REGLUR

um öryggi við vinnslu persónuupplýsinga í söfnum heilbrigðisupplýsinga.

I. KAFLI
Efni, gildissvið o.fl.

1. gr.
Efni og gildissvið.

Reglur þessar lúta að því hvernig tryggja skuli öryggi við vinnslu persónuupplýsinga í söfnum heilbrigðisupplýsinga skv. lögum um lífsýnasöfn og söfn heilbrigðisupplýsinga nr. 110/2000, sbr. lög nr. 45/2014. Að öðru leyti en kemur fram í reglunum skal til leiðbeiningar hafa hliðsjón af eftirfarandi alþjóðlegum stöðlum:

a) ÍST EN ISO/IEC 27001:2017 – Upplýsingatækni – Öryggisaðferðir – Stjórnunarkerfi um upplýsingaöryggi – Kröfur.
b) ÍST EN ISO/IEC 27002:2017 – Upplýsingatækni – Öryggisaðferðir – Starfsvenjur fyrir upplýsingaöryggi.

2. gr.
Grunnreglur.

Í öryggi við vinnslu persónuupplýsinga í söfnum heilbrigðisupplýsinga felst að tryggja varðveislu, eðlilega leynd þeirra, lögmætan aðgang að þeim, gæði og áreiðanleika. Nánar tiltekið felst öryggið í:

a) Að tryggja að persónuupplýsingar séu ekki aðgengilegar þeim sem ekki skulu hafa aðgang að þeim.
b) Að tryggja vandaða meðferð persónuupplýsinga og að þær glatist ekki á ólögmætan hátt.
c) Að tryggja þeim sem þurfa og mega hafa aðgang að persónuupplýsingum slíkan aðgang þegar lögmæt ástæða er til.

II. KAFLI
Öryggisreglur.

3. gr.
Öryggisstefna.

Stjórn safns heilbrigðisupplýsinga skal gefa út og viðhalda öryggisstefnu fyrir safnið. Við það má hafa hliðsjón af 5. kafla staðalsins ÍST EN ISO/IEC 27002:2017 Upplýsingatækni – Öryggisaðferðir – Starfsvenjur fyrir upplýsingaöryggi.

4. gr.
Rekstur safns heilbrigðisupplýsinga.

Rekstur safns heilbrigðisupplýsinga felst í því að veita viðtöku persónuupplýsingum úr vísindarannsóknum á heilbrigðissviði, varðveita þær og veita lögmætan aðgang að þeim. Þeim einum er heimill slíkur rekstur sem hefur leyfi ráðherra skv. 4. gr. laga nr. 110/2000, í reglum þessum nefndur leyfishafi. Honum er skylt að halda rekstri safns heilbrigðisupplýsinga aðskildum frá annarri starfsemi sem hann hefur með höndum. Með aðskildum rekstri er m.a. átt við að tryggja skuli aðskilnað milli annars vegar þeirra er leyfa notkun á gögnum safnsins og hafa eftirlit með henni og hins vegar þeirra sem vilja fá að nota upplýsingarnar eða hafa þar hagsmuna að gæta. Mæla má fyrir um það í samningum safnstjórnar og þeirra sem leggja gögn í safnið á grundvelli 7. gr. b í lögum nr. 110/2000 hvernig þeir hagsmunir skuli tryggðir innan ramma laganna.

5. gr.
Lýsing á stjórnun öryggismála.

