobežota pieejamība vai kuras izpaušana var radīt kaitējumu pacientam, darbiniekam, personālam, Slimnīcai vai citai personai, tostarp personas dati, pacientu dati, medicīniskā dokumentācija, komercnoslēpums, drošības informācija un cita iekšējā informācija;

1.21. **likumiskais pārstāvis** – persona, kura saskaņā ar normatīvajiem aktiem ir tiesīga pārstāvēt datu subjektu;

1.22. **medicīniskā dokumentācija** – dokumenti un ieraksti, kuros tiek fiksēta ar pacienta veselības aprūpi saistīta informācija, tostarp ambulatorās un stacionārās kartes, izraksti, izmeklējumu rezultāti, nosūtījumi, epikrīzes, piekrišanas, atteikumi, ārstniecības ieraksti un cita ārstniecības procesā radīta dokumentācija;

1.23. **NIDA** – novērtējums par ietekmi uz datu aizsardzību, ko veic pirms tādas personas datu apstrādes uzsākšanas, kura var radīt augstu risku fizisku personu tiesībām un brīvībām;

1.24. **Noteikumi** – SIA "Rīgas Austrumu klīniskā universitātes slimnīca" fizisko personu datu apstrādes noteikumi;

1.25. **parole** – simbolu, rakstzīmju vai citu autentifikācijas elementu kopums, kuru izmanto, lai piekļūtu datoram, informācijas sistēmai, lietotāja kontam, lietojumprogrammai vai personas datu apstrādes sistēmai;

1.26. **pārzinis** – fiziskā vai juridiskā persona, valsts vai pašvaldību institūcija, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar likumu. Personas datu apstrādes pārzinis Noteikumu izpratnē ir Slimnīca;

1.27. **personas dati** – jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu. Personas datiem piekļūst tikai pilnvarotas personas savu darba vai citu tiesisko pienākumu izpildei nepieciešamajā apjomā;

1.28. **personas datu apstrāde –** jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrēšana, organizēšana, strukturēšana, glabāšana, pielāgošana, pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot datus pieejamus, saskaņošana, kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

1.29. **personas datu apstrādes sistēma** – strukturēts informācijas sistēmu, datubāzu, lietojumprogrammu, reģistru, kartotēku, dokumentu kopums vai citu tehnisku un organizatorisku līdzekļu kopums, kurā sistematizēti tiek apstrādāti personas dati elektroniskā, papīra vai citā formā;

1.30. **personas datu aizsardzības pārkāpums** – drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai neatļauta piekļuve tiem;

1.31. **personas datu lietotājs** – Slimnīcas darbinieks, personāls, apstrādātāja darbinieks vai cita Slimnīcas pilnvarota persona, kurai amata, līguma, prakses, mācību vai cita tiesiska pamata ietvaros ir piešķirta piekļuve personas datiem vai personas datu apstrādes sistēmām;

1.32. **personas datu minimizācija** – princips, saskaņā ar kuru tiek apstrādāti tikai tādi personas dati un tādā apjomā, kas ir atbilstošs, nepieciešams un samērīgs konkrētā apstrādes nolūka sasniegšanai;

1.33. **personas datu saņēmējs** – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai tiek izpausti personas dati, neatkarīgi no tā, vai tā ir vai nav trešā persona;

1.34. **personas datu saņēmēju kategorijas** – personas datu saņēmēju grupas, piemēram, ārstniecības iestādes, valsts institūcijas, laboratorijas, apdrošinātāji, IT pakalpojumu sniedzēji un citi personas datu saņēmēji;

1.35. **personāls** – Slimnīcas darbinieki, ārstniecības personas, rezidenti, doktoranti, praktikanti, studenti, brīvprātīgie, kā arī citas personas, kuras Slimnīcas uzdevumā vai tās telpās piedalās darba, mācību, prakses, ārstniecības, administratīvo vai atbalsta funkciju izpildē un kurām var tikt nodrošināta piekļuve personas datiem;

1.36. **piekļuves tiesības** - personas datu lietotājam piešķirts tiesību apjoms piekļūt konkrētām informācijas sistēmām, dokumentiem, datu kategorijām vai funkcionalitātēm, ievērojot amata pienākumus un **nepieciešamības zināt (need-to-know)** un minimālo piekļuves tiesību principu.

1.37. **piemērojamie normatīvie akti** – normatīvie akti, kas piemērojami Slimnīcas veiktajai personas datu apstrādei, tostarp VDAR, Fizisko personu datu apstrādes likums, Pacientu tiesību likums, Ārstniecības likums, Medicīnisko dokumentu lietvedības kārtību regulējošie normatīvie

akti, kā arī citi Latvijas Republikas un Eiropas Savienības tiesību akti, kas attiecas uz personas datu apstrādi, pacientu datu aizsardzību, ārstniecības procesu un informācijas drošību;

1.38. **profilēšana** – jebkura veida personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos;

1.39. **pseidonimizācija** – personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu;

1.40. **Slimnīca –** SIA "Rīgas Austrumu klīniskā universitātes slimnīca", kura ir publiskas personas kapitālsabiedrība, kuras 100% valsts kapitālu daļu turētājs ir Latvijas Republikas Veselības ministrija;

1.41. **tehniski un organizatoriski drošības pasākumi** – tehnisku, fizisku, administratīvu un organizatorisku pasākumu kopums, kas paredzēts, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu, nozaudēšanu, pārveidošanu, neatļautu izpaušanu, neatļautu piekļuvi vai citām nelikumīgām apstrādes darbībām, ņemot vērā apstrādes raksturu, apjomu, kontekstu, nolūkus un riskus fizisku personu tiesībām un brīvībām.;

1.42. **trešā persona** – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura nav datu subjekts, pārzinis, apstrādātājs vai persona, kura pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarota apstrādāt personas datus;

1.43. **VDAR** - Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula);

1.44. **veselības dati** – personas dati, kas saistīti ar fiziskas personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu, un kas atspoguļo informāciju par tās veselības stāvokli.

Šajos Noteikumos lietotie termini, kas nav īpaši definēti, interpretējami atbilstoši VDAR, Fizisko personu datu apstrādes likumam un Pacientu tiesību likumam.

II. Noteikumu mērķis un piemērošanas joma

2. Noteikumu mērķis ir noteikt vienotu kārtību personas datu likumīgai, godprātīgai, pārredzamai un drošai apstrādei Slimnīcā, nodrošināt fizisko personu tiesību un brīvību aizsardzību, kā arī Slimnīcas pārskatatbildības principa īstenošanu un spēju uzskatāmi apliecināt personas datu apstrādes atbilstību piemērojamo normatīvo aktu prasībām.
3. Personas datu apstrādi Slimnīcā veic saskaņā ar VDAR, Fizisko personu datu apstrādes likumu, Pacientu tiesību likumu, citiem veselības aprūpes, medicīniskās dokumentācijas, informācijas

atklātības, dokumentu un arhīvu pārvaldības, kā arī informācijas un komunikācijas tehnoloģiju drošības jomu regulējošiem normatīvajiem aktiem un Slimnīcas iekšējiem normatīvajiem aktiem.

4. Noteikumi nosaka personas datu apstrādes principus un vispārīgās prasības, tostarp:
   4.1. personas datu apstrādes organizēšanas un atbildības sadalījuma pamatprincipus;
   4.2. lietotāju piekļuves tiesību piešķiršanas, izmantošanas, pārskatīšanas un anulēšanas pamatprasības;
   4.3. pacientu datu un citas konfidenciālas informācijas aizsardzības prasības;
   4.4. personas datu iegūšanas, izmantošanas, izpaušanas, nosūtīšanas, glabāšanas, arhivēšanas, dzēšanas un iznīcināšanas pamatprasības;
   4.5. personas datu aizsardzības pārkāpumu identificēšanas, iekšējās ziņošanas, izvērtēšanas un paziņošanas pamatprasības;
   4.6. datu subjektu pieprasījumu un sūdzību izskatīšanas pamatprasības;
   4.7. prasības datu apstrādes izmaiņu un ar tām saistīto risku sākotnējai identificēšanai un izvērtēšanai saskaņā ar Slimnīcas Risku pārvaldības metodiku, papildus izvērtējot iespējamo ietekmi uz fizisku personu tiesībām un brīvībām;
   4.8. personāla pienākumus un atbildību personas datu apstrādes jomā.
5. Noteikumu prasības ir saistošas Slimnīcas personālam, kā arī pakalpojumu sniedzējiem, sadarbības partneriem un citām personām tādā apjomā, kādā šīs personas Slimnīcas uzdevumā vai saistībā ar Slimnīcas darbību apstrādā personas datus. Personas datu apstrādē iesaistīto pušu statuss, pienākumi un atbildība nosakāmi atbilstoši faktiskajiem apstrādes apstākļiem, noslēgtajiem līgumiem un piemērojamo normatīvo aktu prasībām.
6. Noteikumi piemērojami personas datu apstrādei, ko Slimnīca veic vai kas tiek veikta Slimnīcas vārdā, neatkarīgi no personas datu formas, izmantotajiem tehniskajiem līdzekļiem, informācijas nesēja, apstrādes vietas vai formas, tostarp informācijas sistēmās, medicīniskajā dokumentācijā, lietvedības un arhīva dokumentos, elektroniskajā pastā, datu nesējos, audio un video ierakstos un videonovērošanas sistēmās.
7. Noteikumos noteiktās konfidencialitātes, informācijas izpaušanas un drošības prasības piemēro arī mutiskai, vizuālai un citā veidā uztveramai informācijai, ciktāl tā satur personas datus, informāciju par pacientu vai citu Slimnīcas aizsargājamu informāciju.
8. Noteikumi neattiecas uz fiziskas personas veiktu pilnībā privātu personas datu apstrādi, kas nav saistīta ar Slimnīcas darbību un kurā netiek izmantoti Slimnīcas rīcībā esoši personas dati vai citi Slimnīcas resursi.
9. Ja Slimnīcas iekšējie normatīvie akti vai šie Noteikumi nosaka stingrākas personas datu aizsardzības prasības, nekā minimāli paredzēts ārējos normatīvajos aktos, personālam un citām personām, uz kurām attiecas Noteikumi, ir pienākums ievērot stingrākās prasības, ciktāl tās nav pretrunā ārējiem normatīvajiem aktiem.
10. Struktūrvienību vadītāji nodrošina, ka viņu padotībā vai pārraudzībā esošais personāls ir iepazīstināts ar šiem Noteikumiem un ievēro tajos noteiktās prasības.

