Útgefið 3. nóvember 2026

Leiðbeiningar um stafræn sjúkraskrárkerfi

Frá 1. desember nk. verður heilbrigðisstarfsmönnum skylt að færa sjúkraskrá í stafrænt sjúkraskrárkerfi samkvæmt lögum nr. 81/2025 sem breyttu lögum nr. 55/2009 um sjúkraskrár.

Í aðdraganda þess hafa Stafræn heilsa og Embætti landlæknis tekið saman leiðbeiningar um þær kröfur sem gerðar eru til stafrænna sjúkraskrárkerfa samkvæmt gildandi rétti.

Hvorki embætti landlæknis né Stafræn heilsa samþykkja einstök sjúkraskrárkerfi eða halda skrá yfir samþykkt kerfi eða kerfisveitur. Það er á ábyrgð hvers ábyrgðaraðila sjúkraskráa að velja kerfi og kerfisveitu og meta hvort þau uppfylli þær kröfur sem hér er lýst. Tilkynna skal embætti landlæknis um hvaða kerfi er notast við og ber veitanda heilbrigðisþjónustu að ábyrgjast að það uppfylli kröfur sem til slíkra kerfa eru gerðar.

Kröfunum má skipta í tvennt. Annars vegar eru kröfur sem leiða beint af lögum nr. 55/2009 um sjúkraskrár, reglugerð nr. 550/2015 um sjúkraskrár og fyrirmælum landlæknis um öryggi og gæði sjúkraskráa og lágmarksskráningu í heilbrigðisþjónustu. Hins vegar kröfur sem leiða má af öðrum lögum, einkum lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

Um leiðbeiningarnar

Skyldan til að færa sjúkraskrá í stafrænt sjúkraskrárkerfi nær einnig til minni starfsstofa, sem sumar þurfa nú í fyrsta sinn að uppfylla kröfur um öryggi stafrænna sjúkraskráa. Leiðbeiningarnar segja hvað þarf að gera en gátlistinn og sniðmátin sem þeim fylgja útskýra hvernig það er gert.

Efnið samanstendur af sex skjölum:

	Skjal	Fyrir hvern	Til hvers
1	**Leiðbeiningar um stafræn sjúkraskrárkerfi**	Alla sem færa sjúkraskrá	Kröfur til sjúkraskrárkerfa og hver ber ábyrgð á hverju. Hvernig tilkynna skal embætti landlæknis þegar rekstur hefst eða skipt er um kerfi. Hverjum ber að tilkynna öryggisbrest og hvenær.
2	**Gátlisti fyrir ábyrgðaraðila sjúkraskráa**	Ábyrgðaraðila sjúkraskráa, þegar kerfi er valið eða yfirfarið	39 spurningar til kerfisveitu (e. application service provider) í átta flokkum: kerfið og kerfisveitan, hýsing og staðsetning gagna, samningar og lok viðskipta, aðgangsstýring og auðkenning, aðgerðaskrá og rekjanleiki, öryggisráðstafanir, atvik, tilkynningar og samfella, og loks virkni og réttindi sjúklinga.

	Skjal	Fyrir hvern	Til hvers
			Hafi kerfisveita birt svörin nægir að vísa til þeirra.
3	**Sniðmát 1: Öryggishandbók**	Allar starfsstofur	Upplýsingaöryggisstefna, neyðaráætlun og verklagsreglur í einu skjali.
4	**Sniðmát 2: Áhættumat**	Allar starfsstofur	Áhættumat á vinnslu sjúkraskrárupplýsinga ásamt áætlun um úrbætur.
5	**Sniðmát 3: Innra eftirlit**	Allar starfsstofur, árlega	Árleg samantekt um innra eftirlit: eftirlit með aðgangi, aðgangsheimildir, afritun og endurheimt, kerfisveita og hýsingaraðili, frávik ársins og æfing neyðaráætlunar.
6	**Sniðmát 4: Frávikaskrá**	Allar starfsstofur, jafnóðum	Skrá yfir atvik og frávik, með viðmiðum um alvarleika og upplýsingum um hverjum ber að tilkynna.

Hvar á að byrja

1. Lesið leiðbeiningarnar (1).
2. Ef þið eruð að velja kerfi, eða hafið ekki enn kannað það kerfi sem þið notið, sendið kerfisveitunni gátlistann (2).
3. Fyllið út öryggishandbókina (3) og áhættumatið (4). Saman mynda þau kjarnann í öryggiskerfi starfsstofunnar.
4. Skráið atvik í frávikaskrána (6) jafnóðum og gerið samantekt um innra eftirlit (5) einu sinni á ári.

