VALSTYBINĖ
DUOMENŲ APSAUGOS
INSPEKCIJA

ASMENS DUOMENŲ, TVARKOMŲ SVEIKATOS PRIEŽIŪROS ĮSTAIGOSE, SAUGUMO UŽTIKRINIMO GAIRĖS

Vilnius, 2017

TURINYS

ĮŽANGA

2017 m. plastinės grožio chirurgijos paslaugas teikiančioje įmonėje įvykęs incidentas, kurio metu buvo pavogti ir vėliau paviešinti pacientų ypatingi asmens duomenys, susiję su jiems teiktomis sveikatos priežiūros paslaugomis, diagnozėmis, atliktomis procedūromis, sulaukė didelio tiek visuomenės, tiek žiniasklaidos dėmesio. Nagrinėjant šį atvejį išaiškėjo, kad duomenų valdytojai – sveikatos priežiūros įstaigos, skiria nepakankamai dėmesio jų tvarkomų asmens duomenų saugumui.

Valstybinė duomenų apsaugos inspekcija (toliau – VDAI), siekdama padėti duomenų valdytojams – sveikatos priežiūros įstaigoms, suprasti, kaip turi būti užtikrintas asmens duomenų ir ypatingų asmens duomenų saugumas, parengė šias gaires.

GAIRIŲ TIKSLAS IR TEISINIS PAGRINDAS

Šiomis gairėmis siekiama paaiškinti sveikatos priežiūros įstaigoms, kokias organizacines ir technines asmens duomenų saugumo priemones reikia įgyvendinti tvarkant pacientų asmens duomenis, kad šie asmens duomenys būtų apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

Asmens duomenų saugumo ir įgyvendinamų asmens duomenų saugumo priemonių reikalavimus nustato:

- Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;
- Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtinti VDAI direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-12 (1.12) (toliau – Bendrieji reikalavimai).

Siekiant užtikrinti asmens duomenų saugumą, taip pat rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos bei tarptautiniais standartais, reglamentuojančiais informacijos (duomenų) saugumą.

TAIKYMO SRITIS IR SUBJEKTAI

Gairės taikomos:

- Duomenų valdytojams – sveikatos priežiūros įstaigoms, tvarkančioms pacientų asmens duomenis automatiniu būdu (informacinių technologijų priemonėmis) ar neautomatiniu būdu susistemintose rinkmenose (pvz., popierinėse ligos istorijose ir pan.);
- Duomenų tvarkytojams – juridiniams ar fiziniams asmenims, duomenų valdytojų įgaliotiems tvarkyti asmens duomenis.

DUOMENŲ TVARKYTOJAI IR JŲ PASIRINKIMAS

Sveikatos priežiūros įstaigos asmens duomenims tvarkyti gali pasitelkti duomenų tvarkytoją.

Duomenų tvarkytoju laikomas juridinis ar fizinis asmuo, duomenų valdytojo įgaliotas tvarkyti asmens duomenis. Atkreiptinas dėmesys į tai, kad sveikatos priežiūros įstaigos darbuotojai nėra laikomi duomenų tvarkytojais. Duomenų tvarkytojais laikomi juridiniai asmenys ar savarankiškai paslaugas atliekantys fiziniai asmenys, teikiantys tokias paslaugas kaip informacinių sistemų ir (ar) kompiuterizuotų darbo vietų priežiūra, interneto svetainės priežiūra, serverių nuoma ir pan.

Sveikatos priežiūros įstaigos, pasitelkdamos duomenų tvarkytojus, su duomenų tvarkytojais turi sudaryti rašytinę asmens duomenų tvarkymo sutartį arba nuostatas, susijusias su asmens duomenų tvarkymu, įtraukti į paslaugų teikimo sutartį.

Atsižvelgiant į teikiamų paslaugų pobūdį, sutartyje turi būti nurodyti konkretūs pavedimai duomenų tvarkytojui dėl asmens duomenų tvarkymo. Turi būti nurodyta:

- Kokius asmens duomenis ir kokiu tikslu pavedama tvarkyti duomenų tvarkytojui;
- Kokius konkrečiai asmens duomenų tvarkymo veiksmus turi atlikti duomenų tvarkytojas;
- Turi būti išdėstytos konkrečios asmens duomenų saugumo priemonės, kurias privalo įgyvendinti duomenų tvarkytojas;
- Turi būti numatyta pareiga duomenų tvarkytojo darbuotojams užtikrinti asmens duomenų konfidencialumą, nurodant, kad pareiga saugoti asmens duomenų paslaptį galioja ne tik perėjus į kitas pareigas, bet ir pasibaigus darbo santykiams;
- Turi būti nustatyta, kad duomenų tvarkytojas asmens duomenis privalo tvarkyti pagal duomenų valdytojo nurodymus ir kt.