11. Ja personas datu apstrādei piemērojami arī citi Slimnīcas iekšējie normatīvie akti, šie Noteikumi piemērojami kopā ar tiem, ciktāl tie nav savstarpēji pretrunā.

III. Galvenie datu aizsardzības principi

12. Slimnīca personas datu apstrādē ievēro likumības, godprātības un pārredzamības, nolūka ierobežojuma, datu minimizēšanas, precizitātes, glabāšanas ierobežojuma, integritātes un konfidencialitātes, kā arī pārskatatbildības principus. Personas dati apstrādājami tikai tad, ja pastāv konkrēts apstrādes nolūks un atbilstošs tiesiskais pamats.
13. Personas dati tiek vākti konkrētiem, skaidriem un leģitīmiem nolūkiem un netiek apstrādāti ar šiem nolūkiem nesavietojamā veidā.
14. Personas dati tiek apstrādāti tikai tādā apjomā, kas nepieciešams konkrētā nolūka sasniegšanai. Personālam ir aizliegts piekļūt, aplūkot, vākt, kopēt, izdrukāt, saglabāt vai citādi apstrādāt personas datus, ja tas nav nepieciešams amata pienākumu izpildei vai uzdevumu izpildei.
15. Slimnīca veic saprātīgus pasākumus, lai personas dati būtu precīzi un, ja nepieciešams, atjaunināti. Neprecīzi personas dati tiek laboti vai dzēsti saskaņā ar piemērojamajiem normatīvajiem aktiem un Slimnīcas iekšējo kārtību.
16. Personas dati tiek glabāti identificējamā veidā ne ilgāk, kā nepieciešams apstrādes nolūka sasniegšanai vai normatīvajos aktos noteikto pienākumu izpildei.
17. Slimnīca nodrošina personas datu integritāti, konfidencialitāti un pieejamību, izmantojot riskam atbilstošus tehniskus un organizatoriskus drošības pasākumus.
18. Slimnīca nodrošina pārskatatbildību, uzturot un dokumentējot būtiskos personas datu apstrādes procesus, lēmumus, piekļuves tiesības, datu izpaušanu, incidentus, veiktos drošības pasākumus un citus pierādījumus par atbilstību piemērojamo normatīvo aktu prasībām.
19. Ikviens Slimnīcas personāla loceklis, kurš amata vai cita tiesiska pamata ietvaros apstrādā personas datus, ir atbildīgs par šo Noteikumu ievērošanu savas kompetences ietvaros un personas datu apstrādi atbilstoši piemērojamo normatīvo aktu prasībām.

IV. Personas datu apstrādes organizēšana

20. Slimnīca katrai personas datu apstrādei nosaka apstrādes nolūku, tiesisko pamatu, datu subjektu un personas datu kategorijas, datu saņēmējus, glabāšanas termiņus, piekļuves tiesības, par personas datu apstrādes organizēšanu atbildīgo struktūrvienības vadītāju vai citu atbildīgo personu (apstrādes procesa īpašnieku), kā arī piemērojamos tehniskos un organizatoriskos drošības pasākumus.
21. Ja tiek plānota jauna personas datu apstrāde, jaunas informācijas sistēmas vai tehnoloģijas risinājuma ieviešana, būtiskas izmaiņas [1] esošā personas datu apstrādes procesā, jaunu personas datu kategoriju izmantošana vai datu nodošana jaunam saņēmējam, atbildīgā struktūrvienība pirms apstrādes uzsākšanas izvērtē nepieciešamību konsultēties ar datu

[1] Par būtiskām izmaiņām uzskata izmaiņas, kas var ietekmēt personas datu apstrādes nolūku, tiesisko pamatu, apstrādājamo datu apjomu, personu piekļuvi datiem, datu saņēmējus, glabāšanas vietu vai personas datu drošību.

aizsardzības speciālistu, informācijas tehnoloģiju drošības vadītāju (ja piemērojams) un kompetentajām struktūrvienībām.

22. Atbildīgā struktūrvienība dokumentē un uztur aktuālu plānotās personas datu apstrādes nolūku, tiesisko pamatu, apstrādājamo personas datu kategorijas, datu subjektu loku, personas datu saņēmējus, glabāšanas termiņus, kā arī paredzētos tehniskos un organizatoriskos drošības pasākumus.
23. Ar plānoto personas datu apstrādi saistītos riskus identificē un izvērtē saskaņā ar Slimnīcas Risku pārvaldības metodiku. Izvērtējot risku, papildus ņem vērā personas datu apstrādes raksturu, apjomu, nolūku, personu loku, kuru dati tiks apstrādāti, kā arī iespējamo ietekmi uz fizisku personu tiesībām un brīvībām. Izvērtējuma ietvaros nosaka nepieciešamos riska mazināšanas pasākumus un izvērtē, vai saskaņā ar VDAR 35. pantu ir veicams novērtējums par ietekmi uz datu aizsardzību (NIDA).
24. Personas datu apstrādi veic tikai Slimnīcas nozīmēts personāls, kuru darba pienākumu veikšanai ir nepieciešams veikt konkrētu personas datu apstrādi noteiktajā kārtībā un apjomā. Pilnvarojums var būt noteikts līgumā, darba līguma pielikumā, amata aprakstā, rīkojumā, noteikumos vai citādā formā.
25. Nosakot personas datu apstrādes nolūku un organizējot personas datu apstrādi, pārzinis dokumentē vismaz:
    25.1. datu apstrādes mērķi, datu veidus, datu subjektu kategorijas;
    25.2. atbildīgo personu par personas datu apstrādi konkrētam nolūkam;
    25.3. personas datu apstrādes tiesisko pamatu un, apstrādājot īpašo kategoriju personas datus, arī piemērojamo VDAR 9. panta 2. punktā noteikto izņēmumu. Ja apstrāde balstīta uz leģitīmajām interesēm, apstrādes procesa īpašnieks sagatavo leģitīmo interešu novērtējumu, nepieciešamības gadījumā konsultējoties ar datu aizsardzības speciālistu;
    25.4. personāla loku, kas piekļūst personas datiem un to piekļuves tiesību apjomu;
    25.5. personas datu glabāšanas termiņu;
    25.6. nosaka personas datu apstrādē izmantojamos tehniskos un organizatoriskos pasākumus, ja tie atšķiras no kopējiem pasākumiem, kas noteikti ar šiem Noteikumiem.
26. Par konkrētas personas datu apstrādes organizēšanu un atbilstību savā darbības jomā atbild attiecīgās struktūrvienības vadītājs vai cita Slimnīcas noteikta atbildīgā persona, kura ir attiecīgās apstrādes procesa īpašnieks.
27. Apstrādes procesa īpašnieks nodrošina, ka viņa atbildībā esošā personas datu apstrāde ir identificēta, dokumentēta un regulāri pārskatīta, atbilst šiem Noteikumiem un piemērojamo normatīvo aktu prasībām, tiek uzturēta aktuāla informācija par apstrādes nolūkiem, tiesisko pamatu, personas datu kategorijām, glabāšanas termiņiem un piekļuves tiesībām, kā arī tiek identificēti un izvērtēti riski un īstenoti nepieciešamie riska mazināšanas pasākumi.
28. Ja konstatēts augsts vai ļoti augsts personas datu apstrādes risks vai atbildīgā struktūrvienība pati nevar risku pietiekami samazināt, apstrādes procesa īpašnieks par to informē datu aizsardzības speciālistu un risku vadības speciālistu. Risku vadības speciālists organizē riska

izvērtēšanu un iekļaušanu Slimnīcas risku reģistrā saskaņā ar Slimnīcas Risku pārvaldības metodiku.

