Sniðmát 4 Frávikaskrá

Sniðmát fyrir sjálfstætt starfandi heilbrigðisstarfsmann eða smærri starfsstofu

Starfsstofa: **[heiti]**
Ábyrgðaraðili: **[nafn]**
Skráin hófst: **[ÁÁÁÁ-MM-DD]**

Ábyrgðaraðili skráir öll frávik og öryggisatvik, sbr. 6. gr. reglugerðar nr. 550/2015 og kafla 4.8 í fyrirmælum landlæknis um öryggi og gæði sjúkraskráa. Skráin nýtist jafnframt sem skrá yfir alla öryggisbresti við meðferð persónuupplýsinga, einnig þá sem ekki eru tilkynntir Persónuvernd, sbr. 5. mgr. 33. gr. reglugerðar (ESB) 2016/679. Atvik sem valdið hafa eða hefðu getað valdið sjúklingi tjóni eru auk þess skráð sem óvænt atvik, sbr. 9. gr. laga nr. 41/2007.

Notkun og varðveisla. Frávikaskráin er lifandi skrá sem einungis er bætt við:

- Lokuðum færslum er ekki breytt. Komi í ljós að færsla er röng er leiðrétting skráð í lið 10 sem ný dagsett athugasemd, og upprunalegi textinn látinn standa.
- Geymið skrána þar sem breytingasaga er skráð sjálfvirkt, t.d. í skýjageymslu með útgáfusögu. Skrá sem einungis er geymd á eigin tölvu hefur enga slíka sögu.
- Þar sem frávik eru mörg má halda hverju atviki í sérstöku skjali, t.d. „Frávik 2026-003“, og vista það sem PDF þegar atvikinu er lokið. Yfirlitið í kafla A er þá haldið sér.
- Óski Persónuvernd eða embætti landlæknis eftir afriti er sent PDF-afrit af stöðu skrárinnar þann dag, aldrei skjalið sjálft til breytingar, og afrit af því sem sent var varðveitt.
- Skráið ekki nöfn eða kennitölur sjúklinga í frávikaskrána. Vísið til þeirra með innra númeri eða tilvísun í sjúkraskrá. Þannig má afhenda afrit af skránni án þess að afmá upplýsingar og skráin verður ekki að enn einu safni heilsufarsupplýsinga.

Gervigreind. Nota má gervigreind við að fylla út og viðhalda skjalinu, en ábyrgðaraðili fer sjálfur yfir efnið, metur það og ber ábyrgð á því. Setjið hvorki persónuupplýsingar sjúklinga né aðgangsorð inn í gervigreindarþjónustu nema hún vinni gögnin samkvæmt vinnslusamningi og noti þau ekki til að þjálfa líkön. Sjá nánar leiðbeiningar um stafræn sjúkraskrárkerfi.

A. Yfirlit

Nr.	Dagsetning	Alvarleiki	Stutt lýsing	Tilkynnt hverjum	Staða
001	[ÁÁÁÁ-MM-DD]			[enginn / Persónuvernd / landlæknir / sjúklingar / lögregla]	[opið / lokað]

Nr.	Dagsetning	Alvarleiki	Stutt lýsing	Tilkynnt hverjum	Staða
002					
003					

B. Skráning atviks (eitt blað fyrir hvert atvik)

Frávik nr. [###]

1. Skráning

- Skráð: [ÁÁÁÁ-MM-DD] af [nafn]

2. Tímalína

- Atvikið hófst (eða áætlað): [ÁÁÁÁ-MM-DD KK:MM]
- Uppgötvað: [ÁÁÁÁ-MM-DD KK:MM]
- Kerfisveita tilkynnti (ef atvikið varð hjá henni): [ÁÁÁÁ-MM-DD KK:MM]
- Fyrstu viðbrögð: [ÁÁÁÁ-MM-DD KK:MM]
- Lokið: [ÁÁÁÁ-MM-DD KK:MM eða opið]

72 klukkustunda frestur til að tilkynna Persónuvernd telst frá því að ábyrgðaraðili varð var við öryggisbrestinn.

3. Lýsing

[Hvað gerðist, hvernig það uppgötvaðist, hvaða gögn eða kerfi og hve margir sjúklingar eiga í hlut. Ekki nöfn eða kennitölur sjúklinga, heldur innra númer eða tilvísun í sjúkraskrá.]

4. Mat á áhrifum

Þáttur	Áhrif (engin / lítil / miðlungs / mikil) og skýring
Trúnaður: komust upplýsingar í hendur óviðkomandi?	
Heilleiki: breyttust eða skemmdust upplýsingar?	
Aðgengi: voru upplýsingar óaðgengilegar?	
Áhrif á sjúklinga og meðferð	

Þáttur	Áhrif (engin / lítil / miðlungs / mikil) og skýring
Heildaralvarleiki (sjá kafla C)	

5. Orsök

[t.d. tæknileg bilun, mistök, ásetningur, árás, atvik hjá kerfisveitu]

6. Viðbrögð

[Hvað var gert til að stöðva atvikið og takmarka áhrif. Vísið í neyðaráætlun öryggishandbókar ef við á.]

7. Tilkynningar (sjá kafla D)

Hverjum	Tilkynnt?	Dagsetning og tilvísun, eða rökstuðningur ef ekki
Persónuvernd	[já / nei]	
Sjúklingar sem í hlut eiga	[já / nei]	
Embætti landlæknis, brot gegn lögum um sjúkraskrár	[já / nei / á ekki við]	
Embætti landlæknis, alvarlegt atvik	[já / nei / á ekki við]	
Netöryggissveitin CERT-IS	[já / nei]	
Lögregla	[já / nei]	

8. Lærdómur

[Hvað þarf að breyta: öryggisráðstafanir, verklag, áhættumat, val á kerfisveitu.]

9. Staða

- ☐ Opið: [hvað er eftir]
- ☐ Lokað [ÁÁÁÁ-MM-DD] af [nafn]

10. Leiðréttingar

[ÁÁÁÁ-MM-DD, nafn: hvað var leiðrétt og hvers vegna. Upprunalegi textinn hér að ofan stendur óbreyttur.]

C. Hvað á að skrá og viðmið um alvarleika

Skrá skal öll frávik sem upp koma í rekstri kerfa sem vinna með sjúkraskráruppl ýsingar, sbr. kafla 4.8 í fyrirmælum landlæknis, þ.e. atvik sem snerta eða hefðu getað snert trúnað, heilleika eða aðgengi upplýsinganna. Venjuleg notkun er ekki frávik. Ekki þarf t.d. að skrá þegar notandi gleymir lykilorði sínu eða læsist úti eftir eigin innsláttarvillu. Læsist aðgangur hins vegar vegna innskráningartilrauna sem notandinn kannast ekki við er það frávik.

Alvarleiki ræður viðbrögðum og forgangi. Hann ræður ekki tilkynningarskyldu, sem fer eftir kafla D hver sem alvarleikinn er. Óheimil uppfletting í sjúkraskrá er t.d. alltaf brot gegn lögum nr. 55/2009 sem tilkynna skal landlækni, einnig þegar hún er metin lítil.

Alvarleiki	Lýsing	Dæmi
Lítill	Engar upplýsingar komust í hendur óviðkomandi og meðferð truflaðist ekki eða óverulega.	Stutt bilun hjá kerfisveitu sem leystist án gagnataps. Röng sjúkraskrá opnuð fyrir mistök og lokað strax án þess að upplýsingar væru skoðaðar.
Miðlungs	Óljóst hvort óviðkomandi sá upplýsingar, upplýsingar um fáa sjúklinga eiga í hlut, eða meðferð truflaðist tímabundið.	Dulkóðuð og læst fartölva tapast. Innskráningartilraunir sem notandi kannast ekki við. Upplýsingar um sjúkling sendar röngum viðtakanda. Kerfið óaðgengilegt hluta úr degi.
Mikill	Staðfestur eða líklegur aðgangur óviðkomandi að upplýsingum, ásetningur, upplýsingar um marga sjúklinga eiga í hlut, gögn glatast eða meðferð truflast verulega.	Gagnagíslataka. Ódulkóðuð tölva með sjúkraskráruppl ýsingum tapast. Óviðkomandi kemst inn á aðgang notanda. Starfsmaður flettir vísvitandi upp í sjúkraskrá einstaklings sem hann annast ekki, t.d. ættingja eða þekkts einstaklings.

D. Hverjum ber að tilkynna

Tilefni	Hverjum og hvenær	Stoð
Öryggisbrestur við meðferð persónuupplýsinga, nema ólíklegt sé að hann leiði til áhættu fyrir sjúklinga	Persónuvernd, án ótilhlýðilegrar tafar og innan 72 klukkustunda	33. gr. reglugerðar (ESB) 2016/679
Öryggisbrestur sem líklega leiðir til mikillar áhættu fyrir sjúklinga	Sjúklingunum sjálfum, án ótilhlýðilegrar tafar	34. gr. reglugerðar (ESB) 2016/679

Tilefni	Hverjum og hvenær	Stoð
Brot gegn lögum um sjúkraskrár, t.d. óheimil uppfletting	Embætti landlæknis	6. mgr. 22. gr. laga nr. 55/2009
Alvarlegt atvik í heilbrigðisþjónustu	Embætti landlæknis án tafar, og sjúklingi án ástæðulausrar tafar	10. gr. laga nr. 41/2007
Óvænt atvik sem valdið hefur eða hefði getað valdið sjúklingi tjóni	Skráð, og yfirlit sent landlækni reglulega	9. gr. laga nr. 41/2007
Alvarlegt atvik í tölvukerfum rekstraraðila nauðsynlegrar þjónustu	Netöryggissveitin CERT-IS svo fljótt sem verða má. Aðrir geta tilkynnt og fengið ráðgjöf.	8. og 15. gr. laga nr. 78/2019
Grunur um refsiverða háttsemi, t.d. gagnagíslataka eða fjárkúgun	Lögregla	

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

E. Varðveisla

Frávikaskráin er hluti af gögnum öryggiskerfisins og er varðveitt með þeim. Embætti landlæknis og Persónuvernd geta óskað eftir henni.

Sniðmát þetta fylgir leiðbeiningum Stafrænnar heilsu og embættis landlæknis um stafræn sjúkraskrárkerfi. Það er ráðgefandi. Aðrar útfærslur sem uppfylla sömu kröfur eru jafngildar.