Gott að vita

- **Sniðmátin eru ráðgefandi.** Nota má eigin skjöl ef þau ná yfir sömu atriði. Sniðmátin eru samin fyrir litlar starfsstofur, einnig þar sem heilbrigðisstarfsmaður starfar einn.
- **Varðveitið skjölin.** Geymið útfylltan gátlista og sniðmát með öðrum gögnum öryggiskerfisins. Embætti landlæknis getur óskað eftir upplýsingum um öryggiskerfið.
- **Gervigreind getur komið að gagni.** Í sniðmátunum er lýst hvernig nota má gervigreind við útfyllingu, í samræmi við gervigreindarstefnu Stafrænnar heilsu.

Hver ber ábyrgð á hverju

Ábyrgð á sjúkraskrá og sjúkraskrárkerfi skiptist á milli nokkurra aðila. Taflan hér að neðan sýnir helstu skyldur hvers þeirra. Sami aðili getur gegnt fleiri en einu hlutverki. Kerfisveita (e. application service provider) er fyrirtæki sem lætur sjúkraskrárkerfið í té og rekur það eftir atvikum.

Heilbrigðisstarfsmaður sem starfar einn á stofu telst umsjónaraðili þeirra sjúkraskráa sem hann færir, sbr. 3. gr. laga nr. 55/2009, og starfsstofa hans er ábyrgðaraðili þeirra. Hann ber því í reynd skyldur beggja hlutverka, auk eigin skyldna sem heilbrigðisstarfsmaður.

Aðili	Helstu skyldur	Laga- og reglugerðarstoð
Heilbrigðisstarfsmaður	Færir sjúkraskrá í stafrænt sjúkraskrárkerfi frá 1. desember 2026, jafnóðum og að jafnaði innan 24 klukkustunda. Við hverja færslu kemur fram nafn, starfsheiti og tímasetning. Ber ávallt ábyrgð á eigin færslum. Undirritar trúnaðaryfirlýsingu.	4. og 5. gr. laga nr. 55/2009, 1. mgr. 7. gr. rg. 550/2015
Ábyrgðaraðili sjúkraskráa (heilbrigðisstofnun eða starfsstofa)	Sér til þess að unnt sé að færa sjúkraskrá í samræmi við lögin. Rekur öryggiskerfi og lætur embætti landlæknis í té upplýsingar um það þegar óskað er. Velur sjúkraskrárkerfi og hýsingaraðila og gengur úr skugga um að hýsingaraðili sé viðurkenndur þjónustuaðili. Gerir vinnslusamning við kerfisveitu og hýsingaraðila. Ber ábyrgð á að unnið sé eftir aðgangsreglum, á varðveislu sjúkraskráa og á tilkynningum um öryggisbresti.	3. mgr. 4. gr. og 9. gr. laga nr. 55/2009, 6., 7. og 10. gr. rg. 550/2015, 28., 33. og 34. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018
Umsjónaraðili sjúkraskráa (læknir eða annar heilbrigðisstarfsmaður sem ábyrgðaraðili felur hlutverkið)	Hefur eftirlit með því að skráning og meðferð sjúkraskráruppplýsinga sé í samræmi við lög. Sér til þess að reglulega sé fylgst með aðgangi að sjúkraskrá og setur verklagsreglur um það eftirlit. Afgreiðir beiðnir sjúklinga um afrit af sjúkraskrá og um upplýsingar um það hverjir hafa aflað upplýsinga úr henni. Tekur afstöðu til beiðna um leiðréttingu. Tilkynnir embætti landlæknis um bann sjúklings við samtengingu og afturköllun þess.	3. gr., 2. mgr. 7. gr. og 1. og 4. mgr. 14. gr. laga nr. 55/2009, 3. mgr. 7. gr., 9. gr. og 19. gr. rg. 550/2015
Kerfisveita og hýsingaraðili (vinnsluaðilar)	Vinna einungis með sjúkraskráruppplýsingar samkvæmt skjalfestum fyrirmælum ábyrgðaraðila og á grundvelli vinnslusamnings. Hýsingaraðili skal vera viðurkenndur þjónustuaðili, þ.e. hafa vottað gæðakerfi skv. ISO/IEC 27001 eða sambærilegum stöðlum. Hvort hýsingaraðili	3. mgr. 10. gr. rg. 550/2015, 28. gr. og 2. mgr. 33. gr. reglugerðar (ESB)