29. Datu aizsardzības speciālists sniedz konsultācijas un ieteikumus personas datu apstrādes jautājumos, taču nepārņem struktūrvienību vadītāju, procesu īpašnieku vai Slimnīcas kā pārziņa atbildību par personas datu apstrādes atbilstību.
30. Slimnīca nodrošina, ka personas datu apstrāde ir dokumentēta tiktāl, cik tas nepieciešams pārskatatbildības nodrošināšanai, tostarp apstrādes darbību reģistrā, līgumos, rīkojumos, amata aprakstos, piekļuves tiesību pieteikumos un citos dokumentos.
31. Ja pakalpojuma sniedzējs Slimnīcas vārdā apstrādā personas datus, apstrādes procesa īpašnieks pirms apstrādes uzsākšanas nodrošina, ka sadarbība ar apstrādātāju atbilst VDAR un šo Noteikumu prasībām, tostarp:
    31.1. nosaka pakalpojuma sniedzēja lomu personas datu apstrādē;
    31.2. izvērtē, vai apstrādātājs sniedz pietiekamas garantijas atbilstošu tehnisko un organizatorisko pasākumu īstenošanai;
    31.3. nodrošina, ka ar apstrādātāju tiek noslēgts VDAR 28. panta prasībām atbilstošs līgums vai cits saistošs tiesisks akts;
    31.4. nodrošina, ka līgumā ir noteikts apstrādes priekšmets, ilgums, raksturs, nolūks, personas datu veidi, datu subjektu kategorijas, drošības prasības, konfidencialitātes pienākumi, incidentu ziņošanas kārtība, apakšapstrādātāju izmantošanas noteikumi, audita tiesības un datu atdošanas vai dzēšanas kārtība pēc pakalpojuma izbeigšanas;
    31.5. nodrošina, ka līgumā noteikts, ka apstrādātājs neiesaista apakšapstrādātāju bez Slimnīcas iepriekšējas rakstveida atļaujas vai līgumā noteiktas vispārējas atļaujas;
    31.6. uzrauga, vai apstrādātājs ievēro līgumā un normatīvajos aktos noteiktās personas datu aizsardzības prasības. Uzraudzības apjomu un biežumu nosaka, ņemot vērā apstrādājamo personas datu veidu un apjomu, pakalpojuma nozīmīgumu Slimnīcas darbībā, iepriekš konstatētos pārkāpumus un citus ar pakalpojuma sniedzēju saistītos riskus;
    31.7. nodrošina, ka apstrādātājs bez nepamatotas kavēšanās informē Slimnīcu par personas datu aizsardzības pārkāpumu vai citu incidentu, kas var ietekmēt personas datu drošību.
32. Apstrādes procesa īpašnieks nodrošina, ka izmaiņas personas datu apstrādē tiek savlaicīgi izvērtētas un nepieciešamības gadījumā dokumentētas, kā arī aktualizēta ar personas datu apstrādi saistītā dokumentācija, tostarp apstrādes darbību reģistrs un citi ar personas datu apstrādi saistītie dokumenti.
33. Ja personas datu apstrādes nolūks vairs nepastāv vai mainās apstrādes nosacījumi, apstrādes procesa īpašnieks nodrošina personas datu apstrādes pārskatīšanu un, ja nepieciešams, personas datu dzēšanu, anonimizēšanu vai citu nepieciešamo pasākumu veikšanu saskaņā ar piemērojamo normatīvo aktu prasībām.

V. Pacientu datu konfidencialitāte

34. Pacienta dati, tostarp informācija par pacienta veselības stāvokli, diagnozi, ārstēšanu, veiktajiem izmeklējumiem, ārstniecības vēsturi, ārstniecības personām, veselības aprūpes pakalpojumu saņemšanu, pacienta atrašanos Slimnīcā un citi ar pacientu saistīti personas dati, ir konfidenciāla informācija un aizsargājami atbilstoši piemērojamo normatīvo aktu prasībām.
35. Personāls drīkst apstrādāt pacienta datus tikai tādā apjomā, kāds nepieciešams amata pienākumu izpildei, ārstniecības procesa nodrošināšanai, pacienta aprūpei, administratīvo funkciju veikšanai vai citu Slimnīcas tiesisku uzdevumu izpildei, ievērojot principu "nepieciešams zināt" (need-to-know).
36. Personālam bez amata pienākumu izpildei nepieciešama tiesiska pamata ir aizliegts piekļūt pacienta datiem, tos aplūkot, meklēt, kopēt, fotografēt, izdrukāt, saglabāt, izpaust vai citādi apstrādāt, tostarp attiecībā uz radinieku, kolēģu, paziņu, sabiedrībā zināmu personu vai citu pacientu datiem personiskas intereses, ziņkārības vai citu ar darba pienākumu izpildi nesaistītu iemeslu dēļ.
37. Personāls nedrīkst apspriest pacienta datus vai citu konfidenciālu informāciju publiskās vietās, gaiteņos, liftos, uzgaidāmajās telpās, ēdnīcā, sabiedriskajā transportā, sociālajos tīklos, privātās elektroniskās saziņas platformās vai citās vietās vai veidos, kuros informācija var kļūt pieejama nepilnvarotām personām.
38. Ja Personāla loceklis tiek iesaistīts pacienta konsultēšanā, lai gan pacients neatrodas viņa tiešā aprūpē, piekļuve pacienta datiem ir pieļaujama tikai konsultācijas sniegšanai nepieciešamajā apjomā. Konsultācijas faktu un piekļuves pamatojumu fiksē attiecīgajā informācijas sistēmā vai, ja sistēmā šāda iespēja nav paredzēta, citā Slimnīcas noteiktā kārtībā, kas nodrošina iespēju pārbaudīt piekļuves tiesiskumu un pamatotību.
39. Informācija par pacientu tiek izpausta pašam pacientam, viņa likumiskajam vai pilnvarotajam pārstāvim, kā arī citām personām vai institūcijām tikai normatīvajos aktos, pacienta piekrišanā vai Slimnīcas iekšējos normatīvajos aktos paredzētajos gadījumos un apjomā.
40. Pirms informācijas izpaušanas personāls pārliecinās par informācijas pieprasītāja identitāti, pilnvarojumu vai citām tiesībām saņemt informāciju, informācijas izpaušanas tiesisko pamatu un pieprasītās informācijas apjoma atbilstību konkrētajam nolūkam. Ja rodas šaubas par informācijas izpaušanas tiesiskumu, informācija netiek izpausta līdz apstākļu noskaidrošanai, konsultējoties ar tiešo vadītāju, juridisko struktūrvienību vai datu aizsardzības speciālistu.
41. Pienākums ievērot pacienta datu konfidencialitāti saglabājas arī pēc ārstniecības procesa, darba tiesisko attiecību vai citu tiesisko attiecību izbeigšanās, kā arī pēc pacienta nāves, ciktāl piemērojamie normatīvie akti nenosaka citādi.
42. Ja personālam rodas aizdomas par nepamatotu piekļuvi pacienta datiem, to neatļautu izpaušanu vai citu pacienta datu konfidencialitātes pārkāpumu, viņš nekavējoties ziņo par to šo Noteikumu XVI nodaļā noteiktajā kārtībā.
43. Ja normatīvajos aktos vai Slimnīcas iekšējos normatīvajos aktos nav noteikts citādi, personālam ir aizliegts fotografēt, filmēt vai citādi fiksēt pacientu vai viņa datus, izmantojot personīgās ierīces.

44. Personāls nodrošina, ka pacienta dati nav redzami vai pieejami nepilnvarotām personām, tostarp neatstāj bez uzraudzības dokumentus, atvērtas informācijas sistēmas vai citas datu nesējierīces.

VI. Personas datu apstrādes tiesiskais pamats un datu subjektu informēšana

45. Slimnīca personas datus apstrādā tikai tad, ja pastāv vismaz viens no VDAR 6. panta 1. punktā noteiktajiem tiesiskajiem pamatiem:
    45.1. datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem;
    45.2. apstrāde ir nepieciešama tāda līguma izpildei, kura puse ir datu subjekts, vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;
    45.3. apstrāde ir nepieciešama, lai izpildītu uz Slimnīcu attiecināmu juridisku pienākumu;
    45.4. apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses;
    45.5. apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot Slimnīcai normatīvajos aktos noteiktas pilnvaras;
    45.6. apstrāde ir nepieciešama Slimnīcas vai trešās personas leģitīmo interešu ievērošanai, ciktāl šā tiesiskā pamata izmantošana ir pieļaujama un datu subjekta intereses vai pamattiesības un pamatbrīvības nav svarīgākas par attiecīgajām leģitīmajām interesēm. Pirms šā tiesiskā pamata izmantošanas dokumentē leģitīmo interešu novērtējumu.
46. Īpašo kategoriju personas datus, tostarp veselības, ģenētiskos un biometriskos datus, Slimnīca apstrādā tikai tad, ja vienlaikus pastāv VDAR 6. pantā noteikts tiesiskais pamats un vismaz viens VDAR 9. panta 2. punktā noteikts izņēmums. Veselības datus Slimnīca galvenokārt apstrādā profilaktiskās vai arodmedicīnas, medicīniskās diagnostikas, ārstniecības, veselības aprūpes vai sociālās aprūpes pakalpojumu sniegšanas, veselības aprūpes sistēmu pārvaldības, sabiedrības veselības, juridisku pienākumu izpildes, vitālo interešu, tiesisku prasījumu, arhivēšanas, zinātniskās pētniecības vai statistikas nolūkos, ja attiecīgā apstrāde atbilst normatīvo aktu prasībām un ir nodrošināta profesionālā konfidencialitāte un citi nepieciešamie aizsardzības pasākumi.
47. Ja personas dati tiek iegūti no datu subjekta, Slimnīca sniedz datu subjektam VDAR 13. pantā noteikto informāciju par personas datu apstrādi: pārziņa nosaukums un kontaktinformācija saziņai par personas datu apstrādi saistītiem jautājumiem, personas datu apstrādes nolūks (mērķis), personas datu saņēmēji, datu glabāšanas periods u.c.
48. Iegūstot personas datus (slēdzot līgumus, veicot videonovērošanu vai citos gadījumos), Slimnīca nodrošina šo Noteikumu 47. punktā minētās informācijas sniegšanu personām. Informācijas sniegšanas pienākums personai var tikt nodrošināts līgumos ar fiziskām personām, videonovērošanas zīmēs, izvietojot informatīvu paziņojumu vai citā piemērotā veidā. Atsevišķos gadījumos, ja tas ir lietderīgi, var tikt veiktas citas informēšanas darbības. Datu

aizsardzības speciālistu iesaista, izstrādājot jaunu vai būtiski grozot esošu personu informēšanas kārtību vai informatīvā paziņojuma saturu.

