Útgefið 3. nóvember 2026

Gátlisti fyrir ábyrgðaraðila sjúkraskráa: upplýsingar um sjúkraskrárkerfi og kerfisveitu

Ábyrgðaraðili sjúkraskráa velur sjúkraskrárkerfi og hýsingaraðila og ber ábyrgð á því að þau uppfylli kröfur laga nr. 55/2009 um sjúkraskrár, reglugerðar nr. 550/2015 um sjúkraskrár og laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga. Gátlistanum er ætlað að auðvelda honum að afla þeirra upplýsinga sem þarf til að leggja mat á kerfi og kerfisveitu , þ.e. fyrirtækið sem lætur sjúkraskrárkerfið í té og rekur það eftir atvikum, hvort sem um nýtt kerfi er að ræða eða kerfi sem þegar er í notkun.

Notkun:

- Kannið fyrst hvort kerfisveitan hafi birt svörin og gögnin opinberlega, t.d. á vef sínum, eða gert þau aðgengileg viðskiptavinum. Ef svo er nægir að vísa til þeirra í svardálkinum, með slóð og dagsetningu, og vista afrit. Gætið þess að þau eigi við þá útgáfu og þjónustu sem notuð er.
- Sendið kerfisveitunni annars spurningarnar og biðjið um þau gögn sem tilgreind eru. Svar án gagna er veikari trygging en svar sem stutt er gögnum.
- Þar sem svarið er nei eða óljóst þarf að meta hvaða áhættu það skapar, óska eftir úrbótum, gera aðrar ráðstafanir eða velja annað kerfi. Niðurstöðuna á að skrá í áhættumati öryggiskerfisins.
- Varðveitið útfylltan gátlista og fylgigögn með gögnum öryggiskerfisins. Embætti landlæknis getur óskað eftir upplýsingum um öryggiskerfið, sbr. 2. mgr. 6. gr. reglugerðar nr. 550/2015.
- Endurtakið upplýsingaöflunina þegar samningur er endurnýjaður, þegar kerfisveitan skiptir um hýsingaraðila eða undirvinnsluaðila og að minnsta kosti árlega fyrir atriði sem breytast, svo sem vottorð og niðurstöður öryggisprófana.

Gátlistinn er hjálpartæki og ekki tæmandi. Stafræn heilsa samþykkir ekki einstök sjúkraskrárkerfi og heldur ekki skrá yfir samþykkt kerfi. Matið er á ábyrgð ábyrgðaraðila.

Heiti kerfis og útgáfa	
Kerfisveita	
Hýsingaraðili	
Útfyllt af	
Dagsetning	
Næsta endurskoðun	

1. Kerfið og kerfisveitan

Stoð: 28. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018, 3. gr. og 20. gr. laga nr. 55/2009

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
1	Hver er kerfisveitan (lögaðili, heimilisfesti) og hver er tengiliður hennar vegna öryggismála og persónuverndar?	Upplýsingar um lögaðila, nafn og netfang tengiliðar	
2	Hvaða undirvinnsluaðila notar kerfisveitan, t.d. vegna hýsingar, afritunar, notendaþjónustu, tölvupósts og SMS-sendinga, og hvar starfa þeir?	Listi yfir undirvinnsluaðila með staðsetningu og hlutverki	
3	Fær hver viðskiptavinur aðskilinn gagnagrunn eða aðskilið tilvik kerfisins, eða eru gögn fleiri veitenda heilbrigðisþjónustu í sama gagnagrunni? Geta notendur eins veitanda séð gögn annars?	Lýsing á því hvernig gögn viðskiptavina eru aðskilin	
4	Er kerfið eða hluti þess CE-merkt lækningatæki, eða notar það gervigreind eða sjálfvirka ákvarðanatöku sem hefur áhrif á meðferð? Eru gögn ábyrgðaraðila notuð til að þjálfa eða bæta gervigreindarlíkön?	Yfirlýsing kerfisveitu, CE-samræmisyfirlýsing ef við á	

2. Hýsing og staðsetning gagna

Stoð: 3. og 4. mgr. 10. gr. reglugerðar nr. 550/2015, V. kafli reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
5	Hvar eru gögnin hýst (land, gagnaver, hýsingaraðili)? Hvar eru öryggisafrit geymd?	Lýsing á hýsingu og staðsetningu öryggisafrita	
6	Hefur hýsingaraðilinn vottun skv. ISO/IEC 27001 eða sambærilegum staðli? Nær gildissvið vottunarinnar til þeirrar þjónustu sem hýsir kerfið og er vottunin í gildi?	Gilt vottorð með gildissviði (e. scope) og gildistíma	
7	Hefur kerfisveitan sjálf slíka vottun, eða óháða úttekt á borð við SOC 2 Type II?	Vottorð eða úttektarskýrsla	

