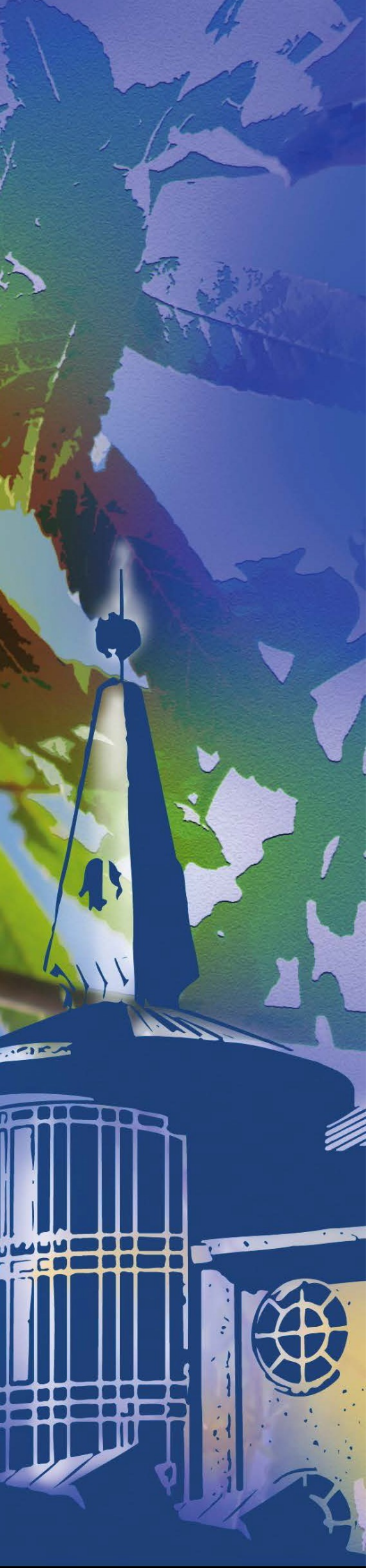


Fyrirmæli landlæknis um upplýsingaöryggi við veitingu fjarheilbrigðisþjónustu (fjarheilbrigðiskerfi)

Janúar 2019

Embætti landlæknis
Directorate of Health

Fyrirmæli landlæknis um upplýsingaöryggi við veitingu fjarheilbrigðisþjónustu (fjarheilbrigðiskerfi)

Útgefandi:
Embætti landlæknis
Barónsstíg 47
101 Reykjavík
www.landlaeknir.is

Reykjavík 2019

1 Inngangur

Fyrirmæli landlæknis um upplýsingaöryggi við veitingu fjarheilbrigðisþjónustu eru sett með vísan til 1. mgr. 5. gr. laga um landlækni og lýðheilsu nr. 41/2007 en þar segir „Landlæknir getur gefið heilbrigðisstofnunum og heilbrigðisstarfsmönnum almenn fagleg fyrirmæli um vinnulag, aðgerðir og viðbrögð af ýmsu tagi sem þeim er skylt að fylgja. Fyrirmælin skulu lögð fyrir ráðherra til staðfestingar og birt."

Við gerð þessara fyrirmæla var leitað umsagnar Persónuverndar sem hefur eftirlit með lögum og reglum um vinnslu persónuupplýsinga. Einnig hefur verið haft samráð við sérfræðinga í upplýsingaöryggi.

2 Gildissvið fyrirmælanna

Fyrirmælin gilda um heilbrigðisstofnanir og heilbrigðisstarfsmenn sem veita fjarheilbrigðisþjónustu. Með fjarheilbrigðisþjónustu er átt við heilbrigðisþjónustu þar sem samskiptatækni er notuð til að veita þjónustuna og sjúklingur og þeir heilbrigðisstarfsmenn sem koma að meðferðinni eru ekki staddir á sama stað.

Fyrirmælunum er ætlað að tryggja:

- að almenningur eigi kost á öruggri fjarheilbrigðisþjónustu.
- örugg fjarsamskipti heilbrigðisstarfsmanna á milli heilbrigðisstofnana og landshluta.

Fyrirmælin gilda í þeim tilvikum þegar lausnir sem ætlaðar eru til fjarheilbrigðisþjónustu eru notaðar á eftirfarandi hátt:

- Fjarheilbrigðisþjónusta er veitt sjúklingi sem staðsettur er utan heilbrigðisstofnana/starfsstöðva. Dæmi um slíka þjónustu eru talmeinafræðingar sem veita þjónustu frá starfsstöð sinni til barna í leikskólum og/eða grunnskólum og sálfræðingar sem veita þjónustu frá starfsstöð sinni til sjúklinga sem eru staðsettir heima hjá sér.
- Fjarsamskipti sjúklings og heilbrigðisstarfsmanns þar sem sjúklingur er staðsettur á einni heilbrigðisstofnun/starfsstöð og heilbrigðisstarfsmaður á annarri heilbrigðisstofnun/starfsstöð. Dæmi um slíka þjónustu er ráðgjöf heimilislæknis sem staðsettur er á einni heilsugæslustöð við hjúkrunarfræðing sem tekur á móti sjúklingi á annarri heilsugæslustöð, hvort sem heilsugæslustöðvarnar tilheyra sömu heilbrigðisstofnun eða ekki. Annað dæmi er ef sjúklingur mætir á heilsugæslustöð til meðferðar hjá sérfræðingi sem staddur er á annarri heilbrigðisstofnun.
- Fjarsamskipti eru milli heilbrigðisstarfsmanna á ólíkum heilbrigðisstofnunum/starfsstöðvum. Dæmi um slíka þjónustu er ráðgjöf sem sérfræðilæknir á spítala veitir heimilislækni.
- Fjarsamskipti eru veitt þar sem heilbrigðisstarfsmaður starfar fyrir heilbrigðisstofnun/starfsstöð en er staðsettur utan stofnunar/starfsstöðvar (sjá nánar

öryggisreglur í kafla 4.4). Dæmi um slíkt er sálfræðingur sem starfar á meðferðarmiðstöð en er jafnframt með starfsstöð annars staðar.

