# Verndun heilbrigðisupplýsinga

Arnaldur F. Axfjörð, MRH, EL


Hádegisfundur Ský

Netöryggi er á ábyrgð okkar allra

28. október 2020

Embætti landlæknis
Directorate of Health

# Hlutverk embættis landlæknis

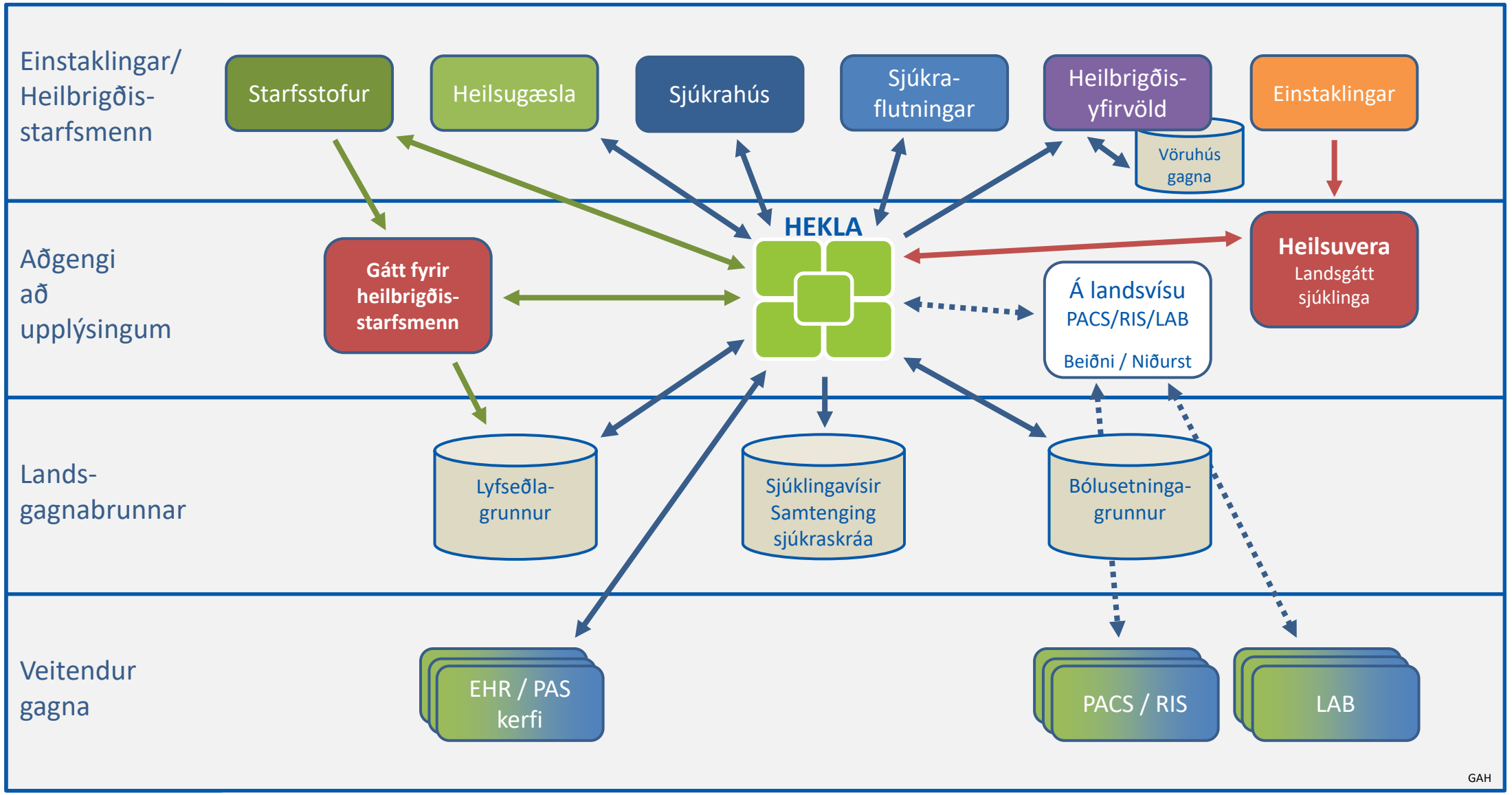
- Hlutverk embættis landlæknis er m.a.
  - Hafa almennt eftirlit með rekstri heilbrigðisþjónustu
  - Skipuleggja og halda heilbrigðisskrár á landsvísu
  - Reka lykil net- og upplýsingakerfi fyrir heilbrigðisþjónustu
- Með NIS-lögunum fær embætti landlæknis nú aukið hlutverk
  - Hafa eftirlit, sem eftirlitsstjórnvald, með framkvæmd NIS-laganna vegna rekstraraðila nauðsynlegrar heilbrigðisþjónustu

