SYKEHUSET ØSTFOLD

Datatilsynet

Vår dato: 15.06.2017
Deres ref.: 16/01531

Vår saks-behandler: Informasjonssikkerhetsleder Lars Cato Skaar

Vår ref: 17/02156

Redegjørelse vedrørende avtale om bruk av ekstern leverandør under Sykehuspartner innenfor IKT-infrastrukturtjenester

1. Innledning

Vi viser til brev datert 26.05.17 med krav om redegjørelse vedrørende avtale om ekstern leverandør innenfor IKT-infrastrukturtjenester.

Datatilsynets brev er sendt til samtlige helseforetak i Helse Sør-Øst som driver sykehusvirksomhet / pasientbehandling. Samtlige helseforetak i Helse Sør-Øst har Sykehuspartner HF som felles IKT-leverandør. Kontrakten med ekstern leverandør er inngått av Sykehuspartner HF, og ekstern leverandør vil være en underleverandør til Sykehuspartner HF som fortsatt er og vil være ansvarlig leverandør overfor helseforetakene. Som følge av dette, er risikovurderinger etc gjennomført i fellesskap for hele foretaksgruppen. Det er derfor utarbeidet likelydende / felles svar fra helseforetakene på de forhold som er felles / like.

Det understrekes innledningsvis at prosjektet inkludert virksomhetsoverdragelse og overdragelse av driftsansvar fra Sykehuspartner til ekstern leverandør, p.t er stilt i bero, jfr styret i Helse Sør-Øst RHF sitt vedtak 24.05.17 i sak 058/2017. Videre har Sykehuspartner HF fått i oppdrag blant annet å utarbeide en plan for styrket tilgangsstyring og en bedre metodikk for risiko- og sårbarhetsanalyser, samt utrede mulige alternativer for etablering av modernisert IKT-infrastruktur. Protokoll fra foretaksmøtet i Sykehuspartner av 31.05.17 der både styret for Helse Sør-Øst RHF sitt vedtak av 24.05.17 og oppdraget som nå er gitt til Sykehuspartner HF fremgår, vedlegges.

Vedlegg 1: Protokoll fra foretaksmøte i Sykehuspartner 31.05.2017
https://www.helse-sorost.no/Documents/Styret/Foretaksmøter/2017/20170531-1000%20Protokoll%20(foreløpig)%20–%20Sykehuspartner%20HF.pdf

Postadresse
Sykehuset Østfold
Fag og utvikling
IKT-avdelingen
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

Generelt bemerkes at det foreligger et felles styringssystem for informasjonssikkerhet i regionen, som forutsetter gjennomføring av risikovurdering i forkant for beslutninger om endringer som kan påvirke risiko og trusselnivå. For å avgjøre om gjenværende risiko er akseptabel, vil tekniske løsninger og håndtering av restrisiko måtte vurderes. Gjennomføring av risikovurdering vil dermed måtte gjennomføres stegvis ettersom faktisk informasjon om en løsning avklares.

Bakgrunnen for beslutningen om å benytte ekstern leverandør, er en kombinasjon av regionens klare behov for oppgradering og fornying av infrastrukturen, og det at fremtidige fellesregionale løsninger vil kreve meget store investeringer i infrastruktur. Eksisterende infrastruktur er fragmentert og til dels utdatert og vurderingen var at en modernisering i egen regi ville ta lengre tid enn ved bruk av ekstern leverandør. Kombinasjonen av de store investeringene som kreves fremover for å opprettholde et forsvarlig nivå på infrastruktur, samt de store investeringene som kreves for å gjennomføre de funksjonelle programmene ledet frem til beslutningen om å benytte en ekstern leverandør i dette arbeidet.

2. Redegjørelse

2.1 Risikovurderingen samt redegjørelse for akseptanse av restrisiko jf. personopplysningsforskriften § 2-4 jf. pasientjournalloven§ 22 som ble lagt til grunn da det ble besluttet at drift og leveranse av IKT-infrastrukturen i helseregionen skulle tjenesteutsettes.

I henhold til personopplysningsforskriften § 2-4 skal det utarbeides risikovurdering når det skal behandles personopplysninger. Det samme gjelder ved endringer som har betydning for informasjonssikkerheten. Risikovurdering må foretas før behandling av personopplysninger iverksettes eller før man iverksetter endring som kan ha betydning for informasjonssikkerheten. Det fremgår ikke av bestemmelsen i § 2-4 at slik vurdering må være foretatt før det tas beslutning om at arbeid med konkurranseutsetting skal påbegynnes. Det vil heller ikke være mulig å fullføre en risikovurdering før omfanget av tjenesteutsettingen, status på informasjonssystemene og kravene som vil bli stilt til informasjonssikkerhet og -tiltak hos leverandøren er nærmere avklart.

Helseforetakene som databehandlingsansvarlige har i en årrekke benyttet Sykehuspartner som databehandler. Tjenesteutsettingen som Datatilsynet refererer til, gjelder en ny underleverandør til Sykehuspartner som selv opprettholder rollen som primærdatabehandler for helseforetakene. Sykehuspartner har allerede en rekke underleverandører, og hverken beslutning om eller inngåelse av kontrakt med ekstern leverandør, innebærer etter vårt syn i seg selv en endring som krever risikovurdering i henhold til personopplysningsforskriften § 2-4.

Forut for beslutningen om å benytte en kommersiell aktør for å modernisere regionenes infrastruktur, gjennomførte DNV GL på vegne av regionen en risikovurdering av alternativer for modernisering av infrastrukturen. Alternativene som ble vurdert var «gjør det selv» eller «ekstern partner», og er presentert i rapporten «Risikoanalyse av alternativer for modernisering av infrastruktur».

> Vedlegg 2: Rapport fra DNV GL datert 30.08.2016, Risikoanalyse av alternativer for modernisering av infrastruktur https://www.helse-

sorost.no/Documents/Styret/Styrem%C3%B8ter/2016/20160908/069-2016%20Vedlegg%204%20-%20Rapport%20risikoanalyse.pdf

Sentralt for denne vurderingen var den stadig økende risiko i den gamle infrastrukturen, som både eksponerer personvernet og pasientsikkerheten. Risikovurderingen ble dermed et valg mellom to tilnærminger, hvorav begge hadde i seg den økende risiko med den gamle infrastrukturen. Alternativene «gjør det selv» og «ekstern partner» har ulike risikofaktorer. Når det gjelder «gjør det selv»-alternativet som vil ta vesentlig lengre tid, er det her angitt som en risiko at «Dersom man kjører på eksisterende plattform over tid og nye sikkerhetsmekanismer ikke lar seg implementere vil det være økt risiko knyttet til hendelser på informasjonssikkerhet» (R-0068). Mens det i «ekstern partner»-alternativet er identifisert som en risiko at «Dersom personopplysninger kan aksesseres fra utlandet og ikke behandles i henhold til norsk lov kan personinformasjon komme på avveie» (R-0037).

Styret i Helse Sør-Øst RHF besluttet i sak 069/2016 å modernisere infrastrukturen ved hjelp av ekstern leverandør. Til grunn for denne beslutningen lå også en forutsetning om at informasjonssikkerhet og personvern var ivaretatt gjennom de krav som var stilt, både gjennom den dialogbaserte anskaffelsen og i avtalen. De angjeldende kravene kommer vi nærmere tilbake til nedenfor.

Størrelsen på kontrakten innebærer at aksept av leverandører fra /i EU/EØS ikke er et valg, men en konsekvens av EØS-avtalen.

Hovedårsaken til tjenesteutsettingen var behovet for bistand til å fornye og modernisere den eksisterende infrastrukturplattformen. I tråd med den risikoen som var identifisert i DNV GL sin risikovurdering, var det en klar forutsetning for anskaffelsen at alle regulatoriske krav til behandling av helseopplysninger og andre personopplysninger skal overholdes. Det fremgår av prekvalifikasjonsgrunnlaget, som setter rammene for konkurransen, at:

> "*The strategic partner needs to treat personal data and personal health data in accordance with Norwegian laws and regulations. This includes, but is not limited to, a requirement for the strategic partner to comply with the Norwegian Personal Data Act, Personal Data Regulations and Personal Health Data Filing System Act. If personal data is intended to be transferred outside of Norway, it may need approval from The Norwegian Data Protection Authority.*"

Kravene inkluderer krav til godkjent risikovurdering mv, og ble nærmere drøftet og presisert i løpet av anskaffelsen.

Anskaffelsen av kontrakt med ekstern leverandør ble gjennomført som konkurransepreget dialog. Konkurranseformen innebærer at leveransens omfang og kravene til leverandøren utarbeides gjennom dialog. Informasjonssikkerhet hadde høyt fokus under denne dialogen. Dette inkluderer spørsmålet om risikovurdering, og det fremgår av de krav som er stilt i kontrakten med leverandøren, at ingen behandling kan overføres til (under)leverandøren før godkjent risikovurdering foreligger.

Våren 2017 ble det i tråd med kontrakten arbeidet med risikovurdering som grunnlag for å fatte beslutning om hvorvidt organisasjon og løsning var klar for overføring til leverandør. Overføring var planlagt gjennomført 1. mai 2017, men ble utsatt. Dette skyldtes blant annet at *TMO readiness review* ikke var tilfredsstillende. Programmet er deretter stilt i bero som følge av styret i Helse Sør-Øst RHF sitt vedtak, beskrevet ovenfor.

I kravene til *TMO readiness review* (Appendix 1-A-6 *Information Security*, punkt 3.1) fremgår det blant annet at:

CT-SEC-TRV-01	Before the contract commence date and Contractor data processing may start, the Customer shall perform a risk assessment to verify that the Contractor has met the requirements in ISFT and that the Contractor is prepared for TMO. This will include a review of the Contractors security procedures, controls, documentation and organization, and the interface between the Contractor and Customer. Before any data processing may take place, the Customer must be assured that the Contractor has established a sufficient level of security. The risk assessment shall review if TMO start-up negatively impacts risk for services, compared to CMO. This assessment is regardless of factual risk of each service, it is simply to assure that TMO does not increase risk levels. The preparation for the risk assessment for TMO acceptance will begin shortly after contract signature date.

Appendix 1-A-6 inneholder også krav til leverandørens *risk management* (punkt 2.5) og en rekke krav til leverandørens risikovurderinger (punkt 2.2).

Når det gjelder risikovurdering knyttet til behandling av personopplysninger utenfor Norge, følger det av Appendix 1-A-6 punkt 2.1:

CT-SEC-PSH-06	The Contractor shall accept that the Data Controller must approve risk assessments before any personal data may be processed outside of Norwegian territories.
CT-SEC-PSH-07	The Contractor shall accept that the Data Controller must approve risk assessments before any changes in the accepted method of personal data processing outside of Norwegian territories are performed.
CT-SEC-PSH-08	The Contractor shall accept that each hospital trust in HSØ is a separate legal entity.
CT-SEC-PSH-09	The Contractor shall support HSØ in defining a single risk acceptance process across the local entities
CT-SEC-PSH-10	The Contractor shall accept that the Security Board is the preparatory and advisory body for risk assessments, where each legal entity's representative approves the appropriate level of risk

Det vises for øvrig til kravene i sub-databehandleravtalen punkt 5 om informasjonssikkerhet, der det blant annet fremkommer følgende:

- *The Sub-processor shall ensure that all processing of personal data falling within this agreement is carried out in accordance with acceptable risk level defined by the Data Controller. As part of this, the Sub-processor shall produce risk assessments of its own and of its eventual sub-contractors' security.*

- *The Sub-processor is presumed to only have access via approved remote access solutions whereby access is provided. Remote connections may only be performed through the Customer's approved remote access service, which prohibits external transfer of data. Any*

other type of data connection where external transfer may be performed, shall only be made possible with the explicit approval from the Data Controller. Any other connection which permits the transfer of data requires separate approval by the Data Controller.

2.2 Risikovurderingene, samt redegjørelse for akseptanse av restrisiko, som ble lagt til grunn da det ble besluttet å legge disse tjenestene til Bulgaria.

Da det mest fordelaktige tilbudet i henhold til den gjennomførte konkurransen ble valgt, ble Bulgaria aktualisert. Inntil denne beslutning ble tatt, var også drift fra Norge en av leverandørenes tilbud. Det ble etter at leverandør var valgt, gjennomført en vurdering av Bulgaria som land. Både økte risikoaspekt ble adressert og behov for ytterligere tiltak ble konkludert, se

Vedlegg 3: Landvurdering, som er gjort etter valg av leverandør

Landvurderingen ble vurdert som mulig, men med noe økt risiko og forutsatt ytterligere sikkerhetstiltak implementert. Landvurderingen gav dermed ikke grunnlag for å utelukke Bulgaria, men først etter videre risikovurdering av de faktiske tiltakene, ville det være grunnlag for å konkludere om restrisiko var akseptabel. Pågående risikovurdering i «TMO readiness verification, risk assessment» vil avgjøre dette. De ytterligere sikkerhetstiltak som det ble identifisert behov for i landvurderingen, omfattet utvidet og systematisk bruk av Sykehuspartners sikkerhetsplattform og bruk av kryptering av informasjon ved lagring. Disse tilleggstiltakene innen sikkerhet var forutsatt sett i sammenheng og supplerer dermed sikkerhetsstrategien i det regionale styringssystem for informasjonssikkerhet og de detaljerte sikkerhetskravene i kontrakten.