3 Almennt um rekstur í heilbrigðisþjónustu

Samkvæmt 4. gr. laga um heilbrigðisþjónustu nr. 40/2007 er heilbrigðisþjónusta skilgreind sem: „Hvers kyns heilsugæsla, lækningar, hjúkrun, almenn og sérhæfð sjúkrahúsþjónusta, sjúkraflutningar, hjálpartækjaþjónusta og þjónusta heilbrigðisstarfsmanna innan og utan heilbrigðisstofnana sem veitt er í því skyni að efla heilbrigði, fyrirbyggja, greina eða meðhöndla sjúkdóma og endurhæfa sjúklinga.“

Lögum samkvæmt hefur landlæknir eftirlit með rekstri heilbrigðisþjónustu. Í reglugerð nr. 786/2007, um eftirlit landlæknis með rekstri heilbrigðisþjónustu og faglegar lágmarkskröfur er kveðið á um þá þætti sem snerta faglegar lágmarkskröfur til rekstrar heilbrigðisþjónustu en þeir eru einkum húsnæði og aðstaða, tæki, búnaður og mönnun. Enn fremur er litið til skilyrða sem lúta að fyrirmælum landlæknis, m.a. um færslu sjúkraskráa, sjúkraskrárkerfi, lágmarksskráningu heilbrigðisupplýsinga vegna færslu heilbrigðisskráa, atvikaskráningu vegna óvæntra atvika, viðbúnað vegna bráðatilvika og um sótt- og sýkingavarnir við veitingu heilbrigðisþjónustu. Loks er kveðið á um hvernig rekstraraðilum ber að uppfylla önnur skilyrði í heilbrigðislöggjöf og reglugerðum sem öðrum aðilum hefur samkvæmt lögum verið falið eftirlit með á einstökum sviðum.

Samkvæmt 6. gr. laga um landlækni og lýðheilsu nr. 41/2007 þurfa þeir sem hyggjast hefja rekstur heilbrigðisþjónustu, þ.m.t. ríki og sveitarfélög, að tilkynna fyrirhugaðan rekstur til landlæknis. Landlæknir staðfestir hvort fyrirhugaður rekstur heilbrigðisþjónustu uppfyllir faglegar kröfur og önnur skilyrði í heilbrigðislöggjöf. Óheimilt er að hefja starfsemi á sviði heilbrigðisþjónustu nema staðfesting landlæknis liggi fyrir.

Allir sem vinna með persónuupplýsingar við veitingu heilbrigðisþjónustu þurfa einnig að uppfylla kröfur laga um persónuvernd og vinnslu persónuupplýsinga, nr. 90/2018, (persónuverndarlaga) sem og laga og reglugerða um sjúkraskrár.

3.1 Sjúkraskrá

Kröfur um skráningu í sjúkraskrá við veitingu fjarheilbrigðisþjónustu og um meðferð sjúkraskrárupplýsinga eru þær sömu og við aðra heilbrigðisþjónustu. Við tilkynningu um rekstur óskar landlæknir eftir lýsingu á því rafræna sjúkraskrárkerfi sem er í notkun. Rafræna sjúkraskrárkerfið þarf að uppfylla lög um sjúkraskrár nr. 55/2009, reglugerð um sjúkraskrár nr. 550/2015 og auk þess fyrirmæli landlæknis um öryggi og gæði sjúkraskráa. Kröfur til rafrænnar sjúkraskrár eiga einnig við um kerfi til fjarheilbrigðisþjónustu sé það útbúið á þann hátt að þar skuli skrá sjúkraskrárupplýsingar.

3.2 Persónuverndarlöggjöf

Þau kerfi sem nýtt eru við veitingu fjarheilbrigðisþjónustu þurfa að uppfylla kröfur persónuverndarlaga og þar með kröfur reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa

miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin).

Allar upplýsingar um heilsuhagi einstaklinga teljast viðkvæmar persónuupplýsingar skv. b. lið 3. tölul. 3. gr. persónuverndarlaga og því ber ábyrgðaraðila þeirra að verja gögnin sérstaklega og fylgja reglum Persónuverndar um öryggi persónuupplýsinga.