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
8	Er unnt að nálgast gögnin frá landi utan EES, t.d. vegna notendaþjónustu eða viðhalds? Ef svo er, á hvaða grundvelli skv. V. kafla reglugerðar (ESB) 2016/679?	Ákvörðun um fullnægjandi vernd eða staðlaðir samningsskilmálar og mat á áhrifum flutnings	
9	Lúta kerfisveitan eða hýsingaraðilinn lögsögu ríkis utan EES sem getur krafist aðgangs að gögnunum? Hvernig er brugðist við slíkri kröfu?	Yfirlýsing kerfisveitu	

3. Samningar og lok viðskipta

Stoð: 28. gr. reglugerðar (ESB) 2016/679, sbr. lög nr. 90/2018, 8.–11. gr. laga nr. 55/2009

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
10	Liggur fyrir vinnslusamningur sem kveður m.a. á um skjalfest fyrirmæli, trúnað, öryggisráðstafanir, samþykki fyrir undirvinnsluaðilum, aðstoð við réttindi sjúklinga, tilkynningu öryggisbresta, úttektarheimild og skil og eyðingu gagna við lok samnings?	Vinnslusamningur, undirritaður áður en vinnsla hefst	
11	Hver eru þjónustustig (uppitími, viðbragðstími við bilunum, þjónustutími)?	Þjónustustigssamningur	
12	Er unnt að flytja öll gögn út, þ.m.t. aðgerðaskrá, á opnu og læsilegu sniði, bæði að beiðni og við lok samnings? Hvað kostar það og hve langan tíma tekur það?	Lýsing á útflutningi og sýnishorn af sniði	
13	Hvernig staðfestir kerfisveitan að gögnum hafi verið eytt að samningi loknum?	Lýsing á eyðingarferli og staðfestingu	
14	Hvað verður um gögnin ef kerfisveitan hættir rekstri eða verður gjaldþrota?	Lýsing á ráðstöfunum, t.d. vörslusamningi	

4. Aðgangsstýring og auðkenning

Stoð: 7. og 14. gr. reglugerðar nr. 550/2015, fyrirmæli landlæknis um öryggi og gæði sjúkraskráa, kafli 5, 32. gr. reglugerðar (ESB) 2016/679

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
15	Fær hver notandi persónulegt og einkvæmt auðkenni? Er unnt að koma í veg fyrir samnýtt notendanöfn?	Lýsing á notendaumsjón	
16	Hvaða auðkenningu styður kerfið? Er fjölþætt sannvottun (e. multi-factor authentication) krafist við fjaraðgang og fyrir kerfisstjóra? Styður kerfið rafræn skilríki?	Lýsing á auðkenningarleiðum	
17	Getur umsjónaraðili skilgreint hlutverk og takmarkað aðgang við það sem starfsmaður þarf vegna starfs síns? Er unnt að tengja aðgang við meðferðarsamband?	Lýsing á aðgangsstýringu, skjámyndir	
18	Er haldin skrá yfir veitingu og breytingar á aðgangi, svo unnt sé að gera úttekt á heimildum?	Sýnishorn af skránni	
19	Er notandi skráður sjálfkrafa út eftir óvirkni? Er auðvelt að loka aðgangi við starfslok?	Lýsing á stillingum	
20	Er til neyðaraðgangur (e. break-glass)? Er ástæða skráð og aðgangurinn yfirfarinn eftir á?	Lýsing á neyðaraðgangi	
21	Hafa starfsmenn kerfisveitunnar aðgang að sjúkraskráruppl ýsingum? Ef svo er, hverjir, í hvaða tilgangi, hvernig er aðgangurinn samþykktur og er hann skráður í aðgerðaskrá?	Lýsing á aðgangi kerfisveitunnar	

5. Aðgerðaskrá og rekjanleiki

Stoð: 3. mgr. 5. gr. og 4. mgr. 14. gr. laga nr. 55/2009, 2. mgr. 7. gr., 9. gr. og 15. gr. reglugerðar nr. 550/2015

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
22	Skráir kerfið sjálfvirkt allan aðgang að sjúkraskrá, þ.m.t. skoðun, auk skráningar, breytinga og eyðingar, með notanda, tíma og sjúklingi?	Lýsing á aðgerðaskrá og sýnishorn	
23	Er upprunaleg færsla varðveitt þegar færslu er breytt? Er eyðing aðeins möguleg með sérstöku ferli?	Lýsing á meðferð breytinga og eyðingar	

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
24	Hve lengi er aðgerðaskrá varðveitt? Getur einhver, þ.m.t. kerfisstjórar, breytt henni eða eytt?	Lýsing á varðveislu og vernd aðgerðaskrár	
25	Getur umsjónaraðili sjálfur kallað fram aðgerðaskrá fyrir tiltekinn sjúkling eða starfsmann, til að sinna eftirliti með aðgangi og svara beiðni sjúklings um það hverjir hafi aflað upplýsinga um hann?	Sýnikennsla eða skjámyndir	