Leyfishafi skal setja fram skriflega lýsingu á stjórnun öryggismála safns heilbrigðisupplýsinga. Þar skulu a.m.k. öll eftirtalin atriði koma fram:

1. Með hvaða hætti rekstri safns heilbrigðisupplýsinga sé haldið aðskildum frá annarri starfsemi leyfishafa, sbr. 4. gr.
2. Með hvaða hætti þess sé gætt að upplýsingar séu án persónuauðkenna, í samræmi við 1. mgr. 8. gr. laga nr. 110/2000, og hvernig persónuauðkenni séu varðveitt. Einnig hvaða starfsmaður beri ábyrgð á vörslu persónuauðkenna og öryggi gagna sem gera kleift að tengja þau við upplýsingar í einstökum rannsóknum. Þar skal einnig tilgreint hver það sé sem beri ábyrgð á dulkóðun auðkenna í samræmi við 6. málsl. 4. mgr. 7. gr. sömu laga.
3. Hvernig staðið hafi verið að mati á áhrifum á persónuvernd í samræmi við 35. gr. reglugerðar (ESB) 2016/679, sbr. 29. gr. laga nr. 90/2018.
4. Hvernig innbyggð og sjálfgefin persónuvernd sé tryggð, sbr. 25. gr. reglugerðar (ESB) 2016/679, sbr. 24. gr. laga nr. 90/2018.
5. Hvernig staðið hafi verið að mati á áhættu í samræmi við 2. mgr. 32. gr. reglugerðar (ESB) 2016/679, sbr. 1. mgr. 17. gr. laga nr. 90/2018.
6. Hvaða öryggisráðstafanir séu viðhafðar í samræmi við 1. mgr. 32. gr. reglugerðar (ESB) 2016/679, sbr. síðastgreint ákvæði laga nr. 90/2018.
7. Hvar upplýsingar séu varðveittar og hver beri daglega ábyrgð á öryggi þeirra.
8. Hvaða leiðbeiningar starfsmenn hafi fengið um viðbrögð við öryggisógnum og öryggisbrestum.
9. Hvernig öryggisráðstafanir einstakra deilda safnsins hafi verið samræmdar, ef safnið er deildarskipt.
10. Hvernig staðið sé að aðgangsstjórnun, þ. á m. í ljósi samninga við ábyrgðarmenn vísindarannsókna á grundvelli 7. gr. b í lögum nr. 110/2000.
11. Hvernig tryggt sé að heilbrigðisupplýsingar úr einstökum vísindarannsóknum séu varðveittar sérgreindar frá upplýsingum úr öðrum rannsóknum.
12. Hvernig tryggt sé að upplýsingar úr einstökum rannsóknum séu ekki tengdar saman á meðan þær séu varðveittar í safninu.

Leyfishafi skal tilkynna Persónuvernd með sannanlegum hætti hver fari með fyrirsvar gagnvart stofnuninni um alla þætti er varða meðferð persónuupplýsinga á vegum safnsins, þ. á m. um að uppfyllt séu skilyrði 3. mgr. 9. gr. laga nr. 110/2000.

Leyfishafi skal að öðru leyti uppfylla þau skilyrði sem Persónuvernd ákveður á hverjum tíma.

Persónuvernd skal hafa aðgang að skjölum samkvæmt reglum þessum hvenær sem eftir er leitað.

6. gr.

Ytra öryggi og aðrar öryggisráðstafanir.

Viðhafa skal ráðstafanir til að hindra og takmarka tjón af völdum óheimils aðgangs að safni heilbrigðisupplýsinga. Í því skyni skal þess gætt að hýsa upplýsingar á fyrirfram skilgreindum svæðum er lúta skýrri aðgangsstjórnun. Þá skal haga ytra umhverfi safnins þannig að það hindri óheimilan aðgang, skemmdir og truflanir.

Viðhafa skal sérstakar ráðstafanir til að draga úr hættu á truflunum, að rekstur rofni eða upplýsingar og persónuvernd skaðist. Í því skyni skal viðhafa vinnuferli er tryggi órofinn rekstur safns heilbrigðisupplýsinga og dragi úr hættu á truflunum vegna óhappa eða annarra atvika sem ógna öryggi þess, t.d. af völdum náttúruhamfara, slysa, bilunar í búnaði eða skemmdarverka. Skal annars vegar viðhafa fyrirbyggjandi ráðstafanir og hins vegar ráðstafanir er geri kleift að endurræsa hrunin kerfi og eftir atvikum að endurheimta upplýsingar sem kunna að hafa glatast eða skemmst.