Aðili	Helstu skyldur	Laga- og reglugerðarstoð
	telst viðurkenndur ræðst af vottuninni en ekki af skráningu eða samþykki embættis landlæknis. Tilkynna ábyrgðaraðila án ótilhlýðilegrar tafar þegar þau verða vör við öryggisbrest og aðstoða hann við að uppfylla skyldur sínar.	2016/679, sbr. lög nr. 90/2018
Embætti landlæknis	Hefur yfirumsjón með stafrænni sjúkraskrá á landsvísu og eftirlit með því að ákvæði reglugerðar nr. 550/2015 séu virt. Tekur við tilkynningum um rekstur heilbrigðisþjónustu og breytingar á honum, þ.m.t. breytt sjúkraskrárkerfi, og staðfestir hvort reksturinn uppfylli kröfur. Samþykkir ekki einstök sjúkraskrárkerfi og heldur ekki skrá yfir samþykkt kerfi eða kerfisveitur. Getur óskað eftir upplýsingum um öryggiskerfi. Staðfestir að skilyrði séu uppfyllt áður en samtenging sjúkraskrárkerfa er heimil. Samþykki landlæknis þarf til að eyða upplýsingum úr sjúkraskrá og synjun um leiðréttingu má kæra til hans. Tekur við sjúkraskrám þegar rekstri sjúkraskrárkerfis er hætt. Tekur við tilkynningum um alvarleg atvik.	4., 6., 8. og 20. gr. rg. 550/2015, 2. mgr. 7. gr. og 2. mgr. 10. gr. laga nr. 55/2009, 6. og 10. gr. laga nr. 41/2007, 6. og 12. gr. rg. 786/2007
Persónuvernd	Hefur eftirlit með öryggi og vinnslu persónuupplýsinga í sjúkraskrám. Tekur við tilkynningum um öryggisbresti við meðferð persónuupplýsinga.	3. mgr. 20. gr. rg. 550/2015, 33. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018
Stafræn heilsa	Gefur út leiðbeiningar og veitir ráðgjöf. Stafræn heilsa samþykkir ekki einstök sjúkraskrárkerfi og heldur ekki skrá yfir samþykkt kerfi. Mat á því hvort kerfi og hýsingaraðili uppfylli kröfurnar er á ábyrgð ábyrgðaraðila.	Á ekki við

Leiðbeiningunum fylgja fjögur ráðgefandi sniðmát sem auðvelda sjálfstætt starfandi heilbrigðisstarfsmönnum og smærri starfsstofum að koma sér upp öryggiskerfi: öryggishandbók (upplýsingaöryggisstefna, neyðaráætlun og verklagsreglur), áhættumat, árleg samantekt um innra eftirlit og frávikaskrá. Aðrar útfærslur sem uppfylla sömu kröfur eru jafngildar.

Nota má gervigreind við að fylla út og viðhalda þessum skjölum, t.d. til að semja texta, draga saman atvik eða kanna hvort eitthvað vanti. Ábyrgðaraðili ber þó áfram ábyrgð á efni skjalanna og þarf sjálfur að fara yfir það og meta, enda kemur gervigreind ekki í stað faglegrar dómgreindar. Skjölin geta sjálf geymt viðkvæmar upplýsingar, svo sem lýsingar

á atvikum, veikleika í öryggi starfsstofunnar eða upplýsingar um sjúklinga. Áður en slíkar upplýsingar eru settar inn í gervigreindarþjónustu þarf að ganga úr skugga um að þjónustan vinni þær sem vinnsluaðili samkvæmt vinnslusamningi, noti þær ekki til að þjálfa líkön og uppfylli skilyrði um flutning gagna úr landi, sbr. 28. gr. og V. kafla reglugerðar (ESB) 2016/679. Að öðrum kosti skal fjarlægja persónuupplýsingar áður. Aðgangsorð og önnur auðkenni eiga aldrei erindi inn í gervigreindarþjónustu.

Þessar meginreglur byggjast á gervigreindarstefnu Stafrænnar heilsu (1. útgáfa, ágúst 2026), einkum grunngildunum um að dómgreind og ábyrgð séu mennskir eiginleikar og um ábyrga meðferð gagna. Stefnan er leiðbeinandi gagnvart heilbrigðisstofnunum og starfsstofum, sem geta haft hana til hliðsjónar.