Sveikatos priežiūros įstaigos turi pasirinkti tokį duomenų tvarkytoją, kuris garantuotų reikiamas organizacines ir technines duomenų apsaugos priemones ir užtikrintų, kad tokių priemonių būtų laikomasi.

Pasirenkant duomenų tvarkytoją siūlytina atsižvelgti į tai, ar duomenų tvarkytojas turi pavedamo atlikti asmens duomenų tvarkymo patirties, ar jis turi pakankamai žmogiškųjų išteklių šiems pavedimams įvykdyti, ar turi technines galimybes įgyvendinti duomenų valdytojo nurodytas asmens duomenų saugumo priemones ir pan.

Jei yra naudojamasi debesų kompiuterijos paslaugų teikėjo paslaugomis, rekomenduojama įvertinti jo teikiamų paslaugų technines sąlygas (pvz., informacijos pasiekiamumas, vientisumas, galimybė informaciją perkelti iš vieno debesų kompiuterijos paslaugų teikėjo kitam). Siekiant užtikrinti informacijos konfidencialumą ir vientisumą, rekomenduojama pasirinkti tokį debesų kompiuterijos paslaugų teikėją, kuris suteiktų galimybę užšifruoti ir iššifruoti duomenis kuo arčiau galutinio jų panaudojimo taško, t. y., kuo arčiau debesų kompiuterijos paslaugų naudotojo galinio įrenginio.

Jei paslaugų teikėjas yra įsidiegęs informacijos saugos ar kibernetinio saugumo standartus (pvz., ISO 27001), rekomenduojama paprašyti pateikti sertifikatus.

PASIRENGIMAS ĮGYVENDINTI ASMENS DUOMENŲ SAUGUMO PRIEMONES

Įstaiga, ketinanti tvarkyti ar tvarkanti asmens duomenis, turi atlikti savo turimų išteklių (techninės ir programinės įrangos) bei tvarkomų asmens duomenų inventorizaciją.

Asmens duomenys turėtų būti klasifikuojami pagal jų svarbą ir žalą, kurią gali asmuo ar įstaiga patirti duomenų praradimo ar sugadinimo atveju.

Inventorizacijos metu turėtų būti atsakyta į klausimus:

- Kokius asmens duomenis įstaiga tvarko ar ketina tvarkyti?
- Kokiu būdu (automatiniu ar neautomatiniu susistemintose rinkmenose) tvarkomi asmens duomenys?
- Kokie darbuotojai atsakingi ir kokios jų funkcijos tvarkant asmens duomenis?
- Kokios darbuotojų funkcijos ir atsakomybės kibernetinių incidentų ir duomenų saugumo pažeidimų atveju?
- Kur saugomi asmens duomenys ir kokiu pavidalu (duomenų bazės, aplankai su failais, turinio valdymo sistemos ir pan.)?
- Koks yra asmens duomenų judėjimas (duomenų srautai įstaigos viduje ir išorėje)?
- Ar atliktas techninės ir programinės įrangos inventorizavimas?
- Ar parengta ir atnaujinta reikalinga dokumentacija (taisyklių, planų, procedūrų, įsakymų, kitų duomenų saugą reglamentuojančių dokumentų inventorizacija)?

Inventorizacija turi būti atliekama periodiškai.

Pagal poreikį asmens duomenis galima suklasifikuoti pagal įvairius kriterijus, kurie padėtų įvertinti, kurie duomenys yra labiausiai saugotini ir jiems reikia taikyti aukščiausias saugumo priemones (pvz., ypatingi asmens duomenys), kurie duomenys konfidencialūs (jie neturi būti vieši, bet jiems užtektų žemesnio saugumo lygio), kurie duomenys yra teikiami trečiosioms šalims (su įstaiga nesusiję duomenų teikėjai/gavėjai).

Techninei ir standartinei programinei įrangai inventorizuoti galima panaudoti tuo tikslu sukurtas programas, kurių rinkoje yra gana daug. Inventorizacija padės kontroliuoti turimus išteklius, jų panaudojimą ir pastebėti nesankcionuotai įdiegtas programas bei neatnaujintas programų versijas.