Gerð er krafa um innbyggða og sjálfgefna persónuvernd við þróun á tæknilegum lausnum sem nota á til fjarheilbrigðisþjónustu skv. 24. gr. persónuverndarlaga, sbr. 25. gr. almennu persónuverndarreglugerðarinnar. Samkvæmt lögunum og reglugerðinni getur komið til lokunar eða jafnvel sekta geti ábyrgðaraðili ekki tryggt öryggi við vinnslu persónuupplýsinga. Þá kveður 27. gr. laganna á um skyldu ábyrgðaraðila til að innleiða tæknilegar og skipulagslegar öryggisráðstafanir til að vernda upplýsingarnar í samræmi við þá áhættu sem vinnslunni fylgir, sbr. 32. gr. reglugerðarinnar. Þar sem heilbrigðisupplýsingar teljast viðkvæmar persónuupplýsingar leiðir það af sér að öryggisráðstafanir sem krafist er við vinnslu þeirra skulu vera miklar. Þannig ber að grípa til allra nauðsynlegra ráðstafana, t.d. dulkóðunar.

Þá er gerð sú krafa að vinnsla persónuupplýsinga sem felur í sér mikla áhættu fyrir réttindi og frelsi einstaklinga, þ.m.t. notkun rafrænna samskipta í heilbrigðisþjónustu, þurfi að undirgangast mat á áhrifum á persónuvernd, skv. 29. gr. persónuverndarlaga, sbr. 35. gr. reglugerðarinnar. Ef mat á áhrifum gefur til kynna að vinnslan hefði mikla áhættu í för með sér, nema ábyrgðaraðilinn grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðilinn hafa samráð við Persónuvernd áður en að vinnsla hefst.

3.3 Staðfesting á rekstri fjarheilbrigðisþjónustu

Heilbrigðisstofnun þarf að tilkynna fyrirhugaðan rekstur heilbrigðisþjónustu eða breytingu á rekstri í heilbrigðisþjónustu á þar til gerðum eyðublöðum til Embættis landlæknis, samkvæmt lögum um landlækni og lýðheilsu nr. 41/2007, sbr. 6. gr. (sjá kafla 3: Almennt um rekstur í heilbrigðisþjónustu í fyrirmælum þessum). Starfsmaður embættisins leiðbeinir viðkomandi í tilkynningarferlinu og landlæknir staðfestir síðan hvort fyrirhugaður rekstur heilbrigðisþjónustu uppfyllir faglegar kröfur og önnur skilyrði í heilbrigðislöggjöf. Það er ekki hlutverk landlæknis að staðfesta öryggi tæknilegra lausna sem nýttar eru við veitingu heilbrigðisþjónustunnar. Með tilkynningu um rekstur þar sem fjarheilbrigðisþjónusta verður nýtt skal því fylgja staðfesting á öryggisúttekt þess kerfis sem verður notað.

Fyrirmæli þessi ná ekki til sjúkraskráa og þarf að halda fjarheilbrigðiskerfi og sjúkraskrárkerfi aðskildu í tilkynningunni (sjá lið 4 og 5 á eyðublaði).

Aðeins heilbrigðisstarfsmenn sem hafa löggilt starfsleyfi frá landlækni samkvæmt lögum um heilbrigðisstarfsmenn nr. 34/2012 og starfa innan heilbrigðisstofnunar/starfsstöðvar sem hefur staðfestingu frá landlækni um leyfi til reksturs geta veitt fjarheilbrigðisþjónustu.

Um réttindi og skyldur heilbrigðisstarfsmanna og annarra starfsmanna í heilbrigðisþjónustu gilda lög um heilbrigðisstarfsmenn nr. 34/2012, lög um réttindi sjúklinga nr. 74/1997, lög um

landlækni og lýðheilsu nr. 41/2007 , lög um sjúkraskrár nr. 55/2009 og önnur lög eftir því sem við á.

Við staðfestingu landlæknis á rekstri þar sem veitt verður fjarheilbrigðisþjónusta staðfestir landlæknir að skráður ábyrgðaraðili rekstursins (heilbrigðisstofnunar/starfsstöðvar) uppfylli kröfur sem getið er um í þessum kafla auk þess að tryggja hámarkskröfur um verndun upplýsinga við veitingu fjarheilbrigðisþjónustu skv. 4. kafla fyrirmælanna. Heilbrigðisstarfsmaður sem ætlar að sinna fjarheilbrigðisþjónustu utan tilkynnts aðseturs þarf að starfa hjá heilbrigðisstofnun/starfsstöð þar sem kröfur um framangreinda þætti eru uppfylltar.

4 Verndun upplýsinga við veitingu fjarheilbrigðisþjónustu

Tilkynningu um rekstur fjarheilbrigðisþjónustu þarf að fylgja lýsing á tæknilegri lausn. Við þróun og val lausna fyrir fjarheilbrigðisþjónustu er mikilvægt að hafa í huga að þær uppfylli kröfur um öryggi og tryggi viðunandi vernd upplýsinga.

