Sniðmát 1: Öryggishandbók

Sniðmát fyrir sjálfstætt starfandi heilbrigðisstarfsmann eða smærri starfsstofu

Starfsstofa: **[heiti starfsstofu]**
Ábyrgðaraðili sjúkraskráa: **[nafn]**
Dagsetning: **[ÁÁÁÁ-MM-DD]**
Útgáfa: **1.0**
Næsta endurskoðun: **[dagsetning, að lágmarki árlega]**

Ábyrgðaraðili sjúkraskráa skal reka öryggiskerfi sem tryggir vernd sjúkraskrárupplýsinga, sbr. 6. gr. reglugerðar nr. 550/2015 um sjúkraskrár. Þessi handbók sameinar þrjá hluta öryggiskerfisins í eitt skjal: upplýsingaöryggisstefnu, neyðaráætlun og verklagsreglur, sbr. kafla 4.1, 4.5 og 4.6 í fyrirmælum landlæknis um öryggi og gæði sjúkraskráa. Áhættumat, innra eftirlit og frávikaskrá eru í sérstökum sniðmátum. Fyllið út hornklofana og strikið út það sem á ekki við.

Notkun og varðveisla. Vinnið í eigin afriti af sniðmátinu. Þegar ný útgáfa er tilbúin er útgáfunúmer hækkað, breytingin skráð í breytingasögu aftast, handbókin undirrituð og vistuð sem PDF með útgáfu og dagsetningu í heiti, t.d. „Öryggishandbók 1.1 2026-11-03.pdf“. Eldri útgáfur eru varðveittar, því embætti landlæknis getur spurt um stöðuna eins og hún var á fyrri tímum. Undirritun getur verið rafræn, eða nafn og dagsetning.

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.

Hluti 1: Upplýsingaöryggisstefna

1.1 Markmið og gildissvið

Handbókin lýsir því hvernig **[heiti starfsstofu]** verndar sjúkraskrárupplýsingar sjúklinga sinna. Hún gildir um allar sjúkraskrárupplýsingar starfsstofunnar, hvort sem þær eru á stafrænu formi eða á pappír, og um alla sem hafa aðgang að þeim.

1.2 Ábyrgð

Hlutverk	Nafn
Ábyrgðaraðili sjúkraskráa	[nafn eða heiti starfsstofu]
Umsjónaraðili sjúkraskráa	[nafn, eða sami og ábyrgðaraðili]

Hlutverk	Nafn
Tengiliður ef ábyrgðaraðili fellur frá eða verður óvinnufær	[nafn og sími]

Heilbrigðisstarfsmaður sem starfar einn á stofu er umsjónaraðili þeirra sjúkraskráa sem hann færir, sbr. 3. gr. laga nr. 55/2009 um sjúkraskrár.

1.3 Sjúkraskrárkerfi og hýsing

Atriði	Upplýsingar
Sjúkraskrárkerfi og útgáfa	[heiti]
Kerfisveita	[heiti fyrirtækis]
Hýsingaraðili	[heiti]
Hvar gögnin eru hýst	[land og gagnaver]
Vottun hýsingaraðila	[t.d. ISO/IEC 27001, gildir til ÁÁÁÁ-MM-DD, afrit í möppu]
Vinnslusamningur	[dagsetning og hvar hann er varðveittur]
Útfylltur gátlisti fyrir ábyrgðaraðila	[dagsetning]
Samtenging við önnur sjúkraskrárkerfi	[nei, eða við hvaða kerfi og dagsetning staðfestingar landlæknis]

1.4 Lykilþættir öryggis

Þáttur	Stefna
Aðgangur	Hver notandi hefur eigið auðkenni og fjölþætta sannvottun. Aðgangur takmarkast við það sem starfið krefst. Allur aðgangur er skráður í aðgerðaskrá kerfisins.
Rekstur	Kerfið er hýst hjá viðurkenndum þjónustuaðila. Afrit eru tekin reglulega og endurheimt prófuð árlega. Búnaður er uppfærður og varinn gegn spilliforritum.
Samskipti og þjónustuaðilar	Öll samskipti eru dulkóðuð. Vinnslusamningur er í gildi við alla sem vinna með gögnin fyrir starfsstofuna.
Starfsfólk	Allir sem hafa aðgang undirrita trúnaðaryfirlýsingu og kynna sér þessa handbók.

Þáttur	Stefna
Atvik	Öll frávik eru skráð í frávikaskrá og tilkynnt þeim sem tilkynna ber, sbr. hluta 2.

1.5 Endurskoðun

Handbókin er endurskoðuð að lágmarki árlega og þegar verulegar breytingar verða, t.d. þegar skipt er um sjúkraskrárkerfi eða hýsingaraðila, kerfið er samtengt öðru kerfi, ný virkni á borð við gervigreind er tekin í notkun eða eftir alvarlegt atvik.