49. Apstrādes procesa īpašnieks pirms jaunas personas datu apstrādes uzsākšanas vai būtisku izmaiņu veikšanas esošajā personas datu apstrādē nosaka un dokumentē apstrādes nolūku, kā arī identificē attiecīgajam nolūkam piemērojamo tiesisko pamatu. Ja tiek apstrādāti īpašo kategoriju personas dati, apstrādes procesa īpašnieks identificē arī piemērojamo VDAR 9. panta 2. punktā noteikto izņēmumu.
50. Apstrādes procesa īpašnieks nodrošina, ka tiek ievākti un apstrādāti tikai tādi personas dati un tādā apjomā, kas nepieciešams konkrētā apstrādes nolūka sasniegšanai. Ja rodas šaubas par apstrādes nolūku, tiesisko pamatu, nepieciešamo personas datu apjomu vai apstrādes pieļaujamību, apstrādes procesa īpašnieks pirms apstrādes uzsākšanas konsultējas ar datu aizsardzības speciālistu un, ja nepieciešams, citām kompetentajām Slimnīcas struktūrvienībām.

VII. Piekļuves tiesības un piekļuves kontrole

51. Piekļuve personas datiem Slimnīcā tiek piešķirta personālam vai citām pilnvarotām personām, kurām tā nepieciešama amata pienākumu, līguma, prakses, mācību vai cita tiesiska pamata ietvaros noteikto uzdevumu izpildei.
52. Piekļuves tiesības piešķir saskaņā ar nepieciešamības zināt (need-to-know) un minimālo piekļuves tiesību principu. Piešķirto piekļuves tiesību apjoms nedrīkst pārsniegt personas amata pienākumu vai citu uzdevumu izpildei nepieciešamo apjomu.
53. Piekļuves tiesību piešķiršanu, maiņu un anulēšanu organizē saskaņā ar Slimnīcas iekšējo kārtību, pamatojoties uz attiecīgās struktūrvienības vadītāja vai citas pilnvarotas personas pieteikumu un saskaņojumu.
54. Par piekļuves tiesību piešķiršanu atbildīgā persona vai struktūrvienība nodrošina, ka piekļuves tiesības tiek nekavējoties pārskatītas un, ja nepieciešams, mainītas, ierobežotas, apturētas vai anulētas, ja mainās personas amats, darba pienākumi, funkcijas, struktūrvienība, prakses vai līgumattiecību statuss, piešķirtais pilnvarojums vai izbeidzas tiesiskais pamats piekļuvei personas datiem.
55. Personāls nedrīkst izmantot citu personu lietotāju kontus, nodot savus piekļuves datus citām personām, pieļaut citu personu darbību savā kontā vai veikt personas datu apstrādi cita lietotāja vārdā.
56. Piekļuves tiesības nekavējoties pārskata un, ja nepieciešams, maina, ierobežo, aptur vai anulē, ja mainās personas amats, darba pienākumi, funkcijas, struktūrvienība, prakses vai līgumattiecību statuss, piešķirtais pilnvarojums vai izbeidzas tiesiskais pamats piekļuvei personas datiem. Piekļuves tiesību piešķiršana, grozīšana un anulēšana tiek dokumentēta Slimnīcas noteiktajā kārtībā.
57. Pagaidu piekļuves tiesības piešķir tikai uz laiku, kas nepieciešams attiecīgā uzdevuma izpildei. Beidzoties piešķiršanas pamatam, piekļuves tiesības nekavējoties pārskata un, ja nepastāv turpmāks tiesiskais pamats, anulē.

VIII. Lietotāju konti, paroles, autentifikācija un darba vietas drošība

58. Katram personas datu lietotājam tiek piešķirts individuāls lietotāja konts. Ja konkrētās sistēmas tehniskās īpatnības objektīvi neļauj izmantot individuālus lietotāju kontus, informē informācijas drošības atbildīgo personu un datu aizsardzības speciālistu, pirms šāda risinājuma ieviešanas. Izņēmuma pamatojumu dokumentē un ievieš citus kontroles pasākumus, kas ļauj identificēt personu, kura veikusi darbības ar personas datiem, lai pēc iespējas samazinātu neatļautas piekļuves risku.
59. Piekļuvei informācijas sistēmām tiek piemēroti autentifikācijas līdzekļi atbilstoši sistēmas drošības klasei. Piekļuvei paaugstinātas drošības informācijas sistēmām, kā arī attālinātai piekļuvei Slimnīcas informācijas sistēmām piemēro daudzfaktoru autentifikāciju. Ja konkrētās sistēmas tehnisko ierobežojumu dēļ daudzfaktoru autentifikāciju nav iespējams ieviest, informācijas sistēmas īpašnieks sadarbībā ar informācijas drošības atbildīgo personu nosaka riska mazināšanas pasākumus un termiņu daudzfaktoru autentifikācijas vai cita līdzvērtīga droša risinājuma ieviešanai.
60. Paroļu sarežģītības, garuma, derīguma un maiņas prasības, kā arī citas tehniskās autentifikācijas prasības nosaka Slimnīcas informācijas tehnoloģiju drošības un lietošanas noteikumi. Personālam ir pienākums ievērot minētās prasības.
61. Paroles, autentifikācijas līdzekļi, viedkartes, piekļuves kartes, drošības kodi un citi identifikācijas līdzekļi ir glabājami droši un nav nododami, izpaužami vai koplietojami ar citām personām.
62. Personālam ir pienākums nekavējoties nomainīt paroli un ziņot IT atbalstam, ja rodas aizdomas, ka parole, autentifikācijas līdzeklis vai lietotāja konts kļuvis zināms citai personai vai varētu būt kompromitēts.
63. Personālam ir pienākums atstājot darba vietu, bloķēt datoru vai citu ierīci, ja tā tiek atstāta bez uzraudzības, un nodrošināt, ka personas dati nav redzami vai pieejami nepilnvarotām personām, ja tas ir tehniski iespējams. Beidzot darbu, personālam ir pienākums aizvērt informācijas sistēmas, izrakstīties no lietotāja konta un sakārtot papīra dokumentus drošā vietā.
64. Personas datus saturoši dokumenti, datu nesēji un izdrukas glabājami tā, lai tiem nevarētu piekļūt nepilnvarotas personas, tostarp pacienti, apmeklētāji, cits personāls bez darba nepieciešamības un ārpakalpojumu sniedzēji.
65. Darba vietās, kur notiek pacientu vai citu personu apkalpošana, personāls organizē dokumentu un ekrānu novietojumu tā, lai personas dati nebūtu redzami trešajām personām vai nejauši izpaužami.
66. Personāls nedrīkst izmantot personīgās ierīces personas datu glabāšanai, apstrādei vai pārsūtīšanai, ja vien tas nav atļauts saskaņā ar Slimnīcas iekšējiem normatīvajiem aktiem.
67. Darba vietās, kur notiek pacientu vai citu personu apkalpošana, personāls organizē dokumentu un ekrānu novietojumu tā, lai personas dati nebūtu redzami trešajām personām vai nejauši izpaužami.

IX. Personas datu izmantošana, glabāšana, labošana

68. Personas datus drīkst izmantot tikai tam nolūkam, kuram tie iegūti. Ja personas datus paredzēts izmantot citam nolūkam, apstrādes procesa īpašnieks pirms datu izmantošanas izvērtē jaunā apstrādes nolūka tiesisko pamatu, tā saderību ar sākotnējo nolūku un iespējamos riskus, iesaistot datu aizsardzības speciālistu. Ja jaunais nolūks rada būtiskas izmaiņas personas datu apstrādē, piemēro šo Noteikumu 25. - 28. punktā noteikto kārtību.
69. Apstrādes procesa īpašnieks nodrošina, ka personas dati ir precīzi un, ja nepieciešams, aktuāli. Konstatējot neprecīzus vai nepilnīgus personas datus, tos bez nepamatotas kavēšanās labo, papildina vai ierobežo to apstrādi. Personas datus dzēš tikai normatīvajos aktos un Slimnīcas iekšējā kārtībā noteiktajos gadījumos.
70. Personas datu glabāšanas termiņus nosaka atbilstoši apstrādes nolūkam, normatīvo aktu prasībām, Slimnīcas lietu nomenklatūrai, līgumiskajām saistībām, noilguma termiņiem un nepieciešamībai celt, īstenot vai aizstāvēt tiesiskus prasījumus. Personas datus nedzēš, ja attiecībā uz tiem ir noteikts dokumentu saglabāšanas pienākums saistībā ar tiesvedību, izmeklēšanu, auditu, incidentu, strīdu vai kompetentas institūcijas pieprasījumu.
71. Slimnīca personas datu apstrādi veic, izmantojot organizatoriskos pasākumus, tostarp ar nepieciešamajiem tehniskajiem līdzekļiem, kas nodrošina godprātīgu un likumīgu personas datu apstrādi un lietošanu paredzētajiem mērķiem, to uzglabāšanas, atjaunošanas, labošanas un dzēšanas veidu.
72. Personas datus drīkst labot, papildināt vai dzēst tikai persona, kurai attiecīgās tiesības piešķirtas saskaņā ar amata pienākumiem, piekļuves tiesībām un Slimnīcas noteikto kārtību.
73. Personas datu apstrādes nodrošināšanai Slimnīca izmanto tehniskos resursus un nodrošina tos ar apstrādes riskam atbilstošiem aizsardzības līdzekļiem pret tīšu bojāšanu, nozaudēšanu un neatļautu piekļuvi, ievērojot ārējos un iekšējos normatīvajos aktos noteikto (drošības pasākumi, lai novērstu nepiederošu personu iekļūšanu, ugunsdrošības sistēma, slēgti dokumentu skapji u.c.). Ja nepieciešamo aizsardzības pasākumu nav iespējams ieviest nekavējoties, atbildīgais apstrādes procesa vai informācijas sistēmas īpašnieks dokumentē radīto risku, nosaka pagaidu riska mazināšanas pasākumus, atbildīgo personu un nepieciešamā risinājuma ieviešanas termiņu saskaņā ar Slimnīcas Risku pārvaldības metodiku.
74. Par glabāšanas termiņu noteikšanu un ievērošanu atbild apstrādes procesa īpašnieks sadarbībā ar dokumentu un arhīvu pārvaldības, juridisko, informācijas tehnoloģiju un citām kompetentajām struktūrvienībām. Datu aizsardzības speciālists sniedz konsultācijas par glabāšanas termiņu un paredzēto aizsardzības pasākumu atbilstību, bet nepārņem apstrādes procesa īpašnieka atbildību.
75. Beidzoties personas datu glabāšanas termiņam, apstrādes procesa īpašnieks nodrošina personas datu dzēšanu, iznīcināšanu vai anonimizēšanu, ja normatīvie akti neparedz citu kārtību.