Landlæknir gerir eftirfarandi kröfur til tæknilegra lausna sem nota á í fjarheilbrigðisþjónustu:

1. Heilbrigðisstarfsmaður skal vera staðsettur á þeirri starfsstöð sem kemur fram í tilkynningu um rekstur eða tengdur á öruggan hátt því kerfi sem notað er við veitingu fjarheilbrigðisþjónustu á viðkomandi heilbrigðisstofnun/starfsstöð.
2. Við uppbyggingu tæknilegra lausna sem nota á í fjarheilbrigðisþjónustu er nauðsynlegt að tryggja gagnaöryggi á sem bestan hátt. Æskilegt er að lausnin byggi á svokallaðri þriggja laga hönnun þar sem vefþjónn, vinnsluþjónn og gagnagrunnsþjónn eru á aðskildum vélbúnaði á sitt hvoru netsvæðinu sem eldveggir skilja að. Engin gögn má geyma á vefþjóninum heldur skal geyma öll gögn á sérstökum gagnagrunnsþjóni og skulu persónugreinanlegar upplýsingar vera dulkóðaðar í gagnagrunninum að lágmarki með 256 bita ES dulritun eða sambærilegri vernd.
3. Öll samskipti milli sjúklings og heilbrigðisstarfsmanns skulu vera dulkóðuð, svo sem með HTTPS með SSL/TLS dulkóðunarsamskiptastöðlunum, og tryggt að enginn utanaðkomandi hafi aðgang að samskiptunum meðan á þeim stendur og þau séu örugglega ekki geymd af þriðja aðila.
4. Þar sem lausnir sem nota á til fjarheilbrigðisþjónustu munu oft geyma viðkvæmar upplýsingar um einstaklinga þurfa þær að standast strangari kröfur um öryggi og aðgangsstýringar en almennt gerist. Sérstaklega þarf því að huga að öryggi persónuupplýsinga við uppsetningu og forritun slíkra samskiptalausna, sbr. 11.-13. gr. persónuverndarlaga. Í því felst m.a. að gera þarf áhættumat og skilgreina öryggisráðstafanir áður en slík samskiptalausn er tekin í notkun.
5. Óheimilt er að flytja heilbrigðisupplýsingar út fyrir Evrópska efnahagssvæðið nema að uppfylltum skilyrðum V. kafla almennu persónuverndarreglugerðarinnar. Ef upplýsingar eru vistaðar erlendis gerir það enn ríkari kröfu á að áhætta sé metin og gripið sé til allra nauðsynlegra ráðstafana til að lágmarka hana.

6. Gerð er krafa um innbyggða og sjálfgefna persónuvernd við þróun á tæknilegum lausnum sem nota á til fjarheilbrigðisþjónustu samkvæmt persónuverndarlögum og almennu persónuverndarreglugerðinni. Samkvæmt þeirri reglugerð getur komið til lokunar eða jafnvel sekta geti ábyrgðaraðili ekki tryggt öryggi þeirra. Þá er gerð sú krafa að öll vinnsla persónuupplýsinga, þ.m.t. notkun rafrænna samskipta í heilbrigðisþjónustu sem fela í sér mikla áhættu fyrir réttindi og frelsi einstaklinga, þurfi að undirgangast mat á áhrifum á persónuvernd. Ef mat á áhrifum gefur til kynna að vinnslan hefði mikla áhættu í för með sér, nema ábyrgðaraðilinn grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðilinn hafa samráð við Persónuvernd áður en vinnsla hefst.
7. Nota skal Heklu-heilbrigðisnet til allra sendinga á heilbrigðisupplýsingum á milli stofnana/starfsstöðva þar sem það er mögulegt, svo sem þegar um samskipti milli heilbrigðisstarfsmanna á mismunandi heilbrigðisstofnunum er að ræða eða ef sjúklingur sem fær heilbrigðisþjónustu er á annarri stofnun en heilbrigðisstarfsmaður sem veita skal þjónustuna.

4.1 Fjarheilbrigðisþjónusta veitt sjúklingi sem staðsettur er utan heilbrigðisstofnunar/starfsstöðvar

Þegar sjúklingur sem fær fjarheilbrigðisþjónustu er staðsettur heima hjá sér eða á öðrum stað utan heilbrigðisstofnunar/starfsstöðvar er sérstaklega mikilvægt að tryggja öryggi þeirrar lausnar sem notuð er, bæði er varðar fullvissu við auðkenningu sjúklingsins en einnig varðandi öryggi þeirra upplýsinga sem snúa að meðferðinni.

Dæmi um slíka þjónustu eru talmeinafræðingar sem veita þjónustu frá starfsstöð sinni til barna í skólum og sálfræðingar sem veita þjónustu frá starfsstöð sinni til sjúklings sem er staðsettur heima hjá sér.

Öryggi - sjúklingar

Ef sjúklingur sækir fjarheilbrigðisþjónustu sína á vefsvæði gerir landlæknir kröfu um að fullgild rafræn skilríki, af fullvissustigi LoA4 skv. ISO/IEC 29115:2013, séu notuð við innskráningu bæði við upphaf meðferðar og í hvert sinn sem meðferð fer fram. Sjúklingur fær aðgang að fjarmeðferð í gegnum læst heimasvæði.

1. Sé sjúklingur ólögráða skal foreldri/forráðamaður stofna til þjónustunnar með eigin rafrænum skilríkjum fyrir hönd sjúklingsins. Foreldri/forráðamanni er heimilt að veita öðrum einstaklingi skriflegt umboð til að skrá sig inn í þjónustuna fyrir hönd sjúklingsins, t.d. ef barn fær þjónustu þegar það er statt í skóla eða leikskóla. Þegar þjónustan er veitt skal foreldri/forráðamaður eða annar sá sem umboð hefur skrá sig inn með rafrænum skilríkjum og auðkenna svo sjúklinginn gagnvart heilbrigðistarfsmanninum sem veitir þjónustuna.
2. Ef sjúklingur gleymir að skrá sig út skal hann sjálfvirkt skráður út í síðasta lagi eftir 15 mínútur ef engin virkni er á tengingu hans.

