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.

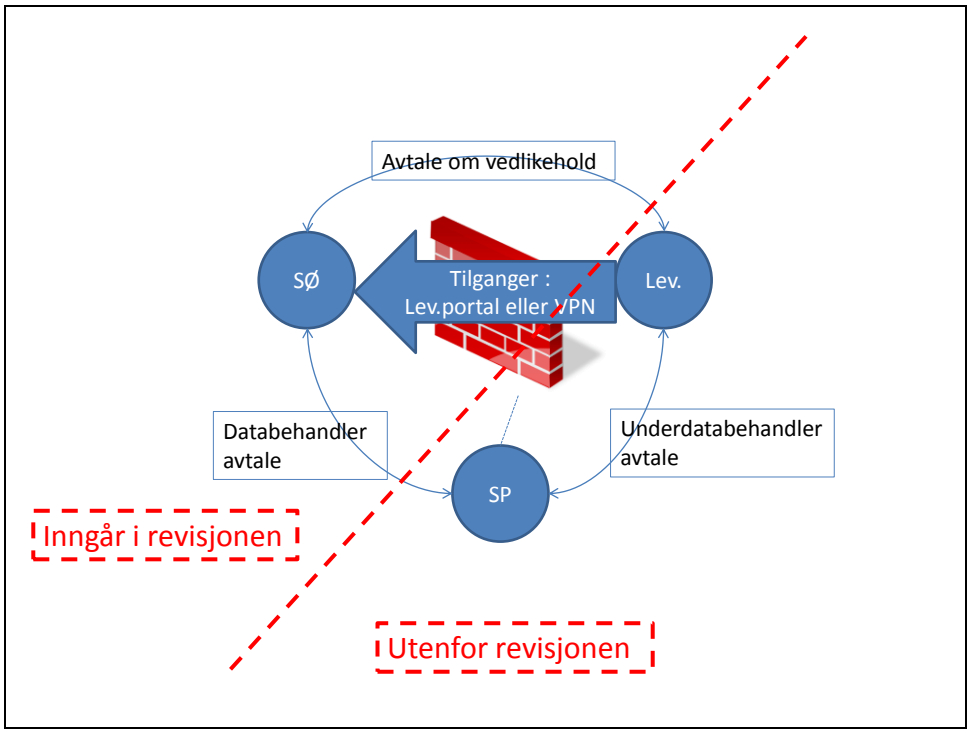
[1] Jf. Norm for informasjonssikkerhet, forord og punkt 1.0 Bakgrunn
[2] Jf. Norm for informasjonssikkerhet, punkt 1.1 Definisjoner.
[3] Jf. Norm for informasjonssikkerhet, punkt 1.1 Definisjoner.
[4] … hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven, 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.

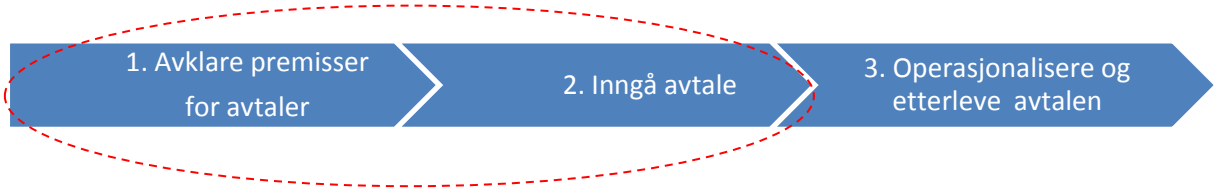
[5] Driftsavtalen – Avtale om kjøp av driftstjenester knyttet til maskinvare, infrastruktur og programvare.

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.

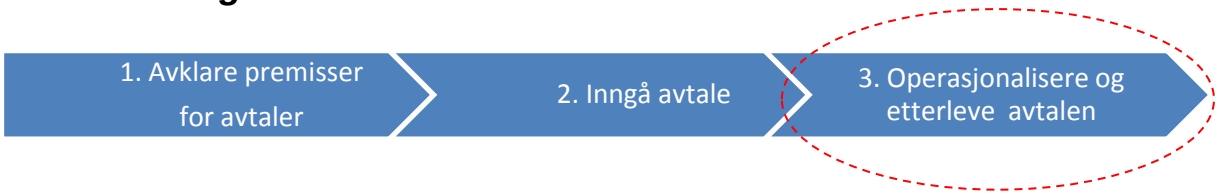
Konsernrevisjonens vurdering er at det gjeldende styringssystemet er lite egnet som en del av Sykehuset Østfold HFs internkontrollsystem.

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