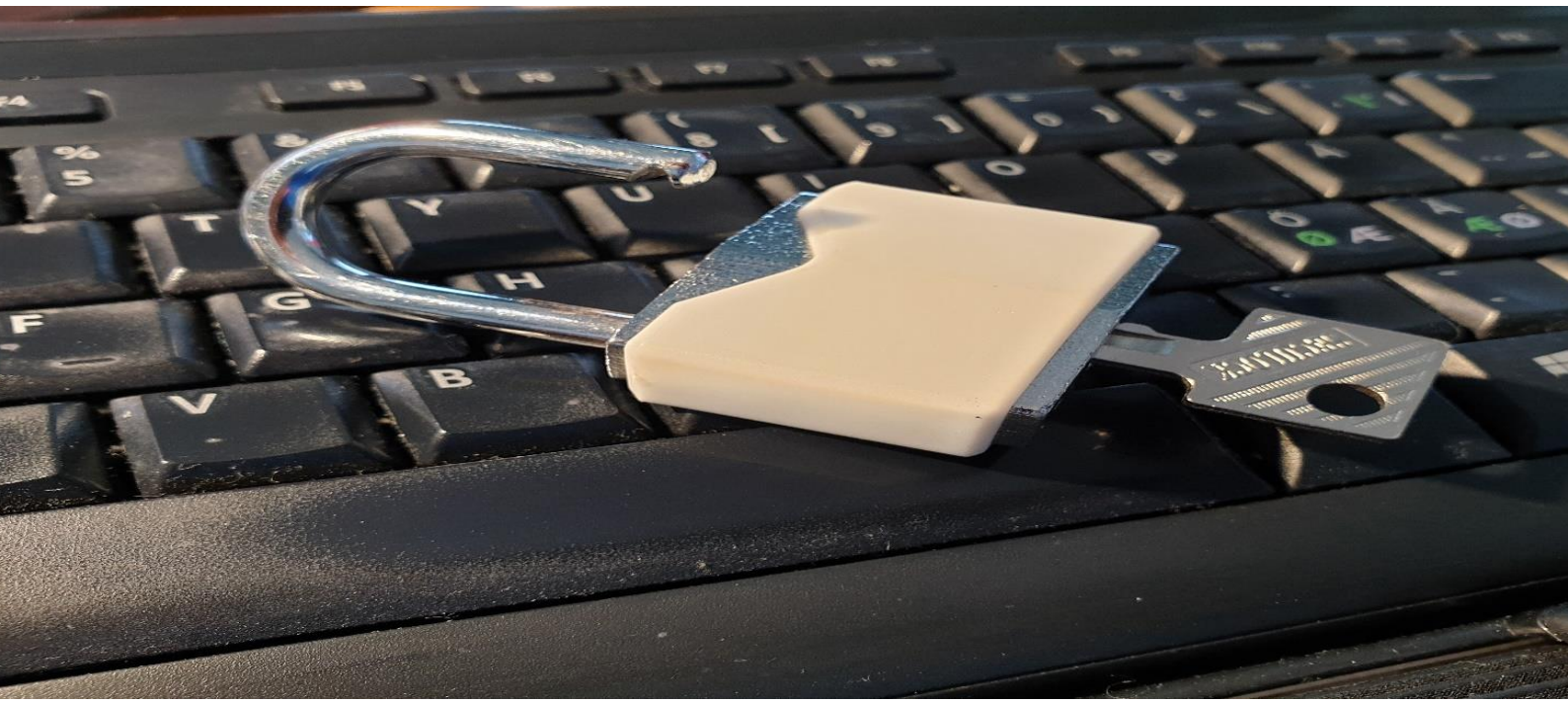
Riksrevisjonen

# Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer

Rapportvedlegg til Dokument 3:2 (2020-2021)



**Revisjonen er gjennomført i henhold til lov om Riksrevisjonen § 9, andre ledd og instruks om Riksrevisjonens virksomhet § 5 andre ledd. Revisjonen er gjennomført i samsvar med Riksrevisjonens faglige retningslinjer for selskapskontroll, Riksrevisjonens faglige retningslinjer for forvaltningsrevisjon og INTOSAIs standard for forvaltningsrevisjon (ISSAI 3000).**

Forsidebilde: Riksrevisjonen

ISBN-978-82-8229-489-8

# Innhold

**Tabelloversikt**



**Figuroversikt**



**Faktaboksoversikt**

# 1 Innledning

## 1.1 Bakgrunn

Digitale løsninger som tas i bruk i helsetjenesten, skal tilfredsstille krav til informasjonssikkerhet. Dagens moderne sykehus digitaliseres i økende grad, og IKT blir en stadig viktigere del av kjernevirksomheten. Dette gir grunnlag for økt kvalitet i pasientbehandlingen. Samtidig øker sårbarhet for digitale angrep og datainnbrudd i helseforetakene, og de potensielle negative konsekvensene av sikkerhetsbrudd blir større.[1]

Dersom helseopplysninger eller IKT-systemer manipuleres eller gjøres utilgjengelige, kan det forårsake pasientskader. Helseopplysninger på avveie kan også få alvorlige konsekvenser for helseforetak og pasienter i form av tapt tillit, uønsket eksponering, identitetstyveri, utpressing mm. Dataangrep kan også få betydelige økonomiske konsekvenser. I behandlingen av Dokument 3:2 (2015-2016)[2] uttalte Kontroll- og konstitusjonskomiteen at informasjonssikkerhet må tas på det største alvor hos alle som er involvert i ulike prosesser i helsevesenet.

Helseforetakene kan være interessante mål for både datakriminalitet, industrispionasje og statlig etterretning, som kan ha til hensikt å stjele, endre, hindre eller påvirke data eller funksjoner. Eksempler på slike data er systematiserte, sensitive helsedata som finnes i registre og journaler. Stjålne helseopplysninger kan være verdifulle til forskning og utvikling, eller brukes som pressmiddel for å oppnå andre mål. Uvedkommende kan også ha interesse av å sette sykehusfunksjoner ut av spill. Bortfall av IKT vil få konsekvenser for sykehusdriften selv om sykehusene har beredskapsrutiner og gjennomfører beredskapsøvelser hvor bortfall av IKT er et av scenariene.

Når informasjon gjøres tilgjengelig digitalt innad i helseforetak, på tvers av helseforetak og på tvers av regioner, kan en sikkerhetsbrist ett sted i nettverket gi angripere adgang til andre deler av nettverket. Små sikkerhetsbrister kan dermed få store konsekvenser.

Med dataangrep menes handlinger med hensikt å skade eller påvirke et IKT-system. Det er en rekke måter angrep kan gjennomføres på, og angrepsformene er i stadig utvikling.[3] Potensielle angripere kan utnytte svakheter i for eksempel nettverk, i medisinsk-teknisk utstyr og behandlingshjelpemidler, i journalsystemene eller i forsystemene til journalsystemene.

Det har vært et økende omfang av dataangrep mot helseinstitusjoner verden rundt de siste årene. I januar 2018 ble Helse Sør-Øst utsatt for dataangrep som kunne ha blitt brukt til å stjele eller kompromittere pasientopplysninger.[4] I august 2020 ble Sykehuset Innlandet utsatt for et dataangrep.[5] Det er også mange eksempler fra utlandet:

- «Wannacry-angrepet» i 2017, der helsesektoren i Storbritannia var blant dem som ble verst rammet. Datasystemer ved omtrent 40 britiske sykehus og private klinikker ble infisert av et løsepengevirus.[6]
- I 2020 ble 400 sykehus/helseinstitusjoner i USA med 90 000 ansatte rammet av et dataangrep som medførte at alt IKT-utstyr måtte slås av i en periode.[7]
- I 2020 ble et sykehus i Tyskland rammet av et løsepengeangrep og det tok i overkant av en måned før dette sykehuset var tilbake i normal drift. En kvinne døde som følge av angrepet.[8]

Det er ikke mulig å beskytte seg mot alle forsøk på å bryte seg inn i helseregionenes IKT-systemer eller nettverk. Det er derfor viktig å etablere flere lag med sikkerhet slik at man gjør det vanskeligere for en angriper å gjøre skade dersom de skulle komme seg inn. Videre er det viktig at virksomheter

[1] Meld. St. 7 (2019-2020), Nasjonal helse- og sykehusplan 2020-2023, Innst. 255 S (2019-2020)
[2] Innst. 186 S (2015-2016) side 12, Kontroll- og konstitusjonskomiteèns merknad til Dokument 3:2 (2015-2016) Sak 3: Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr
[3] https://www.netsecurity.no/fagblogg/hvilke-typer-dataangrep-finnes-det
[4] Meld. St. 7 (2019-2020), Innst. 255 S (2019-2020)
[5] https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/analysearbeidet-etter-dataangrepet-mot-sykehuset-innlandet-er-avsluttet
[6] https://www.digi.no/artikler/slakter-britisk-helsevesen-for-darlig-it-sikkerhet/410948
[7] https://www.wired.com/story/universal-health-services-ransomware-attack/ https://www.uhsic.com/statement-from-universal-health-services/
[8] https:/www.digi.no/artikler7kvinne-dode-etter-losepengevirus-angrep/499582

har systemer og rutiner som gjør at de kan oppdage angrep. Dette legger igjen grunnlaget for at angrep kan håndteres. Helseregionene må etablere sikkerhetstiltak ut ifra hva de mener er et forsvarlig risikonivå.

Direktoratet for e-helse påpeker i sin overordnede risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren i 2019 at avhengighetene mellom IKT, pasientbehandling og pasientsikkerhet øker i takt med digitaliseringen. Sykehusenes IKT-systemer er komplekse og har mange avhengigheter, og utilgjengelige IKT-systemer er en alvorlig trussel for helse- og omsorgssektoren. Videre påpeker direktoratet at aktørbildet er komplekst, at ansvaret for de ulike løsningene, produktene og verdikjedene delvis er fragmentert og noe uoversiktlig, og at utstyret til dels er gammelt og utdatert.[9]

Koronaepidemien bidrar også til å øke risikoen for angrep. Flere har hjemmekontor hvor det ofte er svakere sikkerhet, noe hackere vil kunne forsøke å utnytte.Videre er det i flere tilfeller avdekket svakheter i sikkerhetskulturen i helseforetakene i form av manglende bevissthet og risikoforståelse om informasjonssikkerhet i ledelsen og blant de ansatte.[10] [11] Dette kan utnyttes av angripere, som kan komme seg inn i IKT-systemene ved at ansatte trykker på lenker i e-poster fra ukjente avsendere eller ikke logger seg ut av utstyr som benyttes. Tidligere revisjoner har vist at helseforetakene, inkludert deres IKT-leverandører, har svakheter i rutiner og systemer for å forebygge og følge opp informasjonssikkerhetsbrudd.

Området er i stor grad regulert av lover og forskrifter som foretakene må forholde seg til i sitt arbeid.

Ansvaret for IKT-sikkerheten er delt mellom flere aktører og nivåer i spesialisthelsetjenesten. Helse- og omsorgsdepartementet har det overordnede ansvaret, og de regionale helseforetakene har ansvaret for informasjonssikkerheten i sine helseregioner. Informasjonssikkerheten i helseregionene ivaretas hovedsakelig av helseforetak og regionale IKT-leverandører (Sykehuspartner HF, Helse Nord IKT HF, Helse Vest IKT AS og Hemit[12]). De regionale IKT-leverandørene har ansvar for den tekniske sikringen av helseregionenes felles IKT-infrastruktur, av regionale IKT-systemer, samt av mange av helseforetakenes lokale systemer og utstyr. Helseforetakene har ansvar for at systemer og utstyr brukes på en sikker måte. Der helseforetakene selv har ansvaret for drift av systemer og utstyr, vil de imidlertid ofte selv stå for teknisk sikring.

## 1.2 Samspill for god IKT-sikkerhet

I denne undersøkelsen brukes både begrepene informasjonssikkerhet og IKT-sikkerhet. Begrepene overlapper i stor grad, og brukes ofte som synonymer både i dagligtale og i virksomheters styring av området.[13]

Informasjonssikkerhet handler om å sikre informasjonsbehandlingen, inkludert gjennom å sikre at informasjon

- ikke blir kjent for uvedkommende (*konfidensialitet*),
- ikke blir endret utilsiktet eller av uvedkommende (*integritet*),
- er tilgjengelig ved behov (*tilgjengelighet*).

Informasjonssikkerhet omfatter også informasjon som ikke utveksles og lagres i IKT-systemer eller elektronisk på annen måte.[14]

---

[9] Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren - 25. juni 2019

[10] Direktoratet for e-helse overordnede risiko- og sårbarhetsvurderinger av IKT i helse- og omsorgssektoren av 1. juli 2019 og R Riksrevisjonens undersøkelse av styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler og Riksrevisjonens undersøkelse om helseforetakenes beredskap innen IKT, vann og strøm jf Dokument 3:2 (2014-2015) og Riksrevisjonens undersøkelse ov informasjonssikkerhet i medisinsk-teknisk utstyr jf Dokument 3:2 (2015-2016).

[11] Riksrevisjonens undersøkelse av styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler og Riksrevisjonens undersøkelse om helseforetakenes beredskap innen IKT, vann og strøm jf Dokument 3:2 (2014-2015) og Riksrevisjonens undersøkelse ov informasjonssikkerhet i medisinsk-teknisk utstyr jf Dokument 3:2 (2015-2016).

[12] Hemit er en avdeling i Helse Midt-Norge RHF. IKT-leverandørenes ansvar og oppgaver er forholdsvis like selv om de har ulik selskapsform.

[13] NOU 2018: 14 Sikkerhet i alle ledd

[14] https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

IKT-sikkerhet kan forstås som beskyttelse av IKT-systemer, samvirket mellom systemene, tjenestene som leveres av systemene, og informasjonen som behandles i systemene. Målene med IKT-sikkerhet er gjerne de samme som for informasjonssikkerhet. IKT-systemene, informasjonen som behandles i systemene, og tjenestene tilknyttet systemene skal beskyttes mot urettmessig tilgang, ikke endres utilsiktet eller av uvedkommende, og være tilgjengelig ved behov.[15]

Kravene i lovverket som gjelder spesialisthelsetjenesten omhandler i stor grad behandlingen av helseopplysninger/pasientinformasjon, og helseregionene bruker i hovedsak begrepet informasjonssikkerhet i styringen av området. Når vi i denne undersøkelsen vurderer sikringen av helseregionenes IKT-systemer mot dataangrep, bruker vi i mange tilfeller begrepet IKT-sikkerhet.

Tiltak for å ivareta sikkerheten kan grupperes på ulike måter. Man kan skille mellom sikkerhetstiltak egnet til å forebygge, oppdage og respondere på sikkerhetsbrudd.[16] I denne undersøkelsen har vi avgrenset oss til å se på helseregionenes arbeid med å forebygge og avdekke dataangrep. Vi har altså ikke undersøkt hvor godt rustet de er til å håndtere dataangrep etter at de har inntruffet (beredskap).

Ved valg av sikkerhetstiltak må kravene til konfidensialitet, integritet og tilgjengelighet ses i sammenheng, og det må prioriteres ut ifra risiko og kostnader.[17]

I undersøkelsen ser vi på den tekniske sikringen av helseregionenes IKT-systemer, men også på hvordan IKT-sikkerheten påvirkes av helseregionenes sikkerhetsstyring og -organisering, og av atferden til helse- og IKT-personell i helseforetak og ved regionale IKT-leverandører. Disse forholdene kan ses på som ledd i en sikringskjede eller et samlet forsvar mot dataangrep, og den totale IKT-sikkerheten vil ikke være sterkere enn det svakeste leddet.

Sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå.[18]

## 1.3 Mål og problemstillinger

Målet med undersøkelsen er å vurdere hvordan helseforetakenes IKT-systemer sikres mot dataangrep, hvordan de regionale helseforetakene understøtter dette arbeidet, og hvordan Helse- og omsorgsdepartementet følger opp.

Målet belyses gjennom følgende problemstillinger:

1. I hvilken grad er helseforetakenes IKT-systemer sikret mot dataangrep?
2. Bidrar de regionale IKT-leverandørene og helseforetakenes sikkerhetsstyring til å opprettholde et forsvarlig sikkerhetsnivå?
3. Hvordan tilrettelegger og følger de regionale helseforetakene opp at helseforetakene kan beskytte seg mot dataangrep?
4. Hvordan er Helse- og omsorgsdepartementets oppfølging og virkemiddelbruk på IKT-sikkerhetsområdet i spesialisthelsetjenesten?

[15] NOU 2018: 14 Sikkerhet i alle ledd
[16] https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/sikkerhetstiltak
[17] Jf. personvernforordningen artikkel 32.
[18] NSMs veileder i sikkerhetsstyring https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-sikkerhetsstyring.pdf

# 2 Metodisk tilnærming og gjennomføring

Problemstillingene er belyst bl.a. gjennom analyse av dokumenter (inkludert teknisk dokumentasjon), tekniske kontroller, intervjuer i alle fire helseregioner (se tabell 1). Undersøkelsen omfatter alle helseforetak og de fire regionale IKT- leverandørene i helseregionene.[19] Sykehusapotekene er ikke en del av undersøkelsen.

**Tabell 1 Metoder som er brukt for å belyse problemstillingene**

| | Alle helseforetak og regionale IKT-leverandører | De fem utvalgte helseforetakene | Regionale IKT-leverandører | Regionale helseforetak | Helse- og omsorgs-departementet |
|---|---|---|---|---|---|
| **Dokumentanalyse** | X | | X | X | **X** |
| **Spørrebrev** | X | | | | |
| **Intervju[20]** | | X | X | X | **X** |
| **Angrepssimulering og tekniske kontroller** | X | | | | |
| **Phishingtest og observasjoner** | | X[21] | | | |
| **Analyse av avviksmeldinger** | | **X** | **X** | | |

Kilde: Riksrevisjonen

Fem helseforetak er valgt ut for nærmere analyse − ett fra hvert i helseregionene Nord, Midt-Norge og Vest, og to fra Sør-Øst, som er den største regionen.[22] For å unngå å måtte sette seg inn i for mange ulike tekniske miljøer er det for Helse Sør-Øst valgt helseforetak som har samme teknologiske plattform.[23] Det er lagt vekt på å få en geografisk spredning og å velge helseforetak med ulik størrelse for å få fram bredden i oppgaveportefølje og systemer.

Det er videre valgt ti ulike avdelinger i fem sykehus i de fem utvalgte helseforetakene. Det er valgt avdelinger som dekker et bredt spekter av oppgaver på et sykehus - derfor er det både medisinske avdelinger og avdelinger i administrasjonen og driften valgt ut. På oppstartmøte med regionene ble valg av avdeling presentert. I de tilfeller vi var i tvil om rett avdeling var valgt, ble valget tatt i samråd med helseforetaket. Dette for å hindre at vi valgte avdelinger som i liten grad benytter IKT eller ikke er eksponert for dataangrep.

De innsamlede dataene omfatter i hovedsak tidsrommet 2017–2020.

## 2.1 Dokumentanalyse

Det er innhentet dokumentasjon fra de fire regionale IKT-leverandørene og alle helseforetakene for å forstå hvordan styringssystemet for informasjonssikkerhet er bygget opp i regionene og helseforetakene. Dokumentasjonen av styringssystemene er også analysert, for å undersøke om de regionale helseforetakene og helseforetakene jobber systematisk med kvalitetsforbedring av

[19] Helse Nord IKT HF, Hemit, Helse Vest IKT AS og Sykehuspartner HF.
[20] I tillegg er Direktoratet for e-helse, Sykehusinnkjøp HF og HelseCERT intervjuet.
[21] Phishingtesten er sendt til et utvalg ansatte i hele helseforetaket.
[22] [redacted]
[23] [redacted]

styringssystemene for informasjonssikkerhet. Hensikten har vært å undersøke om det er etablert rutiner for å oppdatere styringssystemet i tråd med teknologisk utvikling og nye trusler om dataangrep, om det er gjort risikovurderinger, satt mål på området og om det er etablert en tydelig ansvarfordeling og klare rapporteringslinjer. Det er innhentet risiko- og sårbarhetsanalyser fra alle helseforetakene og de fire IKT-leverandørene, tilsammen 430[24] risikoanalyser. Ett tilfeldig utvalg[25] (10 prosent (43)) av disse risikoanalysene er analysert nærmere med det formål å kontrollere om det gjøres konkrete risikoanalyser av systemer og utstyr, hva de inneholder og hvordan de er utformet.

For å undersøke styringssystemet og internkontrollen, er det innhentet sikkerhetsrevisjonsrapporter og evalueringer fra beredskapsøvelser som helseforetaket og IKT-leverandørene har gjennomført. Referater fra AD-møter og styremøter er analysert for å belyse hvordan revisjonenes funn og evalueringer følges opp av ledelsen, samt for kvalitetsforbedring av styringssystemet.

Det er innhentet og analysert dokumentasjon fra de regionale IKT-leverandørene og de fem utvalgte helseforetakene som beskriver hvordan IKT-infrastrukturen er bygd opp. Dette har vært viktig for å forstå den tekniske infrastrukturen og gjennomføre kontroller av tekniske sikkerhetstiltak på en mest mulig effektiv måte. Informasjon fra dokumentasjon av IKT-infrastrukturen supplerer resultater fra angrepssimulering og analyse av uttrekk som grunnlag for vår kontroll av tekniske sikkerhetstiltak.

## 2.2 Spørrebrev

Spørrebrev er brukt for å innhente svar på konkrete faktaspørsmål. Spørrebrevene er sendt suksessivt til alle helseforetak og de regionale IKT-leverandørene. Den første helseregionen, Helse Sør-Øst, ble undersøkt i første halvår 2019 og spørrebrevene ble sendt ut 23. januar 2019. Undersøkelsen av den siste regionen, Helse Vest , ble gjennomført i begynnelsen av 2020, og brevene ble sendt ut 6. november 2019.[26] I spørrebrevene er det bedt om redegjørelser for ansvarsfordeling, beskrivelse? /evaluering av styringssystemet og risikovurderinger som omtaler trusler om dataangrep mv.

I spørrebrevene er det også stilt spørsmål som skal belyse sikkerhetskulturen hos helseforetakene og IKT-leverandørene. Dette omfatter opplærings- og informasjonstiltak og ressurser avsatt til konkrete sikkerhetstiltak.

Sammen med spørrebrevene er det innhentet informasjon om ledelsens gjennomgang, referater fra møter i toppledelsen (AD-møter), risikoanalyser, sikkerhetsrevisjoner og -øvelser, oversikter over behandling av helse- og personopplysninger, og beskrivelser av avvikssystemet, inkludert avviksstatistikk.

## 2.3 Intervju

***Intervju med departementet og sentrale aktører i departementets virkemiddelapparat***

For å belyse hvordan Helse- og omsorgsdepartementet følger opp IKT-sikkerheten i helseregionene og hvordan virkemiddelbruken fungerer, er Direktoratet for e-helse, Norsk Helsenett SF ved HelseCert og departementet intervjuet.

***Intervjuer med toppledelsen i de fire helseregionene***

Det er gjennomført intervjuer med administrerende direktør i de fire regionale helseforetakene for å få en nærmere forståelse av hvordan regionene vektlegger informasjonssikkerhetsarbeidet og jobber med å oppdatere og utvikle sine styringssystem for informasjonssikkerhet

[24] HSØ: 186, HN: 152, HMN: 62 og HV: 30. I enkelte tilfeller er samme regionale risikoanalyse sendt inn fra flere helseforetak, så det reelle tallet er noe lavere. Ulikhetene i omfanget mellom regionene skyldes at vi i de siste to regionene (HMN og HV) kun ba om eksempler på risikoanalyser.
[25] Fra helseforetakene og iKT-leverandørene i de fire helseregionene
[26] Brev til Helseforetakene i Helse Sør-Øst ble sendt ut 23. januar 2018, til Helse Nord 8. mai 2019, Helse Midt-Norge 5. september 2019, og til slutt Helse Vest 6.november 2019.

***Intervjuer med toppledelsen og nøkkelpersonell i de fem utvalgte helseforetakene og hos IKT-leverandørene***

Informasjonssikkerhetsleder/rådgiver hos IKT-leverandørene og i helseforetakene har det løpende ansvaret for styringssystemet. Informasjonssikkerhetsledere/rådgivere er intervjuet for å få mer informasjon om organisering og gjennomføring av sikkerhetsarbeidet i IKT-leverandørene, helseforetakene og regionen, samt hvordan myndighet, ansvar og arbeidsoppgaver er fordelt og hva som er eventuelle utfordringer. Videre ønsket vi å få mer informasjon om sikkerhetskulturen, opplæringsrutiner og informasjon om avvikssystemet og hvordan avvik håndteres i praksis.

For å få et inntrykk av hvordan styringssystemet og krav til informasjonssikkerhet påvirker IKT-driften er alle ledere av IKT-leverandørenes driftsavdelinger intervjuet individuelt. Formålet er å kunne si noe mer om risikoen og de utfordringer driftsavdelingene har og hvilke tiltak som kan forebygge dataangrep i den daglige driften. Det er lagt vekt på å få informasjon om hvordan ansvar og arbeidsoppgaver knyttet til sikkerhet er fordelt mellom IKT (drifts)-avdelingen og informasjonssikkerhetsleder og leverandører. Det har også vært et mål å få frem hvordan avdelingsleder jobber med IKT-/informasjonssikkerhet i avdelingen (inkludert opplæring, avvikshåndtering), hvilke praktiske utfordringer avdelingsleder ser i det daglige arbeidet, og indirekte mer informasjon om hvilke risikoer/trusler de er utsatt for.

Det er gjennomført intervjuer med toppledelsen (administrerende direktør/direktør) hos IKT-leverandørene og i de fem utvalgte helseforetakene for å belyse hvordan de følger opp de nasjonale og regionale føringene knyttet til informasjonssikkerhetsarbeidet.[27] Intervjuene er også gjennomført med sikte på å få et innblikk i hvor godt informasjonssikkerhet er forankret i den øverste ledelsen hos IKT-leverandørene og i helseforetakene, samt å undersøke hvordan administrerende direktør og toppledelsen for øvrig tar dette ansvaret i praksis.

Det er skrevet referater etter hvert intervju med ledelsen som er verifisert i etterkant.

***Intervjuer med ledere og ansatte ved utvalgte sykehusavdelinger***

For å kunne si noe om sikkerhetskulturen og hvordan det jobbes med informasjonssikkerhet i sykehus er det gjort dybdeintervjuer i fem utvalgte helseforetak. For å undersøke de ansattes og ledelsens bevissthet og utfordringer de har når det gjelder informasjonssikkerhet og sikkerhetskultur, er det gjennomført individuelle intervjuer i de utvalgte avdelingene med en leder og en ansatt som de selv valgte ut. Formålet med intervjuene har vært å avdekke mer generelle mekanismer som kan bidra til å forebygge dataangrep. For å svare på dette ønsket vi å få frem hvordan avdelingene jobber med informasjonssikkerhet (inkludert opplæring, avvikshåndtering), hvilke utfordringer de møter på i det daglige arbeidet og indirekte mer informasjon om hvilke risikoer de er utsatt for.

Intervjuene er tatt opp på bånd og transkribert. Disse intervjuene ble ikke verifisert.

***Oppfølgingsintervjuer med IKT-leverandørene***

Ettersom det gikk lang tid fra kontrollene i de første til de siste helseregionene, ble det i månedsskiftet mai/juni 2020 avholdt møter med de tre IKT-leverandørene som ble undersøkt først – Sykehuspartner HF, Hemit og Helse Nord IKT HF. Her orienterte IKT-leverandørene om hvilke tiltak de hadde iverksatt siden kontrollen og om aktuell status for arbeidet. I tillegg ble det stilt spørsmål om mulige årsaker til funnene som gjort under angrepssimuleringen. Tilsvarende spørsmål ble stilt Helse Vest IKT HF i januar 2020. Oppsummeringer fra disse møtene er verifisert.

## 2.4 Angrepssimulering og test av tekniske sikkerhetstiltak

Tekniske sikkerhetstiltak har i hovedsak blitt testet ved å:

[27] [redacted]

- [redacted]
- analysere uttrekk av data fra systemer.

Resultatene av testene av tekniske sikkerhetstiltak er vurdert opp mot beste praksis.

Fordelen med bruk av simulerte angrep er at det er mulig å vise hvordan konkrete svakheter kan utnyttes av en angriper. Simulering av dataangrep viser en vei inn for en angriper, men gir ikke nødvendig bredde for å evaluere alle tekniske sikkerhetstiltak i helseregionen. For å få et bredere bilde av helseregionens tekniske sikkerhetstiltak er derfor angrepssimuleringen supplert med analyse av data trukket ut fra helseregionenes systemer.

**Angrepssimulering**

[redacted]

Selv om kontrollen av tekniske sikkerhetstiltak omfatter hele helseregionen, har sykehusene[28] i de fem utvalgte helseforetakene blitt særskilt kontrollert i denne angrepssimuleringen. Målet for angrepssimuleringen er å få kontroll over viktige systemer og tilgang til persondata om pasienter. Framgangsmåten som er brukt for angrepssimuleringen varierer noe mellom sykehusene ettersom en angriper vil følge minste motstands vei mot målet, men følger i hovedsak følgende steg:

- [redacted]
- Få tilgang til en hvilket som helst brukerkonto og tilhørende passord for å få tilgang til ressurser i nettverket som alle brukere har tilgang til.
- Kartlegge nettverk, maskiner og brukerkontoer for å forstå IKT-infrastrukturen og de mest effektive veier for videre angrep mot sykehuset.
- Kartlegge [redacted] hvor alle har tilgang for å se om det her ligger personopplysninger eller sensitiv informasjon om sykehusets IKT-infrastruktur.
- Forsøk å utnytte maskiner med sårbar programvare funnet i kartleggingen, med mål om å ta kontroll over disse maskinene.
- Få tilgang til databaser og brukersystemer med data om pasienter ved å utnytte brukerkontoer vi har fått kontroll over.
- Få tilgang til en brukerkonto med utvidede rettigheter ved å knekke passordet til kontoen.
- På bakgrunn av kontroll over en brukerkonto med utvidede rettigheter, brukes denne til å identifisere og angripe ytterligere brukerkontoer for å få høyere og flere rettigheter inntil det oppnås tilnærmet full kontroll over infrastrukturen.

[redacted]

Simulering av dataangrep skulle også teste helseregionens evne til å oppdage aktiviteter i dataangrep. Av denne grunn har det i varierende grad blitt gjort forsøk på å skjule angrepene. I angrepssimuleringen har vi bevisst enkelte ganger produsert mye nettverkstrafikk og inkludert kjente tegn på angrep. Dette er  signaler som kan oppdages i helseregionenes overvåkning. Vi ba om å bli orientert når helseregionene oppdaget aktiviteter i angrepssimuleringen, men henstilte om at helseregionene ikke grep inn. Dette følger av at formålet med disse kontrollene var å teste helseregionenes evne til å oppdage aktiviteter i et angrep, ikke responsevne og håndtering av sikkerhetshendelser.