6. Öryggisráðstafanir

Stoð: 32. gr. reglugerðar (ESB) 2016/679, sbr. 27. gr. laga nr. 90/2018

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
26	Eru gögn dulkóðuð í hvíld og í flutningi, þ.m.t. öryggisafrit og samskipti við önnur kerfi? Með hvaða aðferðum?	Lýsing á dulkóðun	
27	Hve oft eru tekin öryggisafrit, eru þau dulkóðuð og er til afrit sem ekki er unnt að breyta eða eyða úr kerfinu sjálfu? Hvenær var endurheimt síðast prófuð? Hve miklum gögnum má tapa og hve lengi má kerfið liggja niðri?	Lýsing á afritun og niðurstaða síðustu endurheimtarprófunar	
28	Innan hvaða tímamarka eru öryggisuppfærslur settar upp? Eru allir íhlutir studdir af framleiðanda, þannig að enginn sé kominn á endalok líftíma (e. end-of-life)?	Lýsing á uppfærsluferli	
29	Er prófunar- og þróunarumhverfi aðskilið frá raunumhverfi? Eru raunveruleg sjúkraskrárgögn notuð í prófunum?	Yfirlýsing kerfisveitu	
30	Hefur óháður aðili gert öryggisprófun eða innbrotsprófun (e. penetration test) á kerfinu síðustu 12 mánuði? Hafa alvarlegar niðurstöður verið lagfærðar?	Samantekt niðurstaðna og staða úrbóta	
31	Er aðgangur kerfisstjóra aðskilinn frá aðgangi að klínískum gögnum og eru aðgerðir með ríkum heimildum skráðar?	Lýsing á kerfisstjóraaðgangi	

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
32	Hvernig vaktar kerfisveitan kerfið til að greina innbrot, misnotkun eða óeðlilega notkun?	Lýsing á vöktun	

7. Atvik, tilkynningar og samfella

Stoð: 2. mgr. 33. gr. reglugerðar (ESB) 2016/679, fyrirmæli landlæknis um öryggi og gæði sjúkraskráa, kafli 4.5

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
33	Innan hvaða tíma og hvernig tilkynnir kerfisveitan ábyrgðaraðila um öryggisbrest? Er tengiliður tiltækur allan sólarhringinn?	Ákvæði vinnslusamnings, verklag og tengiliðir	
34	Hefur kerfisveitan orðið fyrir öryggisbresti síðustu þrjú ár sem varðaði gögn viðskiptavina? Hvað var gert til úrbóta?	Yfirlýsing kerfisveitu	
35	Hvað gerist ef kerfið verður óaðgengilegt? Hvernig getur ábyrgðaraðili haldið áfram að veita þjónustu, nálgast nauðsynlegar upplýsingar og fært sjúkraskrá á meðan?	Neyðar- og samfelluáætlun kerfisveitunnar	

8. Virkni og réttindi sjúklinga

Stoð: 7., 14. og 19. gr. laga nr. 55/2009, 11.–13., 18. og 19. gr. reglugerðar nr. 550/2015, 8. gr. a laga nr. 41/2007

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
36	Er unnt að skrá sérstaklega viðkvæmar upplýsingar og takmarka aðgang að þeim að ósk sjúklings?	Lýsing á virkni	
37	Er unnt að afhenda sjúklingi afrit af sjúkraskrá hans og skrá athugasemd hans ef hann telur upplýsingar rangar?	Lýsing á virkni	
38	Styður kerfið lágmarksskráningu samkvæmt fyrirmælum landlæknis og skil gagna til heilbrigðisskráa landlæknis?	Lýsing á virkni og skilum	

Nr.	Spurning til kerfisveitu	Gögn sem óska ætti eftir	Svar og athugasemdir
39	Styður kerfið samtengingu við önnur sjúkraskrárkerfi, og er unnt að virða bann sjúklings við samtengingu?	Lýsing á samtengingu	

Gögn sem ábyrgðaraðili ætti að hafa undir höndum

- Undirritaðan vinnslusamning og lista yfir undirvinnsluaðila.
- Gilt vottorð hýsingaraðila skv. ISO/IEC 27001 eða sambærilegum staðli, með gildissviði.
- Grundvöll flutnings ef gögn eða aðgangur fer út fyrir EES.
- Lýsingu kerfisveitunnar á öryggisráðstöfunum og samantekt nýjustu öryggisprófunar.
- Þjónustustigssamning og lýsingu á útflutningi gagna við lok samnings.
- Útfylltan gátlista og mat ábyrgðaraðila á þeim atriðum þar sem svör voru ófullnægjandi.

Til kerfisveitna

Kerfisveitur geta auðveldað viðskiptavinum sínum valið og stytt þann tíma sem tekur að taka kerfið í notkun með því að birta svör við spurningum gátlistans ásamt fylgigögnum, halda þeim uppfærðum og tilgreina hvenær þau voru síðast uppfærð. Gögn sem ekki henta til opinberrar birtingar, svo sem ítarlegar niðurstöður öryggisprófana, má gera aðgengileg viðskiptavinum eða birta sem samantekt. Ekki er gerð krafa um tiltekið form.