HELSE FONNA

STYRESAK

GÅR TIL: Styremedlemmer
FØRETAK: Helse Fonna HF

DATO: 12.12.17
FRÅ: Olav Klausen
SAKSHANDSAMAR: Kenneth V. Førland, Ingebjørg Kismul
SAKA GJELD: **Leiinga sin gjennomgang av informasjonstryggleik**

STYRESAK: **92/17**

STYREMØTE: **19.12.17**
1 vedlegg

FORSLAG TIL VEDTAK

Styret tar leiinga sin gjennomgang av informasjonstryggleik til orientering

Bakgrunn for saka

Gjennomgangen av informasjonstryggleik er ein kontroll av status på tryggleiksnivået innan IKT i Helse Fonna HF, og om dette er i samsvar med føretakets behov og lovpålagte krav. IKT-sikkerhetsleiar i føretaket utarbeider ein rapport årleg som går gjennom viktige avvik.

Handtering av personopplysningar er regulert i «Norm for informasjonssikkerhet i Helse og omsorgstjenesten».

«Normen» er utarbeidd av organisasjonar i sektoren med sikte på å bidra til tilfredstillande informasjonstryggleik i den einskilde verksemd og i sektoren generelt, samt å bidra til å etablere mekanismar kor verksemdene kan ha gjensidig tillit til at andre verksemder si behandling av helse- og personopplysningar blir gjennomført på eit forsvarlig tryggleiksnivå.

Kommentar
Som vedlegg til saka er leiingas gjennomgang av informasjonstryggleik.
I tre kapittel blir det gjort greie for:

1. Beredskapsøvingar
I dette kapittelet blir det informert om hendingar i 2017 knytt til IKT som har omfatta system for pasientjournal, telefoni, alarmløysningar og datanettverk. Det blir vist til erfaringar som grunnlag for planlegging ved nye innføringar og scenario ved beredskapsøvingar.

2. Utanlandske leverandører.
I dette kapittelet blir det informert om prosess ved utarbeiding av avtalar og tryggleik i løysningar med utanlandske leverandørar.

3. Førebygging av tryggleiksbrot og datakriminalitet.
I dette kapittelet blir det informert om resultat av testing av datanettverk og system i Helse Vest.

Konklusjon

Administrasjonen er av det syn at utviklinga innanfor IKT-sikkerhet er tilfredstillande. Samstundes vil administrasjonen understreke at det er særs viktig å vidareføre og forsterke dette arbeidet. Det er diverre sannsynleg at omfang av datakriminalitet vil auke og/eller vil kunne flytte seg frå andre sektorar.

Vedlegg
Leiingas gjennomgang av informasjonstryggleik

HELSE FONNA

2017

Ledelsens gjennomgang

Informasjonssikkerhet

v/IKT-sikkerhetsleder Kenneth Velde Førland

Innhold

1. Nødvendigheten av beredskapsøvelser 3

2. Bruk av utenlandske leverandører 4

3. Forebygging av sikkerhetsbrudd og datakriminalitet..... 5

1. Nødvendigheten av beredskapsøvelser

Det er viktig å planlegge for håndtering av beredskapshendelser. Forekomster av hendelser innenfor IKT er sannsynlig. Dette er basert på erfaringer de siste årene, og vurdert risikobilde for IKT.

Det er viktig at det gås gjennom ulike scenarioer når en skal øve på beredskapen. Da får helsepersonell øvd på å håndtere sine viktige oppgaver uansett hvilke uønskede hendelser som pågår.

Det siste året har vi opplevd ulike hendelser knyttet til IKT. Dette har vært hendelser som blant annet har omfattet system for pasientjournal, telefoni- og alarmløsninger og datanettverk.

Ved hendelser knyttet til system for pasientjournal, har dette påvirket kapasitet i systemet og tilgjengelighet. Helsepersonell har nødrutiner for å håndtere slike uforutsette hendelser, men dette krever mer ressurser og planlegging i pasientbehandlingen. IKT-personell har også nødrutiner når det oppstår problemer med systemet. Dette innebærer feilretting, og å forberede nødløsninger slik helsepersonell fortsatt har pasientjournaler tilgjengelig i en forenklet form, med pasientkritiske opplysninger.