Vår kontroll av tekniske sikkerhetstiltak har tatt utgangspunkt i IKT-infrastrukturen i helseregionene (nettverk, katalogtjenester, servere, klienter mv.). Denne infrastrukturen understøtter blant annet

[28] [redacted]

medisinske systemer og andre fagsystemer. Som en del av undersøkelsen, er det forsøkt vist hvilke muligheter for tilgang til medisinske data som oppnås ved et angrep mot IKT-infrastrukturen. Undersøkelsen omfatter imidlertid ikke enkeltsystemer og utstyrs tilgangskontroller, sikker konfigurasjon, sikkerhetsoppdatering mv.

Innhenting av dokumentasjon av IKT-infrastrukturen i regionene ga oss en fordel i angrepssimuleringen ved at vi hadde en grunnleggende forståelse av IKT-infrastrukturen og implementerte sikkerhetstiltak. Den har imidlertid hatt begrenset betydning for å målrette angrep. Informasjonen gir en fordel som en ekstern «hacker» ikke ville hatt, men en profesjonell «hacker» ville på den annen side antagelig tatt seg bedre tid til å kartlegge infrastrukturen på egenhånd.

[redacted]

**Analyse av uttrekk av data fra systemer**

Ved hjelp av IKT-leverandørene i helseregionene er det hentet ut uttrekk fra diverse systemer for analyse med formål om å få en mer komplett oversikt over tekniske sikkerhetstiltak. I tillegg har vi selv hentet ut data ved å utnytte sikkerhetshull hos IKT-leverandørene/helseforetakene. Det er hentet ut uttrekk som viser:

- Data om konfigurasjon[29] av maskiner og programvare. Dette har blitt innhentet for å kunne vurdere om disse er sikret (herdet) slik at angripere ikke enkelt kan finne svakheter. [redacted]. Det har også i denne forbindelse blitt hentet ut oversikter over hva som logges på disse systemene for å kunne vurdere helseregionens grunnlag for å kunne oppdage dataangrep.
- Alle brukeridentiteter og deres rettigheter. Dette har blitt innhentet for blant annet å vurdere om brukerrettigheter er avgrenset til tjenstlig behov. Fokus har vært på brukeridentiteter med utvidede rettigheter som kan styre hele eller deler av IKT-infrastrukturen
- Data om enheter i helseregionens nettverk og muligheter til å kommunisere med disse. Skanning av nettverk er benyttet som et grunnlag for denne kontrollen. [redacted].
- Oversikter over programvare installert på servere og klienter. Dette har blitt innhentet for å kunne vurdere tiltak for kontroll med programvare i helseregionene, samt sikkerhetsoppdatering av programvare.

[redacted]

Som et grunnlag for kontrollen av tekniske sikkerhetstiltak ble det innhentet dokumentasjon av helseregionenes IKT-infrastruktur, jf. punkt 2.1. Dette bidro til å gi et bredere bilde av helseregionenes sikkerhetstiltak i undersøkelsen og er således et viktig supplement for evaluering av sikkerhetstiltakene i undersøkelsen.

Systemene i helseregionene er i stor grad satt opp på samme plattform i hele regionen, driftes av en felles IKT-leverandør og det er sentrale datasentre i hver enkelt region. Ved analyse av datauttrekk er det i all hovedsak hentet ut data for hele regionen. På dette grunnlag gir revisjonen av de fleste tekniske sikkerhetstiltak grunnlag for å vurdere hele helseregionen. [redacted]. Enkelte tester vil være spesifikke for utvalgte sykehus. Dette gjelder:

[29] Konfigurasjon er en samlebetegnelse for alle innstillinger som er gjort ved oppsett av en datamaskin (eller annet utstyr) og programvare som kjører på den.

- [redacted].
- Kontroll av om standard passord er endret på utstyr benyttet av et sykehus.
- [redacted].

**Vurdering mot beste praksis**

Resultater av analyser av uttrekk og angrepssimulering er samlet vurdert opp mot beste praksis for sikkerhetstiltak. Revisjonen er avgrenset til kontroll av seks sikkerhetstiltak, jf. omtale av kriterier i punkt 3.1.2. Disse tiltakene er valgt ut fordi disse anses som sentrale for å beskytte virksomheters IKT-systemer mot sikkerhetstrusler. Tiltakene samsvarer i stor grad med de som Center for Internet Security anser som basiskontroller[30], og med tiltak som Nasjonal sikkerhetsmyndighet (NSM )mener er mest effektive for å stoppe dataangrep.[31] På denne bakgrunn er det lagt til grunn at disse sikkerhetstiltakene vil være viktig for alle helseregioner. NSM legger til grunn at det vil variere hvilke anbefalinger som er relevante, men at for store virksomheter vil de fleste anbefalinger i NSM Grunnprinsipper for IKT-sikkerhet være relevante.[32]

Helsevirksomheter skal vurdere sikkerhetstiltak opp mot virksomhetens egenart, herunder forholdsmessighet mellom risiko og tiltakets kostnad.[33] Selv om alle de tekniske sikkerhetstiltakene vi har evaluert i denne undersøkelsen er relevante for alle helseregioner, må den enkelte region vurdere risiko og kostnader ved ulike måter å implementere sikkerhetstiltakene. I undersøkelsen er etterlevelsen av tekniske sikkerhetstiltak evaluert opp mot en fargeskala, fra grønn (sikkerhetstiltak er etablert og fungerer etter sin hensikt) til rød (sikkerhetstiltak er i liten grad implementert eller fungerer ikke etter sin hensikt), jf. punkt 5.1.1. Gitt at helseregionene skal prioritere sikkerhetstiltak, er det i undersøkelsen ikke lagt til grunn at alle helseregioner kan eller bør oppnå «grønn» for alle sikkerhetstiltak. Siden de utvalgte sikkerhetstiltak vi har evaluert er ansett grunnleggende i fagmiljø for IKT-sikkerhet, er det imidlertid lagt til grunn at helseregionene bør ha disse tiltakene på plass i rimelig grad.

Det er umiddelbart etter avslutning av tekniske kontroller gjennomført sluttmøter med den enkelte IKT-leverandør og sykehus som har vært gjenstand for teknisk kontroll. Her har alle resultater fra undersøkelsen blitt presentert. Grunnlagsmateriale for resultatene har blitt overlevert IKT-leverandørene og sykehusene, i form av presentasjoner og dokumentasjon som viser de enkelte avvik funnet ved analyser. Formålet er å gi mulighet for umiddelbart å starte opprettingsarbeidet knyttet til de sikkerhetshull og sårbarheter som er funnet. I tillegg er det avholdt sluttmøte med det regionale helseforetaket for å informere om resultatene fra de tekniske kontrollene etter avsluttet kontroll i de ulike helseregionene.

## 2.5 Phishingtest og observasjoner

For å undersøke sykehusansattes tilbøyelighet til å klikke på lenker i mistenkelig e-post og å laste ned filer er det gjennomført phishing-tester i de utvalgte helseforetakene.[34] Tilbøyeligheten til å klikke er betraktet som en indikasjon på sikkerhetskultur ettersom blant annet kunnskap og bevissthet om e-post som angrepsmetode vil kunne redusere antallet som klikker. Testen omfattet ikke kontroll av tekniske tiltak som kan bidra til å stoppe slike e-poster før de kommer fram til de ansatte, eller hindrer at enkelte typer filer lastes ned.

I phishingtesten ble en falsk e-post, sendt ut til et tilfeldig utvalg ansatte. To ulike historier ble brukt. For å unngå å samle inn sensitiv informasjon, ble det ikke spurt om opplysninger som brukernavn og passord, fødselsnummer mv. i e-posten. For hvert sykehus ble 450 mottakere valgt tilfeldig.[35]

[30] CIS Controls v. 7.1 inneholder 20 kontroller, hvor seks er klassifisert som «Basic».
[31] NSM: Sjekkliste: Fire effektive tiltak mot dataangrep.
[32] NSM: Grunnprinsipper for IKT-sikkerhet, v2.0, side 3.
[33] Jf. Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren,v6.0, punkt 3.1.
[34] [redacted]
[35] Ved ett sykehus ble det sendt til 475 personer

Utvalgskriteriene var at de er tilknyttet sykehuset/helseforetaket, er gyldige brukere og har en personlig e-postadress, samt tilhører en avdeling som benytter e-post jevnlig. Antall mottakere er tilstrekkelig for å kunne trekke slutninger med 95 % konfidensnivå og feilmargin på +/- 5 prosent.

[redacted] Da kunne vi blant annet:

[redacted]

I undersøkelsen ble kun de som responderte på den falske e-posten innen ett døgn etter utsendelse inkludert i resultatet. Ansatte som leste og responderte på e-posten etter ett døgn, ble ikke tatt med i resultatet.

## 2.6 Analyse av avviksmeldinger

Det er innhentet et utvalg på 20 konkrete saker fra hvert av de fem helseforetakene for å undersøke hva slags informasjonssikkerhetshendelser som meldes og hvordan avvik rapporteres, behandles og følges opp i helseforetakene. Meldingene er i hovedsak fra 2019.[36] Det er gjort en nærmere analyse av hva slags informasjonssikkerhetshendelser som meldes. Det er deretter gjennomført intervju med ledelsen og ansatte med særskilt ansvar for avviksoppfølging for å få utdypende forståelse for hvordan avvikene følges opp.

[36] Noen avviksmeldinger fra 2018 fordi avviksmeldingene fra helseforetakene i Helse Sør-Øst ble innhentet tidlig på året i 2019

# 3 Revisjonskriterier

## 3.1 Krav til informasjonssikkerhet i helseforetakene

Både *lov om helseregistre og behandling av helseopplysninger* (helseregisterloven), *lov om helsepersonell mv.* (helsepersonelloven) og *lov om behandling av helseopplysninger ved ytelse av helsehjelp* (pasientjournalloven) stiller krav til helseforetakenes håndtering av helseopplysninger. Helseopplysninger skal behandles i samsvar med prinsippene i personvernforordningen, og på en måte som sikrer informasjonens *integritet*, *tilgjengelighet* og *konfidensialitet*.[37] Lovverket stiller krav til at relevante og nødvendige helseopplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell, samtidig som opplysningene vernes mot innsyn fra uvedkommende. Helseopplysningene skal videre behandles på en måte som sikrer pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning.[38]

I Meld. St. 7 (2019–2020) *Nasjonal helse- og sykehusplan*[39] framkommer det at målbildet for pasientbehandlingen forutsetter at informasjonen om pasientene behandles på en trygg og sikker måte. Pasienter og innbyggere skal ha tillit til at opplysninger ikke kommer på avveie og at uvedkommende ikke får tilgang. Helsepersonell som trenger informasjonen må få tilgang til den raskt og enkelt, og de må ha tillit til at opplysningene er korrekte, oppdaterte og fullstendige.

I henhold til helseregisterloven og pasientjournalloven er *dataansvarlig* den som er ansvarlig for behandling av helseopplysninger etter personvernforordningen artikkel 4 nr 7. *Databehandler* er den som behandler helseopplysninger på vegne av foretaket. Innenfor rammen av taushetsplikten skal dataansvarlig sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig.[40]

I Innst. 186 S (2015–2016)[41] understreket komiteen at informasjonssikkerhet og personvern innen helsesektoren må tas på det største alvor hos alle som er involvert i ulike prosesser i helsevesenet. Komiteen delte Riksrevisjonens oppfatning av at manglende risikovurderinger, retningslinjer, rutiner, samt uklare ansvarslinjer kan føre til at det ikke foretas noen vurdering av sensitiviteten i informasjonen som ligger i medisinsk-teknisk utstyr, og at det dermed blir vanskelig å få en klar oversikt over trusselbildet og eventuelle tiltak.

Det skal gjennomføres tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal sørge for tilgangsstyring, logging og etterfølgende kontroll.[42]

I foretaksmøter med de regionale helseforetakene har Helse- og omsorgsdepartementet i perioden etter 2015 stilt en rekke krav som berører informasjonssikkerhet:

- 2015
    - sørge for effektiv overvåking og forvaltning av IKT-systemer og nødvendig infrastruktur.
    - bidra i det nasjonale arbeidet med informasjonssikkerhet.
    - lukke avvikene fra Riksrevisjonens tidligere undersøkelser på informasjonssikkerhetsområdet[43].
- 2016

[37] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, versjon 6.0, vedtatt 04.02.2020.
[38] Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)§ 1 og Lov om Helseregistre § 1
[39] Jf Innst 255 S (2019-2020) *Innstilling fra Helse- og omsorgskomiteen om Nasjonal helse- og sykehusplan 2020-2023.*
[40] Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) § 19
[41] Jf Dokument 3:2 (2015–2016) Riksrevisjonens undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr.
[42] Helseregisterloven §§ 21-22 og Pasientjournalloven §§ 22-23.
[43] Dokument 3:2 (2014–2015) Riksrevisjonens undersøkelse av styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler i fire helseforetak.

- etablere systemer og rutiner som sikrer oppfølging og lukking av avvikene påpekt i Riksrevisjonens rapport om helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr[44].
- i samarbeid 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.

- 2017
  - sørge for tilfredsstillende informasjonssikkerhet med utgangspunkt i vurdering av risiko og sårbarhet, og oppfølging gjennom internkontroll.

- 2018
  - befolkningen skal ha tillit til at helsetjenesten håndterer personopplysninger på en trygg og sikker måte. Dette stiller krav til både teknologi, prosesser og mennesker.
  - virksomhetenes ledelse har ansvar for å etablere og opprettholde tilfredsstillende informasjonssikkerhet.

- 2019
  - prioritere ivaretakelse av informasjonssikkerhet og personvern gjennom oppfølging av krav til teknologi, prosesser og kultur. Det er viktig å bygge på tidligere erfaringer når det gjelder IKT-sikkerhet og personvern.

Eiere og ledere i helsetjenesten har et generelt ansvar for at tjenestenes drift gjennomføres innen lovfastsatte rammer, herunder legge til rette for at personell som utfører tjenestene blir i stand til å overholde sine lovpålagte plikter.

### 3.1.1 Krav til sikkerhetskultur

I Meld. St. 7 (2019–2020) *Nasjonal helse- og sykehusplan*[45] går det fram at virksomheter i helsetjenesten må utvikle en god sikkerhetskultur, gjennomføre verdi- og skadevurderinger og implementere nødvendige sikkerhetstiltak. Betydningen av å arbeide med kulturutvikling som bidrag til å styrke IKT-sikkerhet er også reflektert i standarden *ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet*[46] og *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren* (Normen)[47].

