

Upplýsingaöryggisstefna HVE

1. Tilgangur

Þessi upplýsingaöryggisstefna lýsir áherslu framkvæmdastjórnar HVE á upplýsingavernd og örugga meðferð upplýsinga eigna hennar. Tryggja þarf öryggi upplýsinga á HVE fyrir öllum ógnum, innri og ytri, af ásetningi eða af slysi. Fagleg vinnubrögð eru lykillinn að árangri og til marks um það er þessi upplýsingaöryggisstefna sett. Innleiðing og framkvæmd stefnunnar er mikilvæg til að fullvissa starfsmenn HVE og notendur þjónustu hennar um heilindi og rétt vinnubrögð í rekstri hennar. Stjórn HVE hefur samþykkt þessa stefnu og styður við framkvæmd hennar.

2. Umfang

Upplýsingaöryggisstefnan tekur til umgengni og vistunar allra upplýsinga í vörslu HVE á rafrænu formi, prentuðu, handskrifuðu, í formi lífsýna eða í mæltu máli. Hér er átt við:

- a. Upplýsingar frá notendum þjónustu HVE, t.d. heilsufarsupplýsingar, lífsýni eða samningar við birgja sem HVE hefur í vörslu sinni.
- b. Upplýsingar sem eru eign HVE og bundnar eignarrétti eða háðar hugverkarétti.
- c. Persónulegar upplýsingar sem tengjast starfsmönnum HVE.

Upplýsingaöryggisstefnan tekur jafnframt til húsnæðis og búnaðar þar sem upplýsingar eru meðhöndlaðar eða vistaðar sem og starfsmanna og samningsbundinna aðila sem hafa aðgang að upplýsingum.

3. Markmið

Markmið HVE með upplýsingaöryggisstefnunni eru að:

- a. Upplýsingar séu réttar og aðgengilegar þeim sem aðgangsrétt hafa þegar þörf er á.
- b. Leynd upplýsinga og trúnaði sé viðhaldið. Trúnaðarupplýsingar séu óaðgengilegar óviðkomandi og varðar gegn skemmdum, eyðingu eða uppljóstrun til aðila sem hafa ekki aðgangsrétt hvort sem er af ásetningi eða vangá.
- c. Upplýsingar sem fara um net komist til réttis viðtakanda óskaddaðar, á réttum tíma og þess sé gætt að þær fari ekki til annarra.
- d. Að áhætta vegna vinnslu (meðferðar) og varðveislu upplýsinga sé innan skilgreindra áhættumarka.
- e. Alltaf séu til áreiðanleg og örugglega varðveitt afrit af gögnum og hugbúnaðarkerfum.
- f. Fylgt sé öllum lögum, reglugerðum og reglum sem heilbrigðisstofnanir lúta. Þess skal sérstaklega gætt að vanda úrlausnir mála þar sem árekstrar kunna að verða milli ákvæða í mismunandi lögum og reglugerðum, t.d. upplýsingalögum og lögum um persónuvernd.
- g. Fylgja öllum samningum sem HVE er aðili að og varða upplýsingaöryggi.
- h. Áætlanir séu gerðar um samfelldan rekstur, þeim sé viðhaldið og þær prófaðar.
- i. Frávik, brot eða grunur um veikleika í upplýsingaöryggi séu tilkynnt og rannsökuð.

4. Leiðir að markmiði

Leiðir HVE að ofangreindum markmiðum eru að:

- a. Halda skrá yfir upplýsingaeygnir og flokka þær eftir mikilvægi leyndar, réttleika og tiltækileika.
- b. Greina reglulega með formlegu áhættumati verðmæti upplýsingaeygna, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.
- c. Stjórna áhættu innan skilgreindra marka með því að hanna, innleiða og starfrækja formlegt stjórnkerfi upplýsingaöryggis samkvæmt ÍST ISO/IEC 27001 (hét áður ISO/IEC 17799).
- d. Gera rafræna skipulagshandbók með verklagsreglum og verkferlum vegna meðferðar upplýsinga og viðhalda henni.
- e. Allir starfsmenn HVE fái þjálfun og fræðslu varðandi upplýsingaöryggi og ábyrgð þeirra hvað varðar upplýsingaöryggi.
- f. Allir starfsmenn fylgi gildandi lögum og reglum.

5. Ábyrgð

Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnu skiptist á eftirfarandi hátt:

- a. Stjórn HVE ber ábyrgð á þessari upplýsingaöryggisstefnu og endurskoðar (rýnir) hana reglulega.
- b. Öryggisstjóri HVE ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
- c. Allir starfsmenn HVE bera ábyrgð á að þeim vinnuferlum sem eiga að tryggja að framkvæmd upplýsingaöryggisstefnunnar sé fylgt. Samstarfsaðilar og verktakar bera ábyrgð á að fylgt sé samningsbundnum vinnuferlum sem eiga að tryggja framkvæmd stefnunnar.
- d. Öllum starfsmönnum HVE ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi. Þeir sem ógna upplýsingaöryggi HVE, notenda þjónustu hennar eða viðskiptavina af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir.

6. Endurskoðun

Þessi stefna skal endurskoðuð árlega og oftár ef þörf krefur til að tryggja að hún samrýmist markmiðum HVE.

7. Samþykki

Samþykkt af framkvæmdastjórn HVE 19. maí 2010

Viðaukar

Aðrar stefnur/ reglur sem styðja upplýsingaöryggisstefnuna

a) Skráning í rafræna sjúkraskrá - Stefna HVE ([skjal 14.02.01](#))

b) Reglur um aðgangsheimildir starfsmanna að upplýsingum í rafrænum sjúkraskrárkerfum á HVE ([skjal 14.03.02](#)).

Tilvísanir í lög og reglur

1. Yfirlit yfir lög, reglur og reglugerðir sem gilda um starfsemi HVE ([sjá fylgiskjal nr. 1](#))

2. Skilgreiningar hugtaka ([sjá fylgiskjal nr. 2](#))

Heimildir

[Öryggisstefna landlæknis](#), 20. desember 2004

Öryggisstefna íslenska heilbrigðisnetsins, 2. nóvember 2005

[Öryggisstefna STIKA](#), 24. febrúar 2010

Ábyrgðaraðili: Þórir Bergmundsson framkvæmdastjóri lækninga á HVE
Gefið út 12. júlí 2010