3. Ef sjúklingurinn fær skilaboð með smáskilaboðum eða tölvupósti vegna fjarmeðferðar mega þau ekki innihalda viðkvæmar persónuupplýsingar, svo sem upplýsingar sem geta gefið til kynna hvaða meðferð skal veitt.
4. Landlæknir gerir kröfu um að sjúklingur samþykki við upphaf meðferðar notkunarskilmála er varða þjónustuna. Þeir skilmálar þurfa að fylgja tilkynningu um rekstur til landlæknis. Notkunarskilmálar skulu innihalda allar nauðsynlegar upplýsingar sem sjúklingur þarf að kunna skil á til að geta treyst því að samskipti séu örugg og staðfest upplýst samþykki fyrir vinnslunni. Sjúklingur á að geta valið um að fá sent afrit af upplýstu samþykki í tölvupósti.
5. Veita skal sjúklingi fræðslu um almennt netöryggi svo sem að nýta sér ekki opin þráðlaus net á almenningsstöðum, hlaða ekki niður upplýsingum eða vista samtöl á búnað sem er aðgengilegur öðrum. Ef krafist er sérstaks hugbúnaðar er mikilvægt að sjúklingur hljóti fræðslu um örugga notkun hans.

Öryggi - heilbrigðisstarfsmenn

1. Landlæknir gerir kröfu um að heilbrigðisstarfsmenn skrái sig inn og hafi aðgang að upplýsingum um sjúklinga sína á lokuðu heimasvæði þar sem meðferð fer fram.
2. Ef kerfið er opið út á Internetið, þ.e. keyrir á vefþjóni sem aðgengilegur er öllum sem tengjast Internetinu, gerir landlæknir kröfu um innskráningu heilbrigðisstarfsmanna með fullgildum rafrænum skilríkjum af fullvissustigi LoA4 skv. ISO/IEC 29115:2013. Ef kerfið er eingöngu aðgengilegt heilbrigðisstarfsmönnum á öruggu lokuðu neti rekstraraðila er hefðbundin innskráning með notendanafni og lykilorði nægjanleg. Um meðferð og styrk lykilorða skal farið eftir 9. kafla ISO/IEC 27002:2013 um aðgangsstjórnun.
3. Landlæknir gerir kröfur um að óháður viðurkenndur sérfræðingur í netöryggi geri öryggisúttekt á kerfinu áður en það er tekið til notkunar. Staðfesting óháðs aðila á öryggisúttekt skal fylgja tilkynningu um rekstur í heilbrigðisþjónustu.

4.2 Fjarheilbrigðisþjónusta þar sem samskipti sjúklings og heilbrigðisstarfsmanns eiga sér stað á milli heilbrigðisstofnana/starfsstöðva

Dæmi um slíka þjónustu er ráðgjöf heimilislæknis sem staðsettur er á einni heilsugæslustöð við hjúkrunarfræðing sem tekur á móti sjúklingi á annarri heilsugæslustöð, hvort sem heilsugæslustöðvarnar tilheyra sömu heilbrigðisstofnun eða ekki. Annað dæmi er ef sjúklingur mætir á heilsugæslustöð til meðferðar hjá sérfræðingi sem staddur er á annarri heilbrigðisstofnun.

1. Ef sjúklingur er staðsettur á heilbrigðisstofnun eða starfsstöð heilbrigðisstarfsmanns þegar meðferð fer fram er það á ábyrgð starfsmanns þeirrar heilbrigðisstofnunar/starfsstöðvar að tryggja auðkenningu sjúklings og að koma honum í samband við heilbrigðisstarfsmanninn.
2. Ef kerfið sem heilbrigðisstarfsmaður og sjúklingur nota til að hafa samskipti er opið út á Internetið, þ.e. keyrir á vefþjóni sem aðgengilegur er öllum sem tengjast Internetinu, gerir landlæknir kröfu um innskráningu með rafrænum skilríkjum. Ef kerfið er eingöngu

aðgengilegt heilbrigðisstarfsmanninum og sjúklingi á öruggu lokuðu neti rekstraraðila er hefðbundin innskráning með notendanafni og lykilorði nægjanleg.

3. Sé sjúklingur ólögráða er heimilt að starfsmaður á þeirri stofnun þar sem sjúklingur er staddur skrái sig inn og auðkenni sjúklinginn gagnvart þeim heilbrigðisstarfsmanni sem skal veita fjarheilbrigðisþjónustuna. Starfsmaður sem skráir sig inn skal gera það með eigin rafrænum skilríkjum eða eftir atvikum eigin notendanafni og lykilorði. Hann skal þá hafa aðgang að lista yfir þá sjúklinga sem hlotið geta fjarheilbrigðisþjónustu og velja þaðan þann sjúkling sem skal hljóta þjónustu hverju sinni. Slíkar innskráningar skal skrá sérstaklega (logga) og yfirfara þann lista með reglubundnum hætti.
4. Landlæknir gerir kröfu um að heilbrigðisstarfsmenn skrái sig inn og hafi aðgang að upplýsingum um sjúklinga sína á lokuðu heimasvæði þar sem meðferð fer fram.
5. Tryggja skal öryggi samskipta á milli starfsstöðva með dulkóðun og öruggri sannvottun milli tengdra kerfa.
6. Landlæknir gerir kröfu um að óháður viðurkenndur sérfræðingur í netöryggi geri öryggisúttekt á lausninni áður en hún er tekin í notkun.