Hluti 2: Neyðaráætlun

2.1 Tengiliðir

Hlutverk	Nafn	Sími	Netfang
Ábyrgðaraðili	[nafn]	[sími]	[netfang]
Umsjónaraðili (ef annar)	[nafn]	[sími]	[netfang]
Kerfisveita, þjónustuborð	[heiti]	[sími]	[netfang]
Tölvuþjónusta (ef önnur)	[heiti]	[sími]	[netfang]
Embætti landlæknis		510 1900	mottaka@landlaeknir.is
Persónuvernd		510 9600	postur@personuvernd.is
Netöryggissveitin CERT-IS			cert@cert.is
Lögregla		112	

2.2 Atvik og fyrstu viðbrögð

A. Sjúkraskrárkerfið er óaðgengilegt

Skráið tímann og hafið samband við kerfisveituna. Metið áhrif á bókaða sjúklinga og skráið nauðsynlegar færslur tímabundið á pappír, sbr. 3.5. Þegar kerfið kemst aftur í lag eru færslurnar færðar inn. Skráið atvikið í frávikaskrá. Hafi atvikið valdið sjúklingi tjóni, eða hefði getað gert það, er það jafnframt skráð sem óvænt atvik og tilkynnt landlækni án tafar ef það er alvarlegt.

B. Gögn hafa glatast, skemmst eða komist í hendur óviðkomandi

Hættið að nota kerfið ef gögn eru að skemmast og hafið samband við kerfisveituna um endurheimt. Skráið atvikið í frávikaskrá og metið án tafar hvort tilkynna þurfi

Persónuvernd (innan 72 klukkustunda), sjúklingum og embætti landlæknis, sbr. frávikaskrá, kafla D.

C. Gagnagíslataka (e. ransomware attack) eða annar spillihugbúnaður

Aftengið sýktan búnað frá neti en slökkvið ekki á honum. Greiðið ekki lausnargjald. Hafið samband við kerfisveituna og tilkynnið lögreglu. Metið tilkynningar til Persónuverndar og sjúklinga eins og í B. Ráðgjöf má fá hjá CERT-IS. Endurheimtið gögn úr afriti sem vitað er að er ósýkt.

D. Búnaður tapast eða er stolið

Lokið aðgangi búnaðarins að sjúkraskrárkerfinu, skiptið um lykilorð og læsið eða hreinsið búnaðinn með fjarstýringu ef unnt er. Tilkynnið lögreglu. Metið hvort sjúkraskráruppplýsingar voru á búnaðinum og hvort hann var dulkóðaður. Hafi ódulkóðaðar upplýsingar verið á honum er að jafnaði um öryggisbrest að ræða sem tilkynna þarf Persónuvernd.

E. Ábyrgðaraðili fellur frá eða verður óvinnufær

Tengiliðurinn í 1.2 gætir þess að enginn óviðkomandi fái aðgang að sjúkraskránum og hefur samband við embætti landlæknis. Sé rekstri hætt skal tilkynna landlækni um það, sbr. 2. mgr. 6. gr. laga nr. 41/2007, og sjúkraskrár fluttar til landlæknis, sbr. 2. mgr. 10. gr. laga nr. 55/2009. Tengiliðurinn þarf að vita hvar þessi handbók er og hvernig ná má sambandi við kerfisveituna.

2.3 Samfella meðferðar

Meðan á atviki stendur er samfella meðferðar tryggð með því að:

- skrá nauðsynlegar færslur tímabundið á pappír,
- hafa samband við sjúklinga sem eiga bókaðan tíma,
- vísa sjúklingum annað ef nauðsyn krefur.

2.4 Upplýsingar til sjúklinga

Hafi atvik áhrif á sjúkling er honum sagt hvað gerðist, hvort upplýsingar um hann hafi orðið fyrir áhrifum, hvað hefur verið gert og hvert hann getur leitað. Upplýsingarnar eru gefnar á skýru og einföldu máli.

Hluti 3: Verklagsreglur

3.1 Aðgangur veittur og honum lokað

Nýr starfsmaður: ákveðið hvaða aðgang starfið krefst, starfsmaður undirritar trúnaðaryfirlýsingu, sbr. 1. mgr. 7. gr. reglugerðar nr. 550/2015, og kynnir sér þessa handbók, notandi er stofnaður með fjölþættri sannvottun og aðgangsveitingin er skráð.

Starfslok: aðgangi að sjúkraskrárkerfinu og tengdum kerfum, svo sem tölvupósti, er lokað á starfslokadegi, búnaði er skilað og lokunin er skráð.

Aðgangsstig (þar sem fleiri en einn hafa aðgang):

- Heilbrigðisstarfsmaður: sjúkraskrár þeirra sjúklinga sem hann annast.
- Móttökuritari eða aðstoðarmaður: tímabókanir og almennar upplýsingar, ekki klínískar upplýsingar nema sérstök þörf sé fyrir hendi.
- Utanaðkomandi tölvuþjónusta: einungis það sem viðhald krefst, og vinnslusamningur er í gildi, sbr. 28. gr. reglugerðar (ESB) 2016/679.