ASMENS DUOMENŲ TVARKYMO RIZIKOS ANALIZĖ

Rizikos vertinimas gali būti atliekamas įvairiais būdais – pasitelkiant į pagalbą išorės įmones ar ekspertus arba naudojantis savo darbuotojų pajėgumais. Metodikų yra įvairių, tačiau bet kuriuo atveju reikėtų įvertinti tokius faktorius ir nustatyti jų poveikį sveikatos asmens duomenų (toliau – SAD) **konfidencialumui**, **saugumui**, **integralumui** ir **pasiekiamumui**. Norint nustatyti galimas rizikas, reikėtų atsižvelgti į šiuos aspektus:

- Ar įstaiga turi dokumentus ir yra įdiegusi politiką ir procedūras rizikai vertinti. Ar kontroliuojamas šių dokumentų ir procedūrų įgyvendinimas bei ar jie periodiškai peržiūrimi ir atnaujinami;
- Ar įstaiga yra įvertinusi visas turimas informacines sistemas ar kitus išteklius, kur tvarkomi SAD pagal tai, kokią įtaką veiklai turės jų neveikimas ar nepasiekiamumas;
- Ar atliekamas rizikos vertinimas įvykus reikšmingam kibernetiniam ar duomenų saugumo incidentui ir pasikeitus veiklos pobūdžiui;
- Ar yra dokumentuota, kaip bus mažinama rizika atlikus rizikos analizę ir nustačius pažeidžiamumus;
- Ar inventorizuoti SAD, suskirstant juos pagal svarbą, atsižvelgiant į žalą, kurią padarytų tų duomenų vagystė, sugadinimas, atskleidimas, pakeitimas ar nepasiekiamumas.
- Ar įstaiga turi informacinės (duomenų) saugos strategijos planą, kurį sudaro: paslaugų teikėjų valdymo ir kontrolės planas, veiklos tęstinumo, veiklos atstatymo ir avarinių situacijų valdymo planai;
- Ar personalui yra teikiama mokomoji medžiaga, ar rengiami mokymai informacijos saugos, asmens duomenų ir kibernetinės saugos klausimais;
- Ar darbo (veiklos) procedūrose numatyta vartotojų veiksmų analizė, įvykių ataskaitos, jų analizės ataskaitos bei auditų žurnalų peržiūra. Ar ši nuostata įgyvendinta, nuolatos, periodiškai peržiūrint informacinės sistemos, duomenų bazių bei tinklo įrenginių audito žurnalus, siekiant pastebėti saugos incidentus, nesankcionuotos prieigos bandymus ir pan.;
- Ar yra paskirtas už asmens duomenų saugą atsakingas darbuotojas – saugos įgaliotinis ar informacijos saugos vadovas, kurio pareiga kurti duomenų saugos taisykles ir procedūras, kontroliuoti jų vykdymą, kuris yra kontaktinis asmuo dėl visų klausimų, susijusių su informacijos (duomenų) sauga, kuris turi kontroliuoti, kaip išoriniai paslaugų teikėjai (duomenų tvarkytojai ir techninių paslaugų teikėjai) laikosi saugos įsipareigojimų?
- Ar yra parengta prieigos prie SAD ir kitų duomenų bei informacinės sistemos išteklių politika;
- Ar yra dokumentuotos prieigos prie duomenų ir techninių išteklių teisės darbuotojams, atsižvelgiant į jų atliekamas funkcijas. Ar jos tinkamai įgyvendintos, suteikiant darbuotojams tik tas teises ir vaidmenis, kurie yra būtini?
- Ar atliktas privilegijuotų vartotojų išorinių prisijungimų, siekiant administruoti informacinę sistemą bei techninius išteklius, ir paprastų vartotojų išorinių prisijungimų prie sveikatos duomenų įvertinimas?
- Ar atliktas vartotojų prieigos prie duomenų identifikavimo politikos įvertinimas?

ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ ĮGYVENDINIMAS

SAD tvarkymas automatiniu būdu pagal Bendruosius reikalavimus priskiriamas 3 saugumo lygiui.

Duomenų apsaugos priemonių pasirinkimas yra kiekvienos sveikatos priežiūros įstaigos atsakomybė.

Tiek techninės, tiek organizacinės priemonės pasirenkamos atsižvelgiant į inventorizacijos ir rizikos vertinimo rezultatus.

Jeigu įstaiga savo veiklos dar nėra pradėjusi, renkantis ar projektuojant sveikatos duomenis tvarkyti skirtą informacinę sistemą, rizikos vertinimą reikėtų atlikti įvairiose projektavimo stadijose, nes nenumatytas projektavimo metu saugumo priemones įdiegti vėliau gali būti sunku ir brangu, o kai kada ir visai neįmanoma, visai nepakeitus informacinės sistemos. Viena iš tokių privalomų priemonių yra vartotojų identifikavimo, vaidmenų paskirstymo ir veiksmų fiksavimo galimybės.

ORGANIZACINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

Saugos ir konfidencialumo politika, taisyklės, procedūros

Įstaiga, tvarkanti SAD, savo veiklą, užtikrinančią duomenų konfidencialumą, saugumą, integralumą ir pasiekiamumą, turi aiškiai ir tiksliai dokumentuoti. Tai būtina, siekiant užtikrinti personalo darbo kultūrą, procesų kontrolę, atskaitomybę ir informuotumą.