Embætti landlæknis
Directorate of Health

# MRH: Miðstöð rafrænna heilbrigðislausna

- Hlutverk
  - Þróa og innleiða upplýsingatækni í heilbrigðisþjónustu
  - Viðhalda og sjá um stefnu í upplýsingatækni í heilbrigðisþjónustu
  - Þróa og innleiða rafræna sjúkraskrá
  - Þróa og innleiða aðgang einstaklinga að eigin heilbrigðisupplýsingum (Mínar síður Heilsuveru)
  - Þróa og reka íslenska heilbrigðisnetið (Hekla)
  - Hafa eftirlit með öryggi net- og upplýsingakerfa stofnana í heilbrigðisþjónustu
- Markmið
  - Tryggja öruggan aðgang heilbrigðisstarfsmanna að sjúkraskrárupplýsingum
  - Tryggja öruggan aðgang einstaklinga að eigin heilsufarsupplýsingum
  - Stuðla að auknu öryggi og gæðum sjúkraskrárupplýsinga
  - Efla miðlun og úrvinnslu upplýsinga úr rafrænum sjúkraskrárkerfum

# HEKLA heilbrigðisnet




Embætti landlæknis
Directorate of Health

# Upplýsingar um heilsufar eru viðkvæmar

*… persónuupplýsingar sem varða líkamlegt eða andlegt heilbrigði einstaklings, þ.m.t.* ***heilbrigðisþjónustu sem hann hefur fengið****, og upplýsingar um lyfja-, áfengis- og vímuefnanotkun*

- Sjá lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga
  - Umtalsverðar sérkröfur um vinnslu viðkvæmra persónuupplýsinga
- Efnislína í tölvupósti getur innihaldið heilsufarsupplýsingar
  - Það þarf ekki mikið til!
- Ógnir í hinum rafrænu heimum eru óvægar og öflugar
  - Ekki sama símtal og myndsímtal!
- **Það er ekki hægt að bæta fyrir óheimila birtingu á heilsufarsupplýsingum!**

Embætti landlæknis
Directorate of Health

# Aðgangur með fullri vissu

- Kröfur um sannvottun einstaklinga byggðar á áhættumati
  - Verndun viðkvæmra persónuupplýsinga um heilsufar
- Hæsta fullvissustig við innskráningu
  - Fullvissustig LoA 4 í ISO/IEC 29115:2013 *Entity Authentication Assurance Framework*
  - Fullvissustig „hátt“ í eIDAS-reglugerðinni (ESB 2014/910) og framkvæmdareglugerð framkvæmdastjórnarinnar (ESB) 2015/1502

Embætti landlæknis
Directorate of Health

# Ekki bara styrkur rafrænna auðkenna

- Þættir fullvissustigs
  - Innritun og skráning (e. enrollment)
  - Umsjón rafrænna auðkenna (e. electronic identification means management)
  - Aðferð við sannvottun (e. authentication mechanism)
  - Stjórnun og skipulag (e. management and organization)

*The **authentication mechanism** implements security controls for the verification of the electronic identification means, so that it is **highly unlikely** that activities such as **guessing**, **eavesdropping**, **replay** or **manipulation of communication** by an attacker with **high attack potential** can subvert the authentication mechanisms.*