7. gr.

Öryggisráðstafanir varðandi starfsmannamál.

Beita skal öryggisráðstöfunum varðandi starfsmannamál í því skyni að draga úr hættu á tjóni af völdum mannlegra mistaka, þjófnaðar, svika eða annarrar misnotkunar.

Taka skal afstöðu til ábyrgðar á öryggismálum við gerð ráðningarsamninga og í annars konar samningum sem varða starfsemina og/eða starfsmanninn. Skal ábyrgð skipt eftir því sem við á til að draga úr hættu á vanrækslu eða vísvitandi misnotkun upplýsinga eða upplýsingakerfa. Fylgjast skal reglulega með því að unnið sé í samræmi við umsamda ábyrgð viðkomandi starfsmanns. Taka skal

afstöðu til þess að hvaða marki kanna skuli hvort tiltekin atriði í ferli umsækjanda um starf gefi tilefni til að óttast að ráðning hans raski öryggi safnsins. Allir starfsmenn, og aðrir sem aðgang hafa að upplýsingum í safni heilbrigðisupplýsinga, skulu bundnir trúnaði og undirrita sérstakar trúnaðaryfirlýsingar því til staðfestingar.

Veita skal starfsmönnum leiðbeiningar um viðbrögð við öryggisógnum og öryggisbrestum.

8. gr.

Aðgangsstjórnun.

Viðhafa skal aðgangsstjórnun í því skyni að stjórna aðgangi að upplýsingum til að tryggja öryggi þeirra, sbr. 2. gr. reglna þessara. Skal þar höfð hliðsjón af öryggiskröfum og þeim ákvörðunum sem leyfishafi, stjórn safns heilbrigðisupplýsinga eða annar þar til bær aðili hefur tekið um miðlun upplýsinga og aðgang að þeim.

9. gr.

Ákvarðanir um öryggismál.

Skilgreina skal, rökstyðja og skjalfesta allar þær ákvarðanir sem teknar eru um öryggismál, þ. á m. um viðbrögð ef öryggisráðstafanir bregðast. Leyfishafi skal staðfesta ákvarðanirnar með formlegum hætti.

III. KAFLI

Önnur atriði.

10. gr.

Endurskoðun og innra eftirlit.

Endurskoða skal reglulega, og eigi sjaldnar en árlega, þær aðgerðir sem gripið er til á grundvelli reglna þessara. Slík endurskoðun skal fara fram með reglulegu millibili og hvenær sem þurfa þykir, s.s. við verulegar breytingar á rekstraraðstæðum og umhverfi.

Viðhafa skal stöðugt innra eftirlit til að prófa og meta skilvirkni tæknilegra og skipulagslegra ráðstafana til að tryggja öryggi vinnslu persónuupplýsinga í safni heilbrigðisupplýsinga, sbr. d-lið 1. mgr. 32. gr. reglugerðar (ESB) 2016/679, sbr. 1. mgr. 17. gr. laga nr. 90/2018. Einnig skal innra eftirlit lúta að því að sannreyna að unnið sé í samræmi við reglur þessar, gildandi lög og reglugerð um lífsýnasöfn og söfn heilbrigðisupplýsinga, löggjöf um vernd persónuupplýsinga og aðrar réttarreglur sem kunna að eiga við um rekstur safna heilbrigðisupplýsinga.

11. gr.

Gildistími o.fl.

Reglur þessar eru settar samkvæmt 9. tölul. 1. mgr. 5. gr. laga nr. 110/2000 um lífsýnasöfn og söfn heilbrigðisupplýsinga og öðlast þegar gildi.

Persónuvernd, 1. júlí 2019.

Björg Thorarensen formaður.

Helga Þórisdóttir.

B-deild – Útgáfud.: 15. júlí 2019