«TMO readiness verification, risk assessment» forutsetter deretter en akseptert risikovurdering av informasjonssikkerheten, herunder at alle sikkerhetskravene i utlysningen imøtekommes, og bekreftes. Det vises her til vedlegg til referat fra iMod Security Board av 24.04.2017, der følgende fremkommer:

Introducing a new service provider for infrastructure services might increase risk with regards to information security. To assess whether the overall level of risk is increased when infrastructure services will be under responsibility of the Consortium, a risk assessment shall be performed. The need for such a risk assessment is anchored in the contract as the following security requirement (CT-SEC-TRV-01):

Before the contract commence date and Contractor data processing may start, the Customer shall perform a risk assessment to verify that the Contractor has met the requirements in ISFT and that the Contractor is prepared for TMO. This will include a review of the Contractors security procedures, controls, documentation and organization, and the interface between the Contractor and Customer. Before any data processing may take place, the Customer must be assured that the Contractor has established a sufficient level of security. The risk assessment shall review if TMO start-up negatively impacts risk for services, compared to CMO. This assessment is regardless of factual risk of each service, it is simply to assure that TMO does not increase risk levels. The preparation for the risk assessment for TMO acceptance will begin shortly after contract signature date.

Vedlegg 4: Referat fra iMod Security Board av 24.04.2017 med vedlegg.

Fremlegging av «TMO readiness verification, risk assessment» 24.04.2017 viste at leverandøren var langt fra å ha gitt nødvendige og tilfredsstillende svar på hvordan sikkerhetskravene skulle møtes og hvordan rutiner og håndtering av sikkerheten hos leverandør ble ivaretatt. Fremlagt dokument «TMO readiness verification, risk assessment» ble dermed avvist, da det ikke gav grunnlag for å gi akseptabelt sikkerhetsnivå.

Føringer for akseptabel risiko er å finne i regionalt styringssystem for informasjonssikkerhet, se:

Vedlegg 5: Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet

Vedlegg 6: Risikovurdering ved nye og endrede IKT-løsninger og databehandlinger
http://ehandboken.ous-hf.no/document/109436

Som kjent igangsatte administrerende direktør i Helse Sør-Øst RHF den 27. april 2017 en ekstern gjennomgang av programmet, herunder tilganger til ekstern leverandør og informasjonssikkerheten. Foreløpig redegjørelse fra PWC, der både mandat og foreløpige funn fremkommer, vedlegges i sin helhet som

Vedlegg 7: Foreløpig redegjørelse knyttet til IKT-tjenesteutsetting (iMod), datert 24.05.17 fra PwC.
https://www.helse-sorost.no/Documents/Styret/Styremøter/2017/20170524/2017-05-24%20HSØ%20RHF%20-%20Foreløpig%20redegjørelse%20iMod%20V1.pdf

2.3 En oversikt for hvor mange eksterne leverandører som har tilgang til sykehusenes informasjonssystem, hvilke land leverandørene har tilgang fra, hvilke type tilganger de har til hvilke systemer og til hvilke personopplysninger (omfang, sensitivitet), samt formålet med tilgangene.

Sykehuspartner er som databehandler og IKT-selskap helt avhengig av å benytte ekstern bistand fra leverandørmarkedet til gjennomføring av prosjekter, konfigurering av leverandørers systemer og driftsbistand (kapasitet eller spesialister). Dette gjelder både på infrastrukturkomponenter, applikasjoner og medisinsk teknisk utstyr. Dette medfører behov for at eksternt personell kan logge inn i vår infrastruktur på en måte som ivaretar en rekke hensyn knyttet til informasjonssikkerhet, personvern, sporbarhet, tilgjengelighet, redundans og driftsvennlighet.

For å oppnå dette har Sykehuspartner etablert en løsning basert på moderne teknologi som kalles «Leverandørportalen». Dette er vår felles sikre inngangsport for oppkobling av eksterne leverandører inn i vår infrastruktur ved hjelp av tofaktorautentisering og tynnklient-arkitektur. Gjennom denne portalen får leverandører tilgang til de tjenestene hvor de har blitt gitt eksplisitte tilganger, hvor tilganger skal følge prinsippet om «least privilege», dvs. tilgangsminimering. Tilgang til leverandørportalen innebærer derfor ikke direktetilgang til helseopplysninger, men gitt et riktig tilgangsnivå i bakkant, kan godkjente leverandører bruke leverandørportalen som en inngangsport mot informasjonssystemene som benyttes i behandlingen av helseopplysninger.

Leverandørbrukere bestilles og godkjennes i henhold til etablerte prosesser, og med begrenset varighet og tilgangsnivå.

Vedlegg 8: Oversikt over eksterne leverandører med forespurt informasjon

Sykehuset Østfold HF har inngått avtaler med leverandører av medisinsk teknologisk utstyr. Flere av disse anskaffelsene har blitt gjort ved etableringen av Nytt Østfoldsykehus og felles for alle leverandører er at de benytter Leverandørportal eller VPN som er driftet av Sykehuspartner.

I mai og juni 2016 ble det gjennomført en konsernrevisjon ved helseforetaket med tittelen: "Leverandørenes tilgang til helse- og personopplysninger i Medisinsk-teknisk utstyr (MTU) i Sykehuset Østfold HF". Rapport og handlingsplan ble styrebehandlet 19. september 2016 (styresak 45-16) og vedlegges i sin helhet.

Vedlegg 9: Konsernrevisjonens rapport "Revisjon Leverandørenes tilgang til helse- og personopplysninger i Medisinsk-teknisk utstyr (MTU) i Sykehuset Østfold HF".
Vedlegg 10: Handlingsplan – konsernrevisjonens gjennomgang av leverandørenes tilgang til helse- og personopplysninger i MTU, oppdatert pr. 28.04.2017.

Den samlede oppsummering i rapporten er:

Revisjonen viser at det er etablert en tjenesteavtale mellom Sykehuset Østfold HF og Sykehus-partner HF for 2016 som regulerer roller og ansvar når det gjelder databehandleransvarlig og data-behandler. Sykehuspartner HF har forpliktet seg til å følge kravene i Normen og å inngå data-behandleravtale med tredjeparter, herunder MTU-leverandører. For en del eldre utstyr ved Syke-huset Østfold HF som er anskaffet før PNØ er det ikke utarbeidet tjenestebeskrivelser.

Konsernrevisjonen vurderer at kriteriet i stor grad er oppfylt, men at det for noe av utstyr anskaffet før PNØ mangler tjenestebeskrivelser.

Revisjonen viser at det er etablert en praksis for risikovurdering ved større omlegginger i MTU-miljøet i Sykehuset Østfold HF, og MTA er inkludert i ledelsens gjennomgang. Det foreligger også rutiner for løpende risikovurderinger som det ikke ennå har vært aktuelt å bruke for MTU. Det er i tillegg påbegynt et arbeid for å systematisere og følge opp utestående risikoer og tiltak fra risiko-vurdering av MTU i PNØ.

Konsernrevisjonen vurderer at risikovurderinger for MTU er satt i system.

Revisjonen viser at det er MTA ved Sykehuset Østfold HF som forvalter administrator-rettighetene på MTU ved sykehuset. Tildeling av MTU-leverandørenes rettigheter er satt i system, med en avklart ansvars- og rolledeling mellom Sykehuset Østfold HF og Sykehuspartner HF. Sykehuset Østfold HF har ikke en samlet oversikt over hvilke leverandører som har tilgang til sykehusets MTU gjennom fjernaksess. MTU-leverandørene får kun tilgang til de serverne og de data de er autorisert for, men utover dette gir de tekniske løsningene begrensede muligheter for styring og kontroll med MTU-leverandørenes aktivitet.

Konsernrevisjonen vurderer at tildeling av MTU-leverandørenes rettigheter, og ansvars- og rolle-delingen mellom Sykehuset Østfold HF og Sykehuspartner HF, er satt i system. Men hverken leverandørportalen eller VPN-tilgangene gir mulighet for å forhindre eller avdekke MTU-leverandørenes eventuelle misbruk av sensitiv informasjon.

Revisjonen viser at avvikshåndteringen, ledelsens gjennomgang og risikovurderinger er satt i system, mens sikkerhetsrevisjoner og oppfølging av databehandler ikke er gjennomført etter PNØ på MTU-området.

Konsernrevisjonen vurderer at dagens oppfølging av informasjonssikkerhet på Sykehuset Østfold HF innenfor MTU-området ikke er tilstrekkelig i henhold til Normen.

Avdekkede funn i konsernrevisjonens gjennomgang er behandlet i vedtatt handlingsplan (se vedlegg).
Det gjenstår et ønske fra SØ om å få større kontroll på Leverandørportalen, ved at helseforetaket regulerer tilgangstidspunkt og filsluse for hver enkelt leverandør.

Pasientnært medisinsk utstyr med systemtilbehør er ivaretatt i sin helhet av MTA fordelt på to plattformløsninger, PaaS og NaaS.
PaaS, Platform as a Service, er en løsning hvor Sykehuspartner drifter plattform opp til og med operativsystem og MTA har drift og forvaltning av applikasjonen.
NaaS, Network as a Service, er en løsning hvor Sykehuspartner drifter nettverkstjenester og MTA har ansvaret for drift og forvaltning av server og klientløsningen utover dette.

Med vennlig hilsen
Sykehuset Østfold HF

Just Ebbesen
Administrerende direktør

Lars Cato Skaar
Informasjonssikkerhetsleder

Vedlegg 3.

SYKEHUSPARTNER

NOTAT

28. februar 2017
(oppdatert 08.mars 2017)

Til: Security Board

Fra: iMod security SP

Risikovurdering – behandling av personopplysninger i Bulgaria

Formål og bakgrunn

Som en del av iMod-programmet og samarbeid med ny strategisk partner er det foreslåttat deler av IKT-tjenestene skal leveres fra utlandet. Drift og forvaltning av IKT infrastrukturtjenester innebærer at partner vil behandle personopplysninger på vegne av Sykehuspartner HF og dermed også for foretaksgruppen i Helse Sør-Øst RHF. En behandling av personopplysninger fra utlandet innbærer også en utlevering av personopplysninger fra Norge til de land hvor behandlingen skal skje.

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

SYKEHUSPARTNER

Utlevering av personopplysninger til utlandet krever vurdering og aksept av risiko og kontrakten stiller også krav til at slike risikovurderinger gjøres før utleveringen skjer. Det er databehandlingsansvarlige som skal kunne gi aksept av risiko.

Formålet med dette notatet er å redegjøre for landrisiko ved databehandling fra Bulgaria, og om det kan gjøres med tilstrekkelig grad av kontroll mht. den registrertes personvern i henholdsvis CMO[1]-, TMO- og FMO-fasene.

Risikovurderingen er delt i seks ulike deler som hver for seg påvirker det totale risikobildet: (1) landrisiko, (2) forholdet til «TMO readiness verification». (3) modenhet i internkontrollen, (4) forholdet til kjente svakheter og sårbarheter, (5) landvurdering for cyberkriminalitet og (6) økonomiske forhold knyttet til endringer i internkontroll,

Målsetningen med risikovurderingen er å vurdere hvorvidt risikonivået prinsippielt endrer seg utenfor risikoakseptkriterier ved eventuell databehandling fra Bulgaria, samt eventuelt identifisere nødvendige tiltak/forutsetninger for å kunne gjennomføre databehandling.

[1] Gjelder det som kalles «knowledge transfer» fra SPHF mot HPE i forkant av TMO 1.5.2017

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

SYKEHUSPARTNER

(1) Landrisiko (politiske og konstitusjonelle forhold)

Når utkontrakteringen innebærer at det skal leveres tjenester fra lavkostland står særlig vurderingen av risiko ved konstitusjonelle og politiske forhold sentralt (landrisiko).

Bulgaria

Som medlem av EU skal Bulgaria ha ratifisert direktiv 95/46 som utgjør grunnlaget for personopplysningsloven i Norge. Som utgangspunkt skal dermed lovgivning innen personvern være relativt likt mellom landene og således er kriterier for utlevering av personopplysninger til Bulgaria ivaretatt i henhold til kapittel 5 i personopplysningsloven. *Inntil EU-forordningen er implementert, vil det være nasjonale fortolkninger av personvernreglene som kan gi ulike utslag for den registrertes rettigheter og krav til informasjonssikkerhet.*

På europakommisjonens nettsider[2] er det publisert det som skal være lov om beskyttelse av personopplysninger i Bulgaria og det legges derfor til grunn at dette faktisk er gjeldende lov i Bulgaria. Denne loven stiller ikke eksplisitte krav til internkontroll, men dekker sentrale rettigheter for den registrerte. En viss usikkerhet vil det derimot være frem til en reell avklaring foreligger på lovens gyldighet i Bulgaria. Det skal også være etablert en prosess[3] for innføring av EU sitt nye personvernregelverk i bulgarsk lovverk innen 25. mai.

Forholdet mellom den bulgarske personopplysningsloven («law for protection of personal data») og andre lover som eventuelt undergraver den registrertes rettigheter eller er til hinder for at databehandlingsansvarlige kan ivareta egne forpliktelser er ikke kartlagt som del av denne risikovurderingen. Av erfaring vet vi at ulike land har etablert lover som begrenser personvernregelverkets virkeområde, særlig i spørsmål som knyttes til bekjempelse av kriminalitet og forhold knyttet til rikets sikkerhet. Derfor er det usikkert hvorvidt personopplysninger om norske pasienter og ansatte er skjermet for bulgarske eller samarbeidende lands myndigheter.