Framkvæmdareglugerð framkvæmdastjórnarinnar (ESB) 2015/1502

# Rafræn vottorð – rafræn skilríki

- Einu rafrænu auðkennin sem uppfylla LoA 4 og fullvissustig „hátt“
- Mikilvægt að byggja réttindi (e. authorization) á sannvottun (e. authentication)
- Makaheilkennið er verulegt áhyggjuefni
  - Of algengt að fólk slái inn PIN til að annar einstaklingur komist inn
  - Ef símanúmer er ekki rétt þá er hætta á að aðgangur sé veittur í nafni annars einstaklings

Embætti landlæknis
Directorate of Health

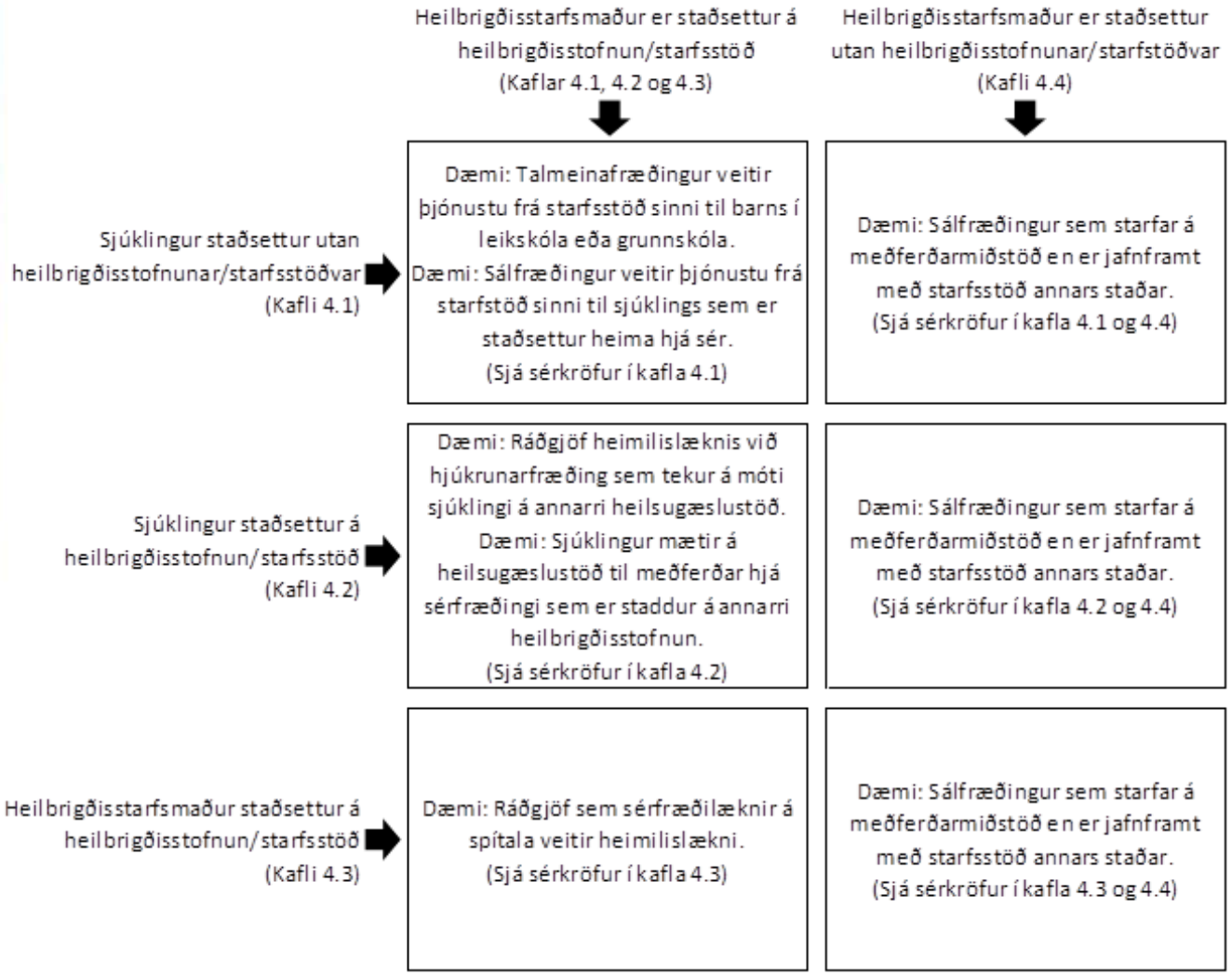
# Mismunandi kröfur til öryggisstýringa

- Samtengingar sjúkraskrárkerfa
- Tengingar við Heilsuveru
- Tengingar við Heklu
- Tengingar við gáttir MRH
  - Lyfjaávísanagátt
  - Bólusetningar
- Fjarheilbrigðisþjónusta
  - Fyrirmæli landlæknis um upplýsingaöryggi við veitingu fjarheilbrigðisþjónustu