Å lede arbeidet med sikkerhetskulturutvikling er en lederoppgave. Det er av stor betydning at toppledelsen er involvert og har forståelse for behovet for å bygge en sikkerhetskultur mot dataangrep.[48] I innstillingen til Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn – Samfunnssikkerhet* uttaler komiteen blant annet på at det er et lederansvar å lage egnede rammebetingelser og utøve gode holdninger i det daglige.[49]

Lederansvaret for å sikre at virksomheten følger krav til informasjonssikkerhet skal ivaretas som en del av arbeidet med virksomhetsstyring og kvalitetsforbedring. Kulturbygging i helseforetakene skal foregå systematisk og i tråd med anbefalinger fra nasjonale sikkerhetsmyndigheter.[50]

Av *Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgssektoren* går det fram at ledelsen skal sørge for at medarbeidere i virksomheten har nødvendig kunnskap om og kompetanse i det aktuelle fagfeltet, relevant regelverk, retningslinjer, veiledere og styringssystemet.[51] Normen setter

[44] Dokument 3:2 (2015–2016) Riksrevisjonens undersøkelse av helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr.
[45] Jf. Innst. 255 S (2019–2020) *Innstilling fra Helse- og omsorgskomiteen om Nasjonal helse- og sykehusplan 2020–2023*.
[46] Punkt 7. https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001
[47] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren – Versjon 6.0. Her legges det til grunn et krav om at helsesektoren i tillegg til teknologi og organisasjon må bygge og forvalte robust sikkerhetskultur.
[48] European Union Agency For Cyber Security, *Cyber Security Culture in organisations* – November 2017. www.enisa.europa.eu.
[49] Innst. 326 S (2016–2017) *Innstilling fra justiskomiteen om Risiko i et trygt samfunn – Samfunnssikkerhet*.
[50] Meld. St. 7 (2019–2020) *Nasjonal helse- og sykehusplan 2020–2023*, kap 8.4.2.
[51] Forskrift om ledelse og kvalitetsforbedring § 7b).

krav til at kompetansebyggingen skal være kontinuerlig og tilpasset ulike roller og brukergrupper, og at det bør følges opp at opplæringstiltakene gir ønsket effekt.

### 3.1.2 Krav til tekniske sikkerhetstiltak

Tekniske sikkerhetstiltak vurderes opp mot beste praksis for hvilke tiltak som bør iverksettes og hvordan disse er implementert. For å konkretisere anbefalinger til helseforetakene om beste praksis for å oppnå et egnet sikkerhetsnivå, er Nasjonal sikkerhetsmyndighets (NSM) *Grunnprinsipper for IKT-sikkerhet* og anbefalinger for grunnleggende IKT-sikkerhet utarbeidet av The Center for Internet Security («CIS Controls») anvendt.[52]

I foretaksmøtet for Norsk Helsenett i 2018 la Helse- og omsorgsdepartementet til grunn at statsforetaket følger råd og veiledning om informasjonssikkerhetsarbeidet i sektoren fra NSM, herunder NSMs Grunnprinsipper for IKT-sikkerhet og Helhetlig IKT-risikobilde 2017.[53] I foretaksmøtet i 2020 stilte departementet krav om at de regionale helseforetakene arbeider systematisk med innføring av NSMS grunnprinsipper for IKT-sikkerhet.[54]

«CIS Controls» er en prioritert oversikt over tiltak som angir beste praksis for å hindre vanlige dataangrep. Anbefalingene er utarbeidet i samspill med eksperter i både offentlig og privat sektor, og er internasjonalt anerkjent. Det er stor grad av samsvar mellom anbefalingene i «CIS Controls» og anbefalingene fra NSM. Begge anbefalingene har som formål å hjelpe virksomheter å få på plass fundamentale prinsipper og tiltak for sikring av IKT-systemer.

Anbefalingene fra NSM og CIS legger vekt på at virksomhetene har oversikt over det som skal beskyttes mot dataangrep, altså IKT-infrastruktur og -systemer. Deretter bør hensiktsmessige tiltak for å sikre infrastruktur og systemer settes i verk, og det bør etableres systemer for å oppdage og håndtere hendelser som dataangrep. I denne revisjonen er det ut fra disse kildene valgt å kontrollere følgende sikkerhetstiltak opp mot beste praksis som angitt av NSM og CIS:

1. Oversikt og kontroll over utstyr[55] som er koblet til foretakets nettverk og hvilken programvare som kjører på denne. Formålet er å unngå at uautoriserte enheter og programvare benyttes som utgangspunkt for dataangrep, samt hindre at svakere beskyttede uautoriserte enheter kan utnyttes som en vei inn for et dataangrep.
2. Kontroll med bruker- og servicekontoer (brukerkontoer som benyttes av programvare) og hvilke tilgangsrettigheter disse er tildelt. Formålet er å hindre angripere i å få tilgang til, eller øke tilgangen til, helseforetakenes IKT-infrastruktur.
3. Sikker konfigurasjon[56] av maskiner og programvare. Formålet er å gi angripere få muligheter til å utnytte svakheter i IKT-infrastruktur.
4. Kontinuerlig sårbarhetsstyring gjennom oppdatering av programvare, skanning av nettverk for å avdekke sårbarheter og oppfølging av disse. Formålet er å hindre at kjente sårbarheter i programvare gir angripere mulighet til å få tilgang til og kontroll over utstyr og programvare i helseforetakene.
5. Inndeling av helseforetakets infrastruktur i soner ut fra hvor sensitive systemene er for virksomheten, og begrense datatrafikk mellom sonene til det som er nødvendig for driften av sykehusene. Formålet er å hindre en angriper tilgang til sensitive deler av helseforetakenes systemer og data selv om de har fått et fotfeste på en maskin.
6. Logging og overvåking - Innsamling, forvaltning og analyse av data fra nettverk og enheter. Formålet er å kunne oppdage, forstå og legge grunnlag for å kunne håndtere angrep.

Utover nevnte kriterier er det i noen tilfeller nødvendig med mer detaljerte kriterier som grunnlag for vurderinger av beste praksis. Det gjelder for eksempel vurdering av hvilke innstillinger som bør vurderes for sikker konfigurasjon av et system eller hvilke hendelser som bør logges. I slike tilfeller er

[52] The Center for Internet Security, CIS Controls.
[53] Foretaksmøte i Norsk Helsenett SF 17. januar 2018.
[54] Foretaksmøter i de regionale helseforetakene 14. januar 2020.
[55] Dette inkluderer både IKT-utstyr, medisinsk teknisk utstyr, bygningsteknisk utstyr og andre enheter.
[56] Sikker konfigurasjon: En samling av innstillinger i et IKT-system som er tilpasset på en slik måte at de gir økt motstandsdyktighet mot dataangrep. For eksempel å fjerne unødvendig funksjonalitet og utdaterte teknologier fra en server for å minske dens angrepsflate.

anbefalinger fra Center for Internet Security eller anbefalinger fra leverandører brukt for å få en mer detaljert framstilling av beste praksis.

## 3.2 Krav om systemer for styring og kontroll

*Lov om helseforetak m.m.* (helseforetaksloven) § 28 omhandler styrets oppgaver. I merknadene til § 28 framgår det at styret i et helseforetak skal sørge for at det etableres interne kontrollsystemer som sikrer at det er betryggende kontroll med foretakets måloppnåelse, økonomi og ressursbruk.[57] God styring og oppfølging innebærer at helseforetakene skal ha en internkontroll som bidrar til at de oppnår fastsatte mål og resultatkrav. Internkontrollen skal bidra til at ressursbruken er effektiv, at virksomheten drives i samsvar med lover og regler, og at virksomheten har tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag.

Ved opprettelsen av foretaksmodellen i 2002 var det en grunnleggende tanke at de regionale helseforetakene skulle foreta samordnende grep på tvers der det var behov for det, inkludert for standardisering av IKT-systemer. Av helseforetaksloven fremgår det at de regionale helseforetakene skal samarbeide med andre når dette er egnet til å fremme foretakets oppgaver og målsettinger.[58] I forarbeidene til helseforetaksloven understrekes det at helseforetakene skal ha stor frihet til å disponere sine ressurser, men at de ikke må tillates å bli så autonome at hensyn til helheten og fellesskapet blir skadelidende.[59]

*Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten* pålegger virksomhetene å ha et styringssystem. Styringssystem defineres som den del av virksomhetens styring som omfatter hvordan virksomhetens aktiviteter planlegges, gjennomføres, evalueres og korrigeres i samsvar med krav fastsatt i eller i medhold av helse- og omsorgslovgivningen.[60] Forskriften utdyper videre hva kravene til å planlegge, evaluere og korrigere aktivitetene innebærer.

I forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 legges det vekt på at det skal etableres en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Omfang og innretning skal være tilpasset risiko.

I helseforetakene er det administrerende direktør som har det overordnede ansvaret for styringssystemet, hvor styringssystemet for informasjonssikkerhet inngår. Styrene i helseforetakene og RHF-ene skal følge aktivt med på om helseforetakene har et forsvarlig styringssystem gjennom sin kontrollfunksjon etter helseforetaksloven. Styrene må også sørge for å være informert hvorvidt helse- og omsorgslovgivningen overholdes, om tjenestene er forsvarlige, og om det arbeides systematisk med kvalitetsforbedring og pasientsikkerhet. Styret plikter å gripe inn i tilfeller der foretaket ikke korrigerer ulovlig og uforsvarlig virksomhet.[61]

Helseforetakene skal sørge for at virksomheten arbeider systematisk for kvalitetsforbedring og pasientsikkerhet.[62] Det er et sentralt element i helseforetakenes systematiske arbeid med pasientsikkerhet at de har systemer for å registrere avvik.[63] Et informasjonssikkerhetsavvik kan også true pasientsikkerheten og må også meldes i avvikssystemet. Systemer og rutiner for avvikshåndtering er en viktig del av helseforetakenes internkontroll. De har plikt til å evaluere og gjennomgå avvik, herunder uønskede hendelser, slik at lignende forhold kan forebygges.[64]

[57] Ot.prp. nr. 66 (2000–2001) *Om lov om helseforetak m.m.*, s. 212.
[58] Helseforetaksloven § 41.
[59] Ot.prp. nr. 66 (2000–2001) *Om lov om helseforetak m.m.*, s. 35.
[60] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 4.
[61] Veileder til forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten. IS-2620 (2017).
[62] *Lov om spesialisthelsetjenesten m.m* (spesialisthelsetjenesteloven) § 3-4 a.
[63] Prop. 91 L (2010–2011) *Lov om kommunale helse- og omsorgstjenester m.m.* (helse- og omsorgstjenesteloven) kap. 21.3.5.2.
[64] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 8 e).

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten utdyper krav til styringssysstem for informasjonssikkerhet, herunder at virksomhetens øverste leder skal gjøre styringssystemet kjent i virksomheten.[65] Formålet med styringssystemet er å:

- sikre at arbeidet med informasjonssikkerhet ivaretas på en systematisk måte
- dokumentere ledelsens krav til informasjonssikkerhet, rutiner som ansatte og medarbeidere skal følge for å nå virksomhetens krav og kontrollmekanismer som skal benyttes for å kontrollere at kravene blir oppnådd
- være grunnlag for at nødvendige sikkerhetstiltak etableres i virksomheten ift relevante trusler som kan påvirke behandlingen av helse- og personopplysninger
- gi dataansvarlig en oversikt over relevante dokumenter i styringssystemet.[66]

Styrene for de regionale helseforetakene og helseforetakene skal minimum én gang i året ha en samlet gjennomgang av virksomheten basert på sammenlignbar statistikk om kvalitetsforbedrings- og pasientsikkerhetsarbeidet. Gjennomgangen skal bidra til å sikre at ledelsen aktivt støtter dette arbeidet, og at det gjøres sammenligninger og gjennomføres læringsoverføring både innad i og mellom sykehusene.[67]

Det er et ledelsesansvaret å håndtere risiko på en helhetlig måte og på bakgrunn av dette gjennomføre tilstrekkelige tiltak, styring og kontroll.[68]

## 3.3 Krav til Helse- og omsorgsdepartementets styring og oppfølging

Helse- og omsorgsdepartementet har det overordnede ansvaret for spesialisthelsetjenesten|jf spesialisthelsetjenesteloven § 2.1. Statens overordnede ansvar innebærer at staten skal sette de regionale helseforetakene i stand til å oppfylle sine plikter til å sørge for spesialisthelsetjeneste til befolkningen innen sine helseregioner. Videre blir staten ansvarlig for å fastsette de overordnede helsepolitiske målsettingene og for gi de regionale helseforetakene rammebetingelser som gjør det mulig for dem å iverksette disse målsettingene. Statens ansvar begrenses dog ikke til å legge til rette for at de regionale helseforetakene skal kunne oppfylle sine forpliktelser. Staten har også et innholdsmessig ansvar for at de regionale helseforetakene oppfyller sine forpliktelser av juridisk og konstitusjonell karakter.

Departementet styrer de regionale helseforetakene gjennom lov, vedtekter, foretaksmøte og oppdragsdokument. Helseforetaksloven stiller krav til at departementet som eier bare skal utøve eierstyring i foretaksmøter. I foretaksmøte skal det blant annet fastsettes økonomiske og organisatoriske krav og rammer for de regionale helseforetakene. Departementet har anledning til å tildele foretak bevilgning og sette vilkår for tildelingen utenfor foretaksmøte.[69]

Departementet skal holde seg orientert om foretakenes virksomhet og om virksomheten drives i samsvar med de krav som er stilt i foretaksmøter og de vilkår som er satt for tildeling av bevilgning. Departementet skal innhente skriftlige opplysninger fra regionale helseforetak og avholde rapporteringsmøter. Rapporteringsmøter kan holdes utenom foretaksmøte.[70]

Det følger av retningslinjer[71] for oppfølging av eierinteressene i de regionale helseforetakene at Helse- og omsorgsdepartementet skal sørge for at styrene i RHFene har etablert systemer for risikostyring for å forebygge, forhindre og avdekke avvik. Hovedelementene i retningslinjene er at det må stilles krav til målrettet, hensiktsmessig og effektiv drift, pålitelig intern og ekstern rapportering og overholdelse av gjeldende lover og regler. Styringssystemene skal tilpasses risikoen for avvik, og hvor vesentlige risikofaktorene er for virksomhetens mål.

[65] Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten, 2.3 Styringssystem.
[66] Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten - faktaark 02.
[67] Innst. 206 S (2015–2016), jf. Meld. St. 11 (2015–2016) *Nasjonal helse- og sykehusplan (2016–2019)*.
[68] Meld. St. 7 (2019–2020) *Nasjonal helse- og sykehusplan 2020–2023*, kap. 9.7.
[69] Lov om helseforetak § 16
[70] Lov om helseforetak §16a
[71] Helse og omsorgsdepartementets (2008) Retningslinjer for oppfølging av Helse- og omsorgsdepartementets eierinteresser de regionale helseforetakene

Det går fram av reglement for økonomistyring i staten (økonomireglementet) og tilhørende bestemmelser om økonomistyring i staten (økonomibestemmelsene) at Helse- og omsorgsdepartementet har det overordnede ansvaret for at de underliggende etatene gjennomfører aktiviteter i samsvar med målene i Stortingets vedtak og forutsetninger.

# 4 Simulerte dataangrep mot helseregionene

I kapittel 4 beskrives resultatene av våre simulerte dataangrep mot helseregionene. [redacted] Målet har vært å oppnå et nivå av kontroll over helseregionenes IKT-systemer som gjør det mulig å stjele, manipulere og slette sensitive helse- og personopplysninger. Det har også vært et mål å oppnå et tilgangsnivå som gjør det mulig å påvirke driften eller låse systemene og kreve løsepenger. I tillegg var det et mål å teste helseregionenes evne til å oppdage aktiviteter i de simulerte angrepene.

Angrepssimuleringen har testet om helseregionene har etablert sikkerhet i dybden for å beskytte seg mot mange ulike typer angrep. [redacted]

I dette kapitlet beskriver vi våre angrepsmetoder og resultater, mens vi i de påfølgende kapitlene beskriver svakhetene i sikkerhetstiltakene som kunne forebygget og oppdaget angrepene.