Įstaiga turi sukurti tikslią, detalią ir aiškią saugos ir konfidencialumo politiką, kurioje būtų nustatyta, kokia informacija yra konfidenciali ir kurie darbuotojai, kokiais teisės aktų reikalavimais vadovaudamiesi turi teises ją tvarkyti. Dokumente turėtų būti aptarti personalo mokymo ir darbo su SAD kultūros kėlimo politika bei sankcijos pažeidimų atvejais. Saugos politikoje numatomas inventorizavimo bei rizikos vertinimo periodiškumas, teikiamos ataskaitos ir kontrolės mechanizmai. Darbuotojai, dirbantys su SAD, turėtų pasirašyti konfidencialumo pasižadėjimą.

Kita, detalesnė dokumentų grupė yra taisyklės. Taisyklėse numatoma darbo su asmens duomenimis tvarka, konkrečios atsakomybės, rizikos vertinimo tvarka, darbo su popierinėmis SAD bylomis tvarka, vartotojų identifikavimo, jų veiksmų registravimo tvarka ir pan.

Konkrečių darbo instrukcijų aprašymai pateikiami darbo procedūrų dokumentuose. Tai instrukcijos, skirtos atlikti konkrečiai užduočiai ar funkcijai: atsarginiam duomenų kopijavimui atlikti, administruoti vartotojus, kontroliuoti vartotojų veiksmų žurnalus ir pan.

Paslaugų teikėjų įsipareigojimų kontrolė

Sutartys su išoriniais paslaugų teikėjais turi užtikrinti, kad paslaugų teikėjai laikysis visų reikalavimų, taikomų SAD apsaugai. Tai turi atsispindėti paslaugų teikimo sutartyse ar susitarimuose dėl paslaugų teikimo lygmens (angl. *SLA, Service Level Agreements*). Įstaiga, perkanti paslaugas, turi patikrinti paslaugų teikėjus tam, kad įsitikintų, jog reikalavimų bus laikomasi. Paslaugų teikėjai, atsižvelgiant į jų funkcijas, turi reguliariai teikti ataskaitas apie pastebėtus saugos pažeidimus ir įtartinus įvykius, kurie gali paveikti duomenų saugumą.

Atsakingo už asmens duomenų saugą asmens (saugos įgaliotinio) paskyrimas

Šią funkciją turėtų atlikti darbuotojas, išmanantis teisės aktus ir turintis žinių duomenų saugos srityje. Jis taip pat būtų kontaktinis asmuo visais klausimais, susijusiais su SAD apsauga. Saugos įgaliotinis rengia ir derina SAD saugos dokumentus bei kontroliuoja jų vykdymą. Saugos įgaliotinis neturi atlikti saugos administratoriaus funkcijų, nes jo užduotis yra kontroliuoti SAD saugą, o administratorius atsako už techninių priemonių diegimą ir jų veikimą.

Personalo švietimas ir mokymas apie duomenų saugą

Tai labai svarbi organizacinė duomenų apsaugos priemonė. Svarbu, kad darbuotojai suprastų duomenų saugumo tikslą ir galimą teigiamą ir neigiamą savo elgesio poveikį organizacijai.

Švietimo apie duomenų saugą programa turėtų būti parengta pagal organizacijos informacijos saugumo politiką ir atitinkamas procedūras, atsižvelgiant į organizacijos tvarkomus (saugomus) duomenis ir saugos valdymo priemones, kurios buvo įgyvendintos duomenims apsaugoti.

Mokymai apie duomenų saugą galėtų apimti tokius aspektus:

- Būtinybę susipažinti su taikomomis organizacijoje duomenų saugos taisyklėmis ir jų laikytis taip, kaip jos apibrėžtos organizacijos saugos politikos dokumentuose;
- Asmeninę atsakomybę už savo veiksmus ir neveikimą bei bendrą atsakomybę už organizacijos tvarkomų duomenų saugą;
- Pagrindines duomenų saugumo procedūras (pvz., pranešimas apie duomenų saugumo pažeidimus) ir bazines saugos valdymo priemones (pvz., slaptažodžių naudojimas, apsaugos nuo kenkimo programų priemonės, švaraus stalo politika);
- Kontaktinius asmenis ir išteklius, skirtus papildomai informacijai ir patarimams duomenų saugumo klausimais, saugos mokymų medžiagą.
- Darbuotojai turi būti apmokyti ir žinoti, kaip dirbti su popierinėmis bylomis bei užtikrinti jose esančių duomenų konfidencialumą.

Švietimas ir mokymas apie duomenų apsaugą turėtų vykti reguliariai. Pirminį darbuotojų švietimą ir mokymą reiktų taikyti ne tik pradedantiesiems, bet ir tiems, kurie perkeliami į naujas pareigas ar pradeda vykdyti naujas funkcijas, kurioms keliami gana skirtingi ar kitokie duomenų saugumo reikalavimai. Mokymai turėtų vykti prieš pradedant atlikti šias pareigas ar vykdyti funkcijas.