3.2 Auðkenning

- Fjölþætt sannvottun er notuð við innskráningu í sjúkraskrárkerfið, helst með rafrænum skilríkjum. Kóðar sendir með smáskilaboðum (SMS) eða tölvupósti nægja ekki fyrir heilsufarsupplýsingar.
- Enginn deilir aðgangi með öðrum.
- Þar sem lykilorð eru notuð eru þau löng, einkvæm og geymd í lykilorðastjóra.
- Skipt er um lykilorð án tafar ef grunur er um að það hafi lekið.

3.3 Afritun og endurheimt

- Kerfisveitan tekur afrit samkvæmt vinnslusamningi. Ábyrgðaraðili veit hve oft afrit eru tekin og hvernig óskað er eftir endurheimt.
- Sé kerfið rekið á starfsstofunni sjálfri eru afrit tekin daglega, dulkóðuð, og eitt afrit hið minnsta geymt utan starfsstofunnar og ótengt kerfinu.
- Endurheimt er prófuð árlega og niðurstaðan skráð í samantekt um innra eftirlit.

3.4 Búnaður

- Tölvur og símar sem notuð eru til að nálgast sjúkraskrár eru með dulkóðaða diska, sjálfvirka skjálæsingu og nýjustu öryggisuppfærslur.
- Sjúkraskráruppl ýsingar eru ekki vistaðar á búnaðinum sjálfum nema kerfið geri ráð fyrir því.
- Sjúkraskráruppl ýsingar eru ekki sendar með almennum tölvupósti eða smáskilaboðum.
- Búnaði sem sjúkraskráruppl ýsingar hafa verið á er fargað með öruggri eyðingu eða eyðileggingu og förgunin skráð.

3.5 Pappír

- Tímabundnar færslur á pappír, t.d. þegar kerfið er óaðgengilegt, eru færðar inn í kerfið um leið og það kemst í lag. Pappírinn er skannaður inn eða varðveittur með öðrum pappírsgögnum sjúkraskrárinnar.

- Eldri pappírssjúkraskrár eru varðveittar í læstu rými. Ef þær eru færðar á stafrænt form má ekki farga frumritum nema með samþykki landlæknis, sbr. 2. mgr. 7. gr. laga nr. 55/2009.

3.6 Tilkynningar innan starfsstofunnar

- Hver sem verður var við atvik eða frávik tilkynnir ábyrgðaraðila það án tafar.
- Ábyrgðaraðili skráir það í frávikaskrá og metur tilkynningarskyldu samkvæmt kafla D í frávikaskránni.

3.7 Beiðnir sjúklinga

Umsjónaraðili afgreiðir beiðnir sjúklinga:

1. Beiðni er móttekin og auðkenni sjúklings, eða umboð umboðsmanns, staðfest.
2. **Afrit af sjúkraskrá:** afhent innan mánaðar, sbr. 14. gr. laga nr. 55/2009 og 12. og 15. gr. reglugerðar (ESB) 2016/679. Synjun má bera undir embætti landlæknis, sbr. 15. gr. a laga nr. 55/2009.
3. **Hverjir hafa aflað upplýsinga úr sjúkraskránni:** upplýsingar úr aðgerðaskrá kerfisins um hverjir, hvar, hvenær og í hvaða tilgangi, sbr. 4. mgr. 14. gr. laga nr. 55/2009.
4. **Leiðrétting:** athugasemd sjúklings er skráð. Bersýnilega rangar upplýsingar má leiðrétta með samþykki umsjónaraðila, sbr. 2. mgr. 7. gr. laga nr. 55/2009.
5. Beiðnin og afgreiðsla hennar eru skráðar.

3.8 Eftirlit með aðgangi

Umsjónaraðili fylgist reglulega með því að aðgangur að sjúkraskrá sé í samræmi við reglur, sbr. 3. mgr. 7. gr. og 9. gr. reglugerðar nr. 550/2015 og kafla 6.2 í fyrirmælum landlæknis.

- **Tíðni:** [t.d. ársfjórðungslega]
- **Það sem skoðað er í aðgerðaskrá:** innskráningar sem ekki er kannast við, aðgangur utan vinnutíma eða frá óvenjulegum stöðum, aðgangur starfsmanna kerfisveitu og, þar sem fleiri starfa, uppflettingar í sjúkraskrám sjúklinga sem viðkomandi annast ekki.
- **Skráning:** dagsetning yfirferðar, hvað var skoðað og hvað kom í ljós. Frávik eru skráð í frávikaskrá.

Eftirlitið á einnig við þegar heilbrigðisstarfsmaður starfar einn, því aðgerðaskráin sýnir ef aðrir hafa komist inn á aðgang hans eða starfsmenn kerfisveitu skoðað gögn.

Breytingasaga

Útgáfa	Dagsetning	Breytingar	Samþykkt af
1.0	[ÁÁÁÁ-MM-DD]	Fyrsta útgáfa	[nafn]

Undirskrift

Ábyrgðaraðili: _____

Dagsetning: _____

Sniðmát þetta fylgir leiðbeiningum Stafrænnar heilsu og embættis landlæknis um stafræn sjúkraskrárkerfi. Það er ráðgefandi. Aðrar útfærslur sem uppfylla sömu kröfur, þ.m.t. aðskilin skjöl fyrir hvern hluta, eru jafngildar.