Upplýsingar frá kerfisveitu

Ábyrgðaraðili skal einungis nota kerfisveitu og hýsingaraðila sem veita nægilegar tryggingar fyrir viðeigandi öryggisráðstöfunum, sbr. 1. mgr. 28. gr. reglugerðar (ESB) 2016/679. Hann þarf þó ekki að afla upplýsinganna með sérstakri fyrirspurn. Hafi kerfisveita birt opinberlega, eða gert aðgengilegar viðskiptavinum sínum, þær upplýsingar og þau gögn sem gátlisti fyrir ábyrgðaraðila sjúkraskráa tilgreinir, svo sem vottorð, lista yfir undirvinnsluaðila, lýsingu á öryggisráðstöfunum og staðlaðan vinnslusamning, nægir ábyrgðaraðila að vísa til þeirra, enda:

- eigi upplýsingarnar við þá útgáfu og þá þjónustu sem hann notar og séu í gildi,
- vistar hann afrit af þeim eða skráir slóð og dagsetningu, þar sem birtar upplýsingar geta breyst,
- hefur vinnslusamningur verið gerður, en hann getur verið staðlaður samningur kerfisveitunnar,
- metur hann sjálfur hvort upplýsingarnar nægja og bregst við þar sem þær gera það ekki.

Ábyrgðin á valinu hvílir eftir sem áður á ábyrgðaraðila. Kerfisveita sem birtir þessar upplýsingar auðveldar viðskiptavinum sínum að uppfylla skyldur sínar og styttir þann tíma sem tekur að taka kerfið í notkun.

Eftirlit með aðgangi

Umsjónaraðili ber ábyrgð á reglubundnu eftirliti með því að aðgangur að sjúkraskrá sé í samræmi við reglur. Þegar sjúkraskrárkerfi hafa verið samtengd ber umsjónaraðili þeirrar stofnunar eða starfsstofu sem heilbrigðisstarfsmaður starfar hjá ábyrgð á eftirliti með aðgangi hans, einnig þegar hann flettir upp gögnum annarrar stofnunar í gegnum samtenginguna, sbr. 2. mgr. 9. gr. reglugerðar nr. 550/2015.

Reglugerðin gerir ráð fyrir eftirlitsnefnd, sem á illa við þegar heilbrigðisstarfsmaður starfar einn. Eðlilegt er að eftirlitið felist þá í reglulegri yfirferð hans sjálfs á aðgerðaskrá kerfisins og að skráð sé hvenær yfirferðin fór fram og hvað kom í ljós. Kerfið þarf því að gera honum kleift að kalla fram aðgerðaskrá á aðgengilegan hátt. Kafli 3.8 í sniðmáti að öryggishandbók lýsir slíku eftirliti.

Varðveisla og lok reksturs

Sjúkraskrár skal varðveita með öruggum hætti þannig að upplýsingar glatist ekki, og ber ábyrgðaraðili ábyrgð á varðveislunni, sbr. 8. og 9. gr. laga nr. 55/2009. Sé rekstri sjúkraskrárkerfis hætt, t.d. þegar starfsstofu er lokað, skal flytja sjúkraskrárnar til landlæknis, sbr. 2. mgr. 10. gr. laganna. Um skyldu til að afhenda sjúkraskrár opinberum skjalasöfnum fer samkvæmt lögum nr. 77/2014 um opinber skjalasöfn, sbr. 11. gr. laga nr. 55/2009.

Ábyrgðaraðili ætti því að tryggja í samningi við kerfisveitu að unnt sé að flytja öll gögn út á opnu og læsilegu sniði, bæði að beiðni og við lok samnings, og að kerfisveitan eyði gögnum að því loknu.

Kröfur sem leiða af regluverki um sjúkraskrár.

Öryggiskerfi og áhættumat

Krafa	**Laga- og reglugerðarstoð**
Skjalfest öryggiskerfi (upplýsingaöryggisstefna, öryggiskröfur, öryggisráðstafanir, áhættumat, neyðaráætlun, verklagsreglur, innra eftirlit, frávikaskráning), endurskoðað reglulega og afhent Embætti landlæknis þegar þess er óskað.	6. gr. rg. 550/2015, fyrirmæli 4–4.9
Áhættumat sem m.a. metur hættu á óheimilum aðgangi, breytingum eða tapi, í samræmi við viðkvæmni gagna, sem grundvöllur fyrir völdum ráðstöfunum.	fyrirmæli 4.4
Neyðaráætlun, skráning allra frávika, og mælanleg rekstrarmarkmið.	fyrirmæli 4.5, 4.8, 4.9

Aðgangsstýring og rekjanleiki

Krafa	**Laga- og reglugerðarstoð**
Aðgangur takmarkaður við það sem starfsfólk þarf vegna starfs síns (hlutverkatengd aðgangsstýring), hver starfsmaður undirritar trúnaðaryfirlýsingu.	1. mgr. 7. gr. rg. 550/2015, fyrirmæli 5