Sykehuspartner HF har i forbindelse med landrisikovurderingen også vært i kontakt med en av etterretningstjenstene. Det er her kommunisert at konfidensialitet er en sentral forventning.

---

[2] http://ec.europa.eu/justice/data-protection/law/files/implementation/bg_data_protection_law_en.pdf
[3] https://www.dlapiperdataprotection.com/index.html?t=law&c=BG

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

I flere artikler[4] omtales utfordringer med korrupsjon i Bulgaria. I følge Transparency International vurderes Bulgaria å ha relativt store utfordringer knyttet til korrupsjon ved at de rangeres på 75. plass på deres korrupsjonsindeks[5]. Problemer med korrupsjon vurderes å redusere virksomheters evne til å ivareta krav til informasjonssikkerhet og internkontroll, og vurderes å være en trussel mot personvernet. Særlig er uttrykt at forholdet til sanksjonering mot avvik er utsatt for korrupsjon for å unngå at eventuelle hendelser gjøres kjent for kunder, myndigheter eller offentligheten for øvrig. Korrupsjon vil i så fall undergrave grunnleggende informasjonssikkerhet og personvern. I hvilken grad partneren har etablert prosesser for antikorrupsjonsarbeid i Bulgaria spesielt eller i virksomheten generelt er ukjent og skal undersøkes nærmere da det vil bidra til å redusere risiko.

I følge UD[6] vurderes Bulgaria å være et trygt land å reise til, men det henvises til utfordringer med korrupsjon i lokale politimyndigheter og behov for å sikre kvitteringer ved betaling av bøter. Dette styrker inntrykket av at korrupsjon utgjør et problem i Bulgaria. I forhold til sikkerhetsmessige spørsmål vurderes det ikke å være relevante risikoer knyttet til Bulgaria, men generelt høyere nivå av politisk uro enn i Norge.

Hensynet til varsling og beskyttelse av varslere er kravstilt i kontrakten. Det vil gjennom TMO Readiness Verification bekreftes at HPE har etablert et tilfredsstillende beskyttelsesnivå for varslere.

I mai 2018 trer EUs nye regelverk for personvern i kraft i Norge og Bulgaria. Det nye regelverket skal bidra til en harmonisering av regelverk på tvers av europeiske land, og således legge til rette for fri flyt av informasjon innen EU, på lik linje som fri flyt av arbeidskraft, kapital og tjenester. Før det nye regelverket er på plass er det nødvendig å gjøre selvstendige vurderinger av utlevering av personopplysninger til hvert land, selv om gjeldende EU-direktiv gir en viss felles plattform. Ut over vurderingen som er gjort her har det ikke blitt gjennomført eller innhentet slike vurderinger.

---

[4] http://www.aftenposten.no/viten/EU-har-tapt-kampen-mot-korrupsjon-i-Bulgaria-70908b.html, http://www.vg.no/nyheter/utenriks/bulgaria/kjempeprotester-stenger-bulgarias-gater/a/10111525/, https://www.nrk.no/urix/--enormt-omfang-av-korrupsjon-i-eu-1.11517190

[5] https://www.transparency.org/news/feature/corruption_perceptions_index_2016

[6] https://www.regjeringen.no/no/tema/utenrikssaker/reiseinformasjon/velg-land/reiseinfo_bulgaria/id2416997/

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

SYKEHUSPARTNER

(2) «TMO readiness verification»

Partner er databehandler (etter personopplysningsloven) for Sykehuspartner HF og i henhold til opprinnelig plan og krav i Appedix 1-A-6 kapittel 3 skal det gjennomføres en risikovurdering før partneren involveres i behandling av personopplysninger. Formålet med TMO readiness verification er å vurdere risiko for at partneren leverer tjenester som ikke er i samsvar med krav og at partneren dermed er klar for å overta ansvar for drift og forvaltning uten at risikonivået for foretaksgruppen i Helse Sør-Øst RHF øker.

I tillegg til risikovurderingen skal partneren gjennomføre en vurdering for å bekrefte at de kjenner til nødvendig sikkerhetsnivå på de ulike tjenestene, at det ikke foreligger vesentlige avvik mot krav og at eventuelle alvorlige sårbarheter er dokumentert slik at nødvendige risikoreduserende tiltak kan iverksettes. Risikoreduserende tiltak skal presenteres for Security Board.

Sykehuspartner HF har startet arbeidet med denne risikovurderingen, men den er ikke ferdig. Partners vurdering er også under arbeid. Frem til risikovurderingen og partnerens vurdering foreligger, er det uavklart hvorvidt partneren ivaretar grunnleggende krav til informasjonssikkerhet og internkontroll, samt personvern. Denne mangelen på avklaringer utgjør en risiko for at partneren ikke evner å ivareta krav til informasjonssikkerhet og internkontroll og risiko for at pasienters og ansattes personvern ikke blir ivaretatt på en tilfredsstillende måte.

Før «TMO readiness verification» er ferdigstilt kan det ikke konkluderes på hvilken endring i risiko eller sikkerhetsnivå behandling av personopplysninger fra partneren vil medføre, herunder også inkludert leveranser fra andre land.

(3) Modenhet i internkontroll

Tjenesteutsetting av IKT infrastrukturtjenester innebærer en endring i kontrollmiljø og -spenn for foretaksgruppen i HSØ. Sykehuspartner HF og foretaksgruppen i Helse Sør-Øst må etablere kapasitet og kompetanse for å inkludere eksterne tjenesteleverandører i internkontrollen da dette er et nytt risikoområde, samt sikkerhetskontroller som sikkerhetsplattformen. En tilnærming for å inkludere leverandør(er) i eget kontrollspenn kan være å innhente eksterne bekreftelser (som ISAE 3402, type II) på internkontrollens utforming og etterlevelse hos leverandøren. Frem til dette eller tilsvarende foreligger utgjør internkontrollen hos partneren en usikkerhet.

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

Frem til denne kapabiliteten er etablert har foretaksgruppen i Helse Sør-Øst begrenset evne til å følge opp partnerens leveranser. Dette bidrar til å øke risikonivået og svekker foretaksgruppens evne til å ivareta forpliktelser etter personopplysningsloven §14 og kapittel 3 i personopplysningsforskriften om internkontroll.

Databehandleravtalen [7]mellom Sykehuspartner og partneren inkluderer partnerens bruk av underleverandører. For at Sykehuspartner skal kunne ivareta egne forpliktelser til å følge opp databehandleravtalens intensjoner og krav, er det en forutsetning å kjenne til enhver underleverandør som er involvert i behandling av personopplysninger på vegne av foretaksgruppen, og hvor disse er lokalisert (land). Risiko for at leverandører utenfor EU- og EØS-området involveres i behandling av personopplysninger eksisterer allerede i dag. Når partneren vil ønske å benytte egne underleverandører, økes risiko for utlevering av personopplysninger om både pasienter og ansatte til tredjeland[8]. Det er nødvendig å etablere en løpende oppfølging av databehandleravtalen.

Sykehuspartner HF sin evne til å lukke avvik påvirker det samlede risikonivået. Behov for gode prosesser for rettidig og tilstrekkelig lukking av avvik vurderes å være en forutsetning for oppfølging av tjenestelevanser over tid og avvik som oppstår som del av dette.

(4) Forholdet til kjente svakheter og sårbarheter

Det foreligger flere kjente svakheter i sikkerhetsnivået og i internkontrollen til Sykehuspartner som påvirker risikonivå ved bruk av eksterne tjenesteleverandører. Eksempler på dette er mangel på kryptering i kjernenettet i Helse Sør-Øst RHF, og svakheter i styring og kontroll rundt systemadministrasjon. Det er også et stort volum av lagring av sensitive personopplysninger på filområder. Noen kjente svakheter utgjør allerede en uakseptabel risiko og det må derfor iverksettes risikoreduserende tiltak før overføring kan skje, hovedsakelig i regi av prosjektet P85. Når en utenlandsk partner introduseres i drift og forvaltning av tjenester med svakheter, økes kompleksitet og svakhetens omfang.

---

[7] https://sikt.sharepoint.com/teams/SP_TnT/_layouts/15/WopiFrame.aspx?sourcedoc=%7BDA0CCA4D-0483-48C2-84F1-7B7110C71E33%7D&file=The%20Services%20Agreement%20-%20Appendix%2012%20-%20Sub-data%20processor%20agreement.docx&action=default

[8] Tredjeland: Land utenfor EU-/EØS-området (som ikke har ratifisert EU-direktiv 95/46) og som ikke er godkjent av Europakommisjonen som mottakere av personopplysninger

SYKEHUSPARTNER

(5) Landvurdering cyberkriminalitet

Det er få relevante tjenester for å sammenligne landrisiko mht. cyberkriminalitet, og måleparameterne er ikke nødvendigvis relevante for en vurdering knyttet til å vurdere forskjellen mellom Norge og Bulgaria.

På Global Security Map[9] er Bulgaria vurdert å ligge på 16. plass, mens Norge er på 205. plass, av totalt 219. Mange av parameterne sier likevel lite om det generelle cyberkriminalitetsnivået, men heller at IKT-infrastrukturen generelt i Bulgaria er sårbar, og at Bulgarsk infrastruktur langt oftere benyttes til C&C, phishing og exploit kit landing pages. Det er ikke mulig ut fra dette å konkludere at bakmennene er hjemmehørende i Bulgaria, men at offentlig og privat sektor i Bulgaria ikke har et sikkerhetsnivå som ville anses som dekkende i Norge, og at etterforsking og nasjonal CERT i Bulgaria heller ikke holder et tilfredsstillende nivå.

IBMs Security Intelligence rapporterte i 2015 at banktrojanere i større grad fokuserer på SEE-området (South-East Europe), inkl. Bulgaria. I rapporten konkluderer IBM med at cyberkrim i Bulgaria i stor grad er knyttet til svindel mot privatpersoner, f.eks. skimming, minibanksvindel, phishing mv.

HPE vil operere i et land med et betydelig lavere nasjonalt operativt sikkerhetsnivå enn Norge og det nivået som kontrakten fastsetter. HPE må derfor være forberedt på at gapet mellom Bulgaria og tilfredsstillende kontraktuelt sikkerhetsnivå må lukkes.

(6) Økonomiske forhold knyttet til endringer i internkontroll

Ved bruk av tjenesteleveranser fra utenlandske selskaper, er det naturlig å anta at dette vil medføre økte kostandene til å gjennomføre kontrollhandlinger som følge av reisevirksomhet, bruk av nye leverandører (som revisorer) og behov for ressurser til oppfølging av regulatoriske forskjeller. Det er uklart hvorvidt Sykehuspartner HF for 2017 har budsjettert med økte rammer for å gjennomføre kontroll av leverandører i utlandet, og dersom dette ikke korrigeres vil det redusere foretaksgruppens evne til å inkludere tjenesteleveranser fra utlandet i internkontrollen.

[9] http://globalsecuritymap.com/#bg

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

SYKEHUSPARTNER

Conclusion

This assessment concludes that the total level of risk will be increased by performing data processing of personal information from Bulgaria. It is therefore necessary for Sykehuspartner HF and HPE to implement controls and checks as to close the information security gap. These are proposed in this chapter. No *specific* risk has been identified that in it self excludes data processing of personal information from Bulgaria, but the six areas addressed will in total elevate the level of risk.

