Sak 3: Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr

Målet med revisjonen er å undersøke om helseforetakene har tilstrekkelig informasjonssikkerhet ved bruk av medisinsk-teknisk utstyr. Undersøkelsen omfatter dokumentanalyse av leverandøravtaler for utvalgte maskintyper, risikoanalyser og retningslinjer i 19 helseforetak. I tillegg er det foretatt intervjuer i fire helseforetak, en regional it-enhet og hos en sentral leverandør av medisinsk-teknisk utstyr. Undersøkelsen omfatter i hovedsak perioden 2012–2014.

Innen helsevesenet benyttes det mange systemer og mye utstyr som inneholder helseopplysninger. I likhet med tradisjonelle ikt-systemer kan også medisinsk-teknisk utstyr inneholde personsensitive opplysninger, og andelen av slikt utstyr øker. Det er en risiko for at personsensitive helseopplysninger som ligger i medisinsk-teknisk utstyr, ikke er godt nok beskyttet.

Undersøkelsen har blant annet tatt utgangspunkt i følgende lover og forskrifter:
- *lov om helseregistre og behandling av helseopplysninger av 18. mai 2001* (helseregisterloven)
- *lov om helsepersonell av 2. juli 1999* (helsepersonelloven)

Utkast til rapport ble forelagt Helse- og omsorgsdepartementet i brev av 19. juni 2015. Departementet har i brev av 19. august 2015 gitt kommentarer til rapportutkastet. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet.

1 Hovedfunn

- Helseforetakene stiller ikke tilstrekkelige krav om informasjonssikkerhet i avtaler med leverandører av medisinsk-teknisk utstyr og har mangelfull oppfølging av leverandører.
- Helseforetakene har mangelfull oversikt over risiko knyttet til informasjonssikkerhet i medisinsk-teknisk utstyr.
- Det er uklare ansvarslinjer for informasjonssikkerhet i medisinsk-teknisk utstyr internt i helseforetakene og mellom helseforetakene og de regionale it-enhetene.

2 Riksrevisjonens merknader

2.1 Helseforetakene stiller ikke tilstrekkelige krav om informasjonssikkerhet i avtaler med leverandører av medisinsk-teknisk utstyr og har mangelfull oppfølging av leverandører

Helseforetakene stiller i liten grad krav om informasjonssikkerhet i avtalene med leverandører. Bare 6 av 19 helseforetak har stilt krav til leverandørens behandling av personopplysninger i én eller flere avtaler som de har inngått. Dette kan være krav til oppdatering av programvare og vedlikehold av utstyr og hvordan personopplysninger skal håndteres. Kravene skal klargjøre hva leverandør skal ha på plass av sikringstiltak for å ivareta informasjonssikkerheten. Videre har få helseforetak stilt krav i avtalene om at de må gi samtykke før leverandøren kan gjøre endringer i systemet. Dette betyr at leverandøren ikke er forpliktet til å varsle helseforetaket når den foretar endringer

og oppdateringer på helseforetakets utstyr. Avtalene inneholder derfor i liten grad krav som kan bidra til å hindre eller oppdage brudd på informasjonssikkerheten.

Leverandørene er i stor grad premissgiver i avtalene. Mange av avtalene som er gjennomgått tar utgangspunkt i maler utarbeidet av leverandør, som ikke omtaler informasjonssikkerhet. Det er videre lite samarbeid mellom helseforetakene om å stille krav til leverandørene ved kravspesifisering, avtaleinngåelse og anskaffelse av utstyr.

Det kan være krevende for helseforetakene å følge lovverket fullt ut ettersom utstyret fra leverandørene ikke har all den funksjonalitet som loven krever, som for eksempel tilgangsstyring, antivirusprogrammer og loggfunksjoner. Leverandørene tilbyr løsninger som er beregnet på det internasjonale markedet med andre lovkrav. De norske helseforetakene har etter loven ikke mulighet til å gjøre endringer på utstyret for å imøtekomme kravene i personopplysningsforskriften om tilgangsstyring, antivirus og logging.

De regionale helseforetakenes it-enheter har utarbeidet felles føringer for styringssystem for informasjonssikkerhet. Det er imidlertid få helseforetak som bruker leverandøravtalene til å stille krav til leverandørene om informasjonssikkerhet. Samtidig framstår helseforetakene som lite koordinerte og samstemte i sin samhandling med leverandørene. Helseforetakene har blant annet ulik praksis om bruk av fjernaksessavtaler. Fjernaksessavtaler inngås i hovedsak for å regulere at leverandøren kan logge seg på utstyret for å foreta oppdatering og service fra andre lokasjoner enn i helseforetakets lokaler der utstyret er plassert. Riksrevisjonen mener at få krav og lite samordning gir økt risiko for mangelfull informasjonssikkerhet.

Helseforetakene foretar ikke egne kontroller av leverandørene, eller innhenter uavhengige revisjoner av leverandørene. Etter Riksrevisjonens vurdering benytter ikke helseforetakene muligheten til kontroll av leverandørene som lovverket hjemler, noe som ville gi bedre kjennskap til leverandørens praktisering av lover og regler knyttet til sensitive personopplysninger.

2.2 Helseforetakene har mangelfull oversikt over risiko knyttet til informasjonssikkerhet i medisinsk-teknisk utstyr

Det er etablert regionale føringer, retningslinjer og rutiner for å gjennomføre risikovurderinger som også omfatter medisinsk-teknisk utstyr. Det utarbeides regionale risikoanalyser hvor medisinsk-teknisk utstyr inngår som et av flere risikoområder på overordnet nivå.

Helseforetakene har i liten grad gjort overordnede risikovurderinger av informasjonssikkerheten i medisinsk-teknisk utstyr. Det foreligger dermed ingen samlet oversikt over risikoen og heller ingen opplysninger om eventuelle forebyggende og korrigerende tiltak. Bare to av 19 helseforetak kan dokumentere at det har vært gjennomført risikoanalyser knyttet til det enkelte medisinsk-tekniske utstyret. De fire helseforetakene som er intervjuet, uttaler imidlertid at det behandlende helsepersonellet som benytter utstyret, har oversikt over hvilken informasjon som ligger der.

Manglende risikovurderinger kan etter Riksrevisjonens mening føre til at det ikke foretas noen vurdering av sensitiviteten i informasjonen som ligger i utstyret. Det er dermed vanskelig å få en klar oversikt over trusselbildet, og om det er iverksatt relevante forebyggende eller korrigerende tiltak. I tillegg kan praktiseringen av regelverket bli ulikt, og kravene til leverandør og fjernaksessløsninger kan bli mangelfulle, men også i enkelte tilfeller unødig strenge.

2.3 Det er uklare ansvarslinjer for informasjonssikkerhet i medisinsk-teknisk utstyr internt i helseforetakene og mellom helseforetakene og de regionale it-enhetene
Helseforetakene har i undersøkelsesperioden i begrenset grad hatt retningslinjer og rutiner som beskriver hvordan personsensitiv informasjon i medisinsk-teknisk utstyr skal behandles.

De regionale helseforetakenes IT-enheter har arbeidet med å få på plass felles regionale føringer, retningslinjer og rutiner, men undersøkelsen viser at dette i begrenset grad er implementert i helseforetakene.

Oppgavefordelingen for å ivareta informasjonssikkerhet både mellom helseforetakene og helseregionenes it-enheter og innad i helseforetakene mellom ikt og medisinsk-teknisk avdeling, er uklar. I tillegg tyder undersøkelsen på at regelverket knyttet til informasjonssikkerhet er vanskelig å anvende i praksis for helseforetakene.

De regionale helseforetakene og helseforetakene har ulike oppfatninger om hvilke krav som skal stilles overfor leverandørene, og hvilke rettigheter leverandører skal ha til å foreta oppdateringer og vedlikehold på utstyr som inneholder person- og helseopplysninger. Etter Riksrevisjonens vurdering kan dette føre til at det blir uklart for aktørene hvordan kravene skal operasjonaliseres og følges opp.

Det er uklare ansvarslinjer for informasjonssikkerhet internt i helseforetakene og mellom helseforetakene og de regionale it-enhetene. Videre er det lite samarbeid mellom helseforetakene på dette området. En felles tilnærming i helseforetakene til hvordan kravene skal forstås og anvendes, vil gjøre det enklere for foretakene å følge opp leverandørene. Mye av det medisinsk-tekniske utstyret som i dag benyttes, er mer likt tradisjonelt ikt-utstyr med egne lagringsenheter og mulighet for å kommunisere via nettverk. Dette fører til større behov for samhandling og samarbeid mellom de ulike avdelingene.

Helseforetakene som er intervjuet, opplever at det ikke er tilstrekkelig klarlagt hvordan informasjonssikkerheten i medisinsk-teknisk utstyr skal ivaretas, og de er usikre på hvordan de skal balansere kravene til pasientsikkerhet og informasjonssikkerhet.

