Leiingas årlege gjennomgang av informasjonssikkerheit 2019 for Helse Førde

Innhold

1 Innleiing

I Helse Førde har vi ikkje utført leiingas årlege gjennomgang av IKT-sikkerheit tidlegare. Det er fleire grunnar til det, blant anna at vi i stor grad styrt av dei regionale sikkerheitsmekanismane. Men som føretak er vi uansett pålagt å utføre denne oppsummeringa årleg. IKT avdelinga til Helse Førde legg dagleg ned mykje arbeid i IKT-sikkerhet og personvern. Blant anna i oppfølging av sikkerheitsavvik, risikovurderingar, gjennomgang av databehandlaravtalar før signering og anna førebyggande arbeid.

Helse Førde kjøper dei fleste IKT tenestestane frå Helse Vest IKT, noko som igjen regulerast av Tenesteavtalen (SLA).

2 Arbeid med IKT-sikkerheit

Informasjonssikkerheita i Helse Førde HF er bygd på det regionale styringssystemet for IKT sikkerheit og personvern. Styringssystemet blei ferdig revidert regionalt med tanke på GDPR i desember 2019 og det har vore arbeidd med å tilpasse det til føretaket vårt i tida etterpå. IKT sikkerheitsleiar har deltatt i dette arbeidet regionalt i Sikkerheitsutvalet i Helse Vest, mens Helse Førde IKT har seinare jobba med lokal tilpassing.

2.1 Sikkerhetsmål

Dette er forankra og definert i «Styringssystem for informasjonssikkerheit og personvern».

Personopplysningar skal:

- Vere tilgjengeleg for rett personell til rett tid i samsvar med fastsette prinsipp for tilgangsstyring.
- Bli behandla i tråd med reglane om teieplikt og vere verna slik at uvedkomande ikkje får kjennskap til opplysningane. Uvedkomande omfattar òg personell som ikkje har tenesteleg behov.
- Vere fullstendige, oppdaterte og korrekte og eit resultat av rettmessige registreringar og kontrollerte aktivitetar.
- Bli avgrensa slik at berre det som er nødvendig av personopplysningar blir behandla.

For helseopplysningar:

- Konfidensialitet er ein grunnleggande pasientrett og diskresjon er føresetnad for tilliten til helsevesenet, føretaket og den enkelte helsearbeidaren. Tilfredsstillande konfidensialitet er derfor høgt prioritert blant sikkerheitsbehovet i føretaket.
- Tilgang til relevante og nødvendige helse- og personopplysningar er ein føresetnad for å kunna yte forsvarleg helsehjelp. Tilfredsstillande sikring av tilgjenge og integritet kan vere livsviktig, og må då prioriterast høgare enn behovet for konfidensialitet.

2.2 Sikkerheitsstrategi

- Verksemda skal nytta Helse vest IKT AS som føretrekt databehandlar for alle IT-løysningar
- All behandling av helse- og personopplysningar skal ha tilgangsstyring
- Sikkerheitstiltaka skal ikkje aktlaust kunna omgåast av medarbeidarane
- Sikkerheitstiltaka skal ikkje kunna omgåast av eksterne sjølv om desse opptrer med forsett
- All behandling av helse- og personopplysningar skal loggast
- Sikkerheitsbrot skal aktivt identifiserast og blir opp følgt som avvik
- Medarbeidarar skal ha tilstrekkelege kunnskap om behandling av helse- og personopplysningar

2.3 Organisasjon

IKT sikkerhet i Helse Førde ligg under IKT-avdelinga der Lars-Inge Eikefjord har ei 50% stilling som IKT-sikkerheitsleiar. Faget krev mykje tid og både IKT sjef og personvernombodet samarbeider i saker der det krevst.

IKT sikkerheitsleiar rapporterer direkte til administrerande direktør. IKT-avdelinga har og månadlege statusmøter (leiardialog) med administrerande direktør.

3 IKT-sikkerheitsarbeidet i 2019

IKT-avdelinga er involvert i ei rekkje prosjekt deriblant i Heliksprogrammet og Alle møter for å påsjå at IKT-sikkerheita og personvernet blir fylgt.

Tidlegare år har en kjørt mini e-læringskurs i diverse kategoriar for IKT-sikkerheit blant dei tilsette, men sidan ein ikkje var heilt nøgd med kvaliteten på kursa i 2018 blei ikkje dette gjort i 2019. Det blir arbeidd med nye kurs for hausten 2020.