X. Medicīniskās dokumentācijas apstrāde

76. Medicīniskā dokumentācija tiek veidota, uzturēta, glabāta, izsniegta, labota un iznīcināta saskaņā ar medicīnisko dokumentu lietvedību regulējošajiem normatīvajiem aktiem, Slimnīcas lietu nomenklatūru un Slimnīcas iekšējiem normatīvajiem aktiem.
77. Medicīniskajā dokumentācijā ierakstus drīkst veikt tikai tam pilnvarotas personāls, ievērojot profesionālos pienākumus, dokumentācijas prasības un konkrētās informācijas sistēmas vai papīra dokumentu aprites kārtību.
78. Medicīniskajā dokumentācijā aizliegts veikt nepamatotus labojumus, dzēsumus vai citas izmaiņas, kas neatbilst normatīvo aktu prasībām vai nepatiesi atspoguļo ārstniecības procesu.
79. Labojumu medicīniskajā dokumentācijā veic tā, lai būtu iespējams konstatēt sākotnējās informācijas saturu, labojuma veicēju, veikšanas laiku un pamatojumu. Ja informācijas sistēma tehniski nenodrošina labojuma pilnīgu izsekojamību, labojumu veic citā Slimnīcas noteiktā un dokumentētā kārtībā. Nav pieļaujama medicīniskās dokumentācijas labošana tādā veidā, kas neļauj noskaidrot sākotnējo ierakstu un veiktās izmaiņas.
80. Medicīniskās dokumentācijas kopijas izsniedz Pacientu tiesību likumā un Slimnīcas iekšējos normatīvajos aktos noteiktajā kārtībā un termiņā.
81. Medicīnisko dokumentāciju nedrīkst atstāt bez uzraudzības telpās, kur tai var piekļūt nepilnvarotas personas. Izdrukas, kopijas un melnraksti, kas satur pacientu datus kas nav medicīniskās dokumentācijas vai citas glabājamas dokumentācijas sastāvdaļa, pēc to izmantošanas iznīcina Slimnīcas noteiktajā drošas dokumentu iznīcināšanas kārtībā.
82. Medicīnisko dokumentāciju ārpus Slimnīcas telpām drīkst iznest vai pārvietot tikai normatīvajos aktos vai Slimnīcas iekšējos normatīvajos aktos paredzētajos gadījumos un noteiktajā kārtībā.

XI. Personas datu izpaušana

83. Personāls amata pienākumu izpildes ietvaros drīkst izpaust personas datus trešajām personām, valsts institūcijām un datu subjektiem, ja personas datu izpaušanai pastāv atbilstošs tiesiskais pamats. Personas datus izpauž tikai tad, ja pastāv konkrēts tiesiskais pamats, izpaušana ir nepieciešama noteiktā nolūka sasniegšanai un izpaužamais datu apjoms nepārsniedz nepieciešamo. Pirms izpaušanas pārbauda datu saņēmēja identitāti, pilnvarojumu vai likumā noteiktās tiesības saņemt informāciju.
84. Pirms personas datu izpaušanas personāls pārbauda:
    - 84.1. pieprasītāja identitāti;
    - 84.2. pārstāvības vai pilnvarojuma tiesības, ja pieprasījumu iesniedz pārstāvis;
    - 84.3. pieprasījuma tiesisko pamatu un nolūku;
    - 84.4. pieprasīto datu apjoma nepieciešamību un samērīgumu;
    - 84.5. izmantojamo datu nodošanas kanālu;
    - 84.6. nepieciešamību dokumentēt izpaušanas faktu.

85. Valsts vai pašvaldību institūcijām personas datus sniedz normatīvajos aktos noteiktajos gadījumos, pamatojoties uz dokumentētu un pārbaudāmu pieprasījumu, normatīvajos aktos paredzētu regulāru datu apmaiņu vai citu tiesisku pamatu. Ja pieprasījums ir neskaidrs, pārmērīgs vai tajā nav iespējams identificēt tiesisko pamatu un nepieciešamo datu apjomu, personāls pieprasa precizējumu vai konsultējas ar juridisko struktūrvienību un datu aizsardzības speciālistu.
86. Informācija par pacientu citām personām tiek sniegta, ievērojot Pacientu tiesību likumu un Slimnīcas iekšējo kārtību. Īpaši rūpīgi izvērtējama informācijas sniegšana radiniekiem, kontaktpersonām, darba devējiem, apdrošinātājiem un plašsaziņas līdzekļiem.
87. Ja personas dati tiek nodoti citam pārzinim, kopīgam pārzinim, apstrādātājam vai citam sadarbības partnerim, pirms nodošanas nosaka katras iesaistītās puses lomu, tiesisko pamatu, datu apjomu, nolūku, drošības prasības, atbildību un nepieciešamo līgumisko regulējumu.
88. Ja informācijas pieprasījums neparedz personas datu izpaušanu, bet pieprasītā informācija nav nodalāma no personas datiem (piemēram, līgumu vai citu dokumentu kopijās), pirms informācijas sniegšanas personas datus aizklāj vai dzēš tiktāl, ciktāl tas nepieciešams personas datu aizsardzībai. Personas datu aizklāšanu veic pilnvarota persona, izmantojot paņēmienu, kas nepieļauj aizklātās informācijas atjaunošanu vai nolasīšanu. Dokumenta oriģinālu saglabā nemainītā veidā.
89. Personas datus uz valsti ārpus ES/EEZ vai starptautisku organizāciju nosūta tikai saskaņā ar VDAR V nodaļu. Pirms nosūtīšanas pārbauda, vai pastāv Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību, vai tiek izmantotas atbilstošas garantijas, piemēram, Eiropas Komisijas standarta līguma klauzulas vai saistošie uzņēmuma noteikumi. Nosūtot personas datus elektroniski, izmanto drošus saziņas kanālus un aizsardzības pasākumus, piemēram, šifrēšanu, piekļuves ierobežojumus, drošus portālus vai citu Slimnīcas apstiprinātu risinājumu.
90. Personas datu nodošanu ārpus ES/EEZ vai starptautiskai organizācijai, pirms tās uzsākšanas saskaņo ar datu aizsardzības speciālistu un Juridisko un risku vadības daļu, izņemot gadījumus, kad datu nodošana notiek iepriekš izvērtēta un Slimnīcā apstiprināta procesa ietvaros. Ja nepieciešams, pirms datu nodošanas veic ar nodošanu saistīto risku izvērtējumu.
91. Informācijas pieprasījuma izskatīšanu un atbildes sagatavošanu organizē apstrādes procesa īpašnieks vai cita Slimnīcas noteikta atbildīgā persona, nepieciešamības gadījumā konsultējoties ar datu aizsardzības speciālistu, juridisko un risku vadības daļu vai citām kompetentajām struktūrvienībām.

XII. Datu subjektu pieprasījumu izskatīšana

92. Datu subjektam VDAR un citos piemērojamajos normatīvajos aktos noteiktajos gadījumos un apjomā ir tiesības:
    92.1. saņemt informāciju par savu personas datu apstrādi;
    92.2. piekļūt saviem personas datiem un saņemt to kopiju;
    92.3. pieprasīt neprecīzu datu labošanu vai nepilnīgu datu papildināšanu;

92.4. pieprasīt personas datu dzēšanu (“tiesības tikt aizmirstam”), ja tam pastāv normatīvajos aktos noteiktais pamats;
92.5. pieprasīt apstrādes ierobežošanu;
92.6. saņemt un pārnest personas datus, ja piemērojamas tiesības uz datu pārnesamību;
92.7. iebilst pret personas datu apstrādi normatīvajos aktos paredzētajos gadījumos;
92.8. atsaukt piekrišanu, ja apstrāde balstīta uz piekrišanu;
92.9. nebūt tāda lēmuma subjektam, kas balstīts tikai uz automatizētu personas datu apstrādi un rada tiesiskas sekas vai līdzīgā veidā būtiski ietekmē datu subjektu;
92.10. iesniegt sūdzību Datu valsts inspekcijā vai izmantot citus normatīvajos aktos paredzētos tiesību aizsardzības līdzekļus.