Umsjónaraðili getur skilgreint hlutverkastýrðan aðgang samkvæmt þrepaskiptingu fyrirmæla, tengt hlutverki og meðferðarsambandi.	14. gr. rg. 550/2015, fyrirmæli 5.1.2
Persónuleg, einkvæm auðkenni, aðgangi lokað við starfslok.	fyrirmæli 5.1.1
Skrá yfir veitingu og breytingar á aðgangi, svo hægt sé að gera úttekt á heimildum.	14. gr. rg. 550/2015
Allur aðgangur að skránni skráður sjálfvirkt í aðgerðaskrá og rekjanlegur til einstaklings, þ.e. hver skoðaði, skráði, breytti eða eyddi, og hvenær. Jafnframt skal tryggt að ekki sé hægt að breyta skráningum án þess að upprunaleg skráning sé varðveitt og það sama gildir um eyðingu, en eyðing er aðeins heimil með samþykki landlæknis.	3. mgr. 5. gr. og 2. mgr. 7. gr. laga nr. 55/2009, 2. mgr. 7. gr. og 15. gr. rg. 550/2015, fyrirmæli 5.1, 2.3

Hýsing og rekstur

Krafa	**Laga- og reglugerðarstoð**
Eigin hýsing: skriflegar verklagsreglur um rekstur (heimildir, raunlægur aðgangur, öryggisafrit, vörn gegn spilliforritum).	2. mgr. 10. gr. rg. 550/2015, fyrirmæli 3.1.1
Hýsing hjá þriðja aðila eingöngu hjá *viðurkenndum þjónustuaðila* (ISO/IEC 27001 eða sambærilegt), fullt samræmi við lög nr. 90/2018 (PVL).	3. mgr. 10. gr. rg. 550/2015, fyrirmæli 3.1.2
Hýsing hjá erlendum aðila eingöngu þar sem skilyrði fyrir flutningi persónuupplýsinga úr landi eru uppfyllt. Innan EES er hýsing heimil á sömu forsendum og innanlands. Utan EES er hún aðeins heimil á grundvelli V. kafla reglugerðar (ESB) 2016/679, t.d. ákvörðunar um fullnægjandi vernd eða staðlaðra samningsskilmála. Jafnframt ber að fylgja lögum og reglum viðkomandi lands.	4. mgr. 10. gr. rg. 550/2015, V. kafli reg. (ESB) 2016/679, sbr. lög nr. 90/2018
Vinnslusamningur í gildi áður en vinnsluaðili meðhöndlar gögnin.	28. gr. reg. (ESB) 2016/679, sbr. lög nr. 90/2018

Samvirkni, samtenging, réttindi og eftirlit

Krafa	Laga- og reglugerðarstoð
Klínískt yfirlit og áreiðanleg skráning samkvæmt kröfum um lágmarksskráningu, styður eftirlit með aðgangi, sérstaklega við samtengingu.	11. gr. og 12. gr. rg. 550/2015
Geta til að skila gögnum til heilbrigðisskráa landlæknis og að skráning sé til samræmis við fyrirmæli embættis landlæknis um lágmarksskráningu.	fyrirmæli 2.3, 2. og 3. mgr. 8. gr. a laga nr. 41/2007
Samtenging: hver tengd stofnun uppfyllir 6. og 7. gr. reglugerðar nr. 550/2015, og staðfesting landlæknis liggur fyrir áður en tengt er.	8. gr. rg. 550/2015, 18. gr. laga nr. 55/2009
Tilkynning um öryggisbrest án ótilhlýðilegrar tafar (72 klst.) til Persónuverndar. Sjá nánar kaflann Tilkynningar vegna öryggisbresta hér að neðan.	33. gr. reg. (ESB) 2016/679, sbr. lög nr. 90/2018
Réttindi sjúklinga í kerfinu: aðgangur að eigin skrá, leiðrétting, merking viðkvæmra upplýsinga, bann við samtengingu. Réttur sjúklings til að sjá eigin aðgangsskrá (e. access log)	7. gr., 1. og 4. mgr. 14. gr. og 19. gr. laga nr. 55/2009, 13., 18. og 19. gr. rg. 550/2015
Engin sjálfvirk klínísk ákvörðun með réttaráhrif án mannlegrar yfirferðar.	22. gr. reg. (ESB) 2016/679, sbr. lög nr. 90/2018
Innra eftirlit reglulega, skýrsla að minnsta kosti árlega, áætlun um úrbætur. Reglubundið eftirlit umsjónaraðila með því að aðgangur að sjúkraskrá sé í samræmi við reglur, samkvæmt skriflegum verklagsreglum.	3. mgr. 7. gr. og 9. gr. rg. 550/2015, fyrirmæli 4.7, 6–6.3

Kröfur sem má leiða af persónuverndarlögum (32. gr.)