Embætti landlæknis
Directorate of Health

# Kröfur um öryggi í fjarheilbrigðisþjónustu

*Fyrirmæli landlæknis um upplýsingaöryggi við veitingu fjarheilbrigðisþjónustu*




*Heilbrigðisþjónusta þar sem* ***samskiptatækni*** *er notuð til að veita þjónustu og sjúklingur og þeir heilbrigðisstarfsmenn sem koma að meðferðinni* ***eru ekki staddir á sama stað****.*

Embætti landlæknis
Directorate of Health

# Kröfur um öryggi í fjarheilbrigðisþjónustu

- Kröfur embættisins snúa að rekstraraðilum heilbrigðisþjónustu – ekki beint að aðilum sem þróa og selja lausnir
- Rekstraraðila ber að skila staðfestingu á öryggisúttekt þess kerfis sem verður notað
  - Óháður viðurkenndur sérfræðingur í netöryggi
  - Úttekt á bæði tæknilegum og skipulagslegum stýringum
- Athugið: Embætti landlæknis vottar ekki lausnir!

Embætti landlæknis
Directorate of Health

# NIS lögin

Lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða

***Stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða***

- Nauðsynleg þjónusta rekstraraðila
  - Nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi
  - Veiting háð net- og upplýsingakerfum
  - Atvik hefðu verulega skerðandi áhrif á veitingu þjónustu
- Ráðherra heldur opinbera skrá yfir rekstraraðila nauðsynlegrar þjónustu

Embætti landlæknis
Directorate of Health

# NIS reglugerðin

Reglugerð nr. 866/2020 um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu

- Markmið
  - Tryggja samfellda virkni og áfallaþol nauðsynlegrar þjónustu með því að kveða nánar á um lágmarkskröfur til umgjarðar net- og upplýsingakerfa
  - Tryggja samhæfð viðbrögð við ógnum og atvikum í net- og upplýsingakerfum
- Innihald
  - Almenn ákvæði
  - Þjónusta sem teljast skal nauðsynleg
  - Lágmarkskröfur um áhættustýringu og ráðstafanir
  - Skipulagslegar og tæknilegar ráðstafanir
  - Viðhald, viðbragðsáætlun, innra eftirlit og atvikatilkynningar
  - Eftirlit, samræmi og viðurlög