Helse Fonna har gjennomført planlagt oppgradering av telefoni- og alarmsystem. Dette arbeidet ble utført av vår leverandør Helse Vest IKT. Det ble satt sammen en arbeidsgruppe bestående av ressurser fra både leverandør og foretaket. Arbeid med planlegging og forberedelser av oppgradering ble gjennomført flere måneder i forveien. Forberedelser omhandlet kvalitetssikring og testing av alle alarmtyper og reserveløsninger. Alle klinikker og seksjoner ble involvert i dette arbeidet. De gjorde en god jobb med å kartlegge behov, og avdekke arbeidsprosesser som fikk konsekvenser i denne oppgraderingen.

I gjennomføring av oppgradering, oppstod uforutsette hendelser, som vi i etterkant lærte hadde liten konsekvens for pasientbehandlingen. Likevel var det viktig å bruke mye ressurser på feilrettingen. Vi var godt bemannet under oppgraderingen og planla for at det ville oppstå hendelser som en ikke kunne forutse. Dette er gode tiltak som er viktig i slikt arbeid som kan ha stor konsekvens for sykehusene.

Erfaring fra denne oppgraderingen er at det er nødvendig å bruke god tid på planlegging, ha med nok ressurser, ha fokus på alle typer feil som oppstår, slik at ingenting blir "glemt" i det store. Det en anser som små feil og hendelser, kan ha stor betydning for helsepersonellet i sitt arbeid.

Oppgraderingen var veldig positiv for foretaket. Det ble avdekket flere arbeidsprosesser som var utsatt, og som nå har fått gode nødrutiner. Foretaket er godt rustet til å håndtere hendelser knyttet til telefoni- og alarmsystemer.

Den største trusselen knyttet til IKT, er bortfall av datanettverk, eller andre forhold som bryter tilgjengeligheten til IKT-løsninger. Dette påvirker tilgang til viktige systemer, og viktig utstyr som blir benyttet i pasientbehandlingen. Slike hendelser er veldig alvorlige, og kan kreve mye koordineringsarbeid og informasjonsarbeid, slik at helsepersonellet kan tilpasse seg situasjonen.

På bakgrunn av dette er det viktig å ha reserveløsninger og gode nødrutiner. Det er også viktig at en etter beste evne, tilpasser løsninger og utstyr slik at disse ikke blir påvirket i stor grad. Dette arbeidet er komplisert på det tekniske nivå, det er også kostnadsrammer knyttet til dette.

Mange av tiltakene knyttet til alvorlige hendelser innen IKT, innebærer innøvde nødrutiner. Helsepersonellet må øve på ulike scenarioer, og det må være fokus på det som fungerer bra, og det som ikke fungerer, for å ta lærdom av erfaringene, og gjøre forbedringer.

2. Bruk av utenlandske leverandører

I 2016/17 har foretaket arbeidet med vurdering av programvare, der en utenlandsk leverandør er en av aktørene, for anskaffelse og innføring. Denne programvaren leveres av norsk leverandør, som benytter underleverandør i Frankrike for lagring av data i løsningen.

Programvaren er ønsket fra helsepersonell, men fordi løsningen lagrer data i utlandet, er ikke dette ønskelig for foretaket. Leverandør ble informert om dette, og anmodet om å endre løsningen slik at lagring av data foregår i Norge. Leverandør kunne ikke møte oss på dette ønsket for aktuell løsning, men tar dette til betraktning for fremtidige løsninger.

I arbeidet for vurdering av løsning har vi kontrollert sikkerheten i løsningen og sett nærmere på de involverte leverandørene. I tillegg er også bruksområdet vurdert for denne løsningen, som innebærer nødvendigheten/behovet, andre alternativer og om vi på noen måte kan unngå å benytte denne løsningen i pasientbehandlingen. Arbeidet pågikk over flere måneder, hvor berørt helsepersonell var involvert, samt leverandør. Leverandør har vært ryddig, imøtekommende og grundig i dette arbeidet, slik at vi har fått tillit til leverandør og løsning. Det er også søkt råd fra Datatilsynet for bruk av denne løsningen, og nødvendige avtaler som må inngås ved en eventuell anskaffelse.

Resultatet av dette arbeidet har vist at det er behov for at pasienter som omfattes av behandling som benytter denne løsningen, må gjøres oppmerksom på hva dette innebærer, og hvilken konsekvens dette får for pasienten. Helsepersonell innhenter skriftlig godkjenning fra pasienten. Pasienten kan velge å ikke benytte seg av dette tilbudet uten at dette får konsekvens for pasientbehandlingen. Pasienten vil få samme behandlingstilbud selv om denne løsningen ikke benyttes av helsepersonellet.

Med grunnlaget fra vurderinger og risikovurdering som er utført, har vi besluttet å gå videre med anskaffelse og innføring av løsningen. Det pågår arbeid med nødvendige avtaler og forberedelser knyttet til innføring av løsning. Leverandør i Norge og underleverandør i Frankrike, er involvert i dette arbeidet.

Før denne anskaffelsen hadde foretaket ingen direkte avtaler med leverandører i utlandet, eller bruk av leverandører som lagrer opplysninger i utlandet. Prosessen som foretaket har gjennomgått i denne anskaffelsen, har foretaket til hensikt å fortsette med for lignende anskaffelser i fremtiden. Det er et klart behov for å foreta grundige vurderinger når det oppstår slike tilfeller og behov.

3. Forebygging av sikkerhetsbrudd og datakriminalitet

Årlig gjennomføres det omfattende testing av datanettverk og systemer i Helse Vest. Testen gjennomføres av Norsk Helsenett sitt HelseCERT, på oppdrag fra Helse- og omsorgsdepartementet. Oppdraget deres er å teste sikkerheten i helsesektoren. I praksis innebærer dette at HelseCERT foretar dataangrep/inntrengningstest (hacking) mot sykehusenes nettverk og systemer. Det er i denne inntrengningstesten forventet å avdekke sårbarheter, og dette er positivt for arbeid med å bedre datasikkerheten.

En slik testing av datasikkerheten til sykehusene er krevende arbeid. Det skal ikke påvirke driften på sykehuset, samtidig som det er viktig å få avdekket potensielle sårbarheter som kan gi store konsekvenser. Det kreves nøye planlegging i forkant, og flere fagmiljø involveres i dette arbeidet.

I 2016 ble det i forbindelse med dette arbeidet, avdekket svakheter som krevde tiltak fra både foretaket og vår leverandør Helse Vest IKT. Det ble avsatt ressurser i foretaket og hos Helse Vest IKT for å planlegge og å rette opp i det tekniske som var årsak til svakheten.

Tidligere i år ble helsesektoren rundt om i verden mål for dataangrep. Dataangrepet rammet også andre sektorer, helsesektoren fikk store konsekvenser som følge av denne hendelsen. Spesielt i Storbritannia ble datamaskiner utsatt og gjort utilgjengelig for helsepersonell. I Norge ble det registrert samme type angrep, men uten konsekvens. Datasikkerheten på datamaskiner i Helse Vest er konfigurert på en slik måte at den type angrep ikke sprer seg videre mellom datamaskiner. Det er også tekniske hinder for at ondsinnet programvare kan infisere og installeres på datamaskiner og skape konsekvenser for system og nettverk i Helse Vest.

Ansatte i Helse Vest er pålagt å gjennomføre sikkerhetskurs annethvert år. Avdelingsledere er ansvarlig for at dette etterfølges. Tidligere tok det lang tid mellom hver gang dette kurset ble oppdatert. Nå følges dette arbeidet etter planlagt årshjul, hvor innholdet blir kontrollert og spisset for det som er aktuelt for helsepersonell å ha fokus på.

Det avdekkes jevnlig feilbruk og misforståelser fra ansatte om bruk av datasystemer. Dette fanges opp via kundesenteret i Helse Vest eller fra overvåking av system og nettverk. Det er forventet at ansatte er ytterste ledd og svakeste ledd, når det gjelder informasjonssikkerhet. Da er det viktig med forebyggende arbeid som jevnlig kursing, og bevisstgjøring når det oppstår situasjoner med feilbruk eller misforståelser. I noen tilfeller dreier dette seg om misbruk, som det også er rutiner for å avdekke.

Det er mange ulike momenter som truer informasjonssikkerhet, derfor er det viktig at dette er et kontinuerlig fokusområde for foretaket og tilknyttede leverandører.