3 Riksrevisjonens anbefalinger

Riksrevisjonen anbefaler at:

- Helse- og omsorgsdepartementet forsikrer seg om at de regionale helseforetakene og helseforetakene etterlever gjeldende regelverk for informasjonssikkerhet og behandling av helseopplysninger

- de regionale helseforetakene sørger for bedre samordning mellom regionene og innad i den enkelte region for å sikre at kravene som stilles til leverandører av medisinsk-teknisk utstyr om informasjonssikkerhet, blir mer ensartet

- de regionale helseforetakene og helseforetakene klargjør ansvarslinjene for håndtering av informasjonssikkerhet mellom de regionale it-enhetene og helseforetakene og innad i helseforetakene, slik at rollene til hver enkelt er klart definert og forstått

- de regionale helseforetakene og helseforetakene sørger for at lover og regler for informasjonssikkerhet blir ivaretatt, ved å stille klarere krav til informasjonssikkerhet overfor leverandørene av medisinsk-teknisk utstyr

- helseforetakene følger opp at leverandørene overholder kravene i leverandøravtalene

- helseforetakene utarbeider risikovurderinger av informasjonssikkerhet i medisinsk-teknisk utstyr for å få oversikt over informasjonen som ligger i utstyret, og hvordan informasjonen blir eksponert

4 Departementets oppfølging

Statsråden mener Riksrevisjonens merknader og anbefalinger er relevante, og at informasjonssikkerhet vil kreve stor grad av oppmerksomhet og prioritet.

Statsråden vil følge opp Riksrevisjonens anbefalinger ved å stille krav til de regionale helseforetakene i foretaksmøtet i januar 2016 og gjennom tertialoppfølgingsmøtene med de regionale helseforetakene. Statsråden påpeker at det må være en riktig balanse mellom ivaretakelsen av pasientsikkerhet og personvern.

Statsråden viser til at de regionale helseforetakene arbeider kontinuerlig for å legge til rette for at helseforetakene skal tolke og praktisere lovverket så likt som mulig, men understreker at helseforetakene selv er ansvarlig for å etterleve gjeldende regelverk. Ansvaret for informasjonssikkerhet er tillagt administrerende direktør i helseforetakene, som er databehandlingsansvarlig etter loven.

Ifølge statsråden pågår det et samarbeid mellom de regionale helseforetakene som vil kunne bidra til bedre samordning mellom helseforetakene og en forenkling og standardisering av rutinene i arbeidet med å ivareta informasjonssikkerheten.

De regionale helseforetakene har igangsatt forbedringsprosesser for å samordne arbeidet med informasjonssikkerhet og personvern for de mer tradisjonelle IKT-områdene som elektronisk pasientjournal og helseforetakenes pasientadministrative systemer. Statsråden peker på at arbeidet med å forbedre informasjonssikkerhet og personvernet i det medisinsk-tekniske utstyret må ses i sammenheng med dette arbeidet.

Ifølge statsråden arbeider de regionale helseforetakene systematisk med å gjennomføre risikovurderinger av alt utstyr hvor sensitive personopplysninger lagres. Dette gjelder også for medisinsk-teknisk utstyr, som i økende grad knyttes opp mot nettet. Helseforetakene deltar i dette arbeidet.

5 Riksrevisjonens sluttmerknad

Riksrevisjonen har ingen ytterligere merknader.

Vedlegg 3: Brev og rapport til sak 3 om helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr

Vedlegg 3.1:

Riksrevisjonen

Vår saksbehandler
Ingrid Engstad Risa 22241402
Vår dato | Vår referanse
22.09.2015 | 2015/01454-4
Deres dato | Deres referanse

Utsatt offentlighet jf. rrevl. § 18(2)

Statsråd Bent Høie
HELSE- OG OMSORGSDEPARTEMENTET
Postboks 8011 Dep
0030 OSLO

Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2014

Vedlagt oversendes saksframstillingen av Riksrevisjonens undersøkelse om helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr, som legges fram for Stortinget i Dokument 3:2 (2015–2016).

Saksframstillingen er basert på en rapport som Helse- og omsorgsdepartementet fikk et utkast til 19. juni, og på departementets svar 19. august 2015.

Statsråden bes om å redegjøre for hvordan departementet vil følge opp Riksrevisjonens merknader og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen.

Departementets oppfølging vil bli sammenfattet i den endelige saksframstillingen til Stortinget. Statsrådens svar vil i sin helhet bli vedlagt i Dokument 3:2.

Dette brevet med vedlegg er også sendt per e-post. Vi ber vennligst om å få svar tilsendt både per post og per e-post til postmottak@riksrevisjonen.no. Videre ber vi om at det elektroniske svaret sendes i word-format.

Svarfrist: 8. oktober 2015

For riksrevisorkollegiet

Per-Kristian Foss
riksrevisor

Vedlegg

Vedlegg 3.2:

DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT

Statsråden

Riksrevisjonen
Postboks 8130 Dep
0032 OSLO

Unntatt offentlighet jf. Offl. § 5 andre ledd

Deres ref	Vår ref	Dato
2015/01454-4	14/2313-	08.10.2015

Vedrørende Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2014

Jeg viser til Riksrevisjonens brev av 22. september 2015 om forvaltningsrevisjon av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk teknisk utstyr.

Jeg oppfatter Riksrevisjonens merknader og anbefalinger knyttet til helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk teknisk utstyr som relevante. Hovedfunnene fra undersøkelsen viser at dette er et område som vil kreve stor grad av oppmerksomhet og prioritet.

Riksrevisjonen anbefaler at departementet forsikrer seg om at de regionale helseforetakene og helseforetakene etterlever gjeldende regelverk for informasjonssikkerhet og behandling av helseopplysninger i det medisinsk tekniske utstyret. Videre at de regionale helseforetakene og helseforetakene klargjør ansvarslinjene mellom de regionale IKT-enhetene og helseforetakene. Helseforetakene er selv ansvarlige for å etterleve gjeldende regelverk. De regionale helseforetakene arbeider kontinuerlig for å legge til rette for å sikre at alle helseforetakene tolker og praktiserer lovverket så likt som mulig, blant annet gjennom regional standardisering. Ansvaret for informasjonssikkerhet er tillagt administrerende direktør i helseforetakene, som er databehandlingsansvarlige etter loven. De regionale helseforetakene har forsikret departementet om at det pågår et systematisk arbeid i helseforetakene med bistand fra de regionale helseforetakene.

Riksrevisjonen anbefaler at de regionale helseforetakene skal sørge for bedre samordning og ensartet oppfølging av leverandørene av medisinsk teknisk utstyr. De regionale helseforetakene har bekreftet at det pågår et samarbeid og standardisering av anskaffelse, vedlikehold og oppfølging av leverandørene. Min oppfatning er at dette vil bidra til bedre samordning mellom helseforetakene og en forenkling av rutinene i arbeidet med å ivareta informasjonssikkerheten, standardisere anskaffelsesprosessene og utvikle felles maler for

avtaler og oppfølging av leverandørene. I flere av regionene er det tatt i bruk standard maler for avtaler som inneholder spesifikke krav til informasjonssikkerhet. Dette omfatter blant annet fjernaksessløsninger for leverandørene, søknad og avtaler om fjernaksess for service av det medisinsk tekniske utstyret.

Implementering av lov- og regelverket for informasjonssikkerhet og personvern kan gjøres på en mer ensartet måte for de mer tradisjonelle IKT-områdene som elektronisk pasientjournal (EPJ) og helseforetakenes pasientadministrative systemer (PAS). De regionale helseforetakene har igangsatt forbedringsprosesser både helseforetaksvist og regionalt for å samordne arbeidet med informasjonssikkerhet og personvern på disse områdene. Vurdering av styringsmodell og kompetansebehov for de to områdene inngår i dette arbeidet. Det er for tidlig å konkludere. Imidlertid tyder mye på større grad av samordning og felles prosjekt.

Riksrevisjonen anbefaler at helseforetakene utarbeider risikovurderinger av informasjons-sikkerheten i medisinsk teknisk utstyr for å få oversikt over informasjonen som ligger i utstyret, og hvordan informasjonen blir eksponert. De regionale helseforetakene har forsikret meg om at det arbeides med å sikre at det systematisk gjennomføres risikovurderinger av alt utstyr hvor sensitive personopplysninger lagres. Dette gjelder også for medisinsk teknisk utstyr som nå i økende grad knyttes opp mot nettet. Helseforetakene deltar i dette arbeidet og skal gjennomføre risikovurdering før det medisinsk tekniske utstyret installeres. I flere av regionene er det utvikles felles malverk for dette arbeidet.

Jeg vil følge opp Riksrevisjonens seks anbefalinger og vil stille krav til de regionale helseforetakene om oppfølging i foretaksmøtet i januar 2016. Dette vil bli fulgt opp blant annet i de felles tertialoppfølgingsmøtene med de regionale helseforetakene. Jeg vil understreke at resultatene fra Riksrevisjonens undersøkelse viser at arbeidet med å ivareta informasjonssikkerheten i det medisinsk tekniske utstyret skal prioriteres høyt, og at det må være en riktig balanse mellom ivaretakelsen av pasientsikkerhet og personvern i dette arbeidet. Forbedringsarbeidet med informasjonssikkerhet og personvernet i det medisinsk tekniske utstyret må samkjøres med arbeidet innenfor elektronisk pasientjournal (EPJ) og helseforetakenes pasientadministrative systemer (PAS).

Med hilsen

Bent Høie

Bent Høie

Vedlegg 3.3: Rapport fra utvidet kontroll om helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr

1 Innledning

1.1 Bakgrunn

Stortinget har i mange år framhevet betydningen av informasjons- og kommunikasjonsteknologi (ikt) for å nå helse- og omsorgspolitiske mål om bedre kvalitet, pasientsikkerhet, effektivitet og ressursbruk.[264] I tillegg har Stortinget vært opptatt av informasjonssikkerheten i samfunnet.

Innen helsevesenet benyttes det systemer og utstyr som inneholder helseopplysninger. I tillegg til tradisjonelle ikt-systemer kan også medisinsk-teknisk utstyr inneholde personsensitive opplysninger. Undersøkelsen omhandler den delen av medisinsk-teknisk utstyr (MTU) som inneholder helseopplysninger. Andelen medisinsk-teknisk utstyr som inneholder personsensitive helseopplysninger, er økende. Det foreligger ingen nasjonal oversikt over omfanget av utstyr, men for eksempel hadde Oslo universitetssykehus HF (OUS) per 1. januar 2015 totalt 39 765 enheter som er definert som medisinsk-teknisk utstyr.[265] Imidlertid er det en begrenset andel av utstyret som kan lagre pasientopplysninger. Helseforetakene har til sammen planlagt å investere 1,3 mrd. kroner i medisinsk-teknisk utstyr i 2015.[266]

Det er en risiko for at personsensitive helseopplysninger som ligger i medisinsk-teknisk utstyr, ikke er godt nok beskyttet. Utstyret inneholder i begrenset grad kontrollfunksjoner, som logging, antivirusprogrammer, brukernavn og passord. Dette er funksjoner som er vanlig for å ivareta informasjonssikkerheten ved bruk av ikt. I tillegg inneholder en del av utstyret gamle operativsystemer som kan være til hinder for oppdatering og sikring av utstyret.

Noe medisinsk-teknisk utstyr har nettbaserte løsninger som gir leverandøren mulighet til å oppdatere, rette og vedlikeholde utstyret uten å være til stede, det vil si at leverandør bistår ved hjelp av fjernaksess. Opplysningene kan potensielt eksponeres for flere, og personer uten lovlig tilgang kan komme seg inn på helseforetakets interne nett via det medisinsk-tekniske utstyret. Helseforetakene har begrensede kontrollmuligheter overfor leverandørene med fjernaksess. Det er derfor en risiko for at drifts-, vedlikeholds- og fjernaksessavtalene som helseforetakene har med leverandører av medisinsk-teknisk utstyr, ikke regulerer sikring av sensitive personopplysninger. Det er også en risiko for manglende eller mangelfull kontroll med hvorvidt leverandørene overholder regler for informasjonssikkerhet.

Enkelte leverandører av medisinsk-teknisk utstyr er lokalisert i andre land eller har outsourcet drift og vedlikehold til andre land. Krav til informasjonssikkerhet varierer mellom landene. Dette øker risikoen for at informasjonen kommer på avveier, siden andre land ikke har like strenge krav til informasjonssikkerhet som Norge. En undersøkelse gjennomført av PwC blant brukere og leverandører innen helsesektoren globalt viste en økning i informasjonssikkerhetshendelser fra 2013 til 2014 på 60 %.

264) Blant annet Meld. St. 9 (2012–2013) *Én innbygger – én journal. Digitale tjenester i helse- og omsorgssektoren.* Jf. Innst. 224 S (2012–2013).
265) Investeringsplan for MTU-anskaffelser 2016–2019 ved OUS HF. Kortfattet versjon – II, Oslo universitetssykehus HF Medisinsk-teknologisk virksomhetsområde, Oslo sykehusservice 17.04.2015.
266) Prop. 1 S (2014–2015), side 96, tabell 4.11.

Undersøkelsen peker på at den teknologiske utviklingen på helse- og omsorgsområdet vil eksponere mer sensitive persondata mot internett og øke risikoen for informasjonssikkerhetsbrudd.[267]

1.2 Formål og problemstillinger

Formålet med undersøkelsen er å undersøke om helseforetakene har tilstrekkelig informasjonssikkerhet ved bruk av medisinsk-teknisk utstyr.

Undersøkelsens formål belyses gjennom følgende problemstillinger:

1 Hvordan sikrer helseforetakene at leverandørene overholder lover og regler for informasjonssikkerhet gjennom avtaler?

2 Har helseforetakene klare ansvarslinjer og tilstrekkelige rutiner for å ivareta informasjonssikkerhet?

Definisjon av medisinsk-teknisk utstyr

Forskrift om medisinsk utstyr definerer medisinsk utstyr som ethvert instrument, apparat, utstyr, programvare mv. som benyttes til diagnostisering, overvåking, kontroll, undersøkelse, behandling osv. Elektromedisinsk utstyr defineres som ethvert medisinsk utstyr, inkludert systemløsninger, som er avhengig av en elektrisk energikilde for å fungere. Denne undersøkelsen omfatter utstyr som går under fellesbetegnelsen elektromedisinsk utstyr. I undersøkelsen er det valgt å benytte begrepet medisinsk-teknisk utstyr (MTU), som er et innarbeidet begrep og en forkortelse som benyttes av helseforetakene.

1.3 Revisjonskriterier

Både helseregisterloven, helsepersonelloven og personopplysningsforskriften stiller krav til helseforetakenes håndtering av taushetsbelagte helse- og personopplysninger. De samme kravene vil gjelde overfor leverandører som gis tilgang til slike opplysninger.[268]

Krav til håndtering av helseopplysninger

Helseregisterloven[269] slår fast at enhver som behandler helseopplysninger, har taushetsplikt etter forvaltningsloven[270] og helsepersonelloven.[271]

Helseregisterloven og pasientjournalloven definerer at databehandlingsansvarlig er den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes. Databehandlingsansvaret vil ligge hos helseforetaket.[272] Databehandler er den som behandler helseopplysninger på vegne av den behandlingsansvarlige. Hvorvidt leverandørene av medisinsk-teknisk utstyr skal defineres som databehandler, avhenger av tilgang på helseopplysninger.[273]

I henhold til helseregisterloven kan tilgang til helseopplysninger bare gis den databehandlingsansvarlige[274], databehandlere[275] og den som arbeider under instruksjons-

267) PWC: *Healtcare cybersecurity challenges in an interconnected world, Survey 2015*.
268) Ny pasientjournallov og ny helseregisterlov trådte i kraft 1. januar 2015 og erstatter helseregisterloven av 2001. Undersøkelsen tar utgangspunkt i avtaler inngått før 2015. Det er dermed helseregisterloven av 2001 som vil være aktuell for disse avtalene. Pasientjournalloven viderefører imidlertid mange av prinsippene fra helseregisterloven når det gjelder krav til informasjonssikkerhet, men etter ny lovgivning kan helseforetak samarbeide om behandlingsrettede helseregistre, dvs. at de kan utveksle pasientopplysninger på tvers av helseforetak.
269) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger, § 15.
270) LOV 1967-02-10: Lov om behandlingsmåten i forvaltningssaker, §§ 13 til 13 e.
271) LOV 1999-07-02-64 Lov om helsepersonell.
272) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger § 6 annet ledd.
273) *Databehandleravtale etter personopplysningsloven og helseregisterloven* – Datatilsynets veileder.
274) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger § 2 nr. 8.
275) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger §2 nr. 9.

myndighet fra disse.[276] Tilgang til helseopplysninger kan dessuten gis i den grad dette er nødvendig for arbeidet og i samsvar med gjeldende regler om taushetsplikt.[277] Dette innebærer at en databehandler bare kan ha tilgang til helseopplysninger i den grad dette er nødvendig for arbeidet. I tillegg må tilgangen være i samsvar med gjeldende bestemmelser om taushetsplikt.

Det følger av helsepersonelloven § 25 at yrkesmessig taushetsplikt[278] ikke er til hinder for at personell som bistår med elektronisk bearbeiding av opplysningene, eller som bistår med service og vedlikehold av utstyr, får tilgang til opplysninger når slik bistand er nødvendig for å oppfylle lovbestemte krav til dokumentasjon. Bestemmelsen åpner opp for at teknisk personell kan få tilgang på taushetsbelagt informasjon, men har samtidig inntatt et krav om at slik informasjon ikke skal gjøres tilgjengelig hvis det ikke vurderes som "nødvendig" for å oppfylle lovbestemte krav til dokumentasjon. Personell som bistår med elektronisk bearbeiding av opplysningene, eller som bistår med service og vedlikehold av utstyr, har samme taushetsplikt som helsepersonell.[279]

Krav til internkontroll

Helseforetakene er pålagt å ha en internkontroll.[280] Videre er de pålagt å ha internkontroll/styringssystem på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder. ISO 27001 er anbefalt forvaltningsstandard for styringssystem for informasjonssikkerhet.[281] Standarden beskriver sikringsteknikker og setter krav til interne kontrolltiltak for å sikre informasjonen i informasjons- og kommunikasjonssystemer.

En databehandler kan ikke behandle helseopplysninger på annen måte enn det som er skriftlig avtalt med helseforetaket. Opplysningene kan heller ikke uten en slik avtale overlates til noen andre for lagring eller bearbeiding. I avtalen med helseforetaket skal det også gå fram at databehandleren plikter å gjennomføre de sikringstiltakene som følger av helseregisterloven.[282]

Helseforetaket og leverandør av medisinsk-teknisk utstyr er pålagt å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger gjennom planlagte og systematiske tiltak. For å oppnå tilfredsstillende informasjonssikkerhet skal både helseforetaket og leverandør dokumentere informasjonssystemet og sikkerhetstiltakene, og dokumentasjonen skal være tilgjengelig for medarbeiderne. Helseforetak som lar andre få tilgang til helseopplysninger, for eksempel en leverandør av medisinsk-teknisk utstyr, skal se til at denne oppfyller disse kravene.[283] Leverandører som bruker informasjonssystemet på helseforetakets vegne, skal tilfredsstille kravene i personopplysningsforskriften kapittel 2 om informasjonssikkerhet.[284]

Helseforetaket (databehandlingsansvarlig) og den som behandler dataene på vegne av helseforetaket (databehandler), skal føre oversikt over hvilke personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Helseforetaket skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd.

276) I henhold til ny LOV-2014-06-20-42 Lov om behandling av helseopplysninger ved ytelse av helsehjelp kan helseopplysningene også gis til andre helseforetak.
277) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger, § 13, første ledd.
278) LOV-1999-07-02-64 Lov om helsepersonell § 21.
279) LOV-1999-07-02-64 Lov om helsepersonell § 25 siste ledd.
280) Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften 1996-12-06) § 4.
281) Punkt 1.7 i Digitaliseringsrundskrivet, siste avsnitt kapittel 4.1 i Nasjonal strategi for informasjonssikkerhet og punkt 2.16 i Difis referansekatalog for it-standarder i offentlig sektor.
282) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger § 16.
283) LOV 2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger § 16.
284) FOR 2000 12 15 1265 Forskrift om behandling av personopplysninger § 2-15 tredje ledd.

Det skal gjennomføres en ny risikovurdering ved endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal dokumenteres.[285]

Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig av de som behandler sensitive personopplysninger. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører.[286]

Helseforetaket skal etablere klare ansvars- og myndighetsforhold overfor leverandører. Ansvars- og myndighetsforhold skal beskrives i en særskilt avtale. Helseforetaket skal ha kunnskap om sikkerhetsstrategien hos leverandører og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.[287]

Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten skal dokumenteres.[288]

De planlagte og systematiske tiltakene som gjøres i henhold til personopplysningsforskriften, skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd.[289] Hvor sensitiv og kritisk informasjonen er, kan variere. Dermed bør også sikringstiltakene variere.

1.4 Metode og gjennomføring

For å få informasjon om kravene som helseforetakene stiller til leverandører av medisinsk-teknisk utstyr, er samtlige helseforetak[290] bedt om å sende kopi av de sist inngåtte og gjeldende leverandøravtalene med tilhørende vedlikeholds-, service- og/eller fjernaksessavtaler for CT-maskiner, ultralydmaskiner og spirometrimaskiner. Disse maskintypene ble valgt fordi informanter[291] har opplyst at dette er utstyr som inneholder personsensitive opplysninger.

Med bakgrunn i krav for behandling av helseopplysninger er det utarbeidet et analyseskjema for å analysere de innsendte avtalene. 51 leverandøravtaler[292] og 24 tilhørende service-/vedlikeholds-/fjernaksessavtaler er analysert. Alle helseforetakene sendte inn avtaler: 12 helseforetak sendte inn avtaler for alle de tre maskintypene, seks sendte inn for to maskintyper og ett for én maskintype. For seks avtaler fra tre helseforetak er også kravspesifikasjonen vedlagt.

For å kartlegge hvilke systemer helseforetakene har etablert for å ivareta informasjonssikkerheten, er helseforetakene også bedt om å sende risikoanalyser som er gjennomført av informasjonssikkerhet for CT-maskiner, ultralydmaskiner og spirometrimaskiner. I tillegg er helseforetakene bedt om å sende eventuelle retningslinjer for behandling av informasjon (informasjonssikkerhet) og eventuelle retningslinjer for leverandøroppfølging og bruk av de samme maskinene. Helseforetakene er også bedt om å sende den siste sikkerhetsrevisjonen rettet mot leverandører av medisinsk-teknisk utstyr.

Det er gjennomført intervju med avdelingsledere ved medisinsk-teknisk avdeling, og informasjonssikkerhetsansvarlige, kvalitetsledere og lokalt it-personell ved Oslo universitetssykehus HF, Sykehuset Telemark HF, Helse Stavanger HF og Helgelandssykehuset HF. Hensikten er å få informasjon om hvordan rutinene i helseforetakene

285) FOR 2000 12 15 1265 Forskrift om behandling av personopplysninger § 2-4.
286) FOR 2000 12 15 1265 Forskrift om behandling av personopplysninger § 2-5.
287) FOR 2000-12-15-1265 Forskrift om behandling av personopplysninger § 2-15.
288) FOR 2000-12-15-1265 Forskrift om behandling av personopplysninger § 2-16.
289) FOR 2000 12 15 1265 Forskrift om behandling av personopplysninger § 2-1 annet ledd.
290) Sunnaas sykehus HF ga tilbakemelding om at de ikke benytter de utvalgte maskintypene. Helseforetaket omfattes derfor ikke av undersøkelsen.
291) Nøkkelpersoner ved Sykehuspartner, Ahus og St. Olavs hospital.
292) 20 avtaler for CT-maskiner, 17 avtaler om ultralydmaskiner og 14 avtaler om spirometrimaskiner.

praktiseres både internt og overfor leverandører, hvordan arbeidet med informasjonssikkerhet i medisinsk-teknisk utstyr generelt fungerer, og hva som er de særskilte utfordringene. Helseforetakene er valgt på bakgrunn av størrelse, funksjon, regiontilknytning og innsendt dokumentasjon. Helse Stavanger HF og Telemarksykehuset HF ble valgt fordi de var de eneste helseforetakene som har utført risikoanalyser som omfatter informasjonssikkerhet av medisinsk-teknisk utstyr.

Hemit – it-enheten i Helse Midt-Norge RHF – er intervjuet for å få inn perspektivet fra en regional it-enhet. De regionale it-enhetene har i stor grad ansvaret for oppkoblingsløsning for leverandørens fjernaksessløsninger og drifter systemene og nettverkene som helseopplysningene i medisinsk-teknisk utstyr blir overført via og til.

For å få fram leverandørperspektivet er én leverandør, som har en stor markedsandel i Norge og også internasjonalt, intervjuet om helseforetakenes kontroll og oppfølging av leverandører.

2 Resultatet av undersøkelsen

2.1 Hvordan sikrer helseforetakene at leverandørene overholder lover og regler for informasjonssikkerhet gjennom avtaler?

2.1.1 Krav til informasjonssikkerhet i leverandøravtaler

Dokumentanalysen viser at det benyttes ulike benevnelser og innhold for avtaler som regulerer leverandørens oppdateringer og vedlikehold av utstyret. Serviceavtaler og vedlikeholdsavtaler benyttes i hovedsak for vedlikehold lokalt i helseforetaket. Fjernaksessavtaler med leverandøren inngås i hovedsak for at leverandøren kan logge seg på utstyret for å utføre oppdatering og service fra andre steder enn i helseforetakets lokaler der utstyret er plassert. En mindre, men økende, andel av dette utstyret har mulighet for fjernaksess.

Mange av de gjennomgåtte avtalene tar utgangspunkt i maler som er utarbeidet av leverandør, der informasjonssikkerhet ikke er omtalt. Dokumentanalysen viser at helseforetakene i liten grad stiller krav om informasjonssikkerhet i avtalene. Bare i 6 av 19 helseforetak kommer plikter for behandling av personopplysninger klart fram i én eller flere av avtalene de har med leverandører. Slike plikter kan være krav knyttet til oppdatering av programvare og vedlikehold av utstyr, og sikringstiltak hos databehandler for å ivareta konfidensialitet, integritet og tilgjengelighet. Avtalene inneholder dermed i liten grad krav som vil bidra til å hindre eller oppdage informasjonssikkerhetsbrudd. De fire intervjuede helseforetakene mener det er viktig at det blir stilt krav til informasjonssikkerhet allerede i kravspesifikasjonen.

De intervjuede helseforetakene uttaler at det ikke har vært noe samarbeid mellom helseforetakene innen de enkelte regionene eller mellom regionene, verken ved kravspesifisering, avtaleinngåelse eller ved anskaffelse av utstyret (innkjøpssamarbeid). OUS HF og Helse Stavanger HF mener helseforetakene i større grad bør samkjøre krav mot leverandørene slik at foretakene får større mulighet til å påvirke. Helse Stavanger HF mener helseforetakene har en tendens til å tilpasse seg krav fra leverandørene, og leverandørene har lite oppmerksomhet rundt informasjonssikkerhet i utstyret de leverer.

Databehandleravtaler kan være et virkemiddel for å regulere roller og ansvar mellom helseforetaket som databehandlingsansvarlig og leverandøren som databehandler. 11 av 19 helseforetak har inngått databehandleravtaler eller regulert leverandørens

tilgang til data i noe som tilsvarer en databehandleravtale eller utarbeidet maler for dette. Helseforetakene[293] som ikke inngår databehandleravtaler, benytter taushetserklæringer i stedet.

De intervjuede helseforetakene har ulikt syn på hvorvidt det skal inngås databehandleravtaler med leverandørene, og om leverandør skal defineres som databehandler. De har heller ikke kjennskap til om det er gitt noen overordnede føringer for bruk av databehandleravtaler. Argumentet mot bruk av databehandleravtaler er at leverandørene ikke skal behandle data, men bare foreta vedlikehold og oppdatering av programvare. En databehandleravtale signaliserer at leverandøren har mulighet til å behandle personsensitiv data, noe som vil gi leverandør større rettigheter enn nødvendig.

Avtalegjennomgangen viser at få helseforetak har stilt krav i avtalene om at de må gi samtykke før leverandøren kan gjøre endringer via fjernaksess i det medisinsk-tekniske utstyret.[294] Dette betyr at leverandøren ikke er forpliktet til å varsle helseforetaket når de går inn og gjør endringer og oppdateringer på helseforetakenes utstyr. Det har forekommet at leverandøren har gjort endringer via fjernaksess som helseforetaket ikke har visst om.[295] Det kan være krevende for helseforetakene å holde oversikt over hva som gjøres av endringer i utstyret hvis de ikke varsles på forhånd.

Det er ulikt syn mellom helseforetakene og mellom regionene om de skal tillate fjernaksessløsninger. Både leverandøren og helseforetakene som er intervjuet, mener foretakene har bedre kontroll på egne data uten fjernaksessløsninger. Imidlertid kan det oppstå feil på det medisinsk-tekniske utstyret som må rettes raskt, slik at HF-ene likevel må godta utveksling av data via fysiske lagringsmedia som minnepinner og CD-er, eller over nettet. Ved manglende fjernaksess må nye komponenter hentes, og servicemedarbeidere må reise fra leverandøren til helseforetaket for å foreta rettelser på stedet. Dette reduserer brukstiden på utstyret, noe som kan gå utover pasientsikkerheten. Hvis leverandøren har kontinuerlig tilgang til overvåking av utstyret, kan de også varsle om slitasje i utstyret, og oppdateringer og nedetid kan planlegges i større grad enn det som er mulig uten fjernaksesstilgang.[296]

Tekstboks 1 Eksempel på informasjonssikkerhetsbrudd

GE Healthcare Systems, som er en leverandør av medisinsk-teknisk utstyr, hentet ubevisst ut helseopplysninger fra ti virksomheter i Norge. Totalt ble helseopplysninger for 126 344 pasienter hentet ut fra leverandøren og overført til USA. Informasjonen omfattet blant annet navn, ID-nummer, fødselsdato, kjønn, høyde, vekt, størrelse, kliniske opplysninger og i noen tilfeller bilder. Det var leverandøren selv som oppdaget avviket og rapporterte tilbake til norske myndigheter.*

* Personvernnemndas avgjørelse PVN 2013-12.

I saken som er beskrevet i tekstboks 1, var det ingen av de berørte helseforetakene som selv oppdaget at leverandøren hadde hentet ut data fra medisinsk-teknisk utstyr. Helseforetakene uttaler at de i liten grad har mulighet til å oppdage denne type hendelser på grunn av manglende kontrollfunksjoner i utstyret, og i tilfeller der det foreligger kontrollfunksjoner, som for eksempel logg, kan det være vanskelig å tolke loggen.

OUS HF uttaler at leverandør ikke tilbyr utstyr som imøtekommer alle norske lovkrav. For eksempel er det i noe utstyr manglende tilgangskontroll, det vil si at det ikke er

293) Intervju med enkelte helseforetak og svarbrev fra helseforetak ved innsendelse av dokumentasjon.
294) Enkelte helseforetak utfører service og vedlikehold av mye av utstyret selv, men ikke for alt utstyr.
295) Referat fra møte med Helse Stavanger HF.
296) Referat fra møte med Helgelandssykehuset HF.

noen påloggingsfunksjon med brukernavn og passord. Det er også svakheter ved loggfunksjonen i medisinsk-teknisk utstyr ved at bare endring av data blir loggført, men ikke lesing eller oppslag. Det fører til at helseforetaket ikke vet om, og eventuelt når, leverandør er inne på utstyret via fjernaksess, med mindre de endrer dataene. Når det gjelder tilgangskontroller, er det eksempler på at leverandører lager egne løsninger, for eksempel passord, slik at det som var ment som individuelle passord for en servicemedarbeider, i realiteten brukes av mange personer.[297]

Medisinsk-teknisk utstyr er typegodkjente løsninger etter spesielle direktiver, og uautoriserte endringer på utstyret opphever typegodkjenningen og leverandørens garanti for utstyret. Lovverket stiller også krav om at medisinsk utstyr skal brukes i samsvar med utstyrets vedlagte anvisninger.[298] Dette innebærer at helseforetaket ikke selv kan installere antivirus, endre loggfunksjoner eller på andre måter endre programvaren i utstyret for å sikre at utstyret imøtekommer krav til konfidensialitet.

Leverandøren som er intervjuet, uttaler at helseforetakene i liten grad etterspør systemer for tilgangskontroll med for eksempel brukernavn og passord, og muligheter for virusoppdateringer. Slike systemer vil bidra til å begrense tilgangen til utstyret og hindre at medisinsk-teknisk utstyr blir infisert med datavirus.

2.1.2 Underleverandører

Avtalegjennomgangen viser at helseforetakene i varierende grad stiller krav knyttet til bruk av underleverandører til leverandører av utstyret. Fem[299] helseforetak har ikke stilt krav knyttet til underleverandør i kjøps- eller serviceavtaler, mens ytterligere ett[300] helseforetak har omtalt bruk av underleverandør i enkelte av avtalene, uten å legge inn krav om at underleverandører skal følge samme krav som hovedleverandør.

Totalt har 13 av 19 helseforetak i én eller flere avtaler stilt samme krav til underleverandør som til hovedleverandør, eller stilt krav om at leverandøren ikke får bruke underleverandører. Ingen helseforetak[301] har stilt krav til underleverandører i alle helseforetakets avtaler som er undersøkt. Underleverandører i utlandet, spesielt utenfor EU, er omfattet av en annen lovgivning enn den norske, noe som kan innebære en risiko for manglende kontroll på data dersom helseforetaket ikke sørger for at det stilles samme krav til underleverandør som til hovedleverandør.

2.1.3 Helseforetakenes kontroll med at leverandører overholder kravene

Ingen av de 19 helseforetakene har dokumentert at de har foretatt reelle kontroller og oppfølging av leverandørene eller gjennomført sikkerhetsrevisjoner det siste året hos leverandør som omfatter medisinsk-teknisk utstyr.[302] Dette indikerer at helseforetakene ikke har kunnskap om hvordan leverandøren jobber med informasjonssikkerhetsutfordringene.

Det er heller ingen helseforetak som har innhentet uavhengige revisjoner av leverandørene.

Seks[303] helseforetak har avtalefestet rett til innsyn i leverandørens systemer i de innsendte avtalene. Tre helseforetak[304] har avtalefestet dette i én av tre avtaler som er sendt inn. Ett helseforetak[305] har sendt inn en mal der det hjemles sikkerhetsrevisjoner

297) Referat fra møte med OUS.
298) Forskrift om håndtering av medisinsk utstyr § 10 Bruk.
299) Sykehuset Vestfold HF, Helse Førde HF, Vestre Viken HF, Nordlandssykehuset HF, Finnmarkssykehuset HF.
300) Helse Møre og Romsdal HF.
301) Imidlertid er dette kravet innarbeidet i flere helseforetaks avtalemaler.
302) Personopplysningsforskriften § 2-5.
303) Sykehuset Østfold HF, Helse Stavanger HF, Helse Fonna HF, Helse Førde HF, Helse Bergen HF og Helgelandssykehuset.
304) For OUS HF, Sørlandssykehuset HF og UNN.
305) Ahus HF.

(Avtale informasjonssikkerhet – ekstern leverandør), men ikke dokumentert at denne benyttes. Ingen helseforetak har benyttet seg av retten til å utføre uavhengige revisjoner.

Ved ikke å foreta egne kontroller eller innhente uavhengige revisjoner av leverandøren vet ikke helseforetakene hvilke rutiner leverandøren har etablert for å sikre informasjonen som helseforetakene er databehandlingsansvarlig for.

2.2 Har helseforetakene en hensiktsmessig oppgavefordeling, og har de etablert tilstrekkelige rutiner for å ivareta informasjonssikkerheten?

2.2.1 Rutiner og retningslinjer for å sikre informasjonen i medisinsk-teknisk utstyr

Alle aktørene som ble intervjuet, peker på at lovene og reglene for informasjonssikkerhet i noen tilfeller er vanskelig å anvende i praksis. Det er vanskelig å forene kravene om konfidensialitet og tilgjengelighet. Dette gjelder spesielt der det norske lovverket stiller krav som leverandørene ikke imøtekommer. Videre påpeker helseforetakene at regelverket er detaljert, og at det er mange regler å forholde seg til.

De regionale helseforetakenes it-enheter har utarbeidet felles føringer for styringssystem for informasjonssikkerhet som skal ligge til grunn for helseforetakenes arbeid med å etablere tilsvarende styringssystem og ivareta krav til håndtering av personopplysninger og informasjonssikkerhet.[306] Det foreligger også rutiner og retningslinjer på enkelte områder lokalt i helseforetakene.

Dokumentgjennomgangen viser imidlertid at helseforetakene i liten grad har retningslinjer og rutiner som beskriver hvordan personsensitiv informasjon i medisinsk-teknisk utstyr skal behandles. 7 av 19 helseforetak[307] har retningslinjer for kontroll med leverandørens arbeid ved oppdateringer og vedlikehold av utstyret, blant annet rutiner for å innhente samtykke fra helseforetaket (databehandlingsansvarlig) før leverandøren kan foreta endringer. Ingen av helseforetakene har rutiner for autorisasjon (tildeling, administrasjon og kontroll) av tilganger til leverandør. Dette har sammenheng med at elektromedisinsk utstyr i liten grad har tilgangskontroller som brukernavn og passord. Imidlertid tildeler it-enhetene brukernavn og passord hvis leverandørene skal inn på det medisinsk-tekniske utstyret via helseforetakets nettverk. Det betyr at helseforetakene i liten grad har oversikt over hvem som er autorisert til å utføre oppgaver i valgte medisinsk-teknisk utstyr.

De fleste helseforetakene (15 av 19) har retningslinjer for taushetserklæring for servicepersonell fra leverandør. I tillegg kan leverandør ha taushetserklæring i egen organisasjon. De fire intervjuede helseforetakene har også etablert rutiner for sletting av data ved destruering av utstyr.

Flere av helseforetakene[308] peker selv på at internkontrollen kan bli bedre. OUS HF uttaler at internkontrollen må settes i system, og at helseforetaket må finne en egnet måte å kontrollere interne rutiner og å følge opp leverandører.

En gruppe nedsatt av Helsedirektoratet er i gang med å utarbeide en egen veileder for elektromedisinsk utstyr. Hemit uttaler at selv om det utarbeides sentrale veiledere, er det viktig at helseforetakene har egne retningslinjer for lokale prosedyrer.

306) HODs svar til Riksrevisjonen av 19. august 2015
307) OUS HF, Vestre Viken HF, Sørlandssykehuset HF, Sykehuset Østfold HF, Helgelandssykehuset HF, Nordlandssykehuset HF og Finnmarkssykehuset HF.
308) Dette kom fram både gjennom intervju og i svar som fulgte med innsendt dokumentasjon.

2.2.2 Risikovurderinger

Det er helseforetakenes oppgave som databehandlingsansvarlig for helseopplysningene i medisinsk-teknisk utstyr å utarbeide risiko- og sårbarhetsanalyser.

Helseforetakenes kunnskap om hvilken personsensitiv informasjon som lagres i medisinsk-teknisk utstyr, og risikoen forbundet med det, er i liten grad dokumentert gjennom risikoanalyser. Departementet opplyser at det eksisterer regionale føringer, retningslinjer og rutiner for gjennomføring av risikovurderinger som også omfatter medisinsk-teknisk utstyr.[309] Det utarbeides regionale risikoanalyser hvor medisinsk-teknisk utstyr inngår som et av flere risikoområder på overordnet nivå.

Ingen helseforetak har utarbeidet overordnede risikovurderinger knyttet til sin utstyrspark av medisinsk-teknisk utstyr eller spesifikt til de tre utvalgte maskintypene. De intervjuede helseforetakene og skriftlig dokumentasjon fra flere av de øvrige helseforetakene tyder på at dette i liten grad gjøres generelt for medisinsk-teknisk utstyr. Det foreligger dermed ingen samlet oversikt over risikoen og heller ingen opplysninger om eventuelle forebyggende og korrigerende tiltak. De fire intervjuede helseforetakene uttaler imidlertid at det behandlende helsepersonell som benytter utstyret, har oversikt over hvilken informasjon som ligger der. I tillegg foretar de regionale it-enhetene egne risikoanalyser av informasjonssikkerheten. Hemit uttaler at de utfører risikoanalyser på vegne av helseforetakene når det gjelder tilganger til nettverket og ikt-utstyret som helseforetakene benytter.[310]

Manglende risikovurderinger kan føre til at det ikke foretas noen vurdering av sensitiviteten i informasjonen som ligger i utstyret. Det er dermed vanskelig å få en klar oversikt over trusselbildet, og om det er iverksatt relevante forebyggende eller korrigerende tiltak. I tillegg kan praktiseringen av regelverket bli ulikt, og kravene til leverandør og fjernaksessløsninger kan bli mangelfulle, men også i enkelttilfeller unødig strenge.

Bare to[311] helseforetak av 19 har dokumentert at de har foretatt risikovurderinger knyttet til informasjonssikkerhet i det utvalgte medisinsk-tekniske utstyret (ultralyd, CT og spirometrimaskiner). Enkelte helseforetak har sendt med maler for risikovurderinger uten å dokumentere at det faktisk er gjort risikovurderinger. De to helseforetakene som har utført risikoanalyser, gir ingen henvisninger til forebyggende og korrigerende tiltak knyttet til den enkelte risiko.

Når det gjelder risikoanalyser for fjernaksessløsninger, er det 5[312] av de 12[313] helseforetakene der det framgår at det er gitt fjernaksess, som har gjort egne risikovurderinger, eller som legger ved risikovurderinger utført av it-enheten i helseregionen. To[314] av de fem har dokumentert at de har foretatt risikovurderinger før de har gitt leverandøren tilgang til å vedlikeholde og oppdatere utstyret. Flere helseforetak viser til at det er it-enhetene som utfører risikoanalyser av fjernaksessløsninger for medisinsk-teknisk utstyr. Skriftlige svar fra helseforetakene og intervju med enkelte helseforetak viser at helseforetakene, som databehandlingsansvarlig, ikke alltid selv har innhentet risikoanalysene fra it-enhetene.

Innsendt dokumentasjon viser at det ikke benyttes noe felles malverk for risikoanalyser for medisinsk-teknisk utstyr. Helseforetakene som er intervjuet, opplyser at det ikke

309) HODs svar av 19. august 2015.
310) Referat fra møte med Hemit.
311) Helse Stavanger HF og Telemarksykehuset HF.
312) Helse Bergen HF, Helse Fonna HF, Helse Førde HF, Helse Stavanger HF, Telemarksykehuset HF.
313) Ahus HF, Helse Innlandet HF, Østfoldsykehuset HF, Helse Førde HF, Helse Fonna HF, Helse Bergen HF, Helse Stavanger HF, Sørlandssykehuset HF, Telemarksykehuset HF, Helse Møre og Romsdal HF, St. Olavs hospital HF, Helse Nord-Trøndelag HF.
314) Helse Bergen HF og Helse Stavanger HF.

er etablert noe samarbeid mellom helseforetakene, helseregionene eller it-enhetene på dette området.

De intervjuede helseforetakene uttaler at de gjør risikovurderinger av den tekniske delen og funksjonaliteten til utstyret av hensyn til pasientsikkerheten. De foretar ikke risikoanalyser av informasjonssikkerhet i medisinsk-teknisk utstyr. Helse Stavanger HF uttaler at de har begrensede ressurser til å foreta risikoanalyser, samtidig som de sitter på en stor utstyrspark. Oppdatering og vedlikehold av utstyret kommer i første rekke, og tar opp mesteparten av ressursene i medisinsk-teknisk avdeling.

Sykehuset Telemark HF uttaler at etter hvert som stadig mer av det medisinsk-tekniske utstyret blir integrert mot annet utstyr over Internett, blir helseforetaket nødt til å risikovurdere utstyrets nettilgang. Sykehuset Telemark HF har henvendt seg til it-enheten i helseregionen, Sykehuspartner HF, for at de sammen skal risikovurdere et medisinsk-teknisk utstyr som skal kobles opp mot nett. Helseforetaket ønsker med dette å oppnå tverrfaglighet for å heve kvaliteten på risikovurderingene.

OUS HF uttaler at ved etablering av nye fjernaksessløsninger for oppdatering og service av medisinsk-teknisk utstyr skal som hovedregel regionens tjeneste som er etablert av Sykehuspartner HF, benyttes. Det er foretaket selv som beslutter om løsningen gir et akseptabelt risikonivå, og om den kan benyttes.

Helgelandssykehuset HF, som ikke har gjennomført risikoanalyser, mener dette blant annet skyldes måten sykehusene i foretaket er organisert på. Alle sykehusene sitter med like stor variasjon i utstyr som større sykehusenheter, men har færre ansatte. Hvert enkelt sykehus har derfor ikke tilstrekkelig administrative ressurser til å foreta risikoanalyser på alt utstyr.

2.2.3 Organisering

Det er en relativ lik formell organisering av arbeidet med medisinsk-teknisk utstyr i helseforetakene, og det er mange som har ansvar på ulike nivåer.[315] I hovedsak er ansvaret delt mellom medisinsk-teknisk avdeling (MTA) og ikt-personell innen helseforetaket og de regionale it-enhetene. Det er helsepersonell som betjener utstyret, og MTA anskaffer, drifter og vedlikeholder utstyret. Ikt-personellet har ansvar for nettverket, pc-er og servere som informasjonen fra medisinsk-teknisk utstyr overføres til. I tillegg er det de regionale helseforetakenes it-enheter som drifter de felles systemløsningene og nettverk i helseforetakene.

Anskaffelse av medisinsk-teknisk utstyr er organisert forskjellig ved at noe utstyr anskaffes regionalt, noe på helseforetaksnivå, og noe anskaffes direkte av det enkelte lokalsykehus. Helseforetakenes innkjøpsservice (HINAS), som er de regionale helseforetakenes eget innkjøpsselskap, anskaffer i liten grad medisinsk-teknisk utstyr.

Medisinsk-teknisk avdeling har i de fleste helseforetakene ansvar for vedlikehold, oppdatering og innkjøp av medisinsk-teknisk utstyr, i tillegg til inngåelse av avtaler med leverandører. Det er den enkelte klinikk som bruker utstyret, som har ansvar for at utstyret brukes riktig. Behandlende klinikk har også ansvar for informasjon som lagres i utstyret, eller på servere eller apparater som er tilknyttet utstyret, og som brukes i behandling av informasjon som genereres av medisinsk-teknisk utstyr.

315) Ansvaret for informasjonssikkerhet på medisinsk-teknisk utstyr på Helgelandssykehuset HF er lagt til hvert enkelt sykehus under helseforetaket. Det er ledelsen i helseforetaket sentralt som er definert som databehandlingsansvarlig for dataene som ligger i medisinsk-teknisk utstyr (MTU). Videre er medisinsk-teknisk avdeling ved sykehusene ved Helgelandssykehuset, henholdsvis Mo i Rana, Mosjøen og Sandnessjøen systemeiere for det medisinsk-tekniske utstyret ved sine lokasjoner, mens klinikksjefene ved den enkelte klinikk er definert som eier av dataene som ligger i utstyret. Helse Nord IKT har ansvar for it-infrastrukturen, inkludert internettlinjer og lagring av data, samt informasjonssikkerhetsspørsmål. Teknisk og administrativt personell på ikt er lagt til Helse Nord IKT.

Dokumentanalysen og intervjuene med de ulike aktørene viser at ansvarsforholdene for informasjonssikkerhet i medisinsk-teknisk utstyr er uklart på spesielt to områder:

a) mellom helseforetakene og helseregionenes it-enheter
b) mellom medisinsk-teknisk avdeling og ikt-avdeling i helseforetakene

Når det gjelder ansvaret mellom helseforetakene og helseregionenes it-enheter, er det uklarheter knyttet til utarbeidelse av risikoanalyser, avtaleinngåelse og oppfølging av leverandørene.

Helse Stavanger HF påpeker at det i praksis er mange databehandlingsbeslutninger som tas utenfor helseforetaket, av regionens it-enhet, og at det derfor er utfordrende for helseforetaket å ta et selvstendig ansvar. Noen av de undersøkte helseforetakene[316] hadde ikke gjenpart av fjernaksessavtalene som it-enhetene har inngått på vegne av helseforetakene som databehandleransvarlig. Helse Stavanger HF uttaler at leverandørene må henvende seg til Helse Vest IKT AS hver gang de ønsker å få fjernaksesstilgang til helseforetaket sitt utstyr. Det er ikke etablert noen fast rutine om at Helse Vest IKT AS varsler Helse Stavanger HF om at leverandøren er gitt tilgang til helseforetakets systemer.

Riksrevisjonen har tidligere påpekt[317] at helseforetakene, som databehandlingsansvarlig, skyver for stort ansvar over på databehandler. Departementet opplyste i den sammenheng blant annet at det foregår et forbedringsarbeid i helseforetakene for å øke bevisstheten om rollen som databehandlingsansvarlig. Datatilsynet påpeker i sin årsmelding for 2014 at viktige deler av databehandlingsansvaret i spesialisthelsetjenesten, slik som tilgangsstyring i helseforetakene, i praksis er ivaretatt av de regionale it-enhetene. Dette kan utfordre de reelt ansvarlige helseforetakenes muligheter til å overholde sine plikter. Datatilsynet påpeker at det er viktig at det legges til rette for at helseforetakene kan utøve sitt ansvar og styre underleverandørene på en god måte.[318]

I de tilfellene der de regionale it-enhetene er databehandler, er det it-enhetene selv som fysisk gir tilgangene til leverandør. Helseforetakene blir ikke alltid varslet på forhånd av den regionale it-enheten eller leverandøren om at leverandøren er inne i deres systemer og foretar oppdateringer og vedlikehold. Helse Stavanger HF opplyser at det har forekommet at leverandører har hatt fjernaksesstilgang til deres systemer uten at helseforetaket har vært klar over det, noe som gjør at helseforetaket mister kontroll over egne data. Helseforetakene, som er databehandleransvarlig, gjennomfører ingen kontroller av it-enhetenes rolle som databehandler.

Alle aktørene som er intervjuet, påpeker at det er uavklarte ansvarslinjer og gråsoner internt i helseforetaket mellom ikt-avdelingen og den medisinsk-tekniske avdelingen. Flere mener det er behov for en tettere organisering og samarbeid mellom disse avdelingene. Helseforetakene påpeker at medisinsk-teknisk utstyr som inneholder en ikt-komponent, ligger i "gråsonen" mellom medisinsk-teknisk avdeling og ikt-avdelingen. Det kan derfor bli uklart hvem som har ansvar for å stille krav til informasjonssikkerhet, både formelt og i den løpende driften. OUS HF mener sentrale myndigheter må bidra til å få klargjort ansvaret mellom de ulike avdelingene for å fjerne denne gråsonen.

316) Ahus, Østfoldsykehuset HF og Helse Stavanger HF svarer at de ikke har disse avtalene. Telemarksykehuset HF viser til Sykehuspartners avtale, men det er uklart om de har avtalen.
317) Dokument 3:2 (2014–2015) *Rapport fra utvidet kontroll om helseforetakenes beredskap innen ikt, vann og strøm.*
318) Datatilsynets årsmelding for 2014, side 32.

Helse Sør-Øst har i 2012–13 gjort en vurdering av mulig tettere organisering av ikt og medisinsk-teknisk utstyr. Enkelte helseforetak[319] har allerede slått sammen medisinsk-teknisk avdeling og ikt-avdelingen.

Hemit uttaler at medisinsk-teknisk utstyr blir mer og mer integrert i ikt-området ved at mye av utstyret i dag er datamaskiner med egne lagringsenheter, og det tilbys oppkobling på nett for mye av utstyret. Elektromedisinsk avdeling[320] og ikt-avdelingene har mange av de samme oppgavene og utfordringene, og Hemit ser behov for organisasjonsmessige endringer mellom disse avdelingene for å sikre en tettere integrasjon mellom ikt og medisinsk-teknisk avdeling (MTA) i helseforetakene.

Helseforetakene og leverandøren som ble intervjuet, peker alle på at medisinsk-teknisk avdeling og ikt-avdelingene i helseforetakene legger vekt på forskjellige sider ved informasjonssikkerheten. De medisinsk-tekniske avdelingene legger større vekt på pasientsikkerhet og tilgjengelighet til utstyr og informasjon. Dette er også parametere de blir kontrollert på av Direktoratet for samfunnssikkerhet og beredskap (DSB). Ikt-avdelingen i helseforetakene og helseregionenes it-enheter legger større vekt på konfidensialitet og å beskytte pasientopplysninger mot innsyn.

En manglende overordnet samhandlings-[321] og sikkerhetsarkitektur[322] bidrar også til uklare ansvarslinjer. Sykehuset Telemark HF påpeker behov for riktig sikkerhetsarkitektur med hensyn til pasientsikkerhet, for å sikre tilgjengelighet og funksjonell sikkerhet av medisinsk-teknisk utstyr. Helseforetaket mener regelverk og veiledere ikke dekker prinsipper for sikkerhetsarkitektur for å sikre forsvarlig pasientsikkerhet (tilgjengelighet og funksjonell sikkerhet) i medisinsk-teknisk utstyr og systemer for medisinsk-teknisk utstyr som koples til helseforetakets nettverk.

Utfordringer knyttet til samhandlingsarkitektur og sikkerhetsarkitektur er påpekt av sektoren selv i ulike rapporter.[323] Det vises til utfordringer i dagens arkitektur, både når det gjelder samhandlings- og kommunikasjonsarkitektur, sikkerhetsarkitektur, personvern og informasjonssikkerhet. Det framkommer at dagens samhandlings- og kommunikasjonsinfrastruktur har lav endringsevne og er ikke tilrettelagt for nye tjenester med mer deling av informasjon.[324]

I en analyse av de regionale helseforetakene på ikt-området, som er bestilt av Helse- og omsorgsdepartementet, påpeker tre av foretakene at det er behov for å forbedre styringsmodellene for ikt.[325]

3 Vurderinger

3.1 Helseforetakene stiller ikke tilstrekkelig krav om informasjonssikkerhet i avtaler med leverandører av medisinsk-teknisk utstyr og har mangelfull oppfølging av leverandører

Undersøkelsen viser at helseforetakene i liten grad stiller krav om informasjonssikkerhet i avtalene med leverandører. Bare 6 av 19 helseforetak har stilt krav om

319) AHUS og Østfoldsykehuset HF.
320) Det samme som medisinsk-teknisk avdeling.
321) Samhandlingsarkitekturen skal gi en overordnet beskrivelse av de ulike elementene som må på plass for å kunne kommunisere elektronisk, og hvordan disse elementene forholder seg til hverandre (e-helse.no).
322) En virksomhetsarkitektur beskriver et system, dets komponenter, innbyrdes sammenhenger mellom komponentene og forholdet til omgivelsene, samt prinsipper for utvikling av arkitekturen (basert på definisjon av "arkitektur" i ISO/IEC32010:2007, Systems and Software Engineering). Sikkerhetsarkitekturen er en del av virksomhetsarkitekturen.
323) Rapport IS-2120 Nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren og IKT utfordringsbilde i helse- og omsorgssektoren – september 2014. Utarbeidet av "Én innbygger – én journal"-prosjektet.
324) HOD – IKT utfordringsbilde i helse- og omsorgssektoren, side 13.
325) HOD – Komparativ analyse av de regionale helseforetakene på ikt-området – september 2014, side 16.

leverandørens behandling av personopplysninger i én eller flere avtaler som de har inngått. Slike krav kan være oppdatering av programvare og vedlikehold av utstyr, behandling av personopplysninger og å klargjøre hva leverandør skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet. Videre har få helseforetak stilt krav i avtalene om at de må gi samtykke før leverandøren kan gjøre endringer i systemet.[326] Dette betyr at leverandøren ikke er forpliktet til å varsle helseforetaket når de går inn og gjør endringer og oppdateringer på helseforetakenes utstyr. Avtalene inneholder derfor i liten grad krav som vil bidra til å hindre eller oppdage informasjonssikkerhetsbrudd.

Undersøkelsen viser videre at leverandørene i stor grad er premissgiver i avtalene. Mange av de gjennomgåtte avtalene tar utgangspunkt i maler utarbeidet av leverandør som ikke omtaler informasjonssikkerhet, og det er videre lite samarbeid mellom helseforetakene om å stille krav til leverandørene i kravspesifisering, avtaleinngåelse og anskaffelse av utstyr. I tillegg imøtekommer ikke alt utstyret alle lovkrav til informasjonssikkerhet.

Undersøkelsen viser også at det kan være krevende for helseforetakene å følge lovverket fullt ut ettersom utstyret fra leverandørene ikke har all den funksjonaliteten som loven krever, som for eksempel tilgangsstyring, antivirus og loggfunksjoner. Leverandørene tilbyr løsninger som er beregnet på det internasjonale markedet med andre lovkrav. De norske helseforetakene har etter loven ikke mulighet til å gjøre endringer på utstyret for å imøtekomme kravene i personopplysningsforskriften om tilgangsstyring, antivirus og logging.

Leverandøravtalene er et sentralt virkemiddel for å ivareta de lovbestemte kravene til informasjonssikkerhet. De regionale helseforetakenes it-enheter har utarbeidet felles føringer for styringssystem for informasjonssikkerhet, inkludert standarder for databehandleravtale og underdatabehandleravtale. Det er imidlertid få helseforetak som bruker avtalene til å stille krav. Helseforetakene framstår også som lite koordinerte og samstemte i sin samhandling med leverandørene. Helseforetakene har blant annet ulik praksis om bruk av fjernaksessavtaler. Revisjonen mener at få krav og lite samordning gir økt risiko for mangelfull informasjonssikkerhet.

Undersøkelsen viser at helseforetakene hverken foretar egne kontroller av leverandørene eller innhenter uavhengige revisjoner av leverandørene. Helseforetakene benytter ikke den muligheten til kontroll av leverandørene som lovverket gir mulighet til, og helseforetakene har dermed i liten grad kjennskap til leverandørens praktisering av lover og regler knyttet til sensitive personopplysninger.

3.2 Helseforetakene har mangelfull oversikt over risiko knyttet til informasjonssikkerhet i medisinsk-teknisk utstyr

Det er etablert regionale føringer, retningslinjer og rutiner for gjennomføring av risikovurderinger som også omfatter medisinsk-teknisk utstyr.[327] Det utarbeides regionale risikoanalyser hvor medisinsk-teknisk utstyr inngår som et av flere risikoområder på overordnet nivå.

Undersøkelsen viser imidlertid at helseforetakene i liten grad har gjort overordnede risikovurderinger av informasjonssikkerheten i medisinsk-teknisk utstyr. Det foreligger dermed ingen samlet oversikt over risikoen og heller ingen opplysninger om eventuelle forebyggende og korrigerende tiltak. Bare 2 av 19 helseforetak kan dokumentere at det har vært gjennomført risikoanalyser knyttet til det enkelte medisinsk-

326) Enkelte helseforetak utfører service og vedlikehold av mye av utstyret selv, men ikke for alt utstyr.
327) HODs svar av 19. august 2015.

tekniske utstyret. De fire intervjuede helseforetakene uttaler imidlertid at det behandlende helsepersonellet som benytter utstyret, har oversikt over hvilken informasjon som ligger der.

Manglende risikovurderinger kan føre til at det ikke foretas noen vurdering av sensitiviteten i informasjonen som ligger i utstyret. Det er dermed vanskelig å få god oversikt over trusselbildet, og om det er iverksatt relevante forebyggende eller korrigerende tiltak. I tillegg kan praktiseringen av regelverket bli ulikt, og kravene til leverandør og fjernaksessløsninger kan bli mangelfulle – men også i enkelte tilfeller unødig strenge.

3.3 Det er uklare ansvarslinjer for informasjonssikkerhet i medisinsk-teknisk utstyr internt i helseforetakene og mellom helseforetakene og de regionale it-enhetene

Helseforetakene har i undersøkelsesperioden i begrenset grad hatt retningslinjer og rutiner som beskriver hvordan personsensitiv informasjon i medisinsk-teknisk utstyr skal behandles.

De regionale helseforetakenes IT-enheter har arbeidet med å få på plass felles regionale føringer, retningslinjer og rutiner, men undersøkelsen viser at dette i begrenset grad er implementert i helseforetakene.

Undersøkelsen viser at oppgavefordelingen for å ivareta informasjonssikkerhet både mellom helseforetakene og helseregionenes it-enheter, og innad i helseforetakene mellom ikt og medisinsk-teknisk avdeling, er uklar. I tillegg tyder undersøkelsen på at regelverket knyttet til informasjonssikkerhet er vanskelig å bruke i praksis for helseforetakene. RHF-ene og helseforetakene har ulike oppfatninger om hvilke krav som skal stilles overfor leverandørene, og hvilke rettigheter leverandører skal ha til å gjøre oppdateringer og vedlikehold på utstyr som inneholder person- og helseopplysninger.

Etter revisjonens vurdering kan dette medføre at det blir uklart for aktørene hvordan kravene skal operasjonaliseres og følges opp. Undersøkelsen tyder på at det er uklare ansvarslinjer internt i helseforetakene og mellom helseforetakene og de regionale it-enhetene. Videre er det lite samarbeid mellom helseforetakene. En felles tilnærming i helseforetakene til hvordan kravene skal forstås og brukes, vil gjøre det enklere for foretakene å følge opp leverandørene. Det medisinsk-tekniske utstyret som i dag benyttes, er mer likt tradisjonelt ikt-utstyr med egne lagringsenheter og mulighet for kommunikasjon via nettverk. Dette medfører større behov for samhandling og samarbeid mellom de ulike avdelingene.

Helseforetakene som er intervjuet opplever at dette saksområdet ikke er tilstrekkelig klarlagt, og de er usikre på hvordan de skal balansere kravene til pasientsikkerhet og informasjonssikkerhet. De regionale helseforetakene bør, som eier, legge til rette for at helseforetakene og it-enhetene gjør en koordinert og samlet innsats for å klargjøre ansvarslinjer og rutiner som bidrar til at kravene til informasjonssikkerhet etterleves. Etter revisjonens mening er ansvarslinjer og rutiner som skal sikre god informasjonssikkerhet i medisinsk-teknisk utstyr uklare.