Rapport informasjonssikkerhet Helgelandssykehuset 2015

1. Innledning

I Oppdragsdokumentet 2015 punkt 4.4. Beredskap, er et av punktene:
Området informasjonssikkerhet med tilhørende status på ROS[1]-analyser skal behandles særskilt av helseforetakets styre innen 01.06.15. Styresaken skal beskrive om databehandler oppfyller de krav i lover og forskrifter som er tillagt databehandlerrollen og om nødvendige krav er nedfelt i leveranseavtaler. Eventuelle avvik skal være lukket innen 31.12.15.

Personvern og informasjonssikkerhet i helse- og omsorgssektoren skal bidra til økt pasientsikkerhet, blant annet ved forsvarlig håndtering av helseopplysninger og at korrekte opplysninger kommer til rett behandler.

Stillingen som informasjonssikkerhetsansvarlig i Helgelandssykehuset (HSYK) innehas av Kvalitetsleder, som er plassert i senter for Fag Forskning og Utdanning. Personvernombud rollen ivaretas av NSD (Norsk samfunnsvitenskapelig datatjeneste).

HSYK deltar i regionens informasjonssikkerhetsforum (IS-forum), som har som formål å bidra til felles fortolkning av lovkrav samt innføring av felles rutiner og prosedyrer innen informasjonssikkerhet. Forumets mandat er for tiden under revisjon. Leder for IS-forum er Sikkerhetssjef ved UNN.

2. Status

Ledelsens gjennomgang informasjonssikkerhet

HSYK gjennomfører årlig ledelsens gjennomgang risikovurderinger, der også ledelsens gjennomgang av informasjonssikkerhet inngår.. Den baserer seg på 24 sjekkpunkt fra faktaark nr. 6 fra Norm for informasjonssikkerhet.

[1] Risiko- og sårbarhetsanalyse

Felles Styringssystem for informasjonssikkerhet

Felles Styringssystem for informasjonssikkerhet i Helse Nord RHF er utarbeidet med bakgrunn i lovverket, samt anbefalinger og krav nedfelt i Norm for informasjonssikkerhet[1]. Det er felles for Helse Nord og eierdirektør i Helse Nord RHF står som godkjenner, DocMap DS6121.
Det ble ferdigstilt på slutten av 2012 og IS-forumet har ansvar for kontinuerlig oppdatering. Noe av innholdet er: Fysisk sikring, håndtering av informasjonssikkerhets-avvik, nødrutiner, pasientjournal, sikkerhetsinstruks, håndtering av pasient-opplysninger lagret i medisinteknisk utstyr med mer.

Informasjonssikkerhetssystemet innebærer bl.a følgende:

- Oppfyllelse av lovkrav er satt sammen i et mer helhetlig dokument
- Sikkerhetsmål og krav er mer konkretisert
- Overordnet akseptabel risiko er definert
- Opplæring i informasjonssikkerhet gjøres obligatorisk (e-læring)
- Mer konkret beskrivelse av ansvarsforhold på de ulike nivåene

I dokumentet Styringssystem for informasjonssikkerhet (MS0318) er obligatorisk e-læring i informasjonssikkerhet omhandlet i kap. 4 Sikkerhetsstrategi. Det heter der at *e ISF-HN har utviklet et eget e-læringskurs for informasjonssikkerhet. Ansatte og ledere skal ha bestått testen i dette kurset. Personer som ikke har bestått testen vil ikke få eller beholde tilgang til informasjonssystemene i Helse Nord sitt IT-systemet.*
E-læringskurset ble utarbeidet i den tidligere e-læringsplattformen. Nordlandssykehuset (NLSH) har konvertert den over til den nye e-læringsplattform Campus. I løpet av 2015 vil det bli foretatt nødvendige endringer i den slik at den kan benyttes ved de øvrige helseforetakene.
E-læringskurset bør gjøres obligatorisk for alle nyansatte med krav om en bestått test innen en gitt frist, for eksempel 30 dager etter påmelding, slik at de ikke vil få videre tilgang til informasjonssystemene (les journalsystemene) før testen er bestått. På den måten sikrer man at ansatte har et minimum av kunnskap om informasjonssikkerhet og personvern. Det bør også stilles samme krav til eksisterende ansatte.
Plan for implementering utarbeides når e-læringskurset er fullt tilgjengelig og i forhold til øvrige IKT-prosjekter.

Sikker utskrift

I 2014 ble "sikker utskrift" begynt innført ved Helgelandssykehuset. Sikker utskrift er en ny måte å skrive ut dokumenter på. Utskriften blir sendt via en server og først skrevet ut når den ansatte skanner sitt adgangskort på skriver (valgfri skriver konfigurert for

[1] https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

sikker utskrift). Utskrifter risikerer dermed ikke å bli sendt til feil skriver, eller bli liggende uavhentet på skriveren.