4.3 Fjarsamskipti milli heilbrigðisstarfsmanna á heilbrigðisstofnunum/starfsstöðvum

Dæmi um slíka þjónustu er ráðgjöf sem sérfræðilæknir á spítala veitir heimilislækni.

1. Ef heilbrigðisstarfsmaður einnar heilbrigðisstofnunar/starfsstöðvar leitar ráða hjá heilbrigðisstarfsmanni annarrar heilbrigðisstofnunar/starfsstöðvar varðandi málefni sjúklings skal tryggt að samskiptin fari fram á öruggan hátt. Tryggja þarf að enginn óviðkomandi hafi aðgang að samskiptunum.
2. Landlæknir gerir kröfu um að heilbrigðisstarfsmenn skrái sig inn og hafi aðgang að upplýsingum um sjúklinga sína á lokuðu heimasvæði þar sem meðferð fer fram.
3. Ef kerfið er opið út á Internetið, þ.e. keyrir á vefþjóni sem aðgengilegur er öllum sem tengjast Internetinu, gerir landlæknir kröfu um innskráningu með rafrænum skilríkjum. Ef kerfið er eingöngu aðgengilegt heilbrigðisstarfsmanninum á öruggu lokuðu neti rekstraraðila er hefðbundin innskráning með notendanafni og lykilorði nægjanleg.
4. Landlæknir gerir kröfu um að óháður viðurkenndur sérfræðingur í netöryggi geri öryggisúttekt á kerfinu áður en það er tekið til notkunar.

4.4 Fjarsamskipti milli sjúklings og heilbrigðisstarfsmanns þar sem heilbrigðisstarfsmaður vinnur utan stofnunar.

Ef fjarsamskipti eru notuð þar sem heilbrigðisstarfsmaður starfar fyrir heilbrigðisstofnun/starfsstöð en er staðsettur utan stofnunar/starfsstöðvar gerir landlæknir auknar kröfur um öryggi. Getur þetta átt við í öllum þeim tilfellum sem getið er hér að framan, þ.e. í kafla 4.1 – 4.3, og gilda þá þær kröfur sem þar koma fram ásamt þeim kröfum sem hér koma fram.

Dæmi um slíkt er sálfræðingur sem starfar á meðferðarmiðstöð en er jafnframt með starfsstöð annars staðar. Sjúklingur getur einnig verið staðsettur heima hjá sér eða á heilbrigðisstofnun/starfsstöð.

Öryggi - heilbrigðisstarfsmenn

1. Ef kerfið er eingöngu aðgengilegt heilbrigðisstarfsmönnum á öruggu lokuðu neti rekstraraðila skal heilbrigðisstarfsmaður tengjast því umhverfi með öruggum hætti, t.d. með VPN tengingu. Eftir það er hefðbundin innskráning með notendanafni og lykilorði inn í lausnina nægjanleg. Um meðferð og styrk lykilorða skal farið eftir 9. kafla ISO/IEC 27002:2013 um aðgangsstjórnun.
2. Heilbrigðisstarfsmaður skal aðeins eiga samskipti við sjúkling frá öruggu neti. Sé notast við þráðlaust net ber heilbrigðisstarfsmanni að velja lykilorð fyrir netið en ekki nýta sjálfgefið lykilorð frá Internetþjónustuveitanda.
3. Heilbrigðisstarfsmanni er ekki heimilt að nýta opið eða samnýtt þráðlaust net, t.d. þráðlaust net á flugvöllum eða hótelum.
4. Heilbrigðisstarfsmaður skal tryggja umhverfi sitt á meðan meðferð stendur á þann hátt að friðhelgi sjúklingsins sé tryggð og að enginn óviðkomandi geti truflað meðferðina.

Viðauki

Sjá skjal *Fullvissustig rafrænna auðkenna.*

Fullvissustig rafrænna auðkenna

Helstu auðkenni á Íslandi og í nágrannalöndum

12. nóvember 2018

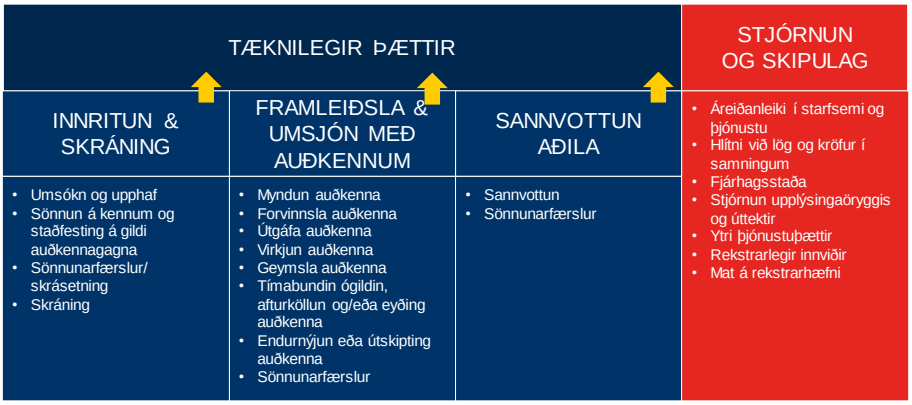
Þegar notandi sækist eftir aðgangi að upplýsingum í tölvukerfi yfir fjarskiptatengingar (úr fjarlægð) þá þarf að vera hægt að staðfesta á einhvern hátt hvaða einstaklingur er á bak við notandann. Algengasta aðferðin byggir á aðgangsorði (leyndarmáli) sem tengist tilteknu notandanafni sem einstaklingnum er úthlutað. Ef upplýsingarnar eru viðkvæmar þannig að það þurfi að vernda þær sérstaklega með takmörkun aðgangs að þeim þá þarf að vera tiltekin vissa fyrir því að sá sem er að óska eftir aðgangi sé í raun sá sem hann segist vera. Það fer eftir því hversu miklar kröfur eru um vernd á upplýsingunum hversu mikil sú vissa þarf að vera. Þessi mismunandi stig af vissu eru kölluð fullvissustig (e. assurance level).