1. Landrisiko	**Økt risiko**	**Tiltak for å muliggjøre databehandling fra Bulgaria**
a) Forskjeller i realisering av direktiv 95/46, herunder lovgivning som udergraver den registrertes rettigheter.	Usikkert	5, 6
b) Utbredt korrupsjon i Bulgaria	Ja	1, 4, 5
c) Andre lover som potensielt undergraver den registrertes rettigheter eller er til hinder for databehandlingsansvarlig.	Usikkert	5, 6
d) Hensyn til varsling og beskyttelse av varslere.	Usikkert	1
e) Fortrolighet for personer av interesse.	Ja	1, 2, 3, 4, 5, 6, 7, 8
2. TMO readiness verification	**Økt risiko**	**Tiltak**
a) Hensyn til varsling og beskyttelse av varslere.	Usikkert	1, 3
b) Ivaretagelse av informasjonssikkerhet og internkontroll	Ja	1, 2, 3, 4, 7, 8
3. Modenhet i internkontroll	**Økt risiko**	**Tiltak**
a) Endring i kontrollmiljø og –spenn.	Ja	2

Fakturaadresse:
Postboks 3562, 3007 Drammen
Besøksadresse hovedkontor:
Vektergården, Grønland 34
3045 Drammen

Telefon: 32 23 53 00
Telefaks: 32 23 53 01

E-post: post@sykehuspartner.no
Org.nr.: 914637651

b) Oppfølging av DBA	Ja	2
c) Evne til å lukke avvik	Usikkert	2
4. Forhold til kjente svakheter og sårbarheter	**Økt risiko**	**Tiltak**
a) Eksisterende svakheter i sikkerhetsnivå og internkontroll	Ja	1, 2, 3, 4, 5, 7, 8
5. Landvurdering Cyberkriminalitet	**Økt risiko**	**Tiltak**
a) Nivå på sikkerhet, etterforsking og nasjonal CERT i Bulgaria.	Ja	1, 4, 5
6. Økonomiske forhold knyttet til endringer i internkontroll	**Økt risiko**	**Tiltak**
a) Økte rammer for å gjennomføre kontroll av leverandører i utlandet.	Ja	2, 4

To reduce the total risk level regarding data processing of personal information from Bulgaria, these mitigating activities are required:

1) Investigate further the internal control of HPE, including anti corruption work and whistleblower protection -> Consortium / ASO, to be presented to the Security Board no later than May 1st.
2) Establish an audit process in SPHF and Helse Sør-Øst that is adjusted to handle data processing in EU/EEA countries -> iMOD Security team SP
3) Perform and approve the TMO readiness verification and P85 -> iMOD Security team SP and Consortium
4) Ensure that the Sykehuspartner security platform is extended to any connectivity to and from partner location -> Sykehuspartner HF.
5) Confer with national security services -> iMOD Security team SP
6) Conducting impact assessment of privacy disadvantage -> iMOD Security team SP and Consortium
    a. Bulgaria CMO
    b. Bulgaria TMO
    c. Bulgaria FMO
7) The Contract needs to include encryption on server fileshares as a default setting, with the possibility to exclude encryption if requested.
8) Known non-compliances related to too wide access levels shall not be transfered to HPE

Vedlegg 4

SYKEHUSPARTNER

SUMMARY

Meeting: **Security Board: TMO RV B**
Date: 24.04.17 **Sted:** Skøyen/Lync
Present: From the Security Board:
Gro Jære (Chair – SPHF), Christian Jacobsen (SPHF), Thor Lunde (SPHF), Baard Lindberg (SPHF), Gaute Lien (Consortium), Dick van Ballegooijen (Consortium), Lars Cato Skaar (SØHF), Johan Krüger (SSHF), Heidi Thorstensen (HSØ), Angélique Colle (SPHF)

Additional attendees: Preben Gustavsen (SPHF), Geirr Gustavsen (Consortium)
Absent: John Vestengen (SPHF – optional)

Item #	1
Item	**TMO RV** - The assessment on TMO RV (see attachment), hereinafter referred to as TMO RV B, was presented in the monthly Security Board meeting the 19.04.17. The goal for this meeting was to evaluate the risk level after SCD and whether the mitigating measures are sufficient. - There was no voting during this meeting, but comments were that the document itself is good, but that there should be some more explanation on the original scope of the TMO Readiness Verification, and what the consequences of the scope reduction is in relation to the overall risk level presented. - From representatives from SPHF it was stated that the Consortium's contribution has so far been somewhat disappointing compared to what was expected. - It is desirable to receive the document with the original scope (hereinafter referred to as TMO RV A) in order to decide whether the overall risk level after SCD is acceptable or not.
Delegation	Preben Gustavsen and Consortium representatives – Further work on the TMO RV and go from TMO RV B to TMO RV A, resubmit to the Security Board. Angélique Colle – Arrange new Security Board meeting for TMO RV A. New date will be sent out ultimo week 18.2017.
Documents	TMO readiness verification - r...
Status	**No voting.** The Consortium has to start by providing answers and documentation related to the measures in the TMO RV B. The author of the document, together with the Consortium representatives, then

	has to go back to the original scope and close the gaps after mapping the delivered documents related to the measures in the TMO RV B, identify the remaining gaps, and the Consortium to start providing information in order to close the remaining gaps. The outcome, TMO RV A, has to be presented to the Security Board for processing.

Angélique Colle
referent
25.04.17

Vedlegg 5

SYKEHUSET ØSTFOLD

Prosedyre **Felles SØ**

Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet

Endring siden forrige versjon
Nytt dokument.

Hensikt
Sikre at SØ har etablert sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet som del av styringssystem for informasjonssikkerhet.

Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet gjelder for all behandling av helse- og personopplysninger, herunder avidentifiserte personopplysninger (indirekte identifiserbare personopplysninger), som benyttes i forbindelse med pasientbehandling og administrering av slik, forskning, undervisning, kvalitetssikring og internkontroll. Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet gjelder videre uavhengig av hvor personopplysningene, inkludert indirekte identifiserbare, oppstår, og omfatter dermed også informasjon som oppstår i MTU og annet teknisk utstyr.

Dokumentet reflekterer også det felles grunnlag for informasjonssikkerhet som spesialisthelsetjenesten er kommet til enighet om. Sikkerhetsmål og -strategi bidrar til å sikre et felles nivå på informasjonssikkerhet på tvers av virksomheter, og gir felles føringer for alle helseforetak, regionale helseforetak, Norsk Helsenett samt øvrige driftsenheter eid av disse. Det endrer imidlertid ikke behovet for databehandleravtaler.

Målgruppe
Alle i Sykehuset Østfold (SØ)

Sykehuset Østfold HF ved administrerende direktør er databehandlingsansvarlig for all behandling av helse- og personopplysninger med tilknytning til Sykehuset Østfold HF. Administrerende direktør har ansvar for at alle personopplysninger blir behandlet iht. gjeldende lovverk, se spesielt pasientjournalloven, helseregisterloven og personopplysningsloven med forskrift.

Klinikksjef har det overordnede ansvar for oppfylling av instruksen i egen klinikk.

Avdelingsleder/leder har ansvaret for oppfylling av sikkerhetsmålene i egen avdeling/seksjon.

Personell som i kraft av sin stilling på Sykehuset Østfold HF har tilgang til helse- og personopplysninger inkludert journal, er ansvarlig for å etterleve Sikkerhetsinstruksen for informasjonssikkerhet.

Fremgangsmåte

Følgende beskrives:

- Sikkerhetsmål
- Akseptabelt risikonivå

<u>Sikkerhetsmål</u>
Sikkerhetsmål er virksomhetens visjon og formål for informasjonssikkerhet.

Sykehuset Østfold HF skal behandle helse- og personopplysning i samsvar med de krav som er gitt i lov og avtaler. Ingen helse- og personopplysninger skal samles inn, bearbeides, lagres eller slettes uten at den opplysningene omhandler har gitt sitt samtykke, eller det er fastsatt i lov at det er adgang til slik behandling.

Sykehuset Østfold HF skal gjennom sikkerhetsmålene forplikte seg til å etablere og kontinuerlig vedlikeholde et tilfredsstillende informasjonssikkerhetsnivå, både internt og hos databehandler og eksterne underleverandører,

slik at Helse Sør-Østs overordnede mål om å gi gode og likeverdige helsetjenester til alle som trenger når de trenger det, uavhengig av alder, bosted, etnisk bakgrunn, kjønn og økonomi, kan oppfylles.

Det er virksomhetens ledelse ved administrerende direktør som er ansvarlig for virksomhetens informasjonssikkerhet og som formelt er databehandlingsansvarlig, jfr. personopplysningsforskriften § 2-3[1]. Virksomhetens Administrerende direktør ved Sykehuset Østfold HF har besluttet å delegere myndighet for informasjonssikkerhet til virksomhetens informasjonssikkerhetsleder, jfr. *Organisering av informasjons-sikkerhetsarbeidet*.

Sykehuset Østfold HF har besluttet følgende sikkerhetsmål:

1. Målet for behandling av informasjon er å tilrettelegge for forsvarlige helsetjenester i Helse Sør-Øst på en måte som ivaretar krav til informasjonssikkerhet og den registrertes personvern.

2. All registrering og bruk av helse- og personopplysninger skal være i overensstemmelse med taushetsplikten og grunnlaget for databehandlingen skal være vurdert og godkjent. Når personopplysninger registreres og behandles, skal den registrertes rettigheter ivaretas.

3. Alle som ber om det, skal få generell informasjon om virksomhetens behandlinger og sikring av person-opplysninger.

4. Sykehuset Østfold HF skal sikre at informasjon behandles iht. krav i relevante lover og forskrifter, samt Normen for informasjonssikkerhet.

5. Sykehuset Østfold HF skal sørge for at sikkerhetsmålene ivaretas ved bruk av databehandler, og at dette dokumenteres i databehandleravtalen.

6. Informasjonssikkerhet ved Sykehuset Østfold HF skal ha forankring i og faglig rapportering til virksomhetens ledergruppe.

7. Informasjonssikkerhet skal ivaretas som en integrert del av hele Sykehuset Østfold HF sin organisasjon, uavhengig av hvor personopplysningene oppstår eller behandles. Dette omfatter også indirekte identifiserbare opplysninger (avidentifiserte personopplysninger) og når opplysningene oppstår ved bruk av medisinsk teknisk og annet tilsvarende utstyr.

8. Sykehuset Østfold HF skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid, riktig omfang og riktig sted for de personer som er autorisert.

9. Tilgang til systemer og informasjon skal kun gis til medarbeidere etter vurdering av tjenstlig behov og i samsvar med taushetsplikten. Tilgang til systemer og informasjon for uvedkommende skal forhindres.

10. Når personell som ikke har et ansettelsesforhold i Sykehuset Østfold HF skal gis tilgang til helse- og personopplysninger, må leder sørge for følgende:

    - at formålet for tilgang for den eksterne er helseforetakets behov. Eksternt behov gir ikke grunnlag for tilgang.
    - at nødvendig taushetserklæring er ivaretatt, normalt dekket av lov
    - at sikkerhetsinstruks er undertegnet
    - at det blir inngått avtaler som sikrer at sikkerhetsmålene oppfylles og at foretaket har nødvendig instruksjonsmyndighet før tilgang til personopplysninger gis.

[1] http://www.lovdata.no/forskrift/2000-12-15-1265/§2-3

11. Sykehuset Østfold HF skal sikre at informasjonen til enhver tid beskyttes mot utilsiktede og uautoriserte endringer.

12. Sykehuset Østfold HF skal sikre at medarbeidere som bruker virksomhetens informasjonssystemer har nødvendig kompetanse for å ivareta tilstrekkelig informasjonssikkerhet.

13. Sykehuset Østfold HF skal sikre at det etableres tekniske kontrollmekanismer, rutiner og prosesser som ivaretar tilfredsstillende informasjonssikkerhet, og som avdekker avvik, håndterer disse og forhindrer gjentagelse.

14. Sykehuset Østfold HF skal forhindre at personer eller systemer er årsak til, eller bidrar til, sikkerhetsmessige uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.

Videre skal etablert internkontroll knyttet til informasjonssikkerhet sikre at helseforetakets behandling av personopplysninger hele tiden er i samsvar med de til enhver tid gjeldende lover og rutiner, og at medarbeidere med autorisert tilgang benytter informasjonssystemet i tråd med nedfelte rutiner. Videre skal internkontrollen sikre at den registrertes rettigheter blir ivaretatt. Når det forekommer avvik fra nedfelte databehandlingsrutiner, skal dette registreres som avvik og avviksbehandles.

Akseptabelt risikonivå

Sikkerhetsbrudd aksepteres ikke. Virksomheten erkjenner like fullt at det eksisterer sannsynlighet for at sikkerhetsbrudd kan forekomme. For å begrense sannsynlighet for uønskede hendelser, etableres akseptkriterier knyttet til risiko.

Med "akseptabel risiko" menes i styringssystemet hvor stor risiko regionen kan akseptere, for at det inntreffer en hendelse som kan forårsake brudd på konfidensialitet, tilgjengelighet eller integritet for helse- og personopplysninger.

Sikkerhetstiltak skal etableres slik at sannsynligheten for, og konsekvensen av, sikkerhetsbrudd ikke overstiger akseptabelt risikonivå.

Virksomheten skal gjennomføre risikovurderinger for å fastslå om akseptabelt risikonivå oppnås. Det er virksomhetens informasjonssikkerhetsleder som godkjenner risiko på Sykehuset Østfold HFsvegne og i samsvar med regionens akseptkriterier.

Sikkerhetstiltak skal etableres slik at:

- tiltakene omfatter både rutiner medarbeiderne forutsettes å følge, og tiltak som i minst mulig grad kan påvirkes eller omgås uaktsomt av medarbeiderne
- tiltakene ikke kan omgås av eksterne, selv om disse opptrer med forsett
- det er liten sannsynlighet for at helse- og personopplysninger kompromitteres
- øvrige personopplysninger skal minimum sikres med tiltak som gir moderat grad av sannsynlighet for kompromittering, forutsatt at dette ikke øker sannsynligheten for kompromittering av sensitive personopplysninger
- ved bruk av nye publiserings- og kommunikasjonskanaler (Internett og sosiale medier) skal det også tas hensyn til at innsynsrett i personopplysninger fra offentligheten ikke er det samme som rett til å publisere de samme personopplysningene
- det går flere år mellom hendelser med moderat konsekvens for helsehjelpen, forholdet til pasienten, helseforetaket/-personellet og for øvrige medarbeidere
- hendelser med alvorlig konsekvens er enda vanskeligere å forårsake og inntreffer enda sjeldnere

For å forebygge vesentlig fare for liv eller alvorlig helseskade, vil kravet til konfidensialitet kunne settes til side for å sikre nødvendig tilgjengelighet på opplysninger. Et slikt brudd på konfidensialiteten skal behandles som sikkerhetsavvik i etterkant og loggføres.

Risikostyring skal inngå i virksomhetsstyringen.

Avvik eller dissens

Informasjonssikkerhetsleder/personvernombud kan benyttes for rådføring, og bistår dersom rådføring med Datatilsynet er ønskelig.