32. gr. reglugerðar (ESB) 2016/679, sbr. 27. gr. laga nr. 90/2018, krefst viðeigandi öryggis í samræmi við áhættu. Heilsufarsupplýsingar eru viðkvæmar persónuupplýsingar. Viðmiðin hér að neðan eru almennt viðurkennd leið til að uppfylla þá skyldu fyrir sjúkraskrárkerfi.

Krafa	**Laga- og reglugerðarstoð**
Dulkóðun: í hvíld (AES-256 eða sambærilegt) og í flutningi (a.m.k. TLS 1.2, helst 1.3), þar á meðal umferð vegna samtengingar.	a-liður 1. mgr. 32. gr. (dulkóðun sérstaklega nefnd)
Dulkóðuð, prófuð öryggisafrit með óbreytanlegu/ótengdu (offline) afriti, endurheimt prófuð, RPO/RTO ákvarðað af áhættu.	b- og c-liður 1. mgr. 32. gr.
Eingöngu studdur hugbúnaður, engir íhlutir sem komnir eru á líftíma (e. end-of-life).	b- og d-liður 1. mgr. 32. gr.
Tímanlegar öryggisuppfærslur miðað við áhættu, eða skjalfest frávik samþykkt af ábyrgðaraðila sjúkraskráa.	b- og d-liður 1. mgr. 32. gr.
Stjórnun breytinga/stillinga, strangur aðskilnaður prófunar- og raunumhverfis, raunveruleg sjúkraskrárgögn eru ekki notuð í prófunar- eða þróunarumhverfi.	b-liður 1. mgr. 32. gr.
Aðgangur kerfisstjóra aðskiljanlegur frá aðgangi að klínískum gögnum, aðgerðir með ríkum heimildum (e. privileged actions) skráðar.	32. gr., fyrirmæli 5.1.2
Útflutningur eða flutningur eigin gagna á opnu sniði að beiðni og við lok samnings, engin innilokun (e. lock-in).	20. gr. reg. (ESB) 2016/679 þar sem við á, 8. gr. rg. 550/2015
Sjálfvirk útskráning (session timeout) ef notandi er óvirkur, MFA fyrir fjaraðgang, admin aðganga og aðgang sjúklinga (SMS/tölvupóstur OTP er ekki fullnægjandi fyrir heilsufarsupplýsingar).	32. gr.
Regluleg prófun á virkni ráðstafana, í samræmi við áhættu, áhættumat persónuverndar (MÁP) þar sem vinnslan hefur í för með sér mikla áhættu.	d-liður 1. mgr. og 2. mgr. 32. gr., 35. gr., sbr. 27. og 29. gr. laga nr. 90/2018

Tilkynning til embættis landlæknis

Ekki þarf að sækja sérstaklega um leyfi fyrir sjúkraskrárkerfi og embætti landlæknis samþykkir ekki einstök sjúkraskrárkerfi og heldur ekki skrá yfir samþykkt kerfi eða kerfisveitur. Sjúkraskrárkerfið er hins vegar hluti af búnaði starfseminnar og landlæknir hefur eftirlit með því að rekstraraðilar uppfylli skilyrði um sjúkraskrár og sjúkraskrárkerfi, sbr. 12. gr. reglugerðar nr. 786/2007 um eftirlit landlæknis með rekstri heilbrigðisþjónustu og faglegar lágmarkskröfur. Því þarf að tilkynna landlækni um sjúkraskrárkerfið, annaðhvort þegar rekstur hefst eða þegar skipt er um kerfi. Staðfesting landlæknis á tilkynningunni lýtur að rekstrinum og felur ekki í sér samþykki eða vottun á sjúkraskrárkerfinu sjálfu.

Tilkynningar eru sendar í gegnum þjónustugátt embættis landlæknis. Eyðublöðin og leiðbeiningar um þau er að finna á síðunni Rekstur heilbrigðisþjónustu á Ísland.is. Fyrirspurnir má senda á rekstur@landlaeknir.is.

Nýr rekstur

Sá sem hyggst hefja rekstur heilbrigðisþjónustu skal tilkynna það landlækni fyrir fram á eyðublaðinu „Tilkynning um rekstur heilbrigðisþjónustu“. Óheimilt er að hefja starfsemi fyrr en staðfesting landlæknis liggur fyrir, sbr. 2. og 3. mgr. 6. gr. laga nr. 41/2007 um landlækni og lýðheilsu. Tilgreinið sjúkraskrárkerfið í tilkynningunni.

Breytt sjúkraskrárkerfi

Rekstraraðili sem tekur upp stafrænt sjúkraskrárkerfi eða skiptir um sjúkraskrárkerfi tilkynnir það á eyðublaðinu „Breytt sjúkraskrárkerfi“, undir „Tilkynning um breytingar á rekstri heilbrigðisþjónustu“. Umtalsverðar breytingar á búnaði teljast meiri háttar breytingar, sem tilkynna skal landlækni og staðfesting hans þarf að liggja fyrir um, sbr. 2. og 3. mgr. 6. gr. laga nr. 41/2007 og 6. gr. reglugerðar nr. 786/2007. Tilkynnið breytinguna því áður en nýja kerfið er tekið í notkun.

Þeir sem færa sjúkraskrá á pappír í dag þurfa að taka upp stafrænt sjúkraskrárkerfi fyrir 1. desember 2026. Afgreiðslutími landlæknis er breytilegur og því er rétt að senda tilkynningu tímanlega.

Á sama stað eru eyðublöðin „Breyting á ábyrgðaraðila sjúkraskráa“ og „Breyting á umsjónaraðila sjúkraskráa“, sem nota skal þegar skipt er um aðila í þessum hlutverkum.

Upplýsingar sem gott er að hafa tilbúnar

- Heiti sjúkraskrárkerfis og útgáfa, og hver kerfisveitan er.
- Hver hýsingaraðilinn er, hvar gögnin eru hýst og hvort gögn eða aðgangur að þeim fari út fyrir EES.
- Hvort vinnslusamningur hafi verið gerður við kerfisveitu og hýsingaraðila.
- Hver er umsjónaraðili sjúkraskráa.

- Hvort kerfið verði samtengt öðrum sjúkraskrárkerfum.

Landlæknir getur óskað eftir frekari upplýsingum, m.a. um öryggiskerfi, sbr. 2. mgr. 6. gr. laga nr. 41/2007 og 2. mgr. 6. gr. reglugerðar nr. 550/2015. Útfylltur gátlisti fyrir ábyrgðaraðila sjúkraskráa, ásamt fylgigögnum, nýtist vel í því skyni.

Samtenging við önnur sjúkraskrárkerfi

Staðfesting landlæknis þarf að liggja fyrir áður en sjúkraskrárkerfi er samtengt öðrum sjúkraskrárkerfum, sbr. 18. gr. laga nr. 55/2009 og 8. gr. reglugerðar nr. 550/2015. Sú staðfesting er sjálfstæð og bætist við staðfestingu á rekstri. Hún lýtur að því að skilyrðin séu uppfyllt hjá þeim sem tengjast og felur ekki í sér samþykki á sjúkraskrárkerfinu sem slíku. Allir sem tengja á saman þurfa að uppfylla kröfur 6. og 7. gr. reglugerðarinnar um öryggiskerfi og aðgangsstýringu.

Umsjónaraðili tilkynnir embætti landlæknis um bann sjúklings við samtengingu og afturköllun þess, svo unnt sé að loka eða opna fyrir samtenginguna, sbr. 19. gr. reglugerðar nr. 550/2015.

Fjarheilbrigðisþjónusta og lok reksturs

Sá sem hyggst veita fjarheilbrigðisþjónustu sækir um það sérstaklega á sama stað. Sé rekstri hætt skal tilkynna landlækni um það, sbr. 2. mgr. 6. gr. laga nr. 41/2007, og flytja sjúkraskrár til landlæknis, sbr. 2. mgr. 10. gr. laga nr. 55/2009.

Tilkynningar vegna öryggisbresta

Ef atvik verður, t.d. ef sjúkraskráruplýsingar komast í hendur óviðkomandi, glatast, eru skoðaðar án heimildar eða kerfið verður óaðgengilegt, getur þurft að tilkynna það fleiri en einum aðila. Tilkynningarskyldurnar eru sjálfstæðar og tilkynning til eins aðila kemur ekki í stað tilkynningar til annars.

Í stuttu máli:

- Hafa persónuupplýsingar glatast, lekið, breyst eða verið skoðaðar án heimildar? Tilkynnið Persónuvernd innan 72 klukkustunda og sjúklingunum sjálfum ef mikil áhætta er fyrir þá.
- Hefur atvikið valdið eða hefði það getað valdið sjúklingi tjóni? Skráið það sem óvænt atvik og tilkynnið embætti landlæknis án tafar ef það er alvarlegt.
- Er starfsemin rekstraraðili nauðsynlegrar þjónustu? Tilkynnið netöryggissveitinni CERT-IS svo fljótt sem verða má.
- Hefur verið brotið gegn lögum um sjúkraskrár, t.d. með óheimilli uppflettingu? Tilkynnið embætti landlæknis.
- Leikur grunur á refsiverðri háttsemi, t.d. gagnagíslatöku (e. ransomware attack) eða fjárkúgun? Tilkynnið lögreglu.