93. Datu subjekta pieprasījumu par šo Noteikumu 92. punktā minēto tiesību īstenošanu pieņem un reģistrē Dokumentu pārvaldības daļa un nekavējoties nodod datu aizsardzības speciālistam, kurš koordinē pieprasījuma izskatīšanu un nepieciešamības gadījumā iesaista kompetentās struktūrvienības. Struktūrvienības un personāls, kuru rīcībā ir pieprasījuma izskatīšanai nepieciešamā informācija, sniedz to datu aizsardzības speciālista noteiktajā termiņā.
94. Pirms pieprasījuma izpildes Dokumentu pārvaldības daļa pārbauda pieprasītāja identitāti un, ja pieprasījumu iesniedz pārstāvis, arī pārstāvības tiesības.
95. Atbildi uz datu subjekta pieprasījumu sniedz bez nepamatotas kavēšanās, bet ne vēlāk kā viena mēneša laikā no pieprasījuma saņemšanas dienas, ja vien normatīvie akti neparedz iespēju termiņu pagarināt. Par termiņa pagarinājumu un tā iemesliem datu subjektu informē normatīvajos aktos noteiktajā kārtībā.
96. Izskatot datu subjekta pieprasījumu, Slimnīca nodrošina, ka netiek nepamatoti izpausti citu personu dati, medicīniskā konfidencialitāte, komercnoslēpums, drošības informācija vai cita aizsargājama informācija.
97. Ja pieprasījums nav pietiekami skaidrs, Slimnīca lūdz datu subjektu precizēt pieprasījuma saturu vai apjomu. Ja pieprasījums ir acīmredzami nepamatots vai pārmērīgs vai to nav iespējams pilnībā izpildīt, Slimnīca sniedz motivētu atbildi, norādot pieņemtā lēmuma iemeslus un informāciju par datu subjekta tiesībām saskaņā ar piemērojamajiem normatīvajiem aktiem.

XIII. Personas datu apstrādes darbību reģistrs

98. Slimnīca uztur personas datu apstrādes darbību reģistru, lai dokumentētu Slimnīcā veiktos personas datu apstrādes procesus un nodrošinātu pārskatatbildību.
99. Personas datu apstrādes darbību reģistrā iekļauj vismaz šo Noteikumu piemērošanai nepieciešamo informāciju, tostarp apstrādes nolūku, tiesisko pamatu, datu subjektu kategorijas, personas datu kategorijas, īpašu kategoriju datu apstrādes pamatu, saņēmēju kategorijas, datu nodošanu ārpus ES/EEZ, glabāšanas termiņus, tehniskos un organizatoriskos drošības pasākumus un atbildīgo struktūrvienību.
100. Par informācijas sniegšanu personas datu apstrādes darbību reģistram atbild attiecīgās apstrādes procesa īpašnieks vai struktūrvienības vadītājs. Informāciju iesniedz datu

aizsardzības speciālistam, kurš koordinē reģistra uzturēšanu, uzrauga tā aktualitāti un sniedz metodisko atbalstu.

101. Ja tiek plānota jauna apstrāde vai būtiski mainās esoša apstrāde, apstrādes procesa īpašnieks pirms apstrādes uzsākšanas vai izmaiņu ieviešanas informē datu aizsardzības speciālistu un iesniedz reģistra aktualizēšanai nepieciešamo informāciju.

102. Datu aizsardzības speciālists apstrādes darbību reģistru pārskata vismaz reizi gadā vai biežāk, ja mainās apstrādes nolūki, tiesiskie pamati, datu kategorijas, saņēmēji, sistēmas vai drošības pasākumi.

103. Apstrādes procesa īpašnieks ir atbildīgs par reģistrā sniegtās informācijas pilnīgumu, pareizību un savlaicīgu aktualizēšanu.

XIV. Personas datu dzēšana un iznīcināšana

104. Ja personas datu apstrādes nolūks vairs nepastāv vai ir beidzies personas datu glabāšanas termiņš, personas datus dzēš vai iznīcina drošā un neatgriezeniskā veidā, ja vien normatīvie akti neparedz pienākumu tos glabāt ilgāk.

105. Personāls nedrīkst patstāvīgi dzēst personas datus, ja konkrētā datu veida dzēšanai nepieciešams pilnvarojums, apstiprinājums vai centralizēts dzēšanas process. Konstatējot personas datus, kuri glabājas bez tiesiska pamata vai ilgāk par noteikto termiņu, personāls rīkojas atbilstoši Slimnīcas apstiprinātajai glabāšanas un dzēšanas kārtībai vai informē atbildīgo apstrādes procesa īpašnieku.

106. Slimnīcas personāls regulāri pārskata savā atbildībā esošos datu nesējus un .iznīcina personas datus dokumentu sagatavēs, darba kopijās, sarakstēs un citos materiālos, kuru glabāšana vairs nav nepieciešama. Ja personālam rodas šaubas par informācijas dzēšanu vai iznīcināšanu, viņš to patstāvīgi neveic un konsultējas ar apstrādes procesa īpašnieku vai par dokumentu pārvaldību atbildīgo struktūrvienību.

107. Dokumentu glabāšanas un iznīcināšanas kārtība Slimnīcā tiek noteikta ar iekšējiem normatīvajiem aktiem. Personas datu dzēšanu vai iznīcināšanu veic tikai tam pilnvarotas personas saskaņā ar Slimnīcas iekšējiem normatīvajiem aktiem.

108. Par personas datu dzēšanas vai iznīcināšanas nepieciešamības izvērtēšanu un uzsākšanu atbild attiecīgās apstrādes procesa īpašnieks sadarbībā ar dokumentu pārvaldības, informācijas tehnoloģiju un citām kompetentajām struktūrvienībām.

XV. Slimnīcas personāla pienākumi, tiesības un atbildība personas datu apstrādē

109. Personālam ir pienākums:

109.1. saglabāt personas datu konfidencialitāti un apstrādāt personas datus tikai saskaņā ar piemērojamajiem normatīvajiem aktiem, šiem Noteikumiem, citiem Slimnīcas iekšējiem normatīvajiem aktiem un tiesiskiem norādījumiem;

109.2. piekļūt tikai tiem personas datiem un veikt tikai tās darbības, kas nepieciešamas konkrēto amata vai citu tiesisko pienākumu izpildei;

109.3. pirms personas datu izpaušanas pārbaudīt saņēmēja identitāti, tiesības saņemt informāciju, pieprasījuma tiesisko pamatu, nepieciešamo datu apjomu un drošu nodošanas kanālu;

109.4. saņemtu datu subjekta pieprasījumu, sūdzību vai lūgumu par personas datu labošanu, dzēšanu vai piekļuvi nekavējoties nodot Slimnīcas noteiktajai atbildīgajai struktūrvienībai un patstāvīgi to neizpildīt, ja personāls nav attiecīgi pilnvarots;

109.5. ziņot apstrādes procesa īpašniekam vai citai atbildīgajai personai par konstatētiem neprecīziem, nepilnīgiem vai neatbilstoši glabātiem personas datiem un veikt labojumus tikai savas kompetences un piešķirto tiesību ietvaros;

109.6. dzēst, anonimizēt vai nodot iznīcināšanai personas datus tikai saskaņā ar noteiktajiem glabāšanas termiņiem, pilnvarojumu un Slimnīcas apstiprināto kārtību;

109.7. ievērot tīrā galda, tīrā ekrāna, ierīču bloķēšanas, drošas dokumentu glabāšanas un drošas saziņas prasības;

109.8. nekavējoties ziņot par informācijas drošības incidentu, iespējamu personas datu aizsardzības pārkāpumu, nepamatotu piekļuvi, kļūdaini nosūtītu informāciju, nozaudētu dokumentu vai ierīci, kompromitētu paroli vai citu personas datu drošības risku;

109.9. piedalīties Slimnīcas noteiktajās datu aizsardzības un informācijas drošības apmācībās un zināšanu pārbaudēs;

109.10. sadarboties ar pilnvarotām personām iekšējās pārbaudēs, auditos, incidentu izmeklēšanā un datu subjektu pieprasījumu izpildē.

109.11. nekavējoties ziņot atbildīgajai personai vai informācijas tehnoloģiju atbalstam, ja personālam piešķirtas personas datu piekļuves tiesības, kas nav nepieciešamas viņa amata pienākumu izpildei, vai ja konstatētas nepamatotas piekļuves tiesības citai personai;

109.12. pēc personas datu aizsardzības pārkāpuma vai informācijas drošības incidenta konstatēšanas sadarboties tā izmeklēšanā un īstenot noteiktos riska mazināšanas pasākumus.

110. Personālam ir tiesības izteikt priekšlikumus personas datu aizsardzības un informācijas drošības uzlabošanai, informējot par tiem tiešo vadītāju vai datu aizsardzības speciālistu.

111. Personālam, ja vien tas nav saistīts ar tiešo pienākumu pildīšanu, ir aizliegts:

111.1. bez darba pienākumu izpildei nepieciešama pamata meklēt, aplūkot, fotografēt, filmēt, kopēt, izdrukāt, eksportēt, saglabāt vai citādi izmantot pacientu, kolēģu, radinieku, paziņu, sabiedrībā zināmu personu vai citu personu datus;

111.2. izmantot citas personas lietotāja kontu, izpaust savu paroli, autentifikācijas kodu vai citu piekļuves līdzekli vai ļaut citai personai strādāt savā lietotāja kontā;

111.3. kopēt personas datus uz ārējiem datu nesējiem, mobilajām ierīcēm vai privātām ierīcēm, izņemot gadījumus, kad tas ir tieši nepieciešams darba pienākumu izpildei, iepriekš rakstveidā saskaņots ar Slimnīcas noteikto atbildīgo personu un tiek izmantots Slimnīcas apstiprināts un atbilstoši aizsargāts risinājums;

111.4. ievadīt, augšupielādēt, nosūtīt vai citādi darīt pieejamus personas datus privātos e-pastos, neapstiprinātās mākoņkrātuvēs, publiski pieejamos vai Slimnīcas neapstiprinātos mākslīgā intelekta rīkos, ziņapmaiņas lietotnēs vai citos ārējos pakalpojumos;

111.5. patvaļīgi mainīt tehnikas vai programmatūras konfigurāciju, atspējot drošības risinājumus vai instalēt neapstiprinātu programmatūru;

111.6. pieļaut nepiederošu personu piekļuvi viņam lietošanā nodotajai datortehnikai, informācijas sistēmām vai dokumentācijai.