TECHNINĖS ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

Prieigos prie SAD kontrolė

Ši priemonė turi užtikrinti, kad visi vartotojai: personalas, pacientai, įstaigos informacinių sistemų ir duomenų bazių administratoriai, paslaugas teikiančių trečiųjų šalių (išoriniai paslaugų teikėjai, teikiantys paslaugas pagal sutartį) administratoriai ir programinę įrangą prižiūrintys paslaugų teikėjai turėtų prieigą tik prie tų duomenų, kurie jiems yra būtini funkcijoms atlikti, ir būtų identifikuojami rizikos lygį atitinkančiomis priemonėmis (pvz., naudojant dviejų faktorių autentifikaciją).

Patartina naudoti tokias prieigos teisių suteikimo priemones, kurios leistų bendro identifikavimo būdu gauti visus tai funkcijai atlikti priklausančius išteklius (pvz., *Active Directory, OpenLDAP*).

Prieigos teisių užsakymas turėtų būti griežtai kontroliuojamas ir vykti pagal nustatytą procedūrą. Informacinės sistemos funkcionalumas turėtų būti suprojektuotas taip, kad galima būtų

detaliai nurodyti, prie kokių duomenų ar jų grupių leidžiama prieiga ir kokias funkcijas su jais galima atlikti.

Patartina įstaigoms turėti prieigos užsakymo formą, kurią užsakymo atveju patvirtina atsakingas asmuo. Pacientų prieiga prie savo asmens duomenų taip pat neturi būti supaprastinta, jiems turi būti taikomi įprasti organizacijoje taikomi prieigos prie SAD reikalavimai. Prieiga prie sveikatos kortelės galėtų būti suteikiama naudojant elektroninio parašo ar kitas patikimas tapatybės nustatymo ir patvirtinimo priemones. Reikalavimų griežtumas turi priklausyti nuo rizikos analizės rezultatų, t. y., kokios rizikos grupės sveikatos duomenys yra prieinami prisijungus atitinkamai identifikuojantis.

Vartotojų prisijungimo veiksmai prie informacinių sistemų, kuriose tvarkomi SAD, taip pat prie SAD duomenų bazių ar failų turi būti kontroliuojami. Kontrolės taisyklės ir tvarka nustato kas, kaip ir kada kontroliuoja šį procesą. Pagrindinis tokios analizės šaltinis yra informacinės sistemos, duomenų bazės, tarnybinės stoties, ugniasienės ir kitų techninių ir programinių įrenginių kuriami elektroniniai įvykių žurnalai. Vartotojų veiksmų su SAD fiksavimas (rašymas, keitimas, šalinimas, peržiūra) turi būti numatytas projektuojant sveikatos priežiūros veiklai skirtą informacinę sistemą, nes techniniuose įvykių žurnaluose gali atsispindėti tik prisijungimo identifikatoriai, data, laikas. Siekiant, kad kontrolės procesas būtų patogus, patartina naudoti papildomas rinkoje platinamas standartines programas, kurios integruoja ir apdoroja elektroninių įvykių žurnalų informaciją bei pateikia suvestines pagal pageidaujamus parametrus.

Jeigu identifikavimas vyksta naudojant slaptažodžius, jie turi būti administruojami pagal nustatytas taisykles: sudėtingumo, keitimo dažnumo, naikinimo, priminimo, saugojimo ir pan. Vartotojui būnant neaktyviam nustatytą laikotarpį, informacinė sistema turi turėti automatinį išjungimą iš sistemos (angl. *logoff*).

Duomenų perdavimo saugumas

Duomenų perdavimo saugumas užtikrinamas juos šifruojant. Šifravimas taikomas perduodant SAD bet kuriuo būdu: interneto tinklu, vidiniu įstaigos tinklu, elektroniniu paštu ar išorinėse duomenų laikmenose. Šifravimo būdas ir jo priemonės turėtų būti taikomos priklausomai nuo SAD rizikos analizės rezultatų.

Jeigu įstaiga teikia ar gauna SAD iš trečios šalies (ne įstaigos valdomos informacinės sistemos) reikėtų įsitikinti, kad prisijungimas prie trečios šalies informacinės sistemos vyksta saugiu protokolu (pvz., SSL, TLS, VPN, WS–Security).

SAD, siunčiamus elektroniniu paštu, apsaugoti labai sunku. Naudojant dvipusius šifravimo raktus galima nustatyti saugų perdavimą tik tarp nuolatinių adresatų, abiejose pusėse įdiegus atitinkamą programinę įrangą. Su kitais, nenuolatiniais adresatais, SAD perduoti elektroninio pašto naudoti negalima, nebent adresatai turi saugią Lietuvos pašto e. pristatymo paslaugos pašto dėžutę.