## 4.1 Sammendrag

I tre av de fire helseregionene fikk vi gjennom angrepssimuleringen høy grad av kontroll over viktige IKT-systemer, og derigjennom tilganger som kunne utnyttes til å volde stor skade.[72] Med de tilganger som ble oppnådd i disse tre helseregionenes systemer kunne en reell angriper blant annet ha:

- stjålet store mengder sensitive helse- og personopplysninger
- slettet eller utilgjengeliggjort opplysninger som er nødvendige for pasientbehandlingen
- stoppet og utilgjengeliggjort systemer og utstyr som er kritisk for driften av sykehusene
- manipulert opplysninger om pasientene

I den siste regionen fikk vi mindre grad av kontroll over IKT-systemene, men kontroll over mange av regionens PCer. Disse kan brukes for videre angrep.

De simulerte angrepene viser også at en angriper kan gjøre betydelig skade selv uten høy grad av kontroll over IKT-systemene. Våre simulerte angrep ga tilgang til store mengder sensitive opplysninger i alle helseregioner.

Angrepene ble dessuten i varierende grad oppdaget av helseregionene. En av regionene oppdaget flere av aktivitetene i angrepssimuleringen, mens de andre tre oppdaget lite eller ingenting. Dette til tross for at vi benyttet støyende metoder og gjorde få forsøk på å skjule de simulerte angrepene.

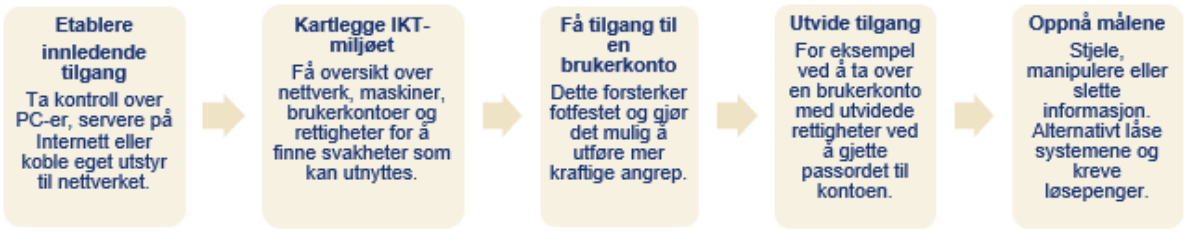
I simuleringen av dataangrep er det benyttet metoder og standardverktøy som er offentlig kjent og lett tilgjengelig på Internett. Angrepssimuleringen er gjennomført med utgangspunkt i en typisk prosess for et dataangrep hvor angripere starter utenfor IKT-systemene og gradvis må etablere et fotfeste og øke sin tilgang. [redacted]

## 4.2 Funn fra gjennomføringen av simulerte dataangrep mot helseregionene

Figur 1 gir en oversikt over og beskrivelse av fasene i de simulerte angrepene mot helseregionene. I kapittel 4.2.1 - 4.2.5 beskrives resultatene fra de enkelte fasene.

[72] Se punkt 4.2.5 for nærmere beskrivelse om forskjellene på hvilket nivå av kontroll som ble oppnådd over helseregionenes IKT-systemer.

## Figur 1 Faser i et dataangrep



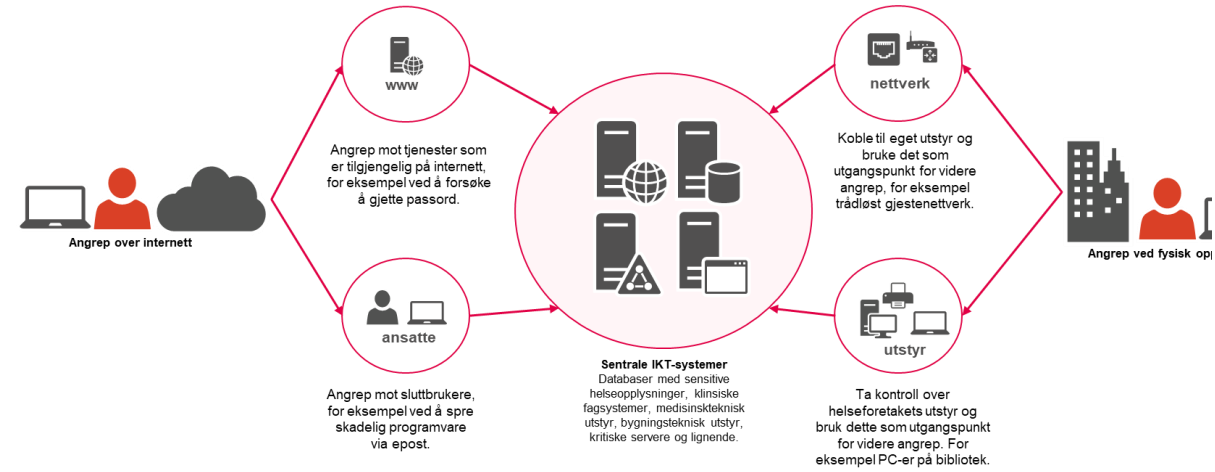

Figur 1 viser typiske faser i et dataangrep fra det etableres en innledende tilgang til nettverket for så å kartlegge IKT-miljøet, skaffe seg større tilganger for til slutt å oppnå målet med angrepet. Kilde: figuren er en forenklet utgave av NSMs figur «Sårbarheter som utnyttes i et dataangrep», NSM Risiko 2017 side 28 - 29.

### 4.2.1 Etablere innledende tilgang

Mange dataangrep starter med at angripere forsøker å etablere et innledende fotfeste i virksomhetens IKT-systemer. Målet er ikke å ta full kontroll over IKT-systemene i første omgang, men å sette seg i en posisjon hvor kartlegging og videre angrep er mulig. En angriper kan forsøke å etablere innledende fotfeste på flere ulike måter, for eksempel ved å:

- koble til eget utstyr i trådløse nettverk eller fysiske nettverkskontakter i ubeskyttede områder
- utnytte sårbarheter ved oppsett av virksomhetens PC-er og ta kontroll over disse
- lure ansatte til å kjøre skadelig programvare som gir angriperen kontroll over deres PC-er
- utnytte teknologiske sårbarheter i servere som er tilgjengelig på Internett, f. eks servere for virksomhetens nettsider

## Figur 2 Ulike metoder for å etablere innledende tilgang



[redacted]

[redacted] 73

[redacted] 74 [redacted]
75 [redacted]
76 [redacted]

### 4.2.2 Kartlegge IKT-miljøet

Etter å ha etablert innledende fotfeste i nettverket vil en angriper forsøke å kartlegge IKT-miljøet. Angriperen er helt avhengig av dette for å identifisere verdifulle mål og for å finne sårbarheter som kan utnyttes til å ta kontroll over disse.

Som en del av angrepssimuleringen er det ved hjelp av vanlige verktøy gjennomført omfattende kartlegging av helseregionenes IKT-miljøer. For alle fire regioner ble det hentet ut detaljert informasjon om nettverksstruktur, tilkoblede enheter, [redacted] samt kontoer og deres tilgangsrettigheter. [redacted] Den gjennomførte kartleggingen har vært bred og dekket mange kritiske IKT-systemer, men den har ikke omfattet samtlige systemer i alle helseregioner. Gjennom kartleggingen fikk vi store mengder informasjon om følgende:

- alle kontoer (brukerkontoer, administratorkontoer og servicekontoer)[77]
- alle tilgangsrettigheter som er tildelt kontoer, inkludert kontoer som er tildelt for mange rettigheter[78]
- systemer som mangler sikkerhetsoppdateringer og derfor har kjente tekniske sårbarheter
- systemer som er sårbare grunnet feil i installasjon og drift
- eldre systemer med færre og svakere sikkerhetsmekanismer
- flere kritiske databaser, for eksempel elektronisk pasientjournal
- flere kritiske servere, for eksempel filservere med sensitive opplysninger
- kontrollpanel for teknisk utstyr (medisinsk og bygningsteknisk)

Ved hjelp av kartleggingen fant vi ut hvilke maskiner og brukerkontoer vi burde angripe for på enklest mulig måte få kontroll over viktige systemer i helseregionene.

### 4.2.3 Få tilgang til en brukerkonto

I forbindelse med etablering av innledende fotfeste og kartlegging av IKT-miljøet er det vanlig at angripere forsøker å få tilgang til en brukerkonto. I første omgang er det tilstrekkelig med en hvilken

---

[73] Konfigurasjon er en samlebetegnelse for alle innstillinger som er gjort ved oppsett av en datamaskin (eller annet utstyr) og programvare som kjører på den.
[74] [redacted]
[75] Forsøk på svindel eller manipulasjon der bakmennene ved å sende en e-post forsøker lure brukeren til å oppgi sensitive opplysninger (f.eks. passord) eller klikke på lenker som laster ned skadevare.
[76] Australian Signals Directorate, Advisory 2020-009: Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services.
[77] Dette gjelder primært katalogtjenesten Active Directory, som er en del av kjernen i helseregionenes IKT-miljøer. [redacted]
[78] For denne kartleggingen gjelder samme avgrensning som for kulepunktet ovenfor.

som helst brukerkonto – selv helt ordinære kontoer har tilgang til informasjon og funksjonalitet som angripere kan utnytte. For eksempel gir en ordinær konto tilgang til felles filområder og informasjon om øvrige kontoer og deres tilgangsrettigheter.

I angrepssimuleringen forsøkte vi å gjette navn på brukerkontoer basert på mønstre (for eksempel initialer eller [redacted]) med utgangspunkt i noen få navn vi fikk tilgang på.
[redacted]. [79]

Etter å ha utarbeidet lister over gyldige og antatt gyldige brukerkontoer forsøkte vi å gjette passordene til kontoene
[redacted]

[redacted].

### 4.2.4 Utvide tilgang

For å realisere sine endelig mål er angripere i de fleste tilfeller avhengig av å oppnå en form for kontroll over virksomhetens IKT-systemer. Dette oppnås ofte ved å utnytte tekniske sårbarheter eller ved å få tak i passordene til kontoer med utvidede tilgangsrettigheter.

Gjennomført angrepssimulering viser at det er flere muligheter for å utvide tilganger i samtlige helseregioner, og at dette kan oppnås med enkle metoder av angripere
[redacted]

En angriper vil ikke nødvendigvis oppnå tilstrekkelig kontroll kun ved å ta over én enkelt konto eller maskin. Arbeidet med å utvide tilganger var derfor ofte en gradvis og gjentagende prosess hvor vi tok kontroll over stadig flere kontoer og maskiner. Dette utnyttet ofte svakheter i flere sikkerhetstiltak, for eksempel utstyr som manglet kritiske sikkerhetsoppdateringer og kontoer med svake passord.

Ved angrepssimuleringen ble utvidelse av tilganger i hovedsak oppnådd gjennom å finne passordet til kontoer med utvidede tilgangsrettigheter, særlig ved bruk av to metoder:

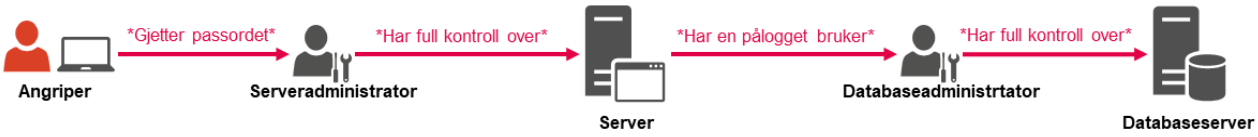
- [redacted][80] [redacted].
- [redacted]

[79] [redacted]

[80] Ved lagring og overføring av passord benyttes som regel matematiske funksjoner for å beskytte passordet. Det lages da et enveiskryptert passord (en «passordhash») At det er enveiskryptert innebærer at det ikke er mulig å finne tilbake til passordet med den matematiske funksjonen. Angripere bruker dermed rå datakraft og genererer tabeller med «passordhaser» ut fra millioner eller milliarder av mulige passord. Hvis angriperen får tak i en reell «passordhash», sammenlignes denne med alle genererte verdier.

[redacted]
[redacted].

## Figur 3 Prosess for å utvide tilgang




**Figur 3:** En angriper som først får tilgang til en konto kan ofte bruke dens begrensede rettigheter til å skaffe seg tilgang til flere kontoer med langt større tilgangsrettigheter. Hvis angriperen får kontroll over en server kan verktøy som [redacted] benyttes for å hente ut passordene til alle som har vært logget inn nylig, og så gjentas prosessen for de nye kontoene og eventuelle servere de kontrollerer. Til slutt oppnår angriper ønsket kontroll, for eksempel over en databaseserver med sensitive helseopplysninger.

### 4.2.5 Oppnå målene med angrepet

Etter å ha oppnådd et tilstrekkelig høyt tilgangsnivå kan en angriper starte arbeidet med å oppnå sine primære mål, for eksempel stjele store mengder sensitive opplysninger, manipulere informasjon eller låse IKT-systemene og kreve løsepenger.

Vår angrepssimulering resulterte i en høy grad av kontroll over IKT-systemene i Helse Midt-Norge, Helse Vest og Helse Nord. [redacted]. Med en slik tilgang kan en angriper sikre seg langvarig kontroll over IKT-infrastrukturen og volde svært omfattende skade som vil være ressurskrevende å rydde opp. Helse Sør-Øst skiller seg ut som regionen der vi oppnådde lavest grad av kontroll over systemene, men analyse av funn i etterkant av angrepssimuleringen viser muligheter som en reell angriper med lengre tidshorisont ville kunne utnyttet til å komme lenger. Angrepssimuleringen ga kontroll over mange av regionens PC-er.

Tilgangene som ble oppnådd i angrepssimuleringen kunne vært utnyttet for å volde store skader, blant annet til å ramme konfidensialiteten, integriteten og tilgjengeligheten i store mengder helse- og personopplysninger. Kontrollen over IKT-systemene som ble oppnådd gjennom angrepssimuleringen ble i liten grad utnyttet. Dette var av hensyn til pasientssikkerhet og personvern. Det ble imidlertid gjort noen handlinger for å illustrere mulighetene:

- innhentet enveiskrypterte passord til flesteparten av brukerkontoer i flere regioner [redacted]
- hentet ut helsedata fra ulike systemer og databaser for enkeltpersoner, for å illustrere at det hadde vært mulig å manipulere data om enkeltpersoner og å hente ut større mengder informasjon
- vist at vi kan få kontroll med både medisinsk-teknisk utstyr og verktøy som benyttes av IKT-leverandørene for drift av systemene ved sykehusene

For å oppnå dette benyttet vi standard angrepsmetoder og kjente verktøy som er tilgjengelig på Internett. En avansert aktør, for eksempel organiserte kriminelle eller en etterretningstjeneste, vil ha tilgang til mer avanserte og større utvalg av verktøy.

## Faktaboks 1 Eksempler på angrep på helsesektoren

Motivasjonen for å angripe helseregionenes IKT-systemer kan variere fra opportunistisk vinningskriminalitet til målrettet etterretning. Det finnes en rekke eksempler på dette internasjonalt, i tillegg til angrepet på Helse Sør-Øst i januar 2018. Presset på helsetjenestene ved Covid-19 ble sett på som en mulighet av kriminelle, til

en slik grad at Interpol i april 2020 gikk ut med en advarsel om en signifikant økning i angrep mot helseorganisasjoner.[81] Eksempler på formål med angrep:

- Kriminelle kan hente ut mengder av helseopplysninger for salg. For eksempel hentet angripere i 2017–2018 ut opplysninger om nesten 1,5 millioner pasienter i Singapore. Dette inkludert sensitive helseopplysninger om landets statsminister, som kan ha interesse for etterretningsorganisasjoner.[82]
- Kriminelle kan kryptere data som et sykehus er avhengig av i pasientbehandlingen, og deretter presse sykehuset til å betale løsepenger for å gjøre dataene tilgjengelige. I USA har det i perioden 2016-2019 vært 172 tilfeller hvor helseinstitusjoner har blitt rammet av slike angrep til en kostnad av mer enn 150 millioner dollar.[83]

Kontroll med systemer kan brukes til å skade enkeltpersoner. Israelske forskere har vist hvordan man kan skade for eksempel profilerte enkeltpersoner ved å manipulere røntgenbilder slik at spor etter lungekreft ikke lenger er synlig, med liten sannsynlighet for at helsepersonell vil oppdage at bildene er manipulert.[84]

### 4.2.6 Helseregionenes evne til å oppdage dataangrep

Det er ikke mulig å forhindre alle dataangrep kun med forebyggende sikkerhetstiltak. Derfor er det viktig at virksomheter er i stand til å oppdage angrep og respondere på en hensiktsmessig måte.