Referanser

F/2.1.2-05	Saksbehandling - E-post, bruk og behandling
F/2.1.4-07	Telefoni - bruk av mobiltelefon
F/17.1-06	Hjemmeområder og e-postkonti - innsyn
F/17.1-09	Passordpolicy - krav til passord
F/17.1-12	Loggføring av aktivitet og kontroll av logg
F/17.1-13	Lagring, arkivering og sletting av helse- og personopplysninger
F/17.1-14	Utlevering av helse- og personopplysninger
F/17.1-15	Anonymisering
F/17.1-16	Sikkerhetsprinsipper og -krav for IKT-infrastruktur
F/17.1-17	Sikkerhetsinstruks - informasjonssikkerhet. Sykehuset Østfold HF
F/17.1-19	Sikkerhetsstrategi - informasjonssikkerhet
F/17.1-20	Organisering av informasjonssikkerhetsarbeidet
Lov 2000.04.14 nr. 31:	Lov om behandling av personopplysninger (personopplysningsloven)
Lov 2000.12.15:	Lov om behandling av personopplysninger (personopplysningsforskriften)
Lov 2014.06.20 nr. 42:	Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)
Lov 2014.06.20 nr. 43:	Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
Lov 1999-07-02 nr. 63:	Lov om pasientrettigheter (pasientrettighetsloven)

•

Vedlegg

Slutt på Prosedyre

Vedlegg 9

HELSE SØR-ØST

Rapport 8/2016
Revisjon
Leverandørenes tilgang til helse- og personopplysninger i Medisinsk-teknisk utstyr (MTU) i Sykehuset Østfold HF

Konsernrevisjonen
Helse Sør-Øst
23.06.2016

Rapport nr.	8/2016
Revisjonsperiode	Mai – juni 2016
Virksomhet	Sykehuset Østfold HF
Rapportmottaker	Styret i Sykehuset Østfold HF v/ styreleder Administrerende direktør Sykehuset Østfold HF
Kopi	Administrerende direktør Helse Sør-Øst RHF Revisjonsutvalget Helse Sør-Øst RHF
Rapportavsender	Konsernrevisjonen Helse Sør-Øst RHF
Oppdragsgiver	Styret i Helse Sør-Øst RHF
Revisor	Liv Todnem (oppdragseier), Tove Kolbeinsen (oppdragsleder), Anders Blix

Innholdsfortegnelse

Sammendrag

I denne rapporten presenteres resultatene av konsernrevisjonens revisjon *Leverandørenes tilgang til helse- og personopplysninger i Medisinsk-teknisk utstyr (MTU).*

Bakgrunnen for revisjonen er at MTU i økende grad inneholder helse- og personopplysninger, og utstyret integreres med andre systemer, herunder IKT-systemer. Roller og ansvar til de ulike aktørene både i bruk og forvaltning er viktig. Det er gjennomført en rekke tiltak i foretaksgruppen i Helse Sør-Øst for å sikre at informasjonssikkerheten knyttet til helse- og personopplysninger er ivaretatt. og Sykehuset Østfold HF har i forbindelse med prosjekt nytt sykehus på Kalnes (PNØ), eiet av Helse Sør-Øst RHF, vært pilot for en rekke av tiltakene som ett ledd i arbeidet med mer helhetlig og målrettet informasjonssikkerhet i helseforetakene.

Revisjonen har kartlagt og vurdert om leverandørenes tilganger til helse- og personopplysninger i MTU er i henhold til informasjonssikkerhetskrav, regulert i avtale, og om tilgangsstyring og kontroller er hensiktsmessige.

Følgende problemstillinger er belyst:

1. Er det etablert et system hvor krav til informasjonssikkerhet i MTU inngår i anskaffelsesprosessen og blir ivaretatt i avtale med MTU-leverandøren?
2. Blir krav til informasjonssikkerhet operasjonalisert og etterlevd?

Konsernrevisjonen har valgt å dele området som er revidert inn i følgende steg:

I tillegg til Sykehuset Østfold HF har Sykehuspartner HF en viktig rolle og ansvar. Det henvises til kapittel 1.5 for mer informasjon.

Revisjonen viser at det ikke er etablert et oppdatert styringssystem som fungerer som et overordnet rammeverk, og som i tilstrekkelig grad bidrar til at informasjonssikkerheten i MTU blir ivaretatt.

Det er i Sykehuset Østfold HF en prosedyre for anskaffelser av MTU, men den beskriver ikke prosesser som eksplisitt ivaretar krav til informasjonssikkerhet i MTU. Konsekvensen er at det er en økt risiko for at Sykehusets Østfold HF's standard for informasjonssikkerhet ikke blir lagt som en forutsetning i avtalen med MTU-leverandørene.

Revisjonen viser at roller og ansvar er fordelt mellom Sykehuset Østfold HF, Sykehuspartner HF og MTU-leverandørene når det gjelder behandlingen av helse- og personopplysninger, og at dette i all hovedsak er tilstrekkelig dokumentert.

Tildeling av MTU-leverandørenes rettigheter er satt i system, med en avklart ansvars- og rolledeling mellom Sykehuset Østfold HF og Sykehuspartner HF. Sykehuset Østfold HF har ikke en samlet oversikt over hvilke leverandører som har tilgang til sykehusets MTU gjennom fjernaksess. MTU-leverandørene får kun tilgang til servere og data de er autorisert for, men leverandørportalen og VPN gir ikke mulighet for å forhindre eller avdekke MTU-leverandørenes eventuelle misbruk av sensitiv informasjon.

Avvikshåndteringen, ledelsens gjennomgang og risikovurderinger er satt i system, mens sikkerhetsrevisjoner og oppfølging av databehandler ikke er gjennomført etter avsluttet PNØ på MTU-området. Det vil si at dagens oppfølging av informasjonssikkerhet på Sykehuset Østfold HF innenfor MTU-området ikke er fullstendig i henhold til kravene i Normen.

Konsernrevisjonens overordnede vurdering er at problemstillingene er delvis oppfylt, og det er gitt anbefalinger med hensyn til svakheter i internkontrollen.

Det henvises til kapitel 2 for mer detaljert informasjon under de ulike problemstillingene.

Det presiseres at denne revisjonen i utgangspunktet kun omfatter ett element av informasjonssikkerheten (konfidensialitet) i MTU ved Sykehuset Østfold HF. Revisjonen vurderer med andre ord ikke totalbildet for informasjonssikkerhet i MTU og den vurderer heller ikke Medisinteknisk avdelings totale forvaltning av MTU på Sykehuset Østfold HF.

1 Innledning

1.1 Bakgrunn og beskrivelse av revisjonen

Revisjon av leverandørenes tilgang til helse- og personopplysninger i Medisinsk-teknisk utstyr (MTU) er gjennomført i henhold til revisjonsplan 2016-2017 for konsernrevisjonen. Revisjonsplanen er godkjent av styret i Helse Sør-Øst RHF.

MTU inneholder i økende grad helse- og personopplysninger, og utstyret integreres med andre systemer, herunder IKT-systemer. Roller og ansvar til de ulike aktørene både i bruk og forvaltning er viktig.
I protokoll fra foretaksmøte i Helse Sør-Øst RHF med eier, 12. januar 2016 - Krav og rammer mv. for 2016, fremkommer det at de regionale helseforetakene i samarbeid skal vurdere organiseringen av enheter for medisinsk-teknisk utstyr og øvrige enheter innen IKT for å sikre en samlet tilnærming og kompetanse på informasjon og personvern i sykehusenes systemer. Videre er det i "Oppdrag og bestilling 2016 for Sykehuset Østfold HF", 18. februar 2016, pekt på at det er av stor viktighet at det arbeides helhetlig og målrettet med informasjonssikkerhet.

Det er gjennomført en rekke tiltak i foretaksgruppen i Helse Sør-Øst for å sikre at informasjonssikkerheten knyttet til helse- og personopplysninger er ivaretatt og Sykehuset Østfold HF har i forbindelse med nytt sykehus på Kalnes (prosjekt betegnet PNØ) vært pilot for en rekke av tiltakene som ett ledd i arbeidet med mer helhetlig og målrettet informasjonssikkerhet i helseforetakene.

1.2 Mål og problemstillinger

Formålet med revisjonen følger av helseforetaksloven § 37a Internrevisjon, og er å bekrefte helseforetakets styring og kontroll, risikostyring og virksomhetsstyring, og bidra til forbedring.

Målet med revisjonen er å kartlegge og vurdere om leverandørenes tilganger til helse- og personopplysninger i MTU er i henhold til informasjonssikkerhetskrav, regulert i avtale, og om tilgangsstyring og kontroller er hensiktsmessige.

For å svare opp dette er det definert følgende problemstillinger:

1. Er det etablert et system hvor krav til informasjonssikkerhet i MTU inngår i anskaffelsesprosessen og blir ivaretatt i avtale med MTU-leverandøren?
2. Blir krav til informasjonssikkerhet operasjonalisert og etterlevd?

1.3 Omfang og avgrensning

I forbindelse med bygging av nytt sykehus har det vært etablert et prosjekt "Nytt Østfoldsykehus (PNØ)" i Sykehuset Østfold HF, og i den forbindelse har prosjektorganisasjonen ivaretatt en del oppgaver knyttet til anskaffelser av nytt MTU.

I forbindelse med PNØ er en svært stor andel av MTU ved Sykehuset Østfold HF nyanskaffet. PNØ er nå avsluttet og overlevert til Sykehuset Østfold HF, og rutiner og systemer tilpasses en løpende driftsfase. Revisjonen vil omfatte systemet som Sykehuset Østfold HF nå har etablert for informasjonssikkerhet knyttet til MTU-leverandørenes tilganger til helse- og personopplysninger.

Det er i regi av Helse Sør-Øst RHF planlagt en evaluering av modell for drift og forvaltning av IKT/MTU i Sykehuset Østfold HF. Ansvarlige for evalueringen og konsernrevisjonen har avstemt planlagt arbeid for å sikre at evalueringen og denne revisjonen er koordinert når det gjelder områder som inngår i revisjonen, tidsplan for gjennomføring og synergier.

Konsernrevisjonen har definert området som inngår i revisjonen i tre steg:

I tillegg til Sykehuset Østfold HF har Sykehuspartner HF en viktig rolle og ansvar. Det henvises til kapittel 1.5 for mer informasjon.

Det presiseres at denne revisjonen i utgangspunktet kun omfatter ett element av informasjonssikkerheten (konfidensialitet) i MTU ved Sykehuset Østfold HF. Revisjonen vurderer med andre ord ikke totalbildet for informasjonssikkerhet i MTU og den vurderer heller ikke MTAs totale forvaltning av MTU på Sykehuset Østfold HF.

Revisjonen vil ikke omfatte:

- Det innkjøpstekniske i anskaffelsesprosessen i forbindelse med inngåelse av avtaler
- Prosesser og systemer som Sykehuspartner HF er ansvarlig for relatert til informasjonssikkerhet i MTU
- Vurdering av Sykehuspartner HF i egenskap av databehandler
- Gjennomgang og bruk av avvikssystemet Synergi.

1.4 Revisjonsgrunnlag og metode

Revisjonsgrunnlaget som er lagt til grunn for utviklingen av revisjonene er hentet fra

- Lov- og forskriftskrav
  - Personopplysningsloven (lov 14. april 2000 nr. 31)
  - Personopplysningsforskriften (forskrift 15. desember 2000 nr. 1256)
  - Helseregisterloven (lov 20. juni 2014 nr. 43)
  - Pasientjournalloven (lov 20. juni 2014 nr 42)
  - Forskrift om internkontroll i helse- og omsorgstjenesten (forskrift 20. desember 2002 nr. 1731)
- Norm for informasjonssikkerhet i Helse- og omsorgstjenesten, 5. utgave (versjon 5.1), 4. juni 2015 (videre i rapporten betegnet Normen)
- Rammeverk for virksomhetsstyring, intern styring og kontroll Helse Sør-Øst
- Sykehuset Østfold HFs egne styrende dokumenter og prosedyrer.

Normen er utarbeidet med sikte på å bidra til tilfredsstillende informasjonssikkerhet hos den enkelte virksomhet og i sektoren generelt. Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Oppfylles disse kravene, er dagens regelverk vedrørende tilfredsstillende informasjonssikkerhet oppfylt[1].

I denne rapporten benyttes begrepet "helse- og personopplysninger" med samme innhold som i Normen, hvor begrepet er en fellesbetegnelse for helse- og/eller personopplysninger[2]. Med "helseopplysninger" menes i Normen taushetsbelagte opplysninger i henhold til helsepersonelloven § 21, jf. helseregisterloven § 2 a) og pasientjournalloven § 2 a). Med "personopplysninger" menes i Normen opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1). Sensitive personopplysninger er opplysninger om blant annet helseforhold, jf. personopplysningsloven § 2 nr. 8).

Revisjonen er utført ved bruk av revisjonsmetodene dokumentundersøkelse og intervju.

1.5 Bakgrunnsinformasjon om behandling av helse- og personopplysninger og samhandlingen mellom SØ HF, SP HF og MTU-leverandører

I rapporten brukes begrepene databehandler og databehandlingsanvarlig. Med databehandlingsansvarlig[3] menes den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes, med visse forbehold[4]. Det er Sykehuset Østfold HF som er databehandlingsansvarlig for behandling av helse- og personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten.