Jeigu įstaiga svarsto galimybę tvarkyti ar saugoti SAD naudojant debesų kompiuteriją, reikia atkreipti dėmesį į pasirenkamą paslaugos teikėją, į fizinę duomenų saugojimo vietą. Patartina naudoti ne viešą, o privatų ar hibridinį debesį, prieš tai išsiaiškinus naudojamas duomenų apsaugos priemones bei įsipareigojimus duomenų prieinamumo ir patikimumo požiūriu. Naudojamai informacinei sistemai ir prieigos kontrolei reikalavimai yra tokie pat, kaip ir tvarkant SAD lokaliai.

Tinklai ir mobilieji įtaisai

Kaip viena iš duomenų saugos priemonių kompiuterių tinkluose gali būti naudojamas kompiuterių tinklų, tinkle teikiamų paslaugų ir sistemų bei naudotojų atskyrimas. Tinklo atskyrimas gali būti atliekamas naudojant fiziškai atskirtus tinklus arba skirtingus loginius tinklus (pvz., virtualius privačius tinklus).

Organizacijoje belaidžiais tinklais turėtų naudotis tik personalas, jei tai yra būtina.

Dėl sunkiai apibrėžiamų tinklų ribų, belaidžiams tinklams reikalinga speciali saugos politika. Kai tvarkomi SAD, prieš suteikiant prieigą prie vidaus sistemų, reikėtų apsvarstyti galimybę visus belaidės prieigos bandymus laikyti išoriniu prisijungimu ir šią prieigą atskirti nuo vidaus tinklų, nors kol prieigos bandymą praleis saugiai sukonfigūruota tinklo ugniasienė.

Siekiant užtikrinti, kad SAD nebūtų atskleisti, naudojant mobiliuosius įtaisus reikėtų laikytis ypatingo atsargumo.

Mobiliuosiuose įrenginiuose turėtų veikti apsauga, kad būtų galima išvengti neteisėtos prieigos prie duomenų, saugomų ir apdorojamų šiais įtaisais, pvz., naudojant įrenginio (išmaniojo telefono, planšetinio kompiuterio) atmintinės šifravimą ir tapatumo nustatymo priemones (PIN, slaptažodžiai, kriptografiniai raktai).

Naudojant mobiliuosius įtaisus organizacijoje reikėtų atsižvelgti į tai, kad kai kurie belaidžio ryšio saugumo protokolai nėra visiškai susiformavę ir turi žinomų trūkumų. Taip pat ne visada galima daryti mobiliuosiuose įtaisuose saugomų duomenų atsargines kopijas dėl riboto tinklo pralaidumo arba dėl to, kad prie mobiliųjų įtaisų negalima prisijungti darant suplanuotas atsargines kopijas.

Atsarginės duomenų kopijos

Turėtų būti nustatyta duomenų ir informacinių sistemų programinės įrangos atsarginių kopijų darymo ir duomenų atstatymo politika. Joje turėtų būti nustatyti išsaugojimo ir apsaugos reikalavimai.

Rengiant atsarginių kopijų darymo planą, reikėtų atsižvelgti į šiuos punktus:

- Turėtų būti parengti tikslūs ir išsamūs atsarginių kopijų duomenys ir dokumentuotos atkūrimo procedūros;
- Atsarginės duomenų kopijos turėtų būti saugomos pakankamu atstumu nuo pagrindinės duomenų buvimo vietos;
- Naudojant ir dirbant su SAD, konfidencialumas labai svarbu, todėl atsarginės duomenų kopijos turėtų būti apsaugotos šifravimo priemonėmis, nepriklausomai nuo to, ar jos laikomos lokaliai ar naudojamasi debesų kompiuterijos paslaugomis;
- Siekiant užtikrinti, kad atsarginių kopijų kūrimo procesas būtų atliekamas iki galo, turėtų būti stebimas šis procesas ir atkreipiamas dėmesys į nepavykusius, nors suplanuotus, atsarginių kopijų kūrimo atvejus;
- Turėtų būti nustatytas atsarginių kopijų saugojimo laikotarpis, atsižvelgiant į esamą poreikį ilgai išsaugoti SAD atsargines kopijas.

Rekomenduojama, jei yra techninių galimybių, kuriant atsargines kopijas, naudoti 3-2-1 ar panašias kopijų darymo strategijas, t. y., turėti tris ypač svarbių duomenų kopijas. Jos turėtų būti laikomos mažiausiai dviejuose skirtinguose įrenginiuose ir bent viena atsarginė duomenų kopija saugoma geografiškai nutolusioje vietoje. Svarbu, kad bent viena atsarginė kopija būtų autonominė (angl. *offline backup*).