Sikker utskrift er tilgjengelig ved alle sykehusenhetene. Antall nye nettverksskrivere må økes for å kunne øke bruken. Det arbeides videre med mål om å redusere lokale skrivere, samt at alle nettverksskrivere er satt opp for sikker utskrift, slik at sensitiv informasjon ikke kommer på avveie.

ROS-analyser (Risiko-og sårbarhetsanalyser)

I perioden 2014-2015 er det gjennomført få risikovurderinger innen informasjonssikkerhet. Dette skyldes i hovedsak mangel på ressurser i forhold til øvrige prosjekter. I de fleste FIKS- og HOS programmets prosesser gjennomføres det fortløpende risikovurderinger. Disse vurderingene fremkommer ikke som egne ROS-rapporter, men er innarbeidet i de løsninger som foreslås gjennomført. ROS-analysene i HOS er særlig vinklet mot risiko for gjennomføring av prosjektet og tap av data i de ulike trinne. Det er fra Sikkerhetssjefen på UNN vurdert at det på nåværende tidspunkt ikke vil være nødvendig med ytterlige ROS-vurderinger av EPJ (Elektronisk pasientjournal). Det vil bli aktuelt å gjennomføre ROS/sikkerhetsrevisjon av EPJ etter at FIKS- og HOS programmet har gjennomført, trinn II – sammenslått elektronisk journal i regionen. Vinklingen av ROS-analysene bør da være på bruk av EPJ.

Tilgangsstyring

Tilgangsstyring skal sikre at nødvendige helse- og personopplysninger er tilgjengelig ut i fra brukerens yrkesfaglige behov og oppgaver. Helsepersonell må kunne søke opp og registrere relevante og nødvendige opplysninger i pasientens journal. Dette innebærer at brukeren må identifiseres i pasientjournalsystemet på en betryggende måte, og gis riktige tilgangsrettigheter i forhold til lesing, registrering, retting og sletting. I dag tildeles brukerrolle etter undertegning av taushetserklæring og kjøreregler for datasystem.

Innføring av regional tilgangsstyring som en del av HOS-prosjektet vil sikre større grad av likhet for alle ansatte i Helse Nord på et overordnet nivå. De vil medføre enklere forvaltning av tilgangsrettigheter ved at brukerroller bygges etter samme prinsipper. Dette vil også gi gjenkjennbarhet for ansatte som ambulerer innad i og mellom foretak.

Beredskap

Helgelandssykehuset har i dag nødrutiner for bruk dersom informasjonssystemet DIPS er utilgjengelig. Beredskapsplan for IKT-svikt (DS 9890) er tatt inn i nytt planverk for beredskap i 2015. Det er foreløpig ikke gjennomført øvelser i forhold til denne delen av planverket, men dette bør gjennomføres årlig, sammen med øvelser i beredskap ved svikt i andre kritiske systemer

Databehandler/databehandleravtaler

En databehandleravtale skal sikre at helse- og personopplysninger ikke skal behandles av databehandler på annen måte enn det som er avtalt med databehandlingsansvarlig. Databehandlingsansvarlig ved sykehusets ledelse har ansvar for å utforme databehandleravtale med databehandler (den eksterne driftsenhet). Prosedyrer vedr. databehandleravtale er beskrevet i egen prosedyre DS7534 som en del av styringssystemet..

Helgelandssykehuset har databehandleravtaler med ulike leverandører både vedr. drift og brukerundersøkelser. Avtalene er relativt omfattende og avtalene er utformet etter den felles mal som benyttes i Helse Nord. Det er foreløpig ikke gjennomført kontroller av våre leverandører om de oppfyller de kravene som står beskrevet i databehandleravtalen. Det er imidlertid jevnlige driftsoppfølgingsmøter med den største leverandøren, Helse Nord IKT.

Det vil i løpet av 2015 bli gjennomført kontroller av utvalgte databehandleravtaler for å sikre at krav i lov og forskrifter samt krav i avtalene oppfylles.

3. Konklusjon

Felles styringssystem for informasjonssikkerhet i Helse Nord følges.

Når e-læringskurs for informasjonssikkerhet er tilgjengelig i ny plattform bør dette bli gjort obligatorisk for alle ansatte etter en egen implementeringsplan.

ROS-analyser av EPJ systemene er blitt ivaretatt via FIKS- og HOS- programmets prosesser. Det vil bli aktuelt å gjennomføre nye ROS-analyser etter at Fiks og HOS programmet er gjennomført.

Svikt i IKT-systemer er tatt inn i nytt planverk for beredskap, og skal inngå i årlig øving.

Det er ikke gjennomført kontroller av våre leverandører på om de oppfyller kravene i databehandleravtalene, men det er jevnlige driftsoppfølgingsmøter med den største leverandøren HN-IKT. Kontroller av utvalgte databehandleravtaler vil bli gjennomført ila høsten 2015.

Praktisk gjennomføringen av de ulike tiltakene må konkretiseres ytterligere, og må tids- og ressursmessig innpasses sammen med øvrige IKT-prosjekter høsten 2015/våren 2016.