Í alþjóðlega staðlinum ISO/IEC 29115:2013 *Entity authentication assurance framework* eru settar fram skilgreiningar og viðmið fyrir ákvörðun á fjórum fullvissustigum byggt á mati á þeirri áhættu sem er tengd rangri sannvottun á notanda og mögulegum áhrifum af skaða. Fullvissustigum ISO29115 staðalsins er lýst í eftirfarandi töflu:

FULLVISSUSTIG	TILTRÚ (á staðhæfðum eða fullyrtum kennslum)	ÁHÆTTA (tengd rangri sannvottun)
Lágt (LoA1)	Lítil eða engin tiltrú.	Lágmarks áhætta.
Meðal (LoA2)	Einhver (dálítil) tiltrú.	Miðlungs áhætta.
Hátt (LoA3)	Mikil tiltrú.	Veruleg áhætta.
Mjög hátt (LoA4)	Mjög mikil tiltrú.	Mikil áhætta.

Ákvæði í nýrri reglugerð Evrópuþingsins nr. 910/2014 um rafræna auðkenningu og traustþjónustu (eIDAS reglugerðin) vísa til sambærilegra fullvissustiga. Þar er LoA2 og lægra kallað lágt fullvissustig, LoA3 kallað verulegt fullvissustig og LoA4 hátt fullvissustig. Frumvarp sem mun innleiða eIDAS reglugerðina verður lagt fyrir Alþingi í febrúar 2019.

Fullvissustig byggja á bæði tæknilegum þáttum og þáttum í stjórnun og skipulagi:



Tæknilegir þættir skiptast niður í fullvissu í þremur lykil þáttum; við innritun og skráningu þegar rafræn auðkenni eru gefin út, við umsjón auðkenna við framleiðslu, útgáfu, virkjun og aðra umsýslu þeirra, og sannvottun á einstaklingi þegar rafrænum auðkennum er síðan beitt við innskráningu í kerfi, meðal annars hversu örugg samskiptin eru þegar innskráning fer fram.

Ráðgjafarfyrirtækið Admon hefur lagt mat á mismunandi útfærslu á rafrænum auðkennum og sannvottun í rafrænni þjónustu[1]. Upprunalegt mat var gert árið 2013 en matið var endurskoðað 2015 með hliðsjón af alþjóðlega staðlinum ISO/IEC 29115:2013.

Taflan hér fyrir neðan sýnir niðurstöðu matsins á sex tegundum rafrænna auðkenna.

Land	Rafrænt auðkenni	Skýring	Fullvissustig (*Level of Assurance*)
--	Hefðbundið notandanafn og aðgangsorð – opinber aðili	Skráning yfir Internetið staðfest í tölvupósti. Veikt aðgangsorð valið af áskrifandanum.	LoA1
Ísland	Veflykill ríkisskattstjóra	Varanlegur aðalveflykill.	LoA1
Ísland	Íslykill Þjóðskrár Íslands	Veflykill gefinn út af Þjóðskrá Íslands.	LoA2
Danmörk	OCES-skilríki og NemID	Miðlæg OCES-skilríki með NemID auðkenningu.	LoA2
Noregur	BankID	Miðlæg fullgild PersonBankID skilríki með BankID auðkenningu.	LoA3
Ísland	Rafræn skilríki undir Íslandsrót (á kortum og á farsímum)	Fullgild skilríki gefin út af Auðkenni með milliskilríkinu Fullgilt audkenni.	LoA4

Hefðbundið notandanafn og aðgangsorð sem gefin eru út af opinberum aðila þar sem kröfur leyfa veikt aðgangsorð (fáir stafir með fáum táknum) ná ekki hærra fullvissustigi en LoA1. Það er þó mögulegt að ná LoA2 ef gerð er krafa um sterkt aðgangsorð (t.d. margir stafir og samsett úr tölustöfum, bókstöfum og táknum), að öðrum kröfum uppfylltum. En hefðbundið notandanafn og aðgangsorð getur ekki undir neinum kringumstæðum náð hærra en LoA2.

Veflykill ríkisskattstjóra nær aðeins LoA1. Það veikir jafnframt veflykilinn hversu algengt er að hann sé notaður sem aðgangslykill að þjónustu frekar en sem persónulegt rafrænt auðkenni. Í raun er mjög lítil vissa fyrir því hver raunverulega er að beita veflyklinum.