FIZINĖS DUOMENŲ APSAUGOS PRIEMONĖS

Fizinės saugumo priemonės

Fizinės apsaugos priemonės turėtų būti numatytos ir naudojamos, siekiant apsaugoti vietas, kuriose laikomi konfidencialūs duomenys ar duomenų saugojimo bei apdorojimo priemonės (tarnybinės stotys, duomenų saugyklos ir pan.). Pastatai ar vietos (saugumo zonos), kuriose yra duomenų apdorojimo priemonės, turėtų būti fiziškai patikimos, tų vietų išorinis stogas, sienos ir

grindys turėtų būti iš vientisų konstrukcijų ir visos išorinės durys turėtų būti tinkamai apsaugotos nuo neteisėto patekimo valdymo mechanizmais (pvz., skląsčiais, signalizacijomis ir spynomis). Kai nėra žmonių, durys ir langai turėtų būti užrakinti, taip pat turėtų būti apsvarstyta langų išorės apsaugos galimybė, ypač pirmame aukšte.

Organizacijos valdomos duomenų apdorojimo priemonės (tarnybinės stotys, kompiuterių tinklai ir pan.) turėtų būti fiziškai atskirtos nuo trečiųjų šalių (kitų įmonių) valdomos įrangos, jeigu jie nėra įgalioti duomenų tvarkytojai.

Saugumo zonos turėtų būti apsaugotos tinkamomis įėjimo valdymo priemonėmis, kurios užtikrintų tik įgalioto personalo įleidimą. Patekti į vietas, kuriose apdorojami arba saugomi konfidencialūs duomenys, turėtų turėti teisę tik leidimą turintys asmenys, įgyvendinus atitinkamas įėjimo valdymo priemones, pvz., įgyvendinus dviejų veiksnių (faktorių) tapatumo nustatymo mechanizmą. Turėtų būti saugiai vedama ir stebima visų patekimo atvejų popierinė registracijos knyga arba elektroninis žurnalas. Ribota prieiga prie saugumo zonų arba prie konfidencialių duomenų apdorojimo priemonių trečios šalies (kitų įmonių) priežiūros paslaugų personalui turėtų būti suteikta tik esant poreikiui. Šiai prieigai turėtų būti duotas leidimas ir ji turėtų būti stebima.

Įrangos ir laikmenų saugumas bei saugus naikinimas

Elektros maitinimo ir telekomunikacijų kabeliai, kuriais perduodami duomenys arba teikiamos paslaugos, turėtų būti apsaugoti nuo slapto prisijungimo, trukdžių arba pažeidimo. Siekiant išvengti trukdžių, elektros maitinimo kabeliai turėtų būti atskirti nuo ryšių (kompiuterių tinklo) kabelių.

Be atitinkamo leidimo įranga, SAD arba programinė įranga neturėtų būti išnešama iš įstaigos patalpų. Jeigu leidimas yra gautas, atsižvelgiant į rizikos įvertinimo rezultatus, įrangoje turi būti įdiegtos apsaugos priemonės. Net jeigu duomenys neišnešami, bet yra galimybė iš įrenginio prisijungti prie įstaigoje esančių SAD, prisijungimai turi būti tinkamai sukonfigūruoti naudojant šifravimo priemones bei kitas technologijas, apsaugančias nuo galimybės pasinaudoti tokiu prisijungimu. Bet kuriuo atveju, įranga ir duomenų laikmenos neturėtų būti paliekamos be priežiūros viešose vietose ir neduodamos naudotis kitiems asmenims (pvz., vaikams).

Asmens duomenų saugojimas išorinėse (keičiamose, pvz., USB, SIM) laikmenose turėtų būti griežtai reglamentuotas, numatant technines ir organizacines priemones bei pastoviai apmokant personalą. Ypač jautrių SAD saugoti išorinėse laikmenose nepatartina.

Prieš sunaikinant arba pakartotinai naudojant IT įrangą, visi jos elementai, kuriuose yra atmintinės, turėtų būti patikrinami, siekiant užtikrinti, kad visi konfidencialūs duomenys būtų sunaikinti arba saugiai perrašyti. Atmintinė su konfidencialia informacija turėtų būti fiziškai sunaikinta arba joje esanti informacija turėtų būti sunaikinta, ištrinta arba perrašyta naudojant būdus, skirtus pirminę informaciją paversti neatkuriama, o ne naudojant standartinę ištrynimo arba formatavimo funkciją. Konfidencialių duomenų atskleidimo riziką galima sumažinti ne tik saugiuoju disko trynimu, bet ir viso disko šifravimu, jei šifravimo procesas yra pakankamai patikimas ir apima visą diską, o patys šifravimo raktai laikomi konfidencialiai (nesaugomi tame pačiame diske) ir yra pakankamai ilgi, kad atlaikytų bandymus juos „nulaužti“.