IKT-Sikkerheitsleiar deltek i det regionale sikkerheitsutvalet (SU) i Helse Vest, som har jamlege møter både fysisk og digitalt.

3.1 Resultatet fra avviksbehandling

Oppfølging av lokale avvik. Gjengangarar her er brukarar som lånar påloggingа frå andre, enten for å spare tid eller grunna manglande tilgang sjølv. Ein anna gjengangar er utskrifter som havnar på feil skrivar. Her har vi spesielt fokus på «sikker utskrift» og alle nye nettverksprintarar blir bestilt med denne funksjonen. Det blei blant anna lagd informasjon spesielt om dette som administrerande direktør la fram på eit allmøte til alle tilsette. Et framtidig ynskje er å køyre et prosjekt for å få brukarane til å nytte denne funksjonen fullt ut og kanskje fjerne moglegheita for å skrive ut på anna måte.

Vi får og ein del avvik frå tenesteleverandøren vår (Helse Vest IKT) som gjennom å være vår databehandlar melder diverse avvik til oss. Dette er typisk alvorlige avvik der vi må vurdere om det skal meldast til Datatilsynet. Vi har ei eiga rutine som vi følgjer i disse tilfella.

Følgende avvik har blitt vurdert meldt til Datatilsynet:

Dato	Synerginr	System/område	Beskriving
19.2.2019	-	Sectra	Økonomi i Helse Førde har tilgang til å sjå alle pasientar som det er planlagt eller gjennomført behandling på både i Helse Førde og Helse Fonna. Dei har og tilgang til opplysningar som er utenfor tenesteleg behov.
10.1.2019	-	DIPS	Det ble tatt kopi av produksjonsdata frå UniLab inn i DIPS testmiljø uten at pasientdata var tilstrekkelig anonymisert. Mengden helseopplysninger som er eksponert i de ulike testbasene er ikkje klarlagt. Nokon labsvar er eksponert.

Oversikt over meldte avvik i 2019

Hendelsetype	Saker, Antall registreringer
Hendelsetype - 3. 5 IKT	7
Hendelsetype - 4. 1 Bruk av eksterne nettverk/program	2
Hendelsetype - 4. 3 Deling/tilgjengeliggjøring av data	5
Hendelsetype - 4. 6 Taushetsplikt - tilgang/spredning av opplysninger	4
Hendelsetype - 4.99 Annet - Informasjonssikkerhet og personvern	12
Hendelsetype - Drift av system- og maskinvare	11
Hendelsetype - Lagring/forsendelse av data	6
Hendelsetype - Skjerming av sensitiv informasjon	22
Hendelsetype - Tilgang til data	5
	Sum 74

3.2 Resultat frå sikkerheitsrevisjonar i eige føretak og hjå andre med innverknad for informasjonssikkerheita.

Hausten 2019 foretok Riksrevisjonen ein «Forvaltningsrevisjon om helseforetakenes forebygging av angrep mot sine IKT-systemer». Her blei spesielt Helse Vest IKT og Helse Bergen plukka ut for grundig sjekk, men og Helse Førde måtte svare ut en del spørsmål. Den endelige rapporten frå revisjonen har vi ikkje fått endå, men det blei avdekka en del klare manglar og i Helse Førde. Blant anna at vi ikkje har utført leiingas årlege gjennomgang slik som det er krav om. Vi manglar og som dei andre føretaka, ei «samlet og oppdatert oversikt over behandlinger av helse- og personopplysninger i virksomheten». Det blir det no jobba med regionalt for å få på plass ei felles løysing (protokoll).

3.3 Resultat fra risikovurderingar

Både IKT-sikkerheitsleiar og personvernombodet har deltatt på ei rekkje regionale risikovurderingar. I tillegg har vi fasilitert nokre ROS-ar sjølv lokalt, deriblant ei for nettbutikk til medisinsk heimebehandling og ei for innkjøp av augelysingsmaskin for MTA. Vi har og delteke i regionale og fasilitert lokale personvernkonsekvensvurderingar (DPIA).