Undersøkelsen viser at tre av helseregionene har store utfordringer med å oppdage at deres IKT-systemer er under angrep. I løpet av angrepssimuleringen ble det generert mye nettverkstrafikk og benyttet kjente angrepsverktøy med standard innstillinger, noe som etterlater tydelige digitale fingeravtrykk og øker sannsynligheten for å bli oppdaget. Reelle angripere kan ta seg bedre tid og tilpasse eller utvikle angrepsverktøy, noe som vil redusere sannsynligheten for at de oppdages.

[redacted]

Flere av helseregionene samler inn loggdata som gir grunnlag for å oppdage aktivitetene, men det gjenstår fortsatt mye arbeid med å etablere et system som kan sortere og tolke loggdataene slik at sikkerhetsbrudd oppdages fortløpende.

**Faktaboks 2 Eksempler på støyende aktiviteter gjennomført i angrepssimuleringen**

[redacted]

[81] Interpol: Cybercriminals targeting critical healthcare institutions with ransomware, 4 april 2020. https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
[82] Direktoratet for e-helse, Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren, side 21.
[83] Forbes: Ransomware Damage To U.S. Healthcare Industry Passes $150 Million In Four Years, 16 februar 2020 https://www.forbes.com/sites/leemathews/2020/02/16/ransomware-damage-to-us-healthcare-industry-passes-150-million-in-four-years/
[84] Yisroel Mirsky, Tom Mahler, Ilan Shelef og Yuval Elovici: CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. Publisert for USENIX Security Symposium 2019.

- [redacted]
- [redacted][85]
- [redacted][86]
- [redacted][87]

[85] [redacted].
[86] [redacted].
[87] [redacted].

# 5 Tekniske sikkerhetstiltak

Hele kapittelet er BEGRENSET i henhold til sikkerhetsloven § 5-3 og § 5-4.

# 6 Informasjonssikkerhetsarbeidet i helseregionene

Dette kapittelet beskriver hvordan arbeidet med informasjonssikkerhet/IKT-sikkerhet styres og organiseres i helseregionene.

## 6.1 Sammendrag

Undersøkelsen viser at helseregionene har satt i verk flere forbedringstiltak for å styrke informasjonssikkerheten. Helseregionene har de siste årene arbeidet med å oppdatere eller utvikle de regionale styringssystemene for informasjonssikkerhet. Det er dedikert flere ressurser til informasjonssikkerhet, og fagmiljøene hos de regionale IKT-leverandørene er styrket. Det er også iverksatt større regionale forbedringsprosjekter for informasjonssikkerhet, og det er opprettet nye regionale fora for samhandling.

Helseregionene har likevel utfordringer med å gjennomføre forbedringstiltak. Flere av de tekniske svakhetene som er påpekt i kapittel 5, var allerede kjent. Undersøkelsen viser at noen av de sentrale utfordringene er:

- **Kompleksitet og omfang av utstyr, systemer og programvare**. Dette gjør at utbedring av kjente svakheter tar tid. Helseregionene mener også at eldre og upraktiske tekniske løsninger i noen tilfeller står i veien for god sikkerhet.
- **Manglende opprydding.** Helseregionene prioriterer innføring av nye løsninger som skal gi økt sikkerhet, uten at de gamle, usikre løsningene fases ut. Det ryddes ikke systematisk i gamle løsninger og sensitive helse- og personopplysninger. Dette kan utnyttes av angripere.
- **Uklar ansvars- og oppgavefordeling.** Det er uklarheter mellom IKT-leverandørene og helseforetakene om hvem som skal gjennomføre informasjonssikkerhetstiltak, og i noen tilfeller uenighet om oppgavefordeling.
- **Ansattes uheldige sikkerhetsatferd.** Både ansatte ved helseforetakene og IKT-personell ved de regionale IKT-leverandørene har en atferd som bidrar til å svekke IKT-sikkerheten. Informasjonssikkerhetsopplæringen i helseforetakene er ikke tilpasset den enkelte ansattes oppgaver.

Helseregionene har forbedret arbeidet med risiko- og sårbarhetsanalyser (ROS-analyser)[88] ved innføring og endring av IKT-løsninger.[89] Undersøkelsen viser imidlertid at det ikke alltid klart hvem som skal følge opp risikoen gjennom konkrete forbedringstiltak.

Styrene i helseregionene behandler i større grad enn tidligere saker som handler om informasjonssikkerhet. Samtidig viser undersøkelsen at ledere i helseregionene i varierende grad får informasjon om den reelle sikkerhetstilstanden. Et begrenset informasjonsgrunnlag kan gjøre det vanskelig for ledelsen å prioritere hvilke tiltak som er viktigst.

I henhold til personvernlovgivningen har helseforetakene det juridiske ansvaret for behandlingen av helseopplysninger overfor sine pasienter (dataansvarlig). Mange helseforetak opplever at de har for lite informasjon om sikkerhetstilstanden i IKT-systemene/infrastrukturen der opplysningene behandles. Imidlertid har helseforetakene i liten grad foretatt kontroller eller revisjoner for å øke kunnskapen om sikkerhetstilstanden.

De regionale helseforetakene har stilt få egne krav til helseforetak knyttet til informasjonssikkerhet, men har i stor grad videreformidlet kravene som departementet har stilt i foretaksmøter. Regionenes samordning av arbeidet med informasjonssikkerhet varierer og det er få samarbeidsfora på tvers av

[88] Risiko- og sårbarhetsanalyser skal beskrive sannsynlighet for at uønskede hendelser oppstår som følger av innføring eller endring av en løsning, mulige konsekvenser dersom disse hendelsene oppstår, og tiltak for å redusere denne risikoen. Analysene omfatter ikke bare den tekniske sikkerheten, men også de tilhørende prosessene. Det kan dreie seg om krav til passord, pålogging, tilganger og lagring av opplysninger.
[89] Helse Midt-Norge: Risikovurdering av IT-sikkerhet. Helse Sør-Øst: Risikovurdering ved nye og endrede IKT-løsninger og databehandlinger. Helse Nord: «Risikovurdering og risikostyring». Helse Vest IKT HF M05 - Plan for risikovurdering der det anbefales at ROS-analysene oppdateres hvert tredje år.

regionene. Det felleseide selskapet Sykehusinnkjøp HF benyttes i liten grad til samordning for å sikre at det stilles samme informasjonssikkerhetskrav til like systemløsninger.

## 6.2 Helseregionene har arbeidet med sikkerhetsorganisering og -styring

### 6.2.1 Tre av regionene har utviklet regionale styringssystemer for informasjonssikkerhet

Et styringssystem for informasjonssikkerhet fungerer som et rammeverk for styring/ledelse og sikkerhetsorganisering i den enkelte virksomhet. Istedenfor å la det være opp til den enkelte virksomhet å utarbeide sitt eget styringssystem for informasjonssikkerhet, har helseregionene valgt å utarbeide styringssystemer for foretaksgruppene som helhet.

Helse Sør-Øst, Helse Vest og Helse Nord har utviklet styringssystemer som skal gjelde både for RHFet, helseforetakene og de regionale IKT-leverandørene i sine respektive regioner.[90] Helse Midt-Norge hadde ikke utarbeidet tilsvarende styringssystem på kontrolltidspunktet, men har besluttet at dette skal gjøres og er i gang med arbeidet.[91]

I Helse Sør-Øst, Helse Vest og Helse Nord består styringssystemene av overordnede dokumenter som tar for seg regionale sikkerhetsmål og -strategi, organisering og ansvarsforhold mv. i virksomhetene, skriftlige retningslinjer med krav til informasjonssikkerhet, og operative rutiner/prosedyrer for hvordan disse skal etterleves i praksis.[92] Retningslinjene og rutinene dekker bl.a.:

- krav til bruken av informasjonssystemene
- krav til tekniske sikkerhetstiltak,
- krav til opplæring av de ansatte
- krav til avviksrapportering og avviksbehandling
- krav til handlinger som skal sikre at man velger de riktige sikkerhetstiltakene og kontinuerlig og forbedrer informasjonssikkerheten (f. eks. krav til risikovurderinger, sikkerhetsrevisjoner, ledelsens gjennomgang).

De viktigste kravene er sammenfattet i en sikkerhetsinstruks, som alle ledere og medarbeidere forventes å kjenne innholdet i.

Helse Midt-Norge har i mindre grad hatt felles dokumenter som beskriver hvordan informasjonssikkerheten skal ivaretas, men de har overordnede dokumenter som omtaler regionens IKT-sikkerhetsmål/policy og plan for teknisk sikkerhet,[93] og tilhørende retningslinjer med krav til tekniske sikkerhetstiltak for regional IKT-leverandør Helse Midt-Norge IKT (Hemit).[94] Regionen har også en felles sikkerhetsinstruks («brukerhåndbok»). For øvrig har foretakene i regionen en del lokale rutiner og retningslinjer. Ved helseforetaket som ble valgt ut til nærmere undersøkelser i denne regionen, uttalte ledelsen at de har fått tilbakemeldinger om at det lokale styringssystemet er fragmentert; det er mange detaljerte, enkeltstående prosedyrer, og vanskelig for ansatte å vite hvilke prosedyrer som gjelder for situasjonen de er i.[95]

---

[90] I tillegg til foretaksgruppen har Helse Vest RHF avtaler med syv private leverandører vedrørende kjøp av helsetjenester. Disse syv virksomhetene inngår i et samarbeid knyttet til det regionale styringssystemet for informasjonssikkerhet og personvern.

[91] Årlig melding 2019 for St. Olavs Hospital HF, side 25.

[92] Styringssystemene til Helse Vest og Helse Sør-Øst er strukturert i tråd med forslag i Norm for informasjonssikkerhet og personvern, med en styrende (mål, strategi, organisering og ansvarsforhold mv.), gjennomførende (retningslinjer og rutiner som skal sikre etterlevelse av krav) og kontrollerende del (retningslinjer og rutiner for kontroll av kravene for informasjonssikkerhet). Det legges opp til at det skal utvikles mer detaljerte operative rutiner/prosedyrer i den enkelte virksomhet. Helse Nord har nettopp gjennomført en større revisjon av sitt styringssystem, og omstrukturert dette etter ISO/IEC 27001. Det er delt inn i fire nivåer: 1) Sikkerhetsmål, sikkerhetsstrategi og ansvarsfordeling, 2) regionale krav til informasjonssikkerhet delt inn etter 24 sikkerhetsområder, 3) regionale retningslinjer og prosedyrer, 4) virksomhetsinterne/lokale operative retningslinjer og prosedyrer.

[93] Overordnet IKT-policy for Helse Midt-Norge 2016-2018 (ikke oppdatert etter 2018), Sikkerhetsplan (SP) Helse Midt-Norge- ID NR 2657. Disse bygger også på *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren*.

[94] Helse Midt-Norge har oversendt retningslinjer for 1) sikkerhetsarkitektur, 2) informasjonsflyt mellom soner, 3) etablering og endring av tjenester, 4) passordpolitikk, 5) bruk av skytjenester, 6) herding av servere, 7) herding av nettverkskomponenter, 8) herding av klienter, 9) delegeringsmodell for admin-brukere.

[95] [redacted]

Målene som defineres i de regionale styringssystemene er overordnede, og dreier seg i stor grad om å innfri krav i personvernlovgivningen og helselovgivningen, samt i *Norm for informasjonssikkerhet og personvern i Helse- og omsorgssektoren* (Normen). I alle regioner er det også et mål at informasjonen som behandles skal være tilgjengelig for helsepersonell ved behov (tilgjengelighet), og ikke kan endres utilsiktet eller av uvedkommende (integritet). Strategiene som er utarbeidet, beskriver overordnede tiltak og krav.[96] Det finnes eksempler på at strategier er konkretisert i handlingsplaner, som Helse Nords *Handlingsplan Informasjonssikkerhet 2017-2022*.[97]

Alle regionene har retningslinjer med overordnede krav til tekniske sikkerhetstiltak som i stor grad dekker de seks områdene som er gjennomgått i kapittel 5.[98] Undersøkelsen viser dermed at svakhetene som er avdekket, også bryter med helseregionenes interne retningslinjer.[99]

Helse Sør-Øst RHF, Helse Vest RHF og Helse Nord RHF gir alle uttrykk for at det gjenstår arbeid med å implementere de nye styringssystemene i virksomhetene i helseregionene.[100] Det innebærer blant annet å integrere styringssystemet for informasjonssikkerhet tettere i virksomhetenes helhetlige kvalitetssystemer.[101]

## Faktaboks 3 Organisering av informasjonssikkerhetsarbeidet i virksomhetene

Alle de fire regionene har dokumenter som beskriver ansvars- og oppgavefordelingen innad i virksomhetene. Helseforetakene og regional IKT-leverandør i Helse Midt-Norge har hatt egne dokumenter som har beskrevet dette.

- Det slås fast at administrerende direktør har det overordnede ansvaret for informasjonssikkerheten gjennom sin rolle som dataansvarlig for behandling av personopplysninger.
- Ledere (klinikksjefer, avdelingsledere, enhetsledere), informasjonssikkerhetsledere/-rådgivere, dataansvarlige/systemeiere og personvernombud har særskilte oppgaver og ansvar.
- Det understrekes at alle medarbeidere har et ansvar for å gjøre seg kjent med sikkerhetsinstruks, følge reglene for informasjonssikkerhet, og for å melde ifra om avvik.[102]

I Helse Sør-Øst, Helse Vest og Helse Nord har informasjonssikkerhetsleder det «utøvende ansvaret» for informasjonssikkerhetsarbeidet i virksomheten. Oppgavene som ligger til rollen er detaljert beskrevet i styringssystemet. I Helse Midt-Norge varierer det mellom helseforetakene hvordan rollen er beskrevet, og det gis generelt en mindre detaljert beskrivelse av rollen.[103] I praksis har informasjonssikkerhetslederne i alle regioner omtrent de samme oppgavene.[104]

---

[96] Helse Sør-Øst: NO-5 - Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet, Sikkerhetsstrategi Helse Sør-Øst RHF NO-6. Helse Nord: Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet - Versjon: 1.2, Handlingsplan for Informasjonssikkerhet 2017-2020 med fokusområder. Helse Vest: Sikkerhetsmål og strategi S07 1. oktober 2018, Forretningsplan for Helse Vest IKT AS Versjon 2.5. Helse Midt-Norge: HMN Sikkerhetsplan 10.02.2017.

[97] I Helse Nords handlingsplan er det utpekt tre områder som skal prioriteres særskilt. Der det gjennomføres større, regionale programmer for å styrke informasjonssikkerheten (Helse Sør-Øst og Helse Nord) er det mer konkrete handlingsplaner for disse programmene. For øvrig har Ahus HF utarbeidet en egen strategi, *Strategi for personvern og informasjonssikkerhet 2019-2020*.

