NORDLANDSSYKEHUSET
NORDLÁNDA SKIPPIJVIESSO

Direktøren

Styresak 107-2017
Orienteringssak - Informasjonssikkerhet - status pr desember 2017

Saksbehandler:	Alisa Larsen
Dato dok:	05.12.2017
Møtedato:	12.12.2017
Vår ref:	2015/1426

Vedlegg (t):

Innstilling til vedtak:

1. Styret tar saken til orientering.
2. Styret ber om å bli orientert om fremdrift på bestillingen fra Helse Nord RHF med status på tiltak.
3. Styret ber om å bli presentert en redegjørelse for fjernlagerløsningen.

Bakgrunn:

I styresak 040-2017 ble følgende vedtatt:

- Styret ber om å bli orientert om fremdrift på bestillingen fra Helse Nord RHF.
- Styret ber om å bli orientert om resultatene av ROS-analysene for MTU med status på tiltak innen utgangen av desember 2017.
- Med henvisning til aktuell global virus-hendelse ønsker styret ved Nordlandssykehuset en redegjørelse fra Helse Nord RHF mht hvilket behov og løsning man har for fjernlagerløsning for de kliniske data som driftes ved de regionale datasenter.

Helse Nord RHF fremmet i november 2015 bestilling til foretakene om gjennomføring av ROS analyser innenfor informasjonssikkerhet med følgende innhold:

Risiko- og sårbarhetsvurderinger rundt hvert enkeltregister innen kategoriene nedenfor:

1. *Applikasjoner som hovedjournalsystem og spesialistmoduler*
    - *Hovedjournalsystem (DIPS)*
    - *Laboratoriesystemer*
    - *Røntgensystemer*
    - *Spesialistmoduler som er egne applikasjoner med et spisset medisinsk spesialistfokus*
2. *Registre som etableres av resultater/prøver/tester fra medisinsk teknisk utstyr, og som lagres i egne strukturerte registerløsninger levert av samme leverandør som har levert MTU.*

3. *Enkle databaser/registre/skåringsverktøy som i begrenset grad kan kalles en applikasjon, men som klart er behandlingsrettede registre. Dette dekker registre/databehandlinger ned til 2-3 brukere. Disse inneholder fokuserte og strukturerte deler av journalen, der nødvendig struktur på informasjonen ikke kan oppnås i de mer generelle og overordnede journalapplikasjonene. De er i noen grad etablert i foretakets registerstøtteverktøy, men også i enkle databaser/Excel-ark som den enkelte kliniker selv har etablert. Mange slike småsystem registreres som kvalitetssystem. Relevante data registreres også i DIPS, som er den formelle journalen.*

Arbeidet med risikoanalysene har blitt utført løpende siden bestillingen ble fremmet.

1. Status på fremdrift og status på tiltak MTU

1.1. Fremdrift punkt 1 - Hovedjournalsystemer

Punkt 1 i bestillingen fra Helse Nord RHF ble rapportert i styresak 040-2017. Risikovurderingene er gjennomført og tiltakene er lukket.

1.2. Fremdrift punkt 2 - MTU

Innenfor punkt 2. i bestillingen fra Helse Nord RHF ble det i juni 2016 startet arbeid med å kartlegge MTU. I kartleggingsarbeidet er det tatt utgangspunkt i *«Veileder i Personvern og informasjonssikkerhet – medisinsk utstyr»* utgitt av Helsedirektoratet i desember 2015.

Vi valgte å gruppere det medisintekniske utstyret i henhold til de kategoriene som veilederen beskriver. Her beskrives det totalt 16 kategorier. Det er fra det helt enkle scenario 1 «MU uten behandling av informasjon» til de mer teknisk komplekse der pasient selv, på eget initiativ hjemmefra, overfører data til skytjeneste (scenario 16). Medisinteknisk seksjon har kartlagt og kategorisert utstyret.

Etter at kartleggingen var ferdigstilt ble det gjennomført risikovurderinger. Alle risikovurderingene ble gjennomført i perioden 29.mars til 07.april.

Denne prosess har vist at det er en stor og relativt kompleks oppgave å skaffe seg oversikt over alt medisinsk utstyr, hvor dette er plassert og hvordan informasjonssikkerheten ivaretas. Et av grunnprinsippene i vår tilnærming var å finne en metodikk som muliggjør ikke bare å gi et korrekt bilde over status pr dags dato, men også bygge et system som gjør det mulig å vedlikeholde dette risikobildet på en forsvarlig måte framover.

Det har vært nedlagt et stort arbeid i seksjonen for medisin teknisk utstyr ved Nordlandssykehuset. Deres innsats med å registrere de enkelte utstyrsgruppene i forhold til de beskrevne scenarioene i veilederen har vært krevende både i volum og presisjon. Gjennom prosessen har arbeidsgruppen gjort en del erfaringer og det er gruppens erkjennelse at veilederen ikke er tilstrekkelig dekkende i forhold til gruppering av utstyr ved NLSH.

Dette problemområdet ble også adressert av forfatterne bak veilederen fra Direktoratet for Ehelse på kurs ved St Olav tidligere i år. Som følge av dette ba forfatterne bak veilederen arbeidsgruppen om å presentere våre funn ved kurs i informasjonssikkerhet for medisinteknisk personell i oktober i år. Basert på våre funn og erfaringer vil veilederen bli endret.

1.2.1 Tiltak MTU

Basert på gjennomgang av de ulike risikoanalysene har vi valgt å trekke fram de risikoelementene som enten har blitt vurdert i rød sone eller som er vurdert å være i gul sone på to eller flere risikoanalyser.

Sikring av utstyr

For mange av våre MU enheter, er det gjennomgående en risiko knyttet til at utstyret ikke har tilgangsstyring samtidig som de inneholder sensitive opplysninger. Her sier veilederen at det må vurderes i hvilket omfang tilgangsstyring skal tas i bruk for MU for å sikre at kun personell med tjenstlig behov får tilgang til sensitive opplysninger.

Videre balanserer veilederen dette gjennom å erkjenne at en del utstyr krever rask tilgang slik at tilgangsstyring ikke alltid lar seg gjennomføre, eller er medisinsk forsvarlig. Et eksempel på dette vil være hjertestartere i bruk hos ambulansetjenesten. Krav til tilgangsstyring gjennom pålogging vil i en akuttsituasjon kunne ha direkte negativ effekt på pasientbehandlingen.

Med gode rutiner for sletting av informasjon etter bruk vil behovet for fysisk sikring kunne reduseres. Det er utformet prosedyre for å ivareta dette kravet. Prosedyren er på nåværende tidspunkt på høring, og det forventes at denne kan være godkjent i desember.

Behandlingshjelpemidler til bruk i hjemmet

Behandlingshjelpemidler som pasient får med seg hjem kan inneholde sensitive opplysninger. Pasienten er selv ansvarlig for hvordan vedkommende håndterer utstyret. Foretaket bør informere pasient om at vedkommende bør ivaretar utstyret slik at sensitive opplysninger ikke havner på avveie. Det er utformet prosedyre for å ivareta dette kravet og de ansatte som deler ut behandlingshjelpemidler er gjort kjent med denne. Prosedyren er på nåværende tidspunkt på høring, og det forventes at denne kan være godkjent og iverksettes i desember.

Ekstern håndtering av opplysninger

Utstyr som har muligheten for ekstern tilgang fra leverandør via VPN, skyløsninger, lokal support på stedet osv. har en usikkerhet knyttet til hvordan sensitive opplysninger blir ivaretatt. Som foretak er vi til tider avhengig av at utenforstående aktører (leverandører, teknisk bistand) får tilgang til MU som inneholder sensitive opplysninger. Problemstillingen er knyttet til hvordan vi sikrer oss at disse aktørene opptrer aktsomt og i tråd med de lovkrav som gjelder. Dette sikres gjennom databehandleravtaler og analysen viser noen mangler.

Vi har startet prosessen med å inngå manglende databehandleravtaler med aktuelle leverandører for å sikre at informasjonssikkerheten blir ivaretatt. Videre har vi presisert eksisterende rutiner for hvordan databehandleravtaler skal utformes og etableres.

I tillegg har vi i handlingsplanen for informasjonssikkerhet i Helse Nord for 2018 planlagt sikkerhetsrevisjoner på leverandører.

1.3. Fremdrift punkt 3 - Øvrig

I henhold til kulepunkt tre i bestillingen har vi til nå gjennomført åtte risikovurderinger. Utvalget av risikovurderinger har hatt følgende prioriteringsfaktorer:

- Omfang – volum av brukere og personer registrert i systemet
- Bruksområde – Grad av kjent sensitiv informasjon som ligger i systemene

Det planlegges ytterligere to risikovurderinger for å dekke dette. Disse planlegges gjennomført første kvartal 2018.

2. Vedtakspunkt 4 fra styresak 040-2017

Med henvisning til aktuell global virus-hendelse ønsker styret ved Nordlandssykehuset en redegjørelse fra Helse Nord RHF mht hvilket behov og løsning man har for fjernlagerløsning for de kliniske data som driftes ved de regionale datasenter.

Dette gjelder regional løsning etablert av Helse Nord. Vi har derfor bedt om en redegjørelse fra Helse Nord for å få beskrevet hvordan en slik løsning er etablert. Basert på denne redegjørelsen kan vi gjøre en vurdering om dette dekker vårt beredskapsbehov og krav til informasjonssikkerhet. Vi ba om svar fra Helse Nord i tide til å kunne presentere dette til denne styresak. Svar fra Helse Nord er imidlertid ikke mottatt.