Visi vartotojai turėtų būti informuoti apie saugumo reikalavimus ir procedūras, taikomus be priežiūros paliekamai įrangai, ir apie jų atsakomybę už tokios apsaugos įgyvendinimą. Vartotojai turėtų atsijungti nuo taikomųjų programų ar tinklo paslaugų, kai jų nebereikia, apsaugoti kompiuterius ar mobiliuosius įtaisus nuo neleistino naudojimo, panaudojant prieigos slaptažodžius arba kitas tapatybės nustatymo priemones.

Popieriniams dokumentams ir keičiamosioms duomenų laikmenoms (USB atmintinėms, išoriniams standiesiems diskams, DVD laikmenoms) turėtų būti taikoma švaraus stalo politika. Taikant šią politiką, sumažėja neteisėtos prieigos prie duomenų, jų praradimo ir sugadinimo įprastu darbo laiku ir po jo rizikos. Popierinės bylos ar elektroninės duomenų laikmenos turėtų būti saugomos

užrakintos (geriausia seife, spintoje arba kitų rūšių apsaugotuose balduose), kai jų nereikia, ypač, kai darbuotojas palieka įstaigą.

PRAKTINIAI ASMENS DUOMENŲ TVARKYMO ASPEKTAI

Atsižvelgiant į VDAI atliktų patikrinimų sveikatos priežiūros įstaigose rezultatus ir informaciją, gautą vykdant kitas funkcijas, sveikatos priežiūros įstaigos, tvarkydamos asmens duomenis, turėtų atsižvelgti į šiuos aspektus:

- Pacientams jungiantis prie išankstinių registracijos pas gydytojus sistemų, kaip prisijungimo vardas ir (ar) slaptažodis, neturėtų būti naudojamas asmens kodas;
- Popierinės pacientų sveikatos istorijos gydytojų kabinetuose, budėjimo postuose ir pan. turėtų būti sudėtos taip, kad su jose esančiais asmens duomenimis (pvz., viršutiniame sveikatos istorijos lape nurodytu vardu, pavarde, adresu ir t. t.) negalėtų susipažinti tokios teisės neturintys pacientai ar kiti asmenys;
- Kompiuterių monitoriai, kuriuose sveikatos priežiūros įstaigos specialistai peržiūri su paciento sveikata susijusią informaciją, turėtų būti nukreipti taip, kad su monitoriuje matomais asmens duomenimis negalėtų susipažinti tokios teisės neturintys kiti pacientai ar kiti asmenys, užėję į gydytojo kabinetą;
- Sveikatos priežiūros įstaigose tiek kalbant su pacientais telefonu, tiek gydytojų kabinetuose, turi būti užtikrintas pokalbių su pacientais konfidencialumas (t. y., pokalbis turi vykti taip, kad pokalbio metu pateiktų asmens duomenų negalėtų girdėti neįgalioti asmenys);
- Telefonu asmens duomenys neturi būti teikiami, jeigu sveikatos priežiūros įstaiga neturi galimybės identifikuoti skambinančio asmens;
- Siunčiant pacientams informaciją (pvz., tyrimų atsakymus ir pan.) elektroniniu paštu, ypatingi asmens duomenys turi būti užšifruoti;
- Pacientų ligos istorijoje turi būti tvarkoma ir saugoma tik su šiam pacientui teiktomis sveikatos priežiūros paslaugomis susijusi informacija. Ligos istorijoje neturėtų būti tvarkoma ir saugoma administracinė informacija (pvz., pacientų skundai ir jų nagrinėjimo rezultatai);
- Gydymo įstaigų, teikiančių stacionarias sveikatos priežiūros paslaugas, koridoriuose neturėtų būti skelbiami pacientų sąrašai su informacija, kuriose palatose, kokie pacientai gydomi;
- Vaizdo stebėjimas neturi būti vykdomas tose patalpose, kuriose pacientams teikiamos sveikatos priežiūros paslaugos, ar tose, kuriose atskleidžiami pacientų ypatingi asmens duomenys (pvz., koridoriuose prie gydytojų kabinetų ir pan.);
- Tvarkant sveikatos priežiūros įstaigos archyvą, pasibaigus nustatytam asmens duomenų saugojimo terminui, šie duomenys turi būti sunaikinami;
- Tiek rašytiniai dokumentai, tiek pačios įgyvendinamos asmens duomenų saugumo priemonės turi būti periodiškai peržiūrimos.

Tikimės, kad šios gairės Jums yra naudingos ir padės tinkamai tvarkyti asmens duomenis, o jeigu turite pastabų ar siūlymų dėl šių gairių tobulinimo, būtume labai dėkingi, jeigu apie tai mus informuotumėte adresu ada@ada.lt.