NORDLANDSSYKEHUSET
NORDLÁNDA SKIPPIJVIESSO

Direktøren

Styresak 69-2015
Orienteringssak - Informasjonssikkerhet

Saksbehandler:	Saksnr.:	Dato:
Alisa Larsen	2015/1426	05.06.2015

Dokumenter i saken:

Trykt vedlegg: Fremdriftsplan
Ikke trykt vedlegg:

Bakgrunn

I oppdragsdokumentet (OD) for 2015 fra Helse Nord RHF til Nordlandssykehuset HF (NLSH) er det gitt følgende oppdrag:

«Området informasjonssikkerhet med tilhørende status på ROS-analyser skal behandles særskilt av helseforetakets styre innen 01.06.05. 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.»

Området informasjonssikkerhet

Økt samhandling på tvers av foretaksgrensene/regioner har gjort det nødvendig å ha et overordnet styringssystem for informasjonssikkerhet for de regionale helseforetakene og Norsk Helsenett AS som tilrettelegger for slik samhandling.

Det er etablert et styringssystem for informasjonssikkerhet hos Helse Nord. Styringssystemet er initiert med bakgrunn i Nasjonal IKT sin vedtatte strategiplan, «Overordnet IKT-strategi for de regionale helseforetakene». Tiltakets mål er å etablere et felles styringssystem for informasjonssikkerhet for de regionale helseforetakene/helseforetakene og Norsk Helsenett AS. Styringssystemet baseres på det lovverk som styrer aktørene (Helseregisterlov, Personopplysningslov og forskrift mfl.) inklusiv Norm for informasjonssikkerhet og aktørenes behov.

Informasjonssikkerhetsforum har utarbeidet styringssystemet for informasjonssikkerhet for Helse Nord. Et resultat av at dette er etablert i Helse Nord er at virksomhetene på en rekke området vil ha felles prosedyrer.

Som eksempler på innhold nevnes: Fysisk sikring, håndtering av informasjonssikkerhetsavvik, nødrutiner, pasientjournal, sikkerhetsinstruks, håndtering av pasientopplysninger lagret i medisin-teknisk utstyr med mer.

På bakgrunn av informasjonssikkerhetssystemet foreligger følgende elementer:

- 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

Som følge av innføring av styringssystemet har e-læringskurs blitt sendt ut til alle ansatte. Videre har informasjonssikkerhetsansvarlig hatt møte med alle klinikker våren 2015. I møtene ble det gitt orientering om prosedyrene innenfor informasjonssikkerhet.

ROS analyser

I forbindelse med implementering av styringssystemet for informasjonssikkerhet har klinikkene fått i oppdrag å gjennomgå de systemene som brukes av klinikken og som inneholder personopplysninger. Dette skal leveres til informasjonssikkerhetsansvarlig innen utgangen av juni 2015.

På bakgrunn av overnevnte vil vi få en oversikt over alle systemer i foretaket. Det vil da kunne gjøres en vurdering over de mest kritiske systemene og på den bakgrunn vil det kunne foretas en prioritering over hvilke systemer som skal ROS analyseres. Det planlegges å starte gjennomføringen av ROS-analysene i august 2015. Informasjonssikkerhetsansvarlig vil ha ansvar for gjennomføring av ROS analysene (se vedlagt handlingsplan).

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier sikres på en tilfredsstillende måte. Innenfor dette ligger det at systemet skal være tilgjengelig for helsepersonell når de trenger det for å yte helsehjelp. Videre skal opplysninger være konfidensielle, verdier og materiell skal ikke være tilgjengelig for uvedkommende. I tillegg skal informasjonen ha integritet, det vil si at det skal være sikret mot utilsiktet endringer eller sletting.

I kommende ROS analyser som skal gjennomføres til høsten vil det settes fokus på overnevnte tema.

I mange av FIKS og HOS programmets prosesser har det blitt gjennomført fortløpende risikovurderinger. Disse vurderingene fremkommer ikke som egne ROS-rapporter innenfor informasjonssikkerhet, men er innarbeidet i de løsninger som foreslås gjennomført. I 2015 er det gjennomført en ROS-analyse som omhandlet bruk av IRX Helsemail. Videre ble det i 2014 gjennomført en risikoanalyse innenfor informasjonssikkerhet for K-fløyen.

I 2014 ble det gjennomført revisjon av Nordlandssykehuset fra Norsk Helsenett. I rapporten ble det kommentert: «… det er god styring på informasjonsbehandlingen og sikkerheten i helseforetaket. Virksomheten fremviser god kompetanse innen sikkerhet og jobber systematisk med forbedring av denne»

Det ble avdekket 1 avvik som omhandler autentiseringsnivå for hjemmekontor. Det arbeides fortløpende med å få lukket avviket.

Databehandler/databehandleravtaler

NLSH har gjennomført revisjon av Helse Nord IKT den 11.november 2014. Tema for revisjonen var å kontrollere hvordan databehandlerrollen praktiseres med spesielt fokus på databehandleravtaler samt kontroll med 3. partsleverandører. Videre ble det kontrollert hvilke rutiner databehandler har etablert for tildeling av administratortilgang for deres ansatte til foretakets systemer for behandling av helseopplysninger/kliniske systemer. Det ble avdekket 5 avvik og 1 forbedringsforslag.

Konklusjonen var at databehandler hadde en god del på plass for området informasjonssikkerhet. Videre ble det avdekket at databehandleravtalen i dagens form ikke er i samsvar med dagens situasjon. Det arbeides fra Helse Nord IKT sin side å lage et forslag til ny databehandleravtale som skal kunne gjelde for alle foretakene i Helse Nord. Forslaget planlegges å bli sendt ut i august.

På bakgrunn av HOS-prosjektet er det inngått midlertidig samarbeidsavtale for deling av helseopplysninger mellom helseforetakene. Før en endelig avtale inngås skal det utredes nærmere hva som skal til for å ivareta informasjonssikkerheten, herunder at opplysningenes integritet styrkes og det er mulig å ivareta taushetspliktreglenes krav til konfidensialitet og tilgjengelighet.

De lovmessige kravene til databehandlere er nedfelt i databehandleravtalene. Enhver databehandler som skal behandle personopplysninger må ha konsesjon fra Datatilsynet for å kunne behandle slike opplysninger. Som følge av konsesjonen er databehandlere pålagt å følge lover, forskrifter samt Norm for informasjonssikkerhet.

På bakgrunn av systemgjennomgangen som klinikkene arbeider med vil vi få en oversikt over databehandlere og databehandleravtaler. Det planlegges å sette opp en matrise over databehandleravtaler som NLSH har inngått. Denne matrisen har som formål å få en lettere oversikt over alle databehandlere. Matrisen vil inneholde følgende punkter:

- Formål
- Behandlingsgrunnlag(lovhenvisning)
- Lagringsinformasjon
- Avdeling/klinikk
- Systemeier
- Databehandler/behandlingsansvarlig

Innstilling til vedtak:

1. Styret tar saken til orientering.
2. Styret ber om å bli orientert om resultatene av det planlagte arbeidet med å få på plass en oversikt over databehandlere og databehandleravtaler og gjennomførte ROS - analyser innen februar 2016.

Avstemming:

Vedtak:

Vedlegg 1 – Fremdriftsplan

Tidsrom	Aktivitet	Ansvarlig	Utførende	Gjennomført
Jan.2015	Informasjon om styringssystemet og implementeringen – informasjon til lederteamet	Direktøren	KIP og informasjonssikkerhetsansvarlig	Utført
Jan-Feb 2015	Opprette ei arbeidsgruppe pr.klinikk for gjennomføring og samordning av felles rutinger, samt utvelgelse av arbeidet med ROS analyser	Klinikksjef	Klinikksjef	Utført
Feb – Mar 2015	Gjennomføre e-læring i informasjonssikkerhet (målgruppe: Foretaksledelsen og øvrige ledere)	Direktøren	Informasjonssikkerhetsansvarlig	Utført
Feb. 2015	Avtale møtetidspunkt med klinikkene for gjennomgang av styringssystemet	Klinikksjef	Klinikksjef og informasjonssikkerhetsansvarlig	Utført
Feb – Mar 2015	Informasjonsmøte med gjennomgang av styringssystemet med klinikkene - Orientere om endrede/nye prosedyrer og hva dette innebærer	Klinikksjef	Informasjonssikkerhetsansvarlig	Utført
Feb-Jun 2015	a)Systemkartlegging av arbeidsgruppen	Klinikksjef	Arbeidsgruppe	Pågående
	b) Kontroll om at informasjonssikkerhetsavvik er inkludert i avdelingens avviksrutiner, se Docmap: DS6280.	Klinikksjef	Arbeidsgruppe og ev. informasjonssikkerhetsansvarlig	Pågående
	c) Orientere øvrige ansatte om styringssystemet	Klinikksjef	Avgjøres av klinikksjef	Pågående
Mars-Jun.2015	Iverksette gjennomføring av E-læringskurset i informasjonssikkerhet for øvrige ansatte	Klinikksjef	Øvrige ansatte	Utført
Juni 2015	Avmelding at styringssystemet er implementert til informasjonssikkerhetsansvarlig	Klinikksjef	Arbeidsgruppe	

Aug. 2015 - løpende	**a)Gjennomføring ROS-analyser på fag spesifikke kliniske systemer** **b) Gjennomføring ROS-analyser på fellessystemer**	**Klinikksjef KIP**	**Arbeidsgruppe med evt. bistand fra informasjonssikkerhetsansvarlig** **Informasjonssikkerhetsansvarlig**	