111.7. telefoniski vai mutiski izpaust personas datus, ja nav droši pārbaudīta saņēmēja identitāte un tiesības saņemt attiecīgo informāciju;

111.8. nosūtīt personas datus, nepārbaudot adresātu, pielikumus un nepieciešamo datu apjomu, vai izmantot nepietiekami aizsargātu saziņas kanālu;

111.9. nosūtot vienu e-pastu vairākiem savstarpēji nesaistītiem datu subjektiem, atklāt viņu e-pasta adreses citiem saņēmējiem, ja vien adresātu savstarpēja atklāšana nav nepieciešama konkrētajam saziņas nolūkam;

111.10. apspriest personas datus publiskās vietās, sociālajos tīklos, privātās sarakstēs vai citās vietās, kur informācija var kļūt pieejama nepilnvarotām personām;

111.11. izmantot personas datus mācību, prezentāciju, demonstrējumu, publikāciju vai citiem ar tiešo ārstniecības vai darba pienākumu izpildi nesaistītiem nolūkiem, ja tam nav atbilstoša tiesiskā pamata vai Slimnīcas noteikta pilnvarojuma.

111.12. izmantot īstus pacientu vai citu fizisku personu personas datus informācijas sistēmu testēšanai, apmācībām vai izstrādei, ja tam nav atbilstoša tiesiskā pamata un Slimnīcas noteiktas kārtības.

112. Personāls ir atbildīgs:

112.1. par tehniku un datu nesējiem (tajā skaitā dokumentiem, nomenklatūras mapēm, kartotēkām), kas satur personas datus un ir nodotas personāla rīcībā vai kam ir piekļuve darba pienākumu izpildes ietvaros;

112.2. par darbībām, kas tiek veiktas ar viņam nodoto tehniku un datu nesējiem;

112.3. par personas datu saglabāšanu, nepieļaujot nejaušu piekļuvi personas datiem, to zaudēšanu, iznīcināšanu, dzēšanu vai sabojāšanu un prettiesisku nodošanu.

113. Personāla prombūtnes laikā darba e-pasta apriti nodrošina ar Slimnīcas apstiprinātu aizvietošanas, deleģēšanas, koplietojamas pastkastes vai automātiskās atbildes risinājumu. Personāls nedrīkst nodot citai personai savu paroli vai pārsūtīt darba e-pastu uz privātu e-pasta adresi.

114. Personāls nodrošina, ka personas datus saturoši dokumenti un informācija tiek novietoti citiem nepieejamā vietā (slēgtās telpās, skapjos, atvilktnēs), bet šādu dokumentu kopijas tiek iznīcinātas dokumentu smalcinātajā vai citādā drošā veidā.

115. Personāla pienākums ir saglabāt un bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību vai citu līgumattiecību izbeigšanas ar Slimnīcu. Šādam pienākumam ir beztermiņa raksturs.

116. Personālam pēc pilnvarotas personas pieprasījuma jāspēj paskaidrot, ar kādu darba uzdevumu vai citu tiesisku pienākumu bija saistīta konkrētā piekļuve personas datiem vai ar tiem veiktā darbība.
117. Par šo Noteikumu vai normatīvo aktu prasību pārkāpumiem personāls ir atbildīgs normatīvajos aktos un Slimnīcas iekšējos normatīvajos aktos noteiktajā kārtībā.
118. Personāls ir informēts, ka viņu veiktās darbības Slimnīcas informācijas sistēmās var tikt reģistrētas auditācijas pierakstos un pārbaudītas personas datu aizsardzības, informācijas drošības, incidentu izmeklēšanas un normatīvo aktu prasību izpildes nolūkā.

XVI. Personāla rīcība drošības incidentu un personas datu aizsardzības pārkāpumu gadījumā

119. Persona, kura konstatējusi iespējamu personas datu aizsardzības pārkāpumu, par to nekavējoties ziņo, negaidot pilnīgas informācijas iegūšanu vai galīgu apstiprinājumu, ka personas datu aizsardzības pārkāpums ir noticis. Ziņojumu iesniedz tiešajam vadītājam un vienlaikus Slimnīcas datu aizsardzības speciālistam, rakstot uz: datu.aizsardziba@aslimnica.lv. Ja incidents ir saistīts ar informācijas sistēmu, ierīci, lietotāja kontu, ļaunprogrammatūru vai sistēmas nepieejamību, par to vienlaikus ziņo arī IT atbalstam vai informācijas tehnoloģiju drošības atbildīgajai personai. Ja elektroniskais pasts nav pieejams, izmanto Slimnīcas noteikto alternatīvo ziņošanas kanālu. Ziņošanas iespēja nedrīkst būt atkarīga tikai no tiešā vadītāja pieejamības.
120. Personālam ir pienākums ziņot par:
    120.1. kļūdaini nosūtītu e-pastu, dokumentu vai medicīnisku informāciju;
    120.2. neatļautu vai iespējami nepamatotu piekļuvi personas datiem;
    120.3. nozaudētu vai nozagtu ierīci, datu nesēju, dokumentu vai piekļuves līdzekli;
    120.4. kompromitētu paroli, lietotāja kontu vai autentifikācijas līdzekli;
    120.5. ļaunprogrammatūru, izspiedējprogrammatūru, sistēmas uzlaušanu vai aizdomīgu informācijas sistēmas darbību;
    120.6. neatļautu personas datu dzēšanu, pārveidošanu, kopēšanu vai izpaušanu;
    120.7. papīra dokumentu neatļautu pieejamību, nozaudēšanu vai iznīcināšanu;
    120.8. sistēmas nepieejamību, ja tā var ietekmēt personas datu pieejamību vai pacientu aprūpi;
    120.9. jebkuru citu notikumu, kas var radīt personas datu aizsardzības pārkāpumu vai apdraudēt personas datu konfidencialitāti, integritāti vai pieejamību.
121. Persona, kura konstatējusi vai pamatoti uzskata, ka varētu būt noticis personas datu aizsardzības pārkāpums vai informācijas drošības incidents, savas kompetences un drošības robežās nekavējoties veic saprātīgus pasākumus kaitējuma ierobežošanai, ja tas nerada papildu risku personas datiem, informācijas sistēmām vai incidenta pierādījumu saglabāšanai. Šādi pasākumi var ietvert, piemēram, kļūdaini nosūtīta ziņojuma atsaukšanu, saziņu ar neparedzēto saņēmēju, ierīces vai lietotāja konta bloķēšanu vai citas neatliekamas darbības, kas nepieciešamas turpmāka kaitējuma novēršanai. Persona nedrīkst dzēst auditācijas pierakstus,

elektroniskās saziņas datus vai citus ar incidentu saistītus pierādījumus, kā arī veikt darbības, kas var traucēt incidenta izvērtēšanai vai izmeklēšanai.

122. Pārkāpuma izvērtēšanā un novēršanā atbilstoši kompetencei var iesaistīt informācijas tehnoloģiju drošības atbildīgo personu, informācijas tehnoloģiju struktūrvienību, apstrādes procesa īpašnieku, juridisko un risku vadības struktūrvienību, kā arī Slimnīcas vadību. Tehniskā incidenta novēršanu vada informācijas drošības vai IT atbildīgā persona, bet apstrādes procesa īpašnieks atbild par procesa atjaunošanu un koriģējošo pasākumu ieviešanu. Datu aizsardzības speciālists konsultē par incidenta kvalificēšanu, risku datu subjektu tiesībām un paziņošanas pienākumiem un uzrauga incidenta izvērtēšanas atbilstību VDAR un šo Noteikumu prasībām.

123. Ja incidents ir būtisks, atkārtojas vai norāda uz sistēmisku procesa vai kontroles trūkumu, par to informē risku vadības speciālistu, kurš izvērtē nepieciešamību attiecīgo risku iekļaut Slimnīcas risku reģistrā.

124. Par katru iespējamu personas datu aizsardzības pārkāpumu Slimnīca bez nepamatotas kavēšanās:

124.1. dokumentē pārkāpuma raksturu, skarto datu subjektu un personas datu kategorijas, aptuveno skarto personu un ierakstu skaitu, iespējamos cēloņus, sekas un veiktos vai plānotos pasākumus;

124.2. novērtē riska iestāšanās iespējamību un iespējamo seku smagumu fizisku personu tiesībām un brīvībām;

124.3. ja nav maz ticams, ka pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām, paziņo par pārkāpumu Datu valsts inspekcijai bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums kļuvis zināms Slimnīcai. Ja paziņošana notiek vēlāk, dokumentē kavēšanās iemeslus;

124.4. ja pārkāpums var radīt augstu risku fizisku personu tiesībām un brīvībām, bez nepamatotas kavēšanās skaidrā un saprotamā valodā informē skartos datu subjektus, ja vien nav piemērojams VDAR noteikts izņēmums;

124.5. dokumentē arī tos pārkāpumus, par kuriem pieņemts lēmums neziņot Datu valsts inspekcijai vai datu subjektiem, norādot lēmuma pamatojumu;

124.6. nosaka incidenta tiešos un sistēmiskos cēloņus, koriģējošos un preventīvos pasākumus, atbildīgās personas un izpildes termiņus, kā arī pārbauda pasākumu īstenošanu un efektivitāti. Ja pasākumi nav pietiekami samazinājuši līdzīga incidenta atkārtošanās risku, nosaka papildu pasākumus;

125. Līgumos ar apstrādātājiem Slimnīca paredz pienākumu bez nepamatotas kavēšanās, bet ne vēlāk kā 24 stundu laikā pēc personas datu aizsardzības pārkāpuma konstatēšanas, informēt Slimnīcu par pārkāpumu, lai Slimnīca varētu izpildīt VDAR noteiktos paziņošanas pienākumus.

126. Personas datu aizsardzības pārkāpumu dokumentāciju un ar incidenta izvērtēšanu saistītos dokumentus glabā atbilstoši Slimnīcas dokumentu pārvaldības un glabāšanas kārtībai.

127. Pēc būtiska personas datu aizsardzības pārkāpuma apstrādes procesa īpašnieks sadarbībā ar datu aizsardzības speciālistu izvērtē nepieciešamību aktualizēt personas datu apstrādes darbību reģistru, veikt ietekmes uz datu aizsardzību novērtējumu vai pārskatīt personas datu apstrādes procesu.
128. Ja personas datu aizsardzības pārkāpums ir saistīts ar apstrādātāja darbību, apstrādes procesa īpašnieks sadarbībā ar datu aizsardzības speciālistu izvērtē nepieciešamību pārskatīt sadarbību ar apstrādātāju vai veikt grozījumus noslēgtajā līgumā.

XVII. Personāla apmācības un konfidencialitātes apliecinājumi

129. Personālam ir pienākums ievērot šo Noteikumu, piemērojamo normatīvo aktu un citu Slimnīcas iekšējo normatīvo aktu prasības personas datu aizsardzības jomā.
130. Pirms piekļuves personas datiem vai informācijas sistēmām personāls vai cita pilnvarota persona tiek iepazīstināta ar tai piemērojamajām datu aizsardzības, pacientu konfidencialitātes un informācijas drošības prasībām un paraksta konfidencialitātes apliecinājumu vai uzņemas konfidencialitātes pienākumu citā tiesiski saistošā veidā.
131. Slimnīca nodrošina regulāras, personāla pienākumiem un ar tiem saistītajam riskam atbilstošas datu aizsardzības un informācijas drošības apmācības. Apmācības organizē vismaz reizi gadā un papildus pēc būtiskām normatīvo aktu, procesu vai informācijas sistēmu izmaiņām, kā arī pēc būtiskiem incidentiem vai konstatētiem pārkāpumiem.
132. Personālam ir pienākums rīkoties un ziņot par incidentiem šo Noteikumu XVI nodaļā noteiktajā kārtībā.
133. Pārkāpumi, kas saistīti ar nepamatotu piekļuvi pacientu datiem, personas datu izpaušanu, apzinātu incidenta noklusēšanu vai piekļuves tiesību ļaunprātīgu izmantošanu, ir uzskatāmi par būtiskiem pārkāpumiem un izvērtējami saskaņā ar Slimnīcas darba kārtības un atbildības regulējumu.
134. Par šo Noteikumu, piemērojamo normatīvo aktu vai konfidencialitātes prasību pārkāpumu personāls var tikt saukts pie disciplinārās, civiltiesiskās, administratīvās vai krimināltiesiskās atbildības atbilstoši piemērojamajiem normatīvajiem aktiem un tiesiskajām attiecībām ar Slimnīcu.
135. Konfidencialitātes pienākums attiecībā uz personas datiem saglabājas arī pēc darba, prakses, mācību, pakalpojuma vai citu tiesisko attiecību izbeigšanas.
136. Slimnīca dokumentē personāla iepazīstināšanu ar šo Noteikumu prasībām, personas datu aizsardzības un konfidencialitātes pienākumiem, kā arī organizētajām datu aizsardzības un informācijas drošības apmācībām.

XVIII. Vadības, apstrādes procesa īpašnieku, struktūrvienību un datu aizsardzības speciālista atbildība

137. Slimnīcas valde un vadība nodrošina personas datu aizsardzības pārvaldības sistēmas izveidi, resursu piešķiršanu, atbildības sadali un iekšējās kontroles ieviešanu.

138. Struktūrvienību vadītāji savā darbības jomā nodrošina, ka personas datu apstrāde tiek veikta atbilstoši šiem Noteikumiem, piekļuves tiesības ir pamatotas, personāls ir informēts par saviem pienākumiem, par incidentiem tiek nekavējoties ziņots, kā arī noteiktajos termiņos tiek īstenoti konstatēto trūkumu novēršanai un risku mazināšanai noteiktie pasākumi.
139. Datu aizsardzības speciālists:
    139.1. informē un konsultē Slimnīcu un tās personālu par datu aizsardzības prasībām;
    139.2. uzrauga VDAR, citu piemērojamo normatīvo aktu un Slimnīcas iekšējo datu aizsardzības noteikumu ievērošanu;
    139.3. sniedz konsultācijas un atzinumus par NIDA un uzrauga tā izpildi;
    139.4. sadarbojas ar Datu valsts inspekciju un darbojas kā kontaktpunkts jautājumos, kas saistīti ar personas datu apstrādi;
    139.5. sniedz konsultācijas par datu subjektu pieprasījumiem, personas datu aizsardzības pārkāpumiem, jauniem apstrādes procesiem, līgumiem, sistēmām un datu nosūtīšanu ārpus ES/EEZ;
    139.6. pilda citus VDAR un piemērojamajos normatīvajos aktos noteiktos uzdevumus.
140. Datu aizsardzības speciālistam jābūt savlaicīgi iesaistītam visos jautājumos, kas saistīti ar personas datu aizsardzību, tostarp jaunu procesu, sistēmu, līgumu, datu nodošanas, incidentu un datu subjektu pieprasījumu gadījumos. Datu aizsardzības speciālists konsultē un uzrauga, bet nepārņem Slimnīcas, apstrādes procesa īpašnieku vai struktūrvienību vadītāju atbildību par personas datu apstrādes atbilstību.
141. Risku vadības speciālists sniedz metodisku atbalstu, bet nepārņem apstrādes procesa īpašnieka, struktūrvienības vadītāja vai datu aizsardzības speciālista atbildību.
142. Apstrādes procesa īpašnieks savā kompetencē nodrošina personas datu apstrādes atbilstību šiem Noteikumiem un piemērojamo normatīvo aktu prasībām, uztur aktuālu informāciju par apstrādes procesu, organizē nepieciešamo risku izvērtēšanu, īsteno noteiktos drošības pasākumus un nodrošina konstatēto trūkumu savlaicīgu novēršanu.

XIX. Iekšējā kontrole, audits un auditācijas pieraksti

143. Slimnīca veic vai organizē personas datu apstrādes iekšējās pārbaudes, tostarp piekļuves tiesību pamatotības, auditācijas pierakstu, datu izpaušanas, dokumentu glabāšanas, incidentu ziņošanas un apmācību izpildes pārbaudes. Pārbaužu apjomu un biežumu nosaka, ņemot vērā apstrādājamo personas datu veidu un apjomu, iepriekš konstatētos incidentus un pārkāpumus, kā arī iespējamo kaitējumu fizisku personu tiesībām un Slimnīcas darbībai.
144. Pārbaužu rezultātus dokumentē. Ja pārbaudē konstatēts pārkāpums, kontroles trūkums vai cits personas datu aizsardzības risks, nosaka nepieciešamos pasākumus, par to izpildi atbildīgās personas un izpildes termiņus. Atbildīgā struktūrvienība nodrošina pasākumu izpildi, bet pārbaudes veicējs vai cita pilnvarota persona pārbauda, vai konstatētie trūkumi ir novērsti.
145. Piekļuve auditācijas pierakstiem tiek nodrošināta tikai pilnvarotām personām. Auditācijas pierakstu saturu, glabāšanas termiņus, aizsardzību un pārbaudes kārtību nosaka atbilstoši

Slimnīcas informācijas tehnoloģiju drošības un lietošanas noteikumiem un normatīvo aktu prasībām.

146. Auditācijas pieraksti tiek izmantoti tikai tiesiskiem nolūkiem, tostarp drošības uzraudzībai, nepamatotas piekļuves pārbaudei, incidentu izmeklēšanai, iekšējām pārbaudēm un auditiem, sistēmu darbības nodrošināšanai un normatīvo aktu prasību izpildei.

147. Ja iekšējā pārbaudē vai auditā tiek konstatēti būtiski personas datu aizsardzības trūkumi vai sistēmiski riski, atbildīgā struktūrvienība sadarbībā ar apstrādes procesa īpašnieku nodrošina koriģējošo pasākumu izstrādi un ieviešanu, kā arī informē datu aizsardzības speciālistu par to izpildi.

XX. Noslēguma noteikumi

148. Noteikumi stājas spēkā nākamajā darba dienā pēc to apstiprināšanas Slimnīcas valdē.

149. Noteikumi tiek publicēti Slimnīcas iekšējā tīmekļa vietnē https://intranet.aslimnica.lv/.

150. Personāls tiek iepazīstināti ar Noteikumiem pēc to apstiprināšanas. Persona, kura pēc šo Noteikumu spēkā stāšanās uzsāk darbu, praksi, mācības vai citu darbību Slimnīcā un kurai amata vai cita tiesiska pamata ietvaros tiek nodrošināta piekļuve personas datiem, pirms piekļuves saņemšanas tiek iepazīstināta ar šiem Noteikumiem.

151. Datu aizsardzības speciālists koordinē šo Noteikumu uzturēšanu un aktualizēšanu, sniedz priekšlikumus par nepieciešamajiem grozījumiem un konsultē struktūrvienības to piemērošanas jautājumos.

152. Struktūrvienību vadītāji un apstrādes procesu īpašnieki bez nepamatotas kavēšanās informē datu aizsardzības speciālistu par procesu, informācijas sistēmu, līgumu vai normatīvo prasību izmaiņām, kuru dēļ var būt nepieciešams aktualizēt šos Noteikumus.

153. Šos Noteikumus pārskata pēc nepieciešamības, jo īpaši pēc būtiskām normatīvo aktu, Slimnīcas darbības procesu vai informācijas sistēmu izmaiņām.