# Heilbrigðisþjónusta

7. gr. reglugerðar nr. 866/2020

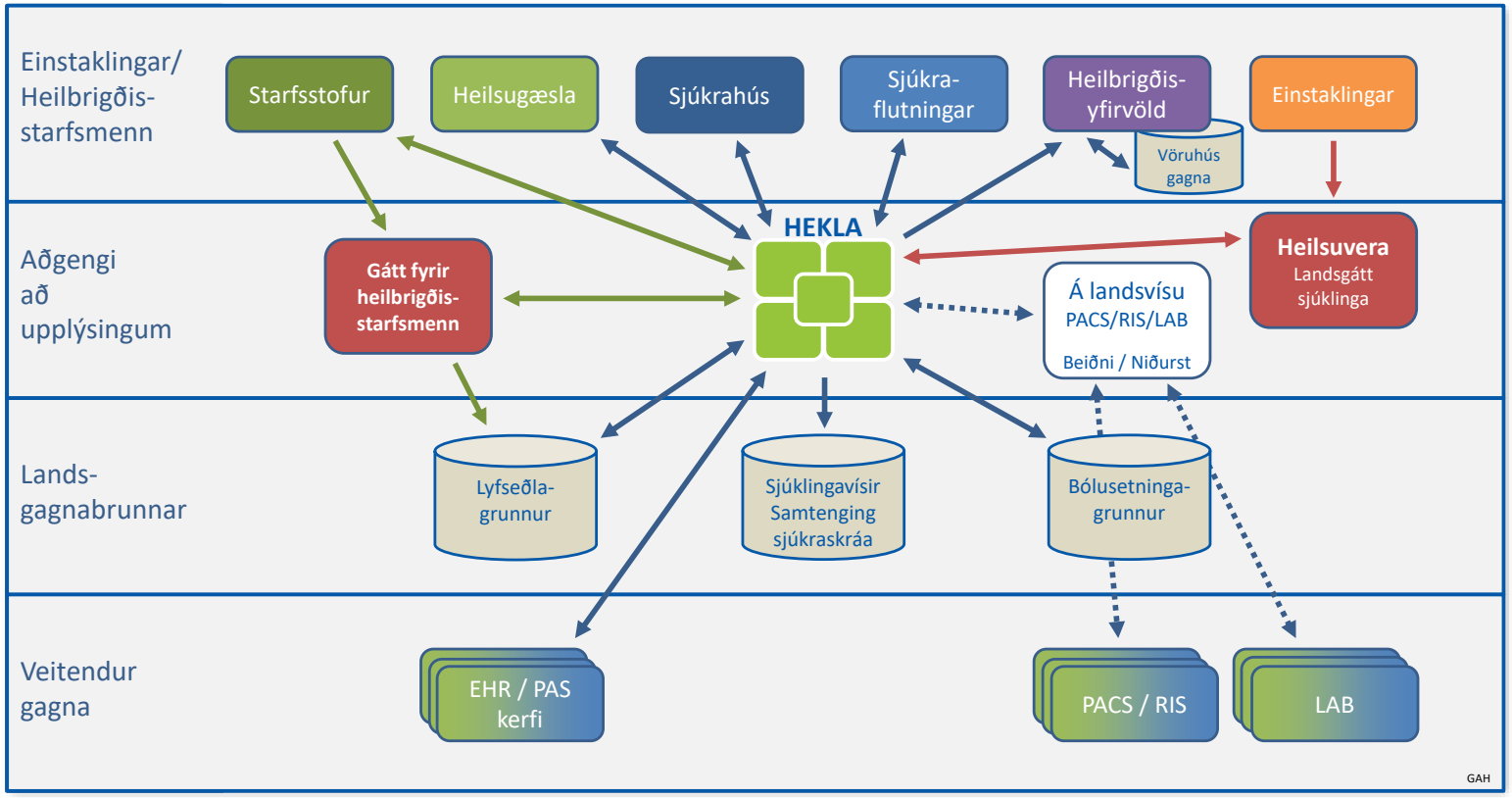
Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði heilbrigðisþjónustu er átt við

a. bráða- og slysamóttöku;
b. heilsugæslu og sjúkrahúsþjónustu;
c. heilbrigðisstofnanir og starfsstofur heilbrigðisstarfsmanna með sjúkrarýmum;
d. heimahjúkrun;
e. sjúkraflutninga;
f. lyfjabúðir þar sem að minnsta kosti 27.500 lyfjaávísanir eru afgreiddar á ári;
g. lyfjabúðir utan höfuðborgarsvæðisins þar sem að minnsta kosti 10.000 lyfjaávísanir eru afgreiddar á ári;
h. lyfjabúðir og lyfsölur sem einar þjóna tilteknum byggðalögum og
i. lyfjaheildsölur (birgðastöðvar fyrir lyf);

sem falla undir heilbrigðisþjónustu samkvæmt lögum nr. 40/2007 um heilbrigðisþjónustu, lyfjalög nr. 100/2020 sem taka gildi 1. janúar 2021 og lyfjalög nr. 93/1994 fram að þeim tíma.

Embætti landlæknis
Directorate of Health

# Takk fyrir!




**Arnaldur F. Axfjörð**
Verkefnastjóri öryggismála
Miðstöð rafrænna heilbrigðislausna
Embætti landlæknis
Katrínartún 2, 105 Reykjavík
Sími 510 1900
www.landlaeknir.is

Embætti landlæknis
Directorate of Health

**ÁBYRGÐ – VIRÐING - TRAUST**