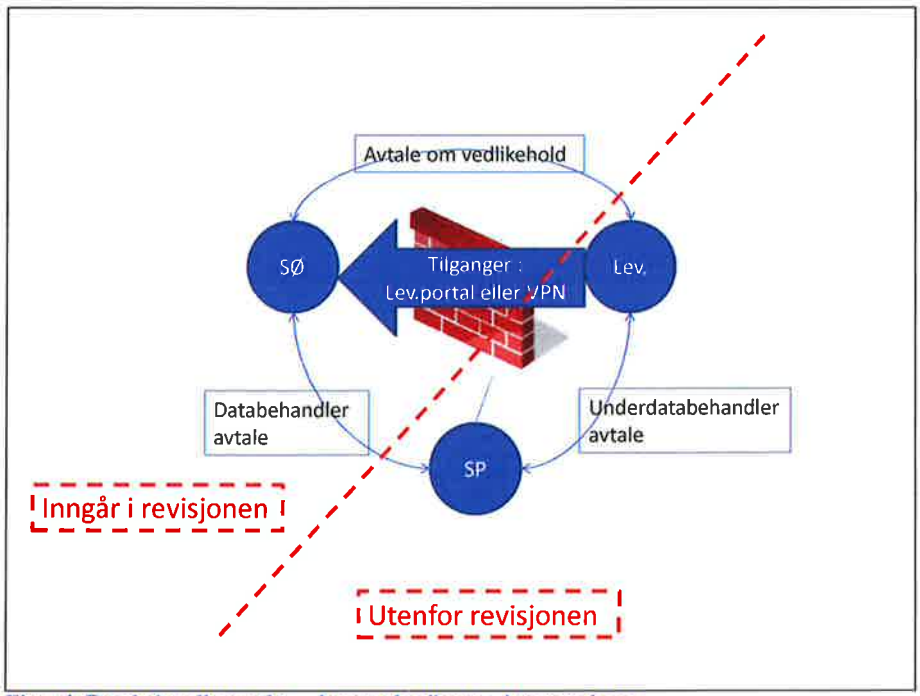
[1] Jf. Norm for informasjonssikkerhet, forord og punkt 1.0 Bakgrunn
[2] Jf. Norm for informasjonssikkerhet, punkt 1.1 Definisjoner.
[3] Jf. Norm for informasjonssikkerhet, punkt 1.1 Definisjoner.
[4] ... hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 e), pasientjournalloven § 2 e) og personopplysningsloven § 2 nr. 4).

Med databehandler menes den som behandler helse- og personopplysninger på vegne av den databehandlingsansvarlige, jf. personopplysningsloven § 2 nr. 5). Databehandler er en ekstern person eller virksomhet utenfor den databehandlingsansvarliges virksomhet.

Sykehuspartner HF er databehandler for alt IKT-utstyr som kjører på Sykehuspartner HFs infrastruktur. Dette omfatter alt MTU ved Sykehuset Østfold HF som er koblet til nett.

Ansvars- og oppgavefordelingen mellom Sykehuset Østfold HF og Sykehusparter HF er nedfelt i en tjenesteavtale[5]. I avtalens bilag 10 Databehandleravtale beskrives formålet med behandling av personopplysninger mv. Sykehuspartner HF er ansvarlig for å tegne underdatabehandleravtale med leverandører som skal ha fjernaksess til Sykehuset Østfold HFs MTU, jf. Figur 1.

Sykehuspartner HF drifter og vedlikeholder en standardløsning – leverandørportalen – for å gi eksterne leverandører tilgang til Sykehuset Østfold HFs utstyr, se Figur 1. VPN-tilgang kan i noen tilfeller gis utenfor standardløsningen. Det er Sykehuset Østfold HF som autoriserer brukere og bestiller tilganger via leverandørportalen.



Figur 1: Databehandleravtale og leverandørtilgang. Avgrensninger.

Medisinsk-teknisk avdeling ved Sykehuset Østfold HF (videre forkortet MTA) har ansvar for service og vedlikehold av sykehusets MTU. Avdelingen har en egen faggruppe for IKT. I tillegg er det en IKT-avdeling, hvor informasjonssikkerhetsleder er plassert. IKT-avdelingen er en premissgiver overfor MTA med hensyn til informasjonssikkerhet. Det er tett dialog mellom avdelingene.

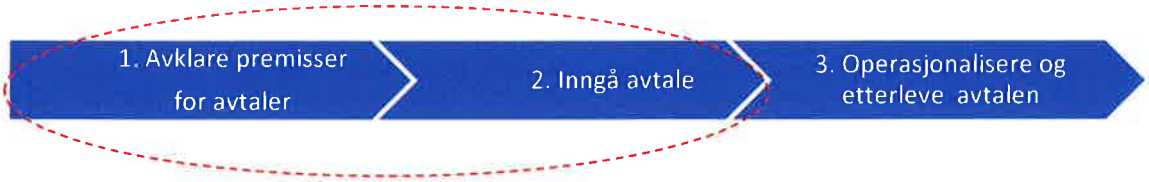
[5] Driftsavtalen – Avtale om kjøp av driftstjenester knyttet til maskinvare, infrastruktur og programvare.

1.6 Veiledning til leseren.

I kapittel 2 presenteres resultat av revisjonen per problemstilling. For hver problemstilling utdypes det enkelte revisjonskriteriet. Deretter beskrives det som er vurdert å være positivt i henhold til revisjonskriteriet (observasjon), hva som er vurdert å være svakheter/mangler, samt konsernrevisjonens vurdering og eventuelle anbefalinger til tiltak.

2 Oppsummering av revisjonen

2.1 Er det etablert et system hvor krav til informasjonssikkerhet i MTU inngår i anskaffelsesprosessen og blir ivaretatt i avtale med MTU-leverandøren?



Revisjonskriterium 1: Det er etablert et styringssystem for informasjonssikkerhet som omfatter behandling av helse- og personopplysninger ved bruk av MTU-leverandører

I henhold til revisjonsgrunnlaget er det en forutsetning at Sykehuset Østfold HF skal ha et styringssystem for informasjonssikkerhet[6]. Styringssystemet skal være kjent, tilgjengelig og oppdatert. Normen spesifiserer kravene som fremkommer av lovverket[7]: Det må blant annet fremgå i styringssystemet ansvar og organisering av anskaffelser, drift og forvaltning av MTU og MTU-leverandører.

Observasjoner

Sykehuset Østfold HF har utarbeidet dokumentet "Styringssystem for informasjonssikkerhet", versjon 1.0, datert 22. mai 2006. I dokumentet omtales de fleste områder som skal inngå i et styringssystem. Revisjonen viser at dagens praksis på flere områder er tilpasset nye krav og den teknologiske utviklingen, selv om dokumentet er fra 2006.

For den felles infrastrukturen på Sykehuset Østfold HF er det planlagt et nivå for sikkerhet som definerer hvordan de enkelte IKT-systemer og utstyrsleveranser skal implementeres. Dette er dokumentert i "E21 - IT-teknisk rammeverk og informasjonssikkerhet", datert 1. mars 2013. Dette rammeverket har vært brukt i forbindelse med PNØ.

Svakheter/mangler

Revisjonen viser at dokumentasjonen av styringssystemet for informasjonssikkerhet ikke er oppdatert og ikke i bruk som styringsverktøy. I dokumentet E21 (jf. forrige avsnitt) er ikke oppdatert siden 2013.

---

[6] Norm for informasjonssikkerhet i Helse- og omsorgstjenesten har krav til innhold i et styringssystem for informasjonssikkerhet, jf. avsnittene 3.2 og 3.3. Sentrale elementene i styringssystemet er: Sikkerhetsmål, sikkerhetsstrategi, nivå for akseptabel risiko (mht. konfidensialitet, integritet og tilgjengelighet), oversikt over behandling av helse- og personopplysninger og risikovurderinger.

[7] Jf. Normen, punktene 3.2 Oversikt over oppgaver som omfattes av det daglige ansvaret for informasjonssikkerhet og 3.3 Dokumentasjon.

Konsernrevisjonen er informert om at det pågår et regionalt arbeid i Helse Sør-Øst RHF med å utarbeide en mal for styringssystem for informasjonssikkerhet. Malen skal danne grunnlag for alle helseforetakene, og et oppdatert styringssystem for informasjonssikkerhet for Sykehuset Østfold HF er under utarbeidelse, men ikke ferdigstilt på revisjonstidspunkt.

Konsernrevisjonens vurderinger

Revisjonen viser at gjeldende dokumentasjon av styringssystemet ikke er oppdatert og således lite egnet som styringsredskap med tanke på at det skal være en del av Sykehuset Østfold HFs internkontrollsystem. Internkontrollsystemet skal angi aktiviteter for å rettlede og styre virksomheten når det gjelder informasjonssikkerhet.

Revisjonen viser at det dokumenterte rammeverket for informasjonssikkerhet (E21) ikke er oppdatert siden 2013. Uten oppdateringer mister rammeverket raskt sin verdi, jamfør følgende sitat fra dokumentet E21: "På grunn av at teknologien er preget av hurtige endringer, vil det være nødvendig å revidere dokumentet med jevne mellomrom, (typisk 1 gang per år)[8]".

På bakgrunn av vurderingene anbefales det følgende:

- Arbeidet med å oppdatere styringssystemet for informasjonssikkerhet ferdigstilles og tilgjengeliggjøres, slik at det danner et grunnlag for informasjonssikkerhet i blant annet MTU.
- Etablere en oppdatert sikkerhetsnorm, -standard eller lignende som stiller krav til informasjonssikkerheten i MTU-miljøet.

Revisjonskriterium 2: Krav til informasjonssikkerhet inngår i anskaffelsesprosessen for MTU

I henhold til revisjonsgrunnlaget er det en forutsetning at det er en prosess for at det utarbeides konkrete krav til informasjonssikkerhet i en kravspesifikasjon, at det involveres ressurser med kompetanse på informasjonssikkerhet til å vurdere leverandørenes svar på kravspesifikasjon og sikre at informasjonssikkerhet blir medtatt i kjøps- og vedlikeholdsavtaler med MTU-leverandørene.

Observasjoner

Det er utarbeidet en prosedyre for anskaffelse av MTU[9]-utstyr som er tilpasset Sykehuset Østfold HF i ordinær drift. Det er utarbeidet et skjema som sendes MTA og godkjennes. Anskaffelser av MTU initieres av MTA, og prosessen som helhet styres av Innkjøpsavdelingen. Ved gjennomføring av selve anskaffelsen blir en rådgiver fra MTA involvert og vedkommende håndterer da informasjonssikkerhetsmessige forhold i prosessen.

Svakheter/mangler

Det er ikke beskrevet noen spesifikk aktivitet i prosedyren for anskaffelser som medfører at kravene til informasjonssikkerhet (jf. E21 - IT-teknisk rammeverk og informasjonssikkerhet) blir ivaretatt i kravspesifikasjonen for MTU.

[8] E21 IT-teknisk rammeverk og informasjonssikkerhet, pkt. 1.1 Orientering, 2. avsnitt.
[9] Prosedyre for medisinsk-teknisk utstyr – anskaffelse

Det er ikke noen standardisert mal for utarbeidelse av serviceavtaler med MTU-leverandører med krav til informasjonssikkerhet. I mange tilfeller benyttes leverandørens avtalemal.

Konsernrevisjonen er informert om at det pågår et arbeid på regionalt nivå i Helse Sør-Øst RHF med å utarbeide mal for inngåelse av avtale om vedlikehold av medisinsk-teknisk utstyr som inkluderer krav til informasjonssikkerhet knyttet til helse- og personopplysninger. Dette dokumentet var ikke implementert ved vår revisjon.

Konsernrevisjonens vurderinger
Revisjonen viser at det er ingen formalisert prosess som på en helhetlig måte sikrer at krav til informasjonssikkerhet blir ivaretatt i anskaffelsesprosessen for MTU.

På bakgrunn av vurderingene anbefales det følgende:

- Etablere en prosess som sikrer at det ved anskaffelser av MTU stilles krav til informasjonssikkerhet overfor leverandøren og ved vurdering av leverandørens svar.
- Ta i bruk ny mal så snart den er ferdig for avtale om vedlikehold av MTU.

Revisjonskriterium 3: Avtaler om kjøp mellom Sykehuset Østfold HF og MTU-leverandør regulerer informasjonssikkerhet

I henhold til revisjonsgrunnlaget er det en forutsetning at det i inngåtte kjøpsavtaler er medtatt konkrete krav til informasjonssikkerhet.

Observasjoner
Konsernrevisjonen har innhentet tre kjøpsavtaler som er inngått i 2014-2016 og undersøkt om krav til informasjonssikkerhet er medtatt i avtalene. De fleste avtaler i denne perioden er inngått i regi av PNØ.

Testen viser at i en av avtalene (Kjøp av CT, 26. juni 2014) er det utarbeidet en kravspesifikasjon der det henvises til kapitel 1.2.11 "VPN og fjerndriftsløsninger" i bilag E21 "IT-teknisk rammeverk og informasjonssikkerhet", som leverandøren har besvart. I det kapitlet stilles det krav om at leverandøren avgir taushetserklæring, aksepterer sluttbrukerpolicy og inngår databehandleravtale.

Svakheter/mangler
Testen viser at to[10] av de tre avtalene ikke inneholder noen krav til informasjonssikkerhet. I en av avtalene er det beskrevet noe om generell sikkerhet i selve avtalen, men krav er ikke tatt med i kravspesifikasjonen som leverandøren har besvart (et av bilagene til avtalen).

Konsernrevisjonens vurderinger
Revisjonen viser at krav til informasjonssikkerhet i varierende grad er regulert i de undersøkte avtalene. Mangelen på konsistens er en konsekvens av at krav til informasjonssikkerhet ikke i tilstrekkelig grad er innarbeidet i de tidligere fasene i anskaffelsesprosessen.

[10] Kjøp av ArbeidsEKG. Avtalen er inngått 26.5.2015
Kjøp av Morsmelkanalysator. Avtalen er inngått 15.2.2016.

På bakgrunn av vurderingene anbefales det følgende:

- Etablere en prosess som sikrer at det ved utarbeidelse av avtale med MTU-leverandører stilles krav til informasjonssikkerhet, jf. revisjonskriterium 2, første anbefaling.

Samlet oppsummering for problemstillingen:

Revisjonen viser at dokumentasjonen av styringssystemet for informasjonssikkerhet, herunder rammeverk for IKT og informasjonssikkerhet, ikke er oppdatert.

Konsernrevisjonens vurdering er at det gjeldende styringssystemet er lite egnet som en del av Sykehuset Østfold HFs internkontrollsystem.

Det er utarbeidet en prosedyre for anskaffelse av MTU som er tilpasset Sykehuset Østfold HF, men det er ikke beskrevet noen spesifikk aktivitet som medfører at krav til informasjonssikkerhet blir ivaretatt i kravspesifikasjoner og i avtaler med MTU-leverandørene.

Revisjonen viser at krav til informasjonssikkerhet i varierende grad er regulert i de undersøkte avtalene.

Konsernrevisjonens vurdering er at krav til informasjonssikkerhet ikke i tilstrekkelig grad er innarbeidet i de tidligere fasene i anskaffelsesprosessen. En mulig konsekvens av dette er en inkonsistens med hensyn til behandlingen av informasjonssikkerhet i avtalene med MTU-leverandørene.

2.2 *Problemstilling 2: Blir krav til informasjonssikkerhet operasjonalisert og etterlevd?*

Revisjonskriterium 1: Det er utarbeidet en tjenesteavtale og tjenestebeskrivelser som regulerer ansvarsforholdet mellom Sykehuset Østfold HF og Sykehuspartner HF

I henhold til revisjonsgrunnlaget er det en forutsetning at det er etablert en tjenesteavtale som regulerer ansvarsforholdet mellom Sykehuset Østfold HF og Sykehuspartner HF. I avtalen skal det fremgå både Sykehuset Østfold HFs og Sykehuspartner HFs oppgaver og ansvar som databehandler og databehandlingsansvarlig, og de respektives ansvar i forholdet til MTU-leverandørene. I tillegg til avtalen skal det være tjenestebeskrivelser som detaljerer tjenesteavtalen med hensyn til drift og forvaltning av MTU. Krav til informasjonssikkerhet skal være regulert mellom partene.

Observasjoner

Det er etablert en tjenesteavtale mellom Sykehuset Østfold HF og Sykehuspartner HF for 2016 som regulerer tjenester, roller og ansvar mv. mellom partene. Avtalens bilag 10 er en databehandleravtale

med Sykehuset Østfold HF som databehandleransvarlig og Sykehuspartner HF som databehandler, hvor Sykehuspartner HF forplikter seg til å følge kravene i Normen.

I tjenesteavtalens bilag 10 fremgår det at Sykehuspartner HF er ansvarlig for å inngå databehandleravtale med tredjeparter, herunder MTU-leverandører. Sykehuspartner HF har utarbeidet en instruks "Databehandleravtale for underleverandører av Sykehuspartner." Instruksen er en mal for avtaler som skal inngås mellom Sykehuspartner HF og MTU-leverandør som behandler helse- og personopplysninger (Underleverandørdatabehandleravtale). Avtalen inneholder eksplisitte krav, herunder krav til oppfyllelse av Normen.

I PNØ ble det anskaffet mye nytt MTU og tjenestebeskrivelser ble utarbeidet for alt utstyret. Det er etablert en rutine som stiller krav til at det utarbeides tjenestebeskrivelser i forbindelse med anskaffelser av nytt MTU.

Svakheter/mangler
Revisjonen viser at for en del eldre utstyr ved Sykehuset Østfold HF som er anskaffet før PNØ ikke er utarbeidet tjenestebeskrivelser.

Konsernrevisjonens vurderinger
Revisjonen viser at det er etablert rutiner som sikrer at både avtaler og tjenestebeskrivelser utarbeides, men at det for deler av utstyret anskaffet før PNØ mangler tjenestebeskrivelser. Dette kan medføre at det kan oppstå usikkerhet rundt vesentlig informasjon med hensyn til drift og forvaltning av utstyret.

På bakgrunn av vurderingene anbefales det følgende:

- Sykehuset Østfold HF gjennomgår utstyr anskaffet før PNØ og i samarbeid med Sykehuspartner HF utarbeider tjenestebeskrivelser på MTU der det mangler.

Revisjonskriterium 2: Risikoanalyser og dokumentert konfigurasjon ligger til grunn for implementering og drift av MTU-utstyr

I henhold til revisjonsgrunnlaget skal det være etablert rutiner med blant annet roller og ansvar for gjennomføring og oppfølging av risikovurderinger og tilhørende tiltaksarbeid.

Risikovurdering gjennomføres før implementering av MTU hvor helse- og personopplysninger behandles, ved endringer i MTU-miljøet som kan påvirke informasjonssikkerheten og jevnlig for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser.

Observasjoner
Ved nyanskaffelser eller større endringer i eksisterende utstyr og modaliteter i MTU-miljøet bestiller Sykehuset Østfold HF en risiko- og sårbarhetsanalyse fra Sykehuspartner HF i henhold til tjenesteavtalen. Sykehuspartner HF utarbeider også et løsningsdesign, der forhold som fremkommer under risiko- og sårbarhetsanalysen innarbeides. Risiko- og sårbarhetsanalysen samt løsningsdesignet ligger til grunn for implementering av nyanskaffelsene og/eller endringene i driftsmiljøet og for den påfølgende driften og forvaltningen av løsningene.

Det er ved Sykehuset Østfold HF en generell rutine i EK[11] for gjennomføring og oppfølging av risikovurderinger som også omfatter MTU. Denne rutinen har så langt ikke vært aktuell for MTU som har blitt anskaffet og risikovurdert i forbindelse med PNØ.

Sykehuset Østfold HF har utover dette påbegynt et arbeid for å systematisere og følge opp utestående risikoer og tiltak fra risikovurdering av MTU i PNØ.

Risikovurderinger som en del av ledelsens gjennomgang ved Sykehuset Østfold HF har vært gjennomført den 6. juni 2016. Gjennomgangen omfattet også MTU.

Konsernrevisjonens vurderinger
Revisjonen viser at det vesentligste av risikohåndtering innenfor MTU har vært rapportert i PNØ. Videre har ledelsens gjennomgang nå i juni også omfattet MTU, og konsernrevisjonen forutsetter at oppfølging av risiko vil skje i henhold til etablerte prosedyrer i EK i henhold til informasjon fra Sykehuset Østfold HF. Konsernrevisjonen legger til grunn at både overleverte risikoer fra PNØ og løpende risiko følges opp. På bakgrunn av dette har konsernrevisjonen ingen anbefalinger.

Revisjonskriterium 3: Prosedyrer for tildeling og administrasjon av tilgangsrettigheter omfatter MTU-leverandører, og leverandørens rettigheter i systemet samsvarer med det han er autorisert for

I henhold til revisjonsgrunnlaget skal det være etablert et system for tildeling og administrasjon av MTU-leverandørenes bruker-rettigheter på utstyr og applikasjoner. Ansvars- og rollefordelingen internt i og mellom Sykehuset Østfold HF og Sykehuspartner HF skal være avklart. Det skal være iverksatt tiltak som sikrer at MTU-leverandørens rettigheter er i samsvar med det han er autorisert for, og for å forhindre og kunne avdekke mulig misbruk.

Observasjoner
Det er MTA ved Sykehuset Østfold HF som forvalter administrator-rettighetene på MTU ved sykehuset. I tillegg til avdelingens egne ingeniører, kan administrator-rettigheter tildeles MTU-leverandører enten ved fjernaksess eller ved lokalt oppmøte.

Sykehuset Østfold HF har en dokumentert rutine for personlig oppmøte fra MTU-leverandør for avtalt vedlikehold og akutte reparasjoner. Leverandørens representant får en tidsbegrenset tilgang til det aktuelle utstyret og han ledsages under oppholdet på sykehuset enten av en medarbeider i MTA eller av en annen betrodd medarbeider ved sykehuset. Ved personlig oppmøte på sykehuset, er det av HSØ RHF vurdert slik at databehandleravtale med MTU-leverandøren ikke er nødvendig.

Det er Sykehuset Østfold HF som bestiller fjernaksess for MTU-leverandørene ved sykehuset. Sykehuspartner HF har ansvar for å sette opp fjernaksess til MTU-leverandører. Fjernaksess settes enten gjennom en løsning som benevnes VPN (Virtual Private Network) eller via en fellesportal som kalles leverandørportalen. Det er en retningslinje fra Sykehuspartner HF for å gi leverandører fjernaksess som blant annet innbefatter at leverandøren må underskrive både taushetserklæring og databehandleravtale.

Såfremt den tekniske løsningen ikke krever noe annet, gis leverandører fjernaksess via leverandørportalen. For at MTU-leverandøren skal kunne logge seg på leverandørportalen, må leverandørens

[11] EK – Elektronisk kvalitetssystem

representant opprettes som en SIKT[12]-bruker. I leverandørportalen logges tilgangs- og sesjonsdata og tilgangene er individuelle.

Tilgang via VPN brukes der driftsinformasjon fra MTU-systemet automatisk skal overføres til MTU-leverandøren. Beroende på avtale, kan MTU-leverandørens egne loggdata være tilgjengeliggjort for Sykehuset Østfold HF.

De tekniske løsningene sikrer at MTU-leverandørene kun får tilgang til de serverne og de data de er autorisert for, og alle MTU-leverandører med tilgang via leverandørportalen skal årlig autoriseres på nytt.

Svakheter/mangler

Med dagens løsninger er det er begrensede muligheter for Sykehuset Østfold HF og Sykehuspartner HF til å føre kontroll med leverandørenes aktiviteter gjennom fjernaksess. De kan ikke føre kontroll med når leverandøren utfører vedlikehold på systemene og med hva som transporteres av data til og fra sykehusets MTU-systemer.

VPN-løsningen gir ikke samme loggmuligheter som leverandørportalen (jf. observasjon over). Hverken Sykehuset Østfold HF eller Sykehuspartner HF har egne loggdata for MTU-leverandørens aktivitet på Sykehuset Østfold HFs systemer, og Sykehuset Østfold HF har ikke satt i system oppfølging av loggdata som leverandør har tilgjengeliggjort, jf. observasjon over.

Det foreligger ikke øvrige rutiner for forvaltning og oppfølging av brukerdatabaser (autorisasjonsregister). Sykehuset Østfold HF har ikke en samlet oversikt over hvilke leverandører som har tilgang til sykehusets MTU gjennom fjernaksess.

Konsernrevisjonens vurderinger

Revisjonen viser at tildeling av MTU-leverandørenes rettigheter er satt i system. Det er en avklart ansvars- og rolledeling mellom Sykehuset Østfold HF og Sykehuspartner HF med hensyn til autorisering og oppsett av fjernaksess for MTU-leverandører.

Revisjonen viser at de tekniske løsningene ikke er på det nivået sykehuset selv ønsker med hensyn til kontroll med leverandørenes aktivitet gjennom fjernaksess. Dette innebærer at Sykehuset Østfold HFs styring og kontroll med MTU-leverandørenes aktivitet samt mulighet til å forhindre og avdekke mulig misbruk av sensitiv informasjon, er begrenset.

Selv om det er et tillitsforhold mellom sykehus og leverandør, og leverandøren har avgitt taushetserklæring og underskrevet databehandleravtale, blir Sykehuset Østfold HF i stor grad avhengig av leverandørens interne kontrollrutiner med tanke på informasjonssikkerhet.

På bakgrunn av vurderingene anbefales det følgende:

- Sykehuset Østfold HF følger opp igangsatte aktiviteter for utvikling og implementering av forbedret tekniske løsninger for styring og kontroll med MTU-leverandørenes fjernaksess på sykehusets nettverk.
- Sykehuset Østfold HF etablerer og vedlikeholder autorisasjonsregister i henhold til krav i Normen.

[12] SIKT-plattformen: Betegnelse på Helse Sør-Øst RHFs tekniske plattform

Revisjonskriterium 4: System for oppfølging av informasjonssikkerhet er etablert

I henhold til revisjonsgrunnlaget skal ledelsen ved Sykehuset Østfold HF følge opp at informasjonssikkerheten på MTU-området ivaretas. Normen spesifiserer flere typer oppfølging[13], og videre er Sykehuset Østfold HF som databehandlingsansvarlig forpliktet til å følge opp Sykehuspartner HF som databehandler som igjen inngår databehandler-avtaler med MTU-leverandøren. Resultatene og konklusjonene fra oppfølgingen skal dokumenteres, og ansvar for oppfølging av tiltak skal være plassert.

Observasjoner

Risikovurderinger gjennomføres innenfor MTU-området i Sykehuset Østfold HF, jf. revisjonskriterium 2 over.

I henhold til tjenesteavtalen er det etablert ulike samhandlingsfora der blant annet informasjonssikkerhet kan være et tema. Det er videre definert en del indikatorer som Sykehuspartner HF rapporterer på til Sykehuset Østfold HF. Sykehuspartner HF varsler Sykehuset Østfold HF dersom hendelser som gjelder informasjonssikkerhet inntreffer. I forbindelse med hendelseshåndtering kan sikkerhetsleder ved Sykehuset Østfold HF involvere administrerende direktør.

Med hensyn til ledelsens gjennomgang, se revisjonskriterium 2 over.

Dersom hendelser som gjelder informasjonssikkerhet inntreffer i MTU som Sykehuset Østfold HF selv drifter, skal avvik registreres i avvikssystemet Synergi.

Svakheter/mangler

Revisjonen viser imidlertid at det ikke har vært gjennomført sikkerhetsrevisjoner i Sykehuset Østfold HF i den senere tid.

I de regelmessige oppfølgingsmøtene mellom Sykehuset Østfold HF og Sykehuspartner HF inngår ikke en systematisk oppfølging av Sykehuspartner HF som databehandler.

Konsernrevisjonens vurderinger

Revisjonen viser at oppfølgingssystemet i Sykehuset Østfold HF for informasjonssikkerhet innenfor MTU-området ikke har kommet fullstendig på plass etter PNØ. Avvikshåndteringen, ledelsens gjennomgang og risikovurderinger er satt i system, mens sikkerhetsrevisjoner og oppfølging av databehandler ikke er gjennomført etter PNØ på MTU-området.

[13] I Normen, avsnitt 6, er formene for oppfølging konkretisert:
- Sikkerhetsrevisjoner
- Risikovurderinger i virksomhetens enheter
- Avvikshåndtering
- Ledelsens gjennomgang
- Kontroll hvem som har hatt elektronisk tilgang til helse- og personopplysninger.

På bakgrunn av vurderingene anbefales det følgende:

- Sykehuset Østfold HF gjennomfører alle former for oppfølgingsaktiviteter med hensyn til informasjonssikkerhet innenfor MTU-området i henhold til Normen.

Samlet oppsummering for problemstillingen:

Revisjonen viser at det er etablert en tjenesteavtale mellom Sykehuset Østfold HF og Sykehuspartner HF for 2016 som regulerer roller og ansvar når det gjelder databehandleransvarlig og databehandler. Sykehuspartner HF har forpliktet seg til å følge kravene i Normen og å inngå databehandleravtale med tredjeparter, herunder MTU-leverandører. For en del eldre utstyr ved Sykehuset Østfold HF som er anskaffet før PNØ er det ikke utarbeidet tjenestebeskrivelser.

Konsernrevisjonen vurderer at kriteriet i stor grad er oppfylt, men at det for noe av utstyr anskaffet før PNØ mangler tjenestebeskrivelser.

Revisjonen viser at det er etablert en praksis for risikovurdering ved større omlegginger i MTU-miljøet i Sykehuset Østfold HF, og MTA er inkludert i ledelsens gjennomgang. Det foreligger også rutiner for løpende risikovurderinger som det ikke ennå har vært aktuelt å bruke for MTU. Det er i tillegg påbegynt et arbeid for å systematisere og følge opp utestående risikoer og tiltak fra risikovurdering av MTU i PNØ.

Konsernrevisjonen vurderer at risikovurderinger for MTU er satt i system.

Revisjonen viser at det er MTA ved Sykehuset Østfold HF som forvalter administrator-rettighetene på MTU ved sykehuset. Tildeling av MTU-leverandørenes rettigheter er satt i system, med en avklart ansvars- og rolledeling mellom Sykehuset Østfold HF og Sykehuspartner HF. Sykehuset Østfold HF har ikke en samlet oversikt over hvilke leverandører som har tilgang til sykehusets MTU gjennom fjernaksess. MTU-leverandørene får kun tilgang til de serverne og de data de er autorisert for, men utover dette gir de tekniske løsningene begrensede muligheter for styring og kontroll med MTU-leverandørenes aktivitet.

Konsernrevisjonen vurderer at tildeling av MTU-leverandørenes rettigheter, og ansvars- og rolledelingen mellom Sykehuset Østfold HF og Sykehuspartner HF, er satt i system. Men hverken leverandørportalen eller VPN-tilgangene gir mulighet for å forhindre eller avdekke MTU-leverandørenes eventuelle misbruk av sensitiv informasjon.

Revisjonen viser at avvikshåndteringen, ledelsens gjennomgang og risikovurderinger er satt i system, mens sikkerhetsrevisjoner og oppfølging av databehandler ikke er gjennomført etter PNØ på MTU-området.

Konsernrevisjonen vurderer at dagens oppfølging av informasjonssikkerhet på Sykehuset Østfold HF innenfor MTU-området ikke er tilstrekkelig i henhold til Normen.

Vedlegg 1 - Informasjonsgrunnlag, gjennomførte intervjuer, saksgang og rapportbehandling

Informasjonsgrunnlag

Dokumentasjon
Styresaker Helse Sør-Øst RHF
Brev om styringssignaler
Styringssystem for informasjonssikkerhet, Sykehuset Østfold HF
Organisasjonskart
Rutinebeskrivelser og håndbøker
Tjenesteavtale- og beskrivelser mellom Sykehuset Østfold HF og Sykehuspartner HF
Risiko- og sårbarhetsanalyser
Løsningsdesign
Databehandleravtale mellom Sykehuset Østfold HF og Sykehuspartner HF, og mal for databehandleravtale mellom Sykehuset Østfold HF og leverandør
Avtaler om kjøp, service og vedlikehold: - ArbeidsEKG - CT - Morsmelkanalysator

Gjennomførte intervjuer

Rolle
Leder Medisinsk-teknisk avdeling, Sykehuset Østfold HF
Informasjonssikkerhetsleder, Sykehuset Østfold HF
Leder avdeling Design og sikkerhet, Sykehuspartner HF

Saksgang og rapportbehandling

Dato	Aktivitet
19.06.16	Verifisering av detaljgrunnlag gjennomført
20.06.16	Oversendt utkast rapport fra revisjonen til administrerende direktør
21.06.16	Tilbakemelding på utkast rapport fra administrerende direktør
23.06.16	Oversendelse endelig rapport
September	Fremleggelse av endelig rapport og administrerende direktørs oppfølging av tiltaksarbeidet for styret

Vedlegg 10

SYKEHUSET ØSTFOLD

Tiltaksplan – konsernrevisjonens gjennomgang av leverandørenes tilgang til helse- og personopplysninger i MTU

Handlingsplan for oppfølging av anbefalinger etter revisjon av leverandørenes tilgang til helse- og personopplysninger i medisinsk teknologisk utstyr

Ansvarlige ledere for tiltaksplanen:
Bengt Thompson (IKT) og Sverre Granmark (MTA)

Anbefaling fra konsernrevisjonens rapport	Tiltak	Frist for gjennom-føring	Ansvarlig for gjennom-føring (utøver)	Mål-oppnåelse (%)	Status per 28.4.17	Videre oppfølging
1. *Arbeidet med å oppdatere styringssystemet for informasjonssikkerhet ferdigstilles og tilgjengeliggjøres, slik at det danner et grunnlag for informasjonssikkerhet i blant annet MTU.*	1-1: Arbeidet med Styringssystem for informasjonssikkerhet ferdigstilles i den regionale arbeidsgruppen, tilpasses og innføres i SØ.	1.10.16	Lars Cato Skaar	100 %	Gjennomført	
2. *Etablere en oppdatert sikkerhetsnorm, -standard eller lignende som stiller krav til informasjonssikkerheten i MTU-miljøet*	2-1: Innarbeide krav til informasjonssikkerhet i kravspesifikasjoner for alle anskaffelser av utstyr som tilkobles datanettverket. Kravene baseres på kravene i Norm for informasjonssikkerhet eller krav fra Sykehuspartner/SØ dersom sistnevnte er strengere enn normens krav.	1.7.16	Lars Cato Skaar	100 %	Gjennomført	

Anbefaling fra konsernrevisjonens rapport	Tiltak	Frist for gjennom-føring	Ansvarlig for gjennom-føring (utøver)	Mål-oppnåelse (%)	Status per 28.4.17	Videre oppfølging
3. *Etablere en prosess som sikrer at det ved anskaffelser av MTU stilles krav til informasjonssikkerhet overfor leverandøren og ved vurdering av leverandørens svar.*	3-1: Informasjonssikkerhetsleder deltar i anskaffelsesprosessen og sørger for at kravene i ovennevnte punkt besvares og oppfylles av leverandør.	1.9.16	Lars Cato Skaar og Cecilie Vitting	100 %	Gjennomført	
4. *Ta i bruk ny mal for avtale om vedlikehold av MTU*	4-1: Ny mal for avtale om vedlikehold av MTU inngås for fremtidige anskaffelser og alle fremtidige revideringer av leverandøravtaler.	1.10.16	Sverre Granmark	100 %	Gjennomført	
5. *Sykehuset Østfold HF gjennomgår utstyr anskaffet før PNØ og i samarbeid med Sykehuspartner HF utarbeider tjenestebeskrivelser på MTU der det mangler.*	5-1: Det utarbeides tjenestebeskrivelse på alt MTU som mangler dette. For utstyr som skal erstattes innen 1. halvår 2017, utarbeides det tjenestebeskrivelse på det nye utstyret.	31.12.16	Sverre Granmark	85 %	Ferdig	For utstyr som har integrasjon med annet utstyr eller servere er det utarbeidet tjenestebeskrivelse
6. *Sykehuset Østfold HF følger opp igangsatte aktiviteter for utvikling og implementering av forbedret tekniske løsninger for styring og kontroll med MTU-leverandørenes fjernaksess på sykehusets nettverk.*	6-1: Sykehuspartner har tilbudt en lokal analyseplattform som inneholder sensorer med mulighet for å overvåke trafikk i VPN. Pristilbudet er ikke akseptert av SØ. Det etterspørres om sensorene kan etableres uten at hele analyseplattformen må anskaffes.	1.11.16	Lars Cato Skaar	75 %	Pågår	Avtale ikke akseptert. Det arbeides med andre løsninger.
7. *Sykehuset Østfold HF gjennomfører alle former for oppfølgingsaktiviteter med*	7-1: Det etableres rutine for jevnlig gjennomgang i egen prosedyre for:	15.9.16	Lars Cato Skaar	100 %	Gjennomført	

Anbefaling fra konsernrevisjonens rapport	Tiltak	Frist for gjennom-føring	Ansvarlig for gjennom-føring (utøver)	Mål-oppnåelse (%)	Status per 28.4.17	Videre oppfølging
hensyn til informasjonssikkerhet innenfor MTU-området i henhold til Normen	▪ Sikkerhetsrevisjon (årlig) ▪ Revisjon av informasjonssikkerhet ved Sykehuspartner ▪ Gjennomgang av logger (kvartalsvis) ▪ Gjennomgang av autorisasjonsregister (årlig) ▪ Risikovurderinger (ved endringer og anskaffelser) ▪ Vurdering av risikobilde og oppfølging av tidligere gjennomførte risikovurderinger (årlig) ▪ Tilpasning av opplæringsmateriell (årlig)					
	7-2: Utarbeide organisasjonskart over roller med informasjonssikkerhet	1.10.16	Lars Cato Skaar	100 %	Gjennomført	
	7-3: Det igangsatte arbeidet med å systematisere aggregert risikobilde fra PNØ fortsetter. Risikoelementene registreres i EK Risikomodul for intern oppfølging.	1.12.16	Lars Cato Skaar	80 %	Gjennomført	Aggregert risikobilde ble gjennomgått og oppdatert i desember. Det gjenstår registrering i EK risikomodul.
	7-4: Etablere autorisasjonsregister for alle MTU med individuell pålogging.	1.12.16	Sverre Granmark	100 %	Ferdig	Etablert oversikt over alle som har tilgang til utstyr som krever innlogging
	7-5:	1.12.16	Lars Cato	100 %	Gjennomført	

Anbefaling fra konsernrevisjonens rapport	Tiltak	Frist for gjennom-føring	Ansvarlig for gjennom-føring (utøver)	Mål-oppnåelse (%)	Status per 28.4.17	Videre oppfølging
	Oppdatere opplæringsmateriell og informere opplæringsansvarlige til å eksplisitt informere om krav til informasjonssikkerhet.		Skaar			
	7-6: Informere medarbeidere i MTA om funn i revisjoner og risikobilde. Informasjonen må gis til MTA straks etter at revisjoner er gjennomgått. Det arrangeres en fagdag i august hvor Direktoratet for e-Helse presenterer Veileder for medisinsk utstyr. Dette markerer starten på en kontinuerlig gjennomgang av informasjonssikkerhet for MTU.	1.9.16	Lars Cato Skaar	100 %	Gjennomført	

Deltagere ved utarbeidelsen:
Lars Cato Skaar
Bengt Thompson
Sverre Granmark