3.4 Oversikt over risikovurderingar 2019

	Risikoobjekt	**Omfang**
1	Forvaltning, drift og vedlikehold for MTU og behandlingshjelpemidler (BHM)	Regional
2	Unilab - deling av pasientinformasjon mellom foretak	Regional
3	CheckWare den totale løsningen.	Regional
4	Pakkeforløp rus og psykiatri	Regional

5	Kursbygger for læringsportalen	Regional
6	Robust mobilt helsenett	Regional
7	Tekniske og funksjonelle risikovurderinger av digitale skjema og brev	Regional
8	DIPS tilgang for kontrollkommisjonen	Regional
9	Skjemarobot Natus	Regional
10	Single Sign On Webcruiter	Regional
11	Innføring av LABAS	Regional
12	Oppkjøp av beredskaps system UMS	Regional
13	Visning av timer fra Aria (strålesystemer) på helsenorge.no	Regional
14	Vestlandspasienten lagring av digitale skjema i Elements	Regional
15	WebRTC og virtuelle møterom (Pexip) NHN	Regional
16	RPA - registrere verdier for blodgass i Natus	Regional
17	Beyond trust remote support - Fjernstyringsprogram som skal fjernstyre pasient-PCer som skal ha videosamtaler med behandler på sykehus.	Regional
18	Klinisk mobil fallback 4G uten APN, samt blåtann og internett.	Regional
19	Bliksund	Regional
20	DMA - Tilgang til bilder/us fra andre foretak	Regional
21	Innføring av brevrobot v2 i foretakene	Regional
22	Fase 2 for innovasjonsprosjekt predikasjon av pasientoppmøte	Regional
23	Elements/Ephorte, inkl. digital forsendelse - funksjonell vurdering	Regional

3.5 Lokale sikkerheitssaker

Problem	**Beskriving**
Sending av sensitive data i post	Korleis skal ein best handsame/sikre internkonvoluttar som inneheld sensitive data?
Sikker digital forsendelse av dokumenter	Finst det gode digitale løysingar for å sende sensitive data? Elements og Digipost? Crypho?
Oneconnect mellom HFD og St Olav HF	Avklare det formelle rundt det å sende teleradiologisk til St Olav HF.
Risikovurderinger i Helse Førde	Et forsøk på å finne ei felles løysing for alle typar risikovurderingar i Helse Førde
Norse Feedback	Arbeid med risikovurdering og DPIA av Norse Feedback-løysinga
Kartlegging av Logging for HelseAtlas	Avklaringar rundt krav til logging av database
Informasjonstryggleik i forskingsprosjekt	Avklaringar rundt utstyret som skal nyttast til prosjektet «Incorporating Psychosocial Aspects of Bariatric Surgery» der Helse Førde er forskningsansvarlig.

Sikker skanning – BHT	Bedrifthelsetenesta ynskjer å nytte multifunksjonsskrivar til å skanne inn dokumenter i deira journalsystem.
Skjermovervåkning ved Nevrologisk avdeling	Nevrologisk avdeling treng nytt utstyr til kameraovervaking. Kva kan nyttast og kva er lov?
databehandleravtale - PasOpp somatikk	Nasjonal undersøkelse om voksne pasienters erfaringer med døgnopphold på somatiske sykehus. Avklaringar rundt kvar ansvaret ligg og korleis løysinga er satt opp.
Svar til Riksrevisjonen	Innhenting av data og svar til Riksrevisjonen.

3.6 Beredskapshendingar

Dato	Alvorlegheitsgrad	Beskrivelse
11.09.2019	Raud	Problem med pålogging i DIPS og fleire system
27.03.2019	Raud	Nettverk nede fleire lokasjoner

3.7 Opplæring

E-læringskurs for informasjonssikkerheit og personvern vart reviderte haust 2019. Kurset skal takast anna kvart år og er tilgjengeleg via læringsportalen i føretaket som normalt.

4 Oppsummering

2019 ha vore eit travelt år med mange tidkrevjande risikovurderingar, ein rekk ikkje å delta på alt så ein er tvungen til å prioritere. Nye løysningar er ofte skybaserte og krev at en er ekstra påpasselig i risikovurderingane og før en signerer ei databehandleravtale. Ein må være sikker på kvar våre data blir lagra.

Mengden med svindelforsøk er økande. Heldigvis blir mykje av dette håndtert av gode sentrale system drifta av Helse Vest IKT, men den menneskelige faktoren er lika vell det svake ledd. Det er derfor viktig å bevisstgjere brukarane slik at dei ikkje let seg lure av telefoner, e-poster, sms osv.

Vegen framover:

2020 – Ein må informere ut i organisasjonen om det reviderte Styringssystemet for informasjonssikkerheit og personvern.