Tilefni	Hver tilkynnir hverjum og hvenær	Laga- og reglugerðarstoð
Öryggisbrestur við meðferð persónuupplýsinga	Ábyrgðaraðili tilkynnir Persónuvernd án ótilhlýðilegrar tafar og eigi síðar en 72 klukkustundum eftir að hann varð var við brestinn, nema ólíklegt sé að hann leiði til áhættu fyrir réttindi og frelsi einstaklinga. Ábyrgðaraðili skráir alla öryggisbresti, einnig þá sem ekki eru tilkynntir.	33. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018
Öryggisbrestur sem líklegur er til að leiða af sér mikla áhættu fyrir sjúklinga	Ábyrgðaraðili tilkynnir hlutaðeigandi sjúklingum án ótilhlýðilegrar tafar, á skýru og einföldu máli.	34. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018
Öryggisbrestur hjá kerfisveitu eða hýsingaraðila	Vinnsluaðili tilkynnir ábyrgðaraðila án ótilhlýðilegrar tafar. Ábyrgðaraðili metur svo hvort tilkynna þurfi Persónuvernd og sjúklingum. Æskilegt er að kveða á um tímafrest og tengiliði í vinnslusamningi.	2. mgr. 33. gr. og 28. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018
Óvænt atvik sem valdið hefur eða hefði getað valdið sjúklingi tjóni, t.d. vegna rangra, glataðra eða óaðgengilegra upplýsinga í sjúkraskrá	Heilbrigðisstarfsmenn skrá öll óvænt atvik og heilbrigðisstofnanir og sjálfstætt starfandi heilbrigðisstarfsmenn senda landlækni yfirlit yfir þau. Alvarleg atvik eru tilkynnt landlækni án tafar og sjúklingi án ástæðulausrar tafar.	9. og 10. gr. laga nr. 41/2007
Alvarlegt atvik í net- og upplýsingakerfum rekstraraðila nauðsynlegrar þjónustu	Rekstraraðili tilkynnir netöryggissveitinni CERT-IS svo fljótt sem verða má. Embætti landlæknis er eftirlitsstjórnvald á sviði heilbrigðisþjónustu.	8. gr. og d-liður 11. gr. laga nr. 78/2019
Atvik í net- og upplýsingakerfum annarra veitenda heilbrigðisþjónustu	Aðrir en rekstraraðilar nauðsynlegrar þjónustu geta tilkynnt netöryggissveitinni CERT-IS um atvik sem hafa umtalsverð áhrif á starfsemi þeirra og fengið ráðgjöf um viðbrögð.	15. gr. laga nr. 78/2019

Tilefni	Hver tilkynnir hverjum og hvenær	Laga- og reglugerðarstoð
Grunur um óheimilar uppflettingar í sjúkraskrá	Umsjónaraðili kannar málið samkvæmt verklagsreglum um eftirlit með aðgangi. Reynist aðgangur hafa verið óheimill er um brot gegn lögum nr. 55/2009 að ræða, sem tilkynna skal landlækni. Jafnframt er um öryggisbrest að ræða og fer þá um tilkynningu til Persónuverndar og sjúklinga eins og að framan greinir.	6. mgr. 22. gr. laga nr. 55/2009, 9. gr. rg. 550/2015, 33. og 34. gr. reglugerðar (ESB) 2016/679
Önnur brot gegn lögum um sjúkraskrár	Ábyrgðaraðila og umsjónaraðila er skylt að tilkynna landlækni um brot gegn lögum nr. 55/2009.	6. mgr. 22. gr. laga nr. 55/2009

Ekki ætti að bíða með tilkynningu þar til öll atriði liggja fyrir. Tilkynna skal það sem vitað er og senda viðbótarupplýsingar eftir því sem þær berast, sbr. 4. mgr. 33. gr. reglugerðar (ESB) 2016/679.

Kröfur sem er skynsamlegt að innleiða

- Neyðaraðgangur (e. break-glass) með aðgerðaskráningu, skráningu á ástæðu þess að neyðaraðgangur er virkjaður og skyldubundinni yfirferð eftir á.
- Aðgangur byggður á meðferðarsambandi, ekki eingöngu hlutverki.
- Auðkenning milli kerfa (M2M), bundin skilríkjum að hætti FAPI, fyrir samtengingu og þjónustur Heklu.
- Formgerð samvirkni (EEHRxF) fyrir forgangsflokka gagna.