Íslykill Þjóðskrár Íslands er með fullvissustig LoA2. Þetta er sama fullvissustig og hefðbundið notandanafn og sterkt aðgangsorð hafa.

Þjóðskrá Íslands býður einnig upp á styrktan Íslykil með því að tengja hann „út-úr-leið“ einskiptis-aðgangsorði yfir farsímakerfið (tala send til notandans með SMS). Þjóðskrá Íslands fullyrðir að styrktur Íslykill ná fullvissustigi LoA3, en á það hefur verið bent að þær aðferðir sem notaðar eru við skráningu og virkjun Íslykils styðji ekki aukningu á styrkleika Íslykilsins umfram LoA2.

NemID í Danmörku nær ekki fullvissustigi yfir LoA2, þrátt fyrir að sannvottunaraðferðir byggi á OCES-skilríkjum sem uppfylla í sjálfu sér meiri kröfur. Ástæðan er sú að kröfur til verklags við auðkenningu áskrifandans og til ferla við útgáfu og afhendingar NemID auðkennanna eru ekki nægilegar til að NemID með OCES-skilríkjum nái LoA3.

[1] *Mat á fullvissustigi auðkenna: Sannvottun á auðkennum fyrir rafræna þjónustu*. Admon ehf., útgáfa 2.0 frá 27. júní 2013 og *Mat á fullvissustigi auðkenna: Rafræn skilríki undir Íslandsrót á farsímum*. Admon ehf., útgáfa 1.0 frá 18. júní 2015.

Í raun er svipað vanmat í Noregi þar sem BankID með PersonBankID skilríkjum nær ekki upp fyrir fullvissustig LoA3. PersonBankID er fullgilt rafrænt skilríki og viðurkennt sem slíkt samkvæmt norskum lögum – og ætti því að uppfylla kröfur til LoA4. En kröfur til verklags við skráningu (sannvottun á áskrifanda og ferla við útgáfu og afhendingu) eru ekki nægilega traustar.

Rafræn skilríki undir Íslandsrót eru einu rafrænu auðkennin sem metin voru af Admon sem ná fullvissustigi LoA4. Á það bæði við um rafræn skilríki á snjallkortum og á SIM-kortum farsíma – svokölluð farsímaskilríki.

Eftirfarandi tafla er notuð í ISO29115 til að meta kröfu um fullvissustig út frá mögulegum áhrifum af skaða vegna rangrar auðkenningar.

TEGUND AFLEIÐINGA	MÖGULEG ÁHRIF AF BRESTI Í AUÐKENNINGU			
	ÁHRIFASTIG 1 (LoA1)	ÁHRIFASTIG 2 (LoA2)	ÁHRIFASTIG 3 (LoA3)	ÁHRIFASTI 4 (LoA4)
Óþægindi, nauð eða skaði á stöðu eða orðspori	Lítil	Miðlungs	Veruleg	Mikil
Fjárhagslegur skaði eða skaðabótaskylda	Lítil	Miðlungs	Veruleg	Mikil
Skaði á starfsemi fyrirtækisins, verkefnum þess eða á hagsmunum viðskiptavina eða almennings	Á ekki við	Lítil	Miðlungs	Mikil
Óheimil opinberun viðkvæmra upplýsinga	Á ekki við	Miðlungs	Veruleg	Mikil
Öryggi manna	Á ekki við	Á ekki við	Lítil Miðlungs	Veruleg Mikil
Lögbrot eða refsiverð brot	Á ekki við	Lítil	Veruleg	Mikil

Ef um persónugreinanlegar upplýsingar er að ræða þarf að meta áhættu fyrir réttindi og frelsi einstaklinga þar sem sérstaklega er lagt mat á áhrif á vernd upplýsinganna ef auðkenning reynist röng.

Þegar talið er að röng auðkenning geti valdið áhættu fyrir réttindi og frelsi einstaklinga og þar sem mögulegur skaði hefur veruleg áhrif á vernd persónuupplýsinga ætti að krefjast fullvissustigs LoA3 við sannvottun á kennslum. Í þeim tilvikum er ekki ásættanlegt að nota almenn notendanöfn og aðgangsorð, veflykil ríkisskattstjóra eða Íslykil Þjóðskrár Íslands til innskráningar á kerfi sem veitir aðgang að persónugreinanlegum upplýsingum.

Þegar um er að ræða aðgang að heilsufarsupplýsingum eða öðrum viðkvæmum persónuupplýsingum samkvæmt skilgreiningu í lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga er almennt talið að áhrif á persónuvernd af óheimilli opinberun viðkvæmra persónuupplýsinga séu í flestum tilvikum mikil, og í undantekningartilvikum veruleg (sjá töfluna hér fyrir ofan). Það ætti því ætíð að krefjast fullvissustigs LoA4, eða að lágmarki LoA3 ef rökstutt er að áhrifin af skaða geta ekki talist mikil.

Á Íslandi eru það einungis rafræn skilríki sem uppfylla kröfur til rafrænna auðkenna um fullvissustig LoA4. Rafræn skilríki undir Íslandsrót eru fullgild rafræn vottorð samkvæmt skilgreiningu í eIDAS reglugerðinni og uppfylla því kröfur í lögum um auðkenni með háu fullvissustigi.