[98] [redacted]

[99] Retningslinjer tilsier f. eks. at rettigheter til brukerkontoer skal begrenses til tjenstlig behov, at datakommunikasjon på tvers av sikkerhetssoner skal begrenses til det nødvendige, at brukerkontoer skal deaktiveres når behov for kontoen opphører, og at programvare skal oppdateres raskt for å hindre sårbare systemer. Revisjonen viser at praksis avviker fra retningslinjene på alle disse områdene.

[100] Intervjuer med administrerende direktører i Helse Sør-Øst RHF, Helse Vest RHF og Helse Nord RHF.

[101] [redacted]

[102] Helse Nord: *Organisering av informasjonssikkerhetsarbeidet i Helse Nord*, Helse Sør-Øst: *Organisering av informasjonssikkerhetsarbeidet*, Helse Vest - ISMS, Hemit (Helse-Midt Norge)- styringssystemet, Informasjonssikkerhet, organisering og ansvar

[103] Ved St. Olavs Hospital HF og Helse Møre- og Romsdal HF heter det at informasjonssikkerhetsansvarlig skal være faglig rådgiver og utføre operative oppgaver innen informasjonssikkerhetsarbeidet. I Helse Nord-Trøndelag HF skilles det mellom informasjonssikkerhetsansvarlig og IT-sikkerhetsansvarlig, der sistnevnte har et ansvar for drift av informasjonssystemer, og alle sikkerhetsfunksjoner og rutiner for konfigurering og administrasjon av disse.

[104] De skal være rådgivere ute i virksomhetene i ulike informasjonssikkerhetsspørsmål, drive opplærings-/opplysningsvirksomhet om informasjonssikkerhet, holde oversikt over behandlingsaktiviteter for helse- og personopplysninger (herunder oversikt over informasjonsbehandlingen i IKT-løsninger, personregistre og forskningsprosjekter) delta i og kvalitetssikre risikovurderinger av IKT-løsninger, bidra til å utvikle og forvalte lokale og regionale retningslinjer og

Ved de regionale IKT-leverandørene har administrerende direktør det overordnede ansvaret for informasjonssikkerhet, som databehandler for helseopplysninger som behandles i IKT-løsningene og tjenestene de leverer til helseforetakene (og som dataansvarlig for personopplysninger internt).

Organiseringen av informasjonssikkerhetsarbeidet ved Sykehuspartner HF, Helse Vest IKT AS, Hemit og Helse Nord IKT HF skiller seg fra helseforetakene, men den grunnleggende ansvarsfordelingen internt er omtrent den samme. Informasjonssikkerhetsleder er gitt et utøvende ansvar for arbeidet, og for øvrig følger ansvaret linjen. En viktig forskjell er at dette ansvaret ikke bare omfatter informasjonssikkerheten i egen virksomhet, men også den tekniske sikkerheten i IKT-løsningene de leverer til HFene i regionen.[105]

Kilde: Innsendt dokumentasjon

Tilsendt dokumentasjon viser at mange helseforetak ikke har oppdatert styringssystemene systematisk/fortløpende før de store oppdateringene i perioden 2017 til 2020 i forbindelse med (EUs personvernforordning) GDPR. Viktige endringer det siste tiåret - som økt bruk av skytjenester og mobilt utstyr (nettbrett, smarttelefon ol.), utvikling av felles behandlingsrettede helseregistre, samt at flere kliniske IKT-systemer og journalløsninger har blitt regionale - har dermed ikke nødvendigvis blitt reflektert i helseregionenes rammeverk underveis.

### 6.2.2 Informasjonssikkerhet prioriteres i økende grad i helseforetakene

Svar på spørrebrev viser at mange helseforetak har styrket ressursbruken på informasjonssikkerhet siden 2018 i form av ansatte som jobber med dette området. Alle helseforetakene har ansatte med informasjonssikkerhet som primæroppgave. Som hovedregel er det, uavhengig av størrelse på helseforetaket, ansatt én informasjonssikkerhetsleder/-rådgiver eller tilsvarende og ett personvernombud.[106] I noen helseforetak ivaretas begge disse rollene av samme person.[107] De større helseforetakene har i tillegg også andre dedikerte personer som jobber med e-helse samt flere tekniske IKT-ressurser. Noen av helseforetakene oppgir at de planlegger å opprette nye stillinger på informasjonssikkerhetsområdet.[108]

Mange av helseforetakene har nylig gjort endringer av informasjonssikkerhetsleders organisasjonsmessige plassering slik at denne rollen stort sett hører under stabsfunksjonen. [redacted].[109] Alle informasjonssikkerhetsledere som ble intervjuet ved de utvalgte helseforetakene, ga uttrykk for at støtte hos ledelsen er viktig for å få gjennomført nødvendige tiltak.

Også hyppigheten på rapporteringen er økt, og rapporteringen går nå mer direkte til ledelsen. I Helse Sør-Øst, Helse Vest og Helse Nord legger de oppdaterte styringssystemene klarere føringer for organisering og oppgavefordeling mellom ulike roller (se faktaboks over). Det er også foretatt organisatoriske endringer ved det utvalgte helseforetaket i Helse Midt-Norge.

Flere av de administrerende direktørene som er intervjuet, erkjenner at det har vært en «oppvåkning» eller «gryende bevissthet» ved mange helseforetak om ansvaret deres for informasjonssikkerhet som dataansvarlige, og om trusselbildet.[110] Samtidig viser undersøkelsen at helseforetakenes

prosedyrer for informasjonssikkerhet, delta i regionale råd der informasjonssikkerhet er tema, og følge opp informasjonssikkerhetsavvik. De har også et ansvar for å kontrollere at krav til informasjonssikkerhet etterleves bl.a. gjennom å foreslå revisjoner, og et ansvar for å følge opp avdekkede IKT-sårbarheter hos HFet. Videre skal de rapportere oppover om status på informasjonssikkerhetsområdet, slik at ledelsen får en oversikt over risikoen på området.

[105] Styringskrav gjennom oppdrag og bestilling fra helseregionene

[106] Det brukes også mange andre betegnelser for denne rollen, som informasjonssikkerhets-koordinator, IKT-sikkerhetsleder ol.

[107] Med innføring av personvernforordningen i 2018 er det påkrevd at virksomhetene utnevner personer til disse rollene.

[108] Dette gjelder blant andre Sunnaas Sykehus HF (opplyst i svar på spørrebrev til Riksrevisjonen), [redacted]

[109] [redacted]

[110] [redacted]

oppgaveportefølje på informasjonssikkerhetsområdet har økt i omfang og kompleksitet, og at helseforetakene har hatt lite ressurser på dette området i forhold til oppgavemengden.[111]

### Faktaboks 4 Kort om helseforetakenes og de regionale IKT-leverandørenes oppgaver

IKT-miljøet i spesialisthelsetjenesten er svært omfattende og komplekst, og ivaretakelse av IKT-sikkerheten krever et samspill mellom flere aktører. Oppgavene til de regionale IKT-leverandørene og helseforetakene kan grovt sett beskrives slik:

**De regionale IKT-leverandørene.** Sykehuspartner, Helse Vest IKT, Hemit og Helse Nord IKT står for den tekniske sikringen av den regionale IKT-infrastrukturen[112], av regionale IKT-systemer[113], samt av mange av helseforetakenes lokale systemer og utstyr.

**Helseforetakene.** Bruken av applikasjoner og utstyr i helseforetakene vil kunne avgjøre om de tekniske sikkerhetstiltakene fungerer etter hensikten, og helseforetakene må sørge for sikker bruk. Helseforetakene må også stille krav til sikkerhetsnivå og tekniske sikkerhetstiltak i de regionale IKT-leverandørenes løsninger. Der HFene selv har ansvar for IKT-drift[114] vil de ofte selv stå for de tekniske sikkerhetstiltakene; de må selv sikre disse bl.a. ved sikkert oppsett (konfigurasjon), sikkerhetsoppdateringer, tilgangskontroller og overvåking.

**Regional sikkerhet.** Siden IKT-infrastrukturen og en stor andel av systemene som benyttes er regionale, og siden de lokale nettverkene, applikasjonene og utstyret også kommuniserer med regionale nettverk og maskinvare, kan sikkerhetsnivået ved ett helseforetak påvirke sikkerhetsnivået i et annet.

Kilde: Svar på spørrebrev fra helseforetakene og de regionale IKT-leverandørene, samt intervju med ledere i helseregionene.

#### 6.2.3 De regionale IKT-leverandørene har bygget opp fagmiljøer for informasjonssikkerhet

De regionale IKT-leverandørene har langt større sikkerhetsmiljøer enn helseforetakene, og generelt mer IKT-teknisk kompetanse, ettersom informasjonssikkerhetsarbeid ligger nærmere primæroppgaven deres enn hos helseforetakene jf vedlegg 2.

Helse Vest IKT, Helse Nord IKT og Sykehuspartner har de siste årene ansatt flere personer som skal jobbe med informasjonssikkerhet. Sykehuspartner oppbemannet betydelig på sikkerhetssiden etter IKT-angrepet i 2018, særlig i avdeling for operativ sikkerhet (Sykehuspartner Cert).[115] Informasjonssikkerhetslederne som er intervjuet i de fire regionale IKT-leverandørene, opplever å ha støtte hos toppledelsen og andre ledere internt. Alle rapporterer jevnlig og direkte til administrerende direktør eller ledergruppen. I Sykehuspartner er informasjonssikkerhetsleder en del av ledergruppen.[116] Se vedlegg 2 for nærmere beskrivelse av fagmiljøene for IKT-sikkerhet ved de regionale IKT-leverandørene.

[redacted].[117]

[111] Svarbrev og intervju med helseforetakene.
[112] IKT-infrastrukturen er i alle helseregioner i hovedsak regional og de fleste IKT-systemer driftes av de regionale IKT-leverandørene. Disse står for drift av regionale nettverk, datasentre og størstedelen av maskinene (PC-er og servere) tilknyttet nettverkene.
[113] Applikasjonene/programvarene som benyttes er i økende grad regionale, selv om det fortsatt er en stor portefølje av lokale applikasjoner i helseforetakene. For eksempel er journalsystemer, laboratoriesystemer, radiologisystemer og økonomisystemer enten regionale eller i ferd med å bli det i alle helseregionene.
[114] Helseforetakene drifter noe utstyr selv, blant annet medisinsk-teknisk og bygningsteknisk utstyr, og servere/PC-er knyttet til disse. Helseforetakene har også lokale nettverk for slike oppgaver, og noen steder også egne serverrom/datarom og kabling.
[115] Intervju med direktør for IKT-tjenester i Sykehuspartner. Sykehuspartner Cert økte antall ansatte fra ca. 12 til ca. 22 årsverk etter hendelsen. Tidligere var de organisert som en seksjon under avdeling for produksjonskontroll.
[116] Avdeling for operativ sikkerhet (Sykehuspartner Cert) rapporterer til direktør for IKT-tjenester, som også sitter i ledergruppa.
[117] [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

- [redacted]

### 6.2.4 Det er satt i verk større forbedringsprosjekter for informasjonssikkerhet

I to av regionene - Helse Nord og Helse Sør-Øst - er det satt i gang større forbedringsprosjekter som helt eller delvis har som formål å bedre informasjonssikkerheten (se oversikt i vedlegg 3).[122] Helse Vest og Helse Midt-Norge har ikke sett samme behov for større forbedringsprosjekter.

Forbedringsprosjektene i Helse Nord og Helse Sør-Øst er i stor grad rettet mot særskilte utfordringer i disse regionene. Enkelte av programmene dreier seg om å redusere porteføljen av IKT-systemer og applikasjoner, og å få bedre oversikt over systemer og komponenter/eiendeler (programvare). I Helse Sør-Øst er det også et viktig mål å oppgradere regionens IKT-infrastruktur, samt å etablere en felles teknologisk plattform for hele regionen. Helse Sør-Øst har en særskilt stor og uoversiktlig portefølje av IKT-systemer, samt utfordinger knyttet til eldre IKT-infrastruktur.[123] Dette gir igjen større utfordringer i informasjonssikkerhetsarbeidet. En bakenforliggende årsak er sammenslåingen av helseregion Sør og helseregion Øst, der helseforetakene i de to regionene hadde mange ulike systemer og ulike strategier.

Prosjektene i Helse Sør-Øst og Helse Nord inneholder også flere andre tiltak som adresserer svakheter vist i kapittel 4 og 5. Blant annet skal det i begge regioner anskaffes og innføres nye løsninger for tilgangsstyring for administratorer og brukere. Løsningene skal bl.a. gjøre det enklere å holde oversikt over hvem som har hvilke rettigheter. I Helse Nord inneholder *Prosjekt for Helhetlig Informasjonssikkerhet (HIS)* anskaffelse og innføring av ny og sikrere påloggingsløsning. HIS-prosjektet inneholder også et delprosjekt som dreier seg om å styrke regionens evne til å oppdage dataangrep (jf. kapittel 6.2.3). I begge regionene er innføring av Windows 10 del av

[redacted]

[122] Styresak 036-2020 Helse Sør-Øst: STIM - Fem av ni prosjekter har fremdrift i henhold til plan, tre prosjekter ligger noe etter plan, mens Windows-10-prosjektet har fremdrift langt etter plan.

[123] Helse Nord gjennomførte i perioden 2011 til 2016 et større program, Felles innføring av kliniske systemer (FIKS), som har redusert systemporteføljen. Ifølge Helse Nord RHF er det fortsatt en del eldre, lokal programvare ute i helseforetakene. Standardisering av denne inngår ikke i forbedringsprosjektene, men er ifølge RHFet del av rullerende langtidsplan (ØLP). RHFet har gjennom foretaksmøter pålagt helseforetakene å rapportere behov for *ny* programvare. Helse Vest har satset på mer standardisering i regionen ved for eksempel felles radiologisystem (Sectra), felles økonomisystem (SAP) og felles journalsystem DIPS (Arena). Helse Midt-Norge etablerer Helseplattformen, og har mange standardiserte kliniske systemer.

forbedringsprosjektene, mens dette gjøres som en del av det løpende oppdateringsarbeidet i Helse Vest og Helse Midt-Norge. Både i Helse Sør-Øst og Helse Nord er forbedringsprosjektene forsinket ut ifra opprinnelige planer. [124]

I Helse Midt-Norge gjennomføres det også, i forbindelse med innføring av Helseplattformen, noen konkrete prosjekter som skal bidra til å styrke informasjonssikkerheten i ny, felles pasientjournal.[125] Styret for Helseplattformen har uttalt at tidsplanen for produksjonssetting av ny journalløsning ikke kan gjennomføres og har bedt om en justert innføringsplan.[126]

### 6.2.5 Det er opprettet regionale samarbeidsforum for informasjonssikkerhet

I alle de fire regionene er det opprettet ett eller flere samarbeidsfora på informasjonssikkerhetsområdet, der representanter for RHFene, HFene og de regionale IKT-leverandørene møtes. Alle regionene har et forum som skal behandle risiko- og sårbarhetsanalyser (ROS-analyser) av systemer og utstyr som skal settes i drift eller endres. Videre har de et forum med ansvar for å forvalte de regionale styringssystemene for informasjonssikkerhet og personvern, og for å gi råd om strategi og prinsipielle spørsmål knyttet til området.

I løpet av undersøkelsesperioden 2017–-2019 er det opprettet flere nye fora, og regionene har arbeidet med å tydeliggjøre mandatet til de allerede eksisterende samarbeidsorganene. Mange av de nyopprettede foraene er etablert for å involvere virksomhetsledere i viktige informasjonssikkerhetsspørsmål i større grad enn tidligere. En fullstendig oversikt over foraene kan ses i vedlegg 4.

## 6.3 Helseregionene har ikke ryddet opp i viktige, kjente svakheter

### 6.3.1 Flere av de tekniske svakhetene er påpekt tidligere

Det framgår av svar fra de regionale IKT-leverandørene at de kjenner til flere av de tekniske sikkerhetssvakhetene som er påpekt i kapittel 5. En gjennomgang av rapporter fra HelseCert, som foretar periodiske penetrasjonstester av helseforetak og IKT-leverandører, viser at de har tatt opp flere temaer med helseregionene som samsvarer med tekniske funn i denne undersøkelsen. [redacted].[127]

Til tross for mange sammenfall mellom funn i denne revisjonen og HelseCerts tidligere revisjoner, mener HelseCert at det har vært en utvikling hva gjelder oppfølgingen av resultatene i inntrengingstestene, og at helseforetakene og IKT-leverandørene jobber mer systematisk med funnene. De første årene etter at HelseCert begynte å gjennomfør inntrengingstester (2013) var det mer vanlig at man fortsatt kunne finne det samme som man hadde gjort i foregående test. HelseCert mener det har vært en modning i alle helseregionene, særlig der de tester internetteksponerte tjenester (skallsikring).[128]

### 6.3.2 Komplekse IKT-miljøer med stort omfang av utstyr og programvare gjør det vanskelig å gjennomføre sikkerhetstiltak

Alle helseforetakene og de fire regionale IKT-leverandørene har i brev blitt bedt om å svare på hva som er den største utfordringene deres knyttet til forebygging og avdekking av dataangrep. Både

[124] Helse Nord IKT HF uttaler at HIS-prosjektet planlegges videreført i en ny fase / nytt HIS 2.0. Det skal vedtas en ny investeringsplan for HIS del 2. Det har til en viss grad vært en ressurskonflikt mellom HIS-prosjektet og oppfølging av tiltak etter Riksrevisjonens funn.
[125] [redacted]
[126] https://helseplattformen.no/nyheter/ber-om-justert-innforingsplan
[127] Intervju med HelseCert
[128] Intervju med HelseCert

helseforetakene og regionale IKT-leverandører i alle regioner trekker fram kompleksiteten i informasjonsbehandlingen i spesialisthelsetjenesten, og det store omfanget av IKT-systemer, IKT-utstyr og programvare, som en av hovedutfordringene.[129] For eksempel er det i Helse Sør-Øst 170 000 medisinsk-tekniske enheter i bruk basert på mer enn 10 000 servere.[130] Ledere i de regionale IKT-leverandørene viser til at det er satt i gang utbedringstiltak på flere områder der Riksrevisjonen har påpekt sårbarheter, men at omfang og kompleksitet gjør at arbeidet tar tid.

Kompleksitet og omfang påvirker helseregionenes evne til å få oversikt over alt utstyr og programvare, og ikke minst avhengigheter mellom disse. Manglende oversikt gjør det vanskeligere å identifisere og gjennomføre viktige sikkerhetstiltak som sikkerhetsoppdateringer, sikker konfigurasjon av systemer og å styre tilgangsrettigheter.

Det beskrives for eksempel som utfordrende å holde oversikt over avdekkede sårbarheter, og å sikre at alle systemer har de siste oppdateringer som fungerer for de tjenestene som kjører på systemet. De regionale IKT-leverandørene peker på at det er svært mange private leverandører, ulike måter og frekvenser å slippe oppdateringer på, og mange avhengigheter mellom ulike leverandørers systemer. For en del eldre IKT-systemer, programvare og utstyr er det heller ikke mulig å få installert sikkerhetsoppdateringer. I noen tilfeller kan man ved forsøk på oppdateringer av programvare som understøtter medisinsk-teknisk utstyr, risikere å påføre utstyret feil som i verste fall kan gi pasientskader. Det er imidlertid ikke dokumentert slike skader.

Flere helseforetak og regionale IKT-leverandører trekker også fram at de mangler oversikt over *bruk av skytjenester*, som beskrives som relativt lett å ta i bruk for ansatte. [131] Noen helseforetak bemerker også at de må forholde seg til et komplekst aktørbilde, og at det er utfordrende å ha tilstrekkelig innsikt og kjennskap til sikkerhetsnivået hos både de regionale IKT-leverandørene, samt andre leverandører og underleverandører.[132]

En annen kompliserende faktor er at mange av systemene og utstyret som benyttes inneholder helse- og personopplysninger. Helseforetakene skal utarbeide samlede oversikter over *behandlingsaktiviteter* for helse- og personopplysninger som foregår under deres ansvar etter innføringen av EUs personvernforordning. Behandlingsaktiviteter omfatter bl.a. behandling av informasjon i IKT-systemer, applikasjoner/programvare, personregistre og forskningsprosjekter. På kontrolltidspunktet var alle helseforetak i gang med dette arbeidet, men det var kun en tredjedel av helseforetakene som anså seg å være i mål. Flere intervjuobjekter mener imidlertid at helseforetakene burde hatt slike oversikter på plass tidligere, fordi det kan bidra til oversikt over hvor de største utfordringene på informasjonssikkerhetsområdet ligger.

Den samlede kompleksiteten er en utfordring i alle regioner, men intervjuer og svar på spørrebrev viser at det er en større utfordring i Helse Sør-Øst enn i de andre regionene. Årsaken er at regionen har en særlig kompleks og omfattende portefølje av utstyr, systemer og programvare/applikasjoner.

Alle helseforetakene og regional IKT-leverandør i Helse Sør-Øst sier i svar på spørrebrev at kompleksitet er en hovedutfordring. Sykehuspartner trekker fram en stor og kompleks portefølje av utstyr, systemer og programvare som den viktigste årsaken til de tekniske funnene i undersøkelsen (kapittel 4 og 5), og den største utfordringen i det videre forbedringsarbeidet av informasjonssikkerheten i regionen.

Flere applikasjoner betyr bl.a. mer arbeid med oppdateringer. Dette reflekteres ved at Helse Sør-Øst har kommet kortest med oppgradering av enheter til Windows 10, som gir bedre sikkerhet enn tidligere versjoner av operativsystemet. I februar var Helse Vest og Helse Midt-Norge nesten i mål med

[129] Helseforetakene og IKT-leverandørenes svar på vårt spørrebrev.
[130] https://sykehuspartner.no/ny-ikt-infrastruktur
[131] Intervju med informasjonssikkerhetsledere, svar på spørrebrev fra helseforetak og regionale IKT-leverandører.
[132] Det ble et krav å utarbeide oversikter over behandlingsaktiviteter for helse- og personopplysninger med ny personopplysningslov som fikk virkning i juli 2018 og innførte EUs personvernforordning i Norge.

oppgradering til Windows 10, og Helse Nord hadde oppgradert omtrent 60 prosent av sine enheter, mens Helse Sør-Øst var i startfasen av oppgraderingsarbeidet.[133]

Reduksjon av porteføljen har vært et viktig mål med de større forbedringsprogrammene i regionen (se kapittel 6.2.4). Porteføljen av applikasjoner er redusert, men det er mye arbeid som gjenstår.[134] Som del av Program for standardisering og IKT-infrastrukturmodernisering (STIM) ble det i 2019 gjennomført en kartlegging av alle applikasjonene i regionen og deres kompatibilitet mot Windows 10. Denne kartleggingen viste vesentlig større omfang og kompleksitet i applikasjonsporteføljen enn man fram til da hadde vært klar over.[135] Ifølge Helse Sør-Øst RHF har større kompleksitet enn først antatt ført til manglende fremdrift og forsinkelser i STIM-prosjektet.[136]

De regionale IKT-leverandørene peker også på eldre og upraktiske tekniske løsninger som en utfordring. De viser til at de planlegger innføring av nye tekniske løsninger som vil øke sikkerhetsnivået. Dette gjelder særlig nye systemer for tilgangsstyring for administratorer og brukere, samt nye løsninger for enklere pålogging for brukere.

[redacted]

I forbindelse med innføring av Helseplattformen i Helse Midt-Norge skal det innføres nye løsninger for identitets- og tilgangsstyring for administratorer og brukere i ny, felles pasientjournal. Ifølge Hemit vil en viktig forbedring med de nye tilgangsstyringssystemene være at admin-rettigheter kan tildeles periodisk, slik at mer utvidede tilganger utløper automatisk når perioden er over.[137] [138]

### 6.3.3 Helseregionene prioriterer ikke systematisk rydding i gamle løsninger og sensitive helse- og personopplysninger

Selv om komplekse IKT-miljøer er en viktig forklaring på svakheter omtalt i kapittel 5, er det også forhold som har større sammenheng med ledelse og prioriteringer i den daglige driften. Der det innføres nye løsninger som i utgangspunktet skal øke IKT-sikkerhetsnivået, er det mange eksempler på at man enten ikke greier å fase ut de gamle løsningene, eller at man ikke greier å rydde opp i gamle løsninger som skal videreføres. Dermed får man en situasjon der nye, sikre løsninger eksisterer parallelt med gamle, usikre løsninger.

Manglende opprydding på viktige områder har blitt utnyttet i angrepssimuleringen i alle helseregioner. Det varierer hvorvidt det er regional IKT-leverandør, helseforetak eller begge parter som må foreta seg noe. Noen eksempler på områder med behov for rydding er:

- ***Rydding i gamle grupper for tilganger.*** I alle regioner opprettes nye grupper i katalogtjenesten Active Directory som skal sikre at brukeres rettigheter tilsvarer behov for tilgang, men gamle grupper er fortsatt aktive og gir mer utvidede rettigheter, jf. punkt 5.3.2.

- ***Rydding i eldre domener.***
  [redacted][139]
  [redacted]

[133] Av omtrent 60 000 klienter var 2700 oppgradert til Windows 10 i starten av februar. Se: https://www.digi.no/artikler/windows-7-dominerer-fortsatt-hos-ett-av-de-regionale-helseforetakene/484545
[134] Sykehuspartner rapporterte i årlig melding i 2018 at porteføljen av applikasjoner var redusert fra 5652 til 3848. Imidlertid har kartlegging i etterkant av dette funnet at applikasjonsporteføljen var vesentlig større enn antatt i 2018.
[135] Oppdatering om programmene til styret i Sykehuspartner HF, vedlegg 2 til styresak 003-2020.
[136] Helse- og omsorgsdepartementets tilbakemelding på utkast til rapport 29. september 2020.
[137] Per i dag må man manuelt aktivere og deaktivere admin-rettigheter, og/eller melde brukere inn og ut av grupper. Dette beskrives som tungvint, og noe som i mange tilfeller vil nedprioriteres
[138] [redacted].
[139] Et domene er en sammenkobling av flere systemer under én felles kontrollfunksjon, ofte kalt en domenekontroller. Gjennom domenekontrolleren defineres prosesser, tilganger og sikkerhetsnivå, og det er mot domenekontrolleren brukere autentiserer seg.

[redacted]

- **Rydding i gamle løsninger og sensitive helse- og personopplysninger.**
  [redacted]

- ***Rydding av kontoer som ikke er i bruk.*** Helseforetakene og de regionale IKT-leverandørene sikrer stort sett at ordinære brukerkontoer blir deaktivert når for eksempel personell slutter. For andre typer kontoer som ikke lenger er i bruk gjenstår det en ryddejobb.
  [redacted]

Intervjuer med ledere ved de regionale IKT-leverandørene viser at de har vært kjent med mange av disse forholdene, men at opprydding i mange tilfeller ikke har blitt prioritert.

[redacted]

Informasjonssikkerhetsledere som er intervjuet peker på flere årsaker til at oppryddingsarbeid har blitt nedprioritert:

- Det kan oppstå en konflikt mellom daglig drift og opprydding i gamle saker. Det kan f. eks. være krevende å få de som jobber med tilgangsstyring til å prioritere rydding i gamle tilganger, når de er opptatt med å legge til nye brukere og administrere brukere og tilganger i bruk.[140]
- Endringsbehovet i sektoren er generelt drevet av ønsker om funksjonalitet; at nye systemer eller oppdateringer leverer funksjonalitet som er etterspurt. Utfasing av gamle systemer bidrar ikke til ny funksjonalitet for helsetjenesten, og vil derfor lettere nedprioriteres. [141]
- Det kan være arbeidskrevende å rydde opp når dette ikke har blitt prioritert fortløpende.[142]
- I mange tilfeller er IKT-leverandørene avhengig av at helseforetakene prioriterer rydding og utskifting. Helseforetakene kan ha mindre vilje til å prioritere ressurskrevende oppryddingsarbeid blant annet fordi ressurser til slike oppgaver til enhver tid må veies opp mot andre oppgaver nærmere pasientbehandlingen.[143]

[140] Oppfølgingsmøte med Sykehuspartner 27. mai 2020.
[141] Oppfølgingsmøte med Hemit 28. mai 2020.
[142] [redacted]
[143] [redacted]

- Noen helseforetak ønsker å beholde gamle domener, fordi det gir mer frihet til å installere og drifte som helseforetakene selv ønsker. Det er også eksempler i Helse Nord og Helse Sør-Øst på at helseforetak ønsker nye, lokale domener.[144]
- I en del tilfeller er det uavklart om det er helseforetak eller regional IKT-leverandør som har ansvaret for den nødvendige oppryddingen.[145]

## 6.4 Uklare ansvarsforhold og oppgavefordeling hindrer forbedringsarbeidet

### 6.4.1 Uklarheter om ansvar og myndighet for ivaretakelse av sikkerheten i regional infrastruktur

Rolle- og ansvarsfordelingen mellom aktørene i den enkelte region defineres bare i noen grad i styringssystemene for informasjonssikkerhet. Ansvaret helseforetakene og de regionale IKT-leverandørene har overfor hverandre som kunde-leverandør og dataansvarlig-databehandler, defineres gjennom databehandleravtaler og avtaler som regulerer enkelttjenester (drifts- og tjenesteavtaler). I styrings-systemene vises det til disse avtalene.

RHFene gir i tillegg de regionale IKT-leverandørene og HFene oppgaver knyttet til informasjonssikkerhet i årlige oppdragsbrev, som også kan ha betydning for ansvarsfordelingen mellom dem. Det er i flere tilfeller også foretatt prinsipielle avklaringer om ansvarsfordelingen mellom aktørene gjennom styrevedtak i RHFenes styrer.[146]

I alle de fire regionene er det opprettet samarbeidsforum/råd på informasjonssikkerhetsområdet, jf. omtale i 6.2.5. Det framgår av intervjuer i helseregionene og av tilsendt dokumentasjon at det i disse forumene arbeides aktivt med mange av uklarhetene som påpekes av regionale IKT-leverandører og helseforetak.

På spørsmål om myndighet, ansvar og arbeidsoppgaver i deres helseregion er klart fordelt, svarer over halvparten[147] i spørrebrevet at det gjenstår praktiske avklaringer mellom regional IKT-leverandør og helseforetak.[148] Tre av helseforetakene og de tre regionale IKT-leverandørene Hemit, Helse Nord IKT og Sykehuspartner oppgir at dette er av de største utfordringene knyttet til forebygging og avdekking av dataangrep.[149] I Helse Vest framstår det noe klarere hvem som har hvilke oppgaver enn for de andre regionene.[150]

En større problemstilling som tas opp i Helse Nord, Helse Midt-Norge og Helse Sør-Øst er hva slags oppgaver og myndighet de regionale IKT-leverandørