SYKEHUSET ØSTFOLD

Notat

Vår dato
12.02.2021

Utarbeidet av
Lars Cato Skaar

Deres dato
12.02.2021

Til

Innlegg fra Sykehuset Østfold HF v/ adm. direktør Hege Gjessing

Sykehuset Østfold (SØ) er glad for at Riksrevisjonen gjennomførte revisjonen hos oss fordi det gir viktige målepunkter i arbeidet med informasjonssikkerhet.
Denne revisjonen viser at vi har et godt sikkerhetsnivå i SØ samtidig som funnene viser at vi må fortsette det viktige arbeidet med å forbedre informasjonssikkerheten.

Roller og ansvar innen informasjonssikkerhet

Vi opplever at roller og ansvar for informasjonssikkerhet i regionen er tydelig avklart og godt definert. Databehandleravtalen mellom SØ og Sykehuspartner definerer SØ som dataansvarlig og Sykehuspartner som databehandler.
Denne rollefordelingen har vært gjeldende siden opprettelsen av Sykehuspartner. Samhandlingen om informasjonssikkerhet begynte for oss under byggeprosjektet for nytt sykehus på Kalnes ved at Sykehuspartner i 2013 fikk oppdraget med å risikovurdere alle løsninger som skulle anskaffes til det nye sykehuset. Risikovurderingene ble presentert for vår informasjonssikkerhetsleder som forankret vurderingene hos egen ledelse. Denne måten å samarbeide på er fortsatt den samme selv om både rutiner og maler har blitt forbedret over tid.

Risikovurderingene har over tid blitt både mer detaljerte og omfangsrike. SØ er allikevel innforstått med at en risikovurdering aldri kan dekke alle risikoene fullt ut. Kontinuerlige forbedringsprosesser (revisjoner,

Postadresse
Sykehuset Østfold
Juridisk avdeling
Postboks 300, 1714 Grålum

Besøksadresse Tuneteknikeren, Tuneveien 20, 1710 Sarpsborg
Telefon 977 37 915
Org.nr. NO 983 971 768 MVA
E-postadresse lars.cato.skaar@so-hf.no
www.sykehuset-ostfold.no

avvikshåndtering, Sykehuspartner sikkerhetsfunksjon etc) er med på å redusere ukjent risiko.

HSØ som sykehusets eier har fastslått at Sykehuspartner har ansvar for sikkerheten i IKT-infrastrukturen og at SØ må følge de bruksvilkår som Sykehuspartner fastsetter. Det er allikevel slik at SØ har et selvstendig ansvar for å vurdere risiko. Fordelen med denne modellen er det gode sikkerhetsmiljøet som er etablert i Sykehuspartner og som vi ikke ville klart å etablere lokalt i de enkelte sykehusene.

Sikkerhetsnivå

Det regionale samarbeidet innen informasjonssikkerhet foregår på flere plan. Informasjonssikkerhetsledere har eget forum, Regionalt Sikkerhetsfaglig Råd (RSR) for å diskutere aktuelle tema, og de deltar også i Regionalt SikkerhetsVurderingsteam (RSV) hvor Sykehuspartner presenterer risikovurderinger for felles diskusjon.
I tillegg er det etablert blant annet IKT-lederforum, MTU-lederforum og systemeierforum hvor informasjonssikkerhet også er tema.

Ledelsessystem for informasjonssikkerhet

Ledelsessystem for informasjonssikkerhet er etablert i Helse Sør-Øst og det er utarbeidet i fellesskap i regionen. Systemet er innført i hvert enkelt sykehus slik at det er en del av virksomhetsstyringen i sykehusene.
I SØ opplever vi derfor at HSØ legger til rette for at sykehusene kan opprettholde et forsvarlig sikkerhetsnivå gjennom styrende, utøvende og kontrollerende dokumenter og aktiviteter.

Teknisk infrastruktur

SØ ble tilknyttet den regionale infrastrukturplattformen SIKT i 2013 og nytt lokalt datanettverk ble installert hos oss i 2014/15, i tett samarbeid med Sykehuspartner. Vi bestilte Norsk Helsenett til å gjøre en sikkerhetstest av infrastrukturen i 2017 med tilsvarende formål som Riksrevisjonens sikkerhetstester.

Infrastrukturen inkluderer sterke, logiske skiller mellom lokale datasystemer, herunder medisinsk teknisk utstyr.

Riksrevisjonens resultater viser at sikkerhetsmekanismene i all hovedsak fungerer som tiltenkt ved SØ. Testene viste blant annet at medisinsk teknisk utstyr (MTU) og server-infrastruktur var tilstrekkelig beskyttet. Revisjonsrapporten påpekte to funn for SØ. Dette var kjente funn som er akseptert etter risikovurderinger. Sykehuspartner og SØ har allikevel innført tiltak for å redusere risikoen ytterligere.

Beredskapsplaner

Dersom driftsbrudd på kritiske IKT-systemer oppstår vil etablerte nødrutiner, såkalte manuelle rutiner, iverksettes på hver enkelt avdeling for å opprettholde pasientbehandlingen, mens feilretting pågår.

Informasjonssikkerhetskultur og ledelsens årlige gjennomgang av informasjonssikkerhet

I 2011 lagde vi *Kompetanseprogram for informasjonssikkerhet* og har siden jobbet kontinuerlig med å sikre at medarbeidere følger retningslinjene. Vi er opptatt av informasjonssikkerhetskultur og informasjonssikkerhetslederen vår har skrevet masteroppgave om dette. Riksrevisjonens rapport fremhever informasjonssikkerhetskulturarbeidet som godt ved SØ.

Rapporten trekker også fram ledelsens gjennomgang av informasjonssikkerhet ved SØ som et positivt funn. I etterkant av revisjonen har vi økt antallet formelle gjennomganger og vi har også hyppigere gjennomganger av aktuelle problemstillinger. Ledelsens gjennomgang av informasjonssikkerhet er presentert for styret ved SØ og er lagt inn som rutine.