NORDLANDSSYKEHUSET
NORDLÁNDA SKIPPIJVIESSO

Direktøren

Styresak 040-2017
Orienteringssak - informasjonssikkerhet - status pr april 2017

Saksbehandler:	Alisa Larsen
Dato dok:	28.04.2017
Møtedato:	15.05.2017
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.
3. Styret ber om å bli orientert om resultatene av ROS-analysene for MTU med status på tiltak innen utgangen av desember 2017.

Bakgrunn

Vedtak fra styresak 106-2016:

- Styret ber om å bli orientert om resultatene av ROS-analysene med status på tiltak innen utgangen av juni 2017.

Oppdragsdokument 2017 – Fra Helse Nord RHF til helseforetakene:

- Området informasjonssikkerhet med status på risiko- og sårbarhets (ROS)-analyser skal behandles av helseforetakets styre innen 01.06.17. Styresaken skal beskrive om databehandler oppfyller krav i lover og forskrifter som er tillagt databehandlerrollen, og om nødvendige krav er nedfelt i leveranseavtaler.

Innledning

Helse Nord RHF har i november 2015 fremmet 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.

Status pr. april 2017

Punkt 1 i bestillingen ble prioritert først. Pr utgangen av april 2017 har vi i gjennomført analysene i hht fremdriftsplanen som ble fremlagt styret i styremøte 16.02.16. Noen få datoer er blitt endret, men helhetlig framdrift har vært tilfredsstillende. De analyser som er planlagt gjennomført innenfor bestillingens punkt 1 er ferdige.

Vi har valgt bort to planlagte analyser. Dette gjelder DIPS for Diagnostisk klinikk. Begrunnelsen for dette er at klinikken i svært liten grad benytter seg av DIPS EPJ. Klinikken benytter DIPS LAB i arbeidet. En analyse av DIPS EPJ hos denne klinikken vil derfor ha svært liten verdi. AMK-113 er også valgt bort. Dette er på grunn av at dette ikke er et journalsystem. Det planlegges at AMK-113 blir med i vurderingen for bestillingens punk 3.

Informasjonssikkerhetsansvarlig har sammen med klinikkene vært ansvarlig for at ROS-vurderingene har blitt gjennomført i hht fremdriftsplan. Analysene har blitt dokumentert i verktøyet What If.

Tiltak

En risiko som ikke anses for å være akseptabel og som er avdekket i alle analysene er manglende loggkontroller. Kravet dekkes av den regionale prosedyren for kontroll av logger PR1573. Prosedyren legger imidlertid ikke føringer for hvem som har ansvar for gjennomføringen. På nåværende tidspunkt har KIP påtatt seg ansvaret for å gjennomføre kontrollene. Interne prosedyrer hos NLSH for ansvarsforhold og gjennomføring er enda ikke ferdige, det avventes derfor med å lukke tiltaket.

Videre er det i enkelte klinikker avdekket at ansatte låner tilganger hos hverandre. Dette skjer gjerne i tilfeller der vikarer har mistet tilgangene sine og for å få arbeidet gjort må de låne tilganger hos andre ansatte. Dette er forhold som kan løses av hver klinikk med bedre oppfølging fra de som tildeler tilganger. Tiltakene er lukket hos de klinikkene som omfattet av denne problemstillingen. Det er også avdekket forhold der ansatte beholder tilganger dersom de endrer arbeidsområde/slutter. I de tilfellene der denne risiko har blitt avdekket, har ledere blitt gjort kjent med prosedyre for oppfølging av tilganger samt gitt en frist for å rydde i tilganger. Tiltakene er lukket hos de klinikkene som omfattet denne risikoen.

De øvrige risikoene som er avdekket og som er vurdert til ikke å være akseptable har raskt blitt møtt med tiltak. Dette gjelder f.eks. fysisk sikring av skrivere, sikring av arbeidsstasjon og sletting av tilganger.

Fremdrift øvrig bestilling

Innenfor punkt 2. i bestillingen fra Helse Nord RHF ble det i juni 2016 startet arbeid med å kartlegge MTU. Dette arbeidet har tatt lengre tid enn først antatt grunnet kompleksitet og antall MTU enheter i NLSH. (2 500 ulike utstyrstyper, 22 000 enheter I kartleggingsarbeidet er det tatt utgangspunkt i *«Veileder i Personvern og informasjonssikkerhet – medisinsk utstyr»* utgitt av Helsedirektoratet i desember 2015.

Vi har valgt 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.

Pr. utgangen av april er alle planlagte risikoanalyser innenfor dette punkt gjennomført hos NLSH. De siste analysene er nylig gjennomført og vi utarbeider nå rapporten som skal vise full oversikt over alle tiltakene.

En noe overordnet risiko som har blitt avdekket for MTU er at det foreligger uklare ansvarsforhold når det gjelder inngåelse av databehandleravtaler. NLSH har ikke klare rutiner for hvem som er ansvarlig for at det inngås databehandleravtaler på MTU og oppfølging av disse. Det arbeides på nåværende tidspunkt med å kartlegge ansvarsforholdene.
Innenfor punkt 3. i bestillingen fra Helse Nord RHF er vi i planleggingsfasen. Vi legger opp til en gjennomgående kartlegging og registrering av registre/verktøy på hver klinikk før vi gjennomfører analysene.

En samlet rapport for alle analysene i hht bestillingen fra Helse Nord RHF vil bli presentert styret når bestillingens punkt 3 er gjennomført.

Revisjon av leverandører (Databehandlere)

Det er på nåværende tidspunkt gjennomført få revisjoner av leverandører. I 2014 ble det gjennomført revisjon av HN IKT. 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 som nå er lukket.

Konklusjonen fra revisjonen var at databehandler hadde en god del på plass for området informasjonssikkerhet. Videre ble det avdekket at databehandleravtalen ikke var oppdatert i hht lovverket. Det ble på den bakgrunn inngått ny databehandleravtale i 2015.

Når risikoanalysene i bestillingen fra Helse Nord er gjennomført vil vi ha en god oversikt over alle øvrige databehandlere og tilhørende databehandleravtaler som vi vil bruke i gruppering og planlegging av revisjoner av de ulike leverandører/databehandlere.

Fagråd for informasjonssikkerhet(FRIS) planlegger å revidere leverandører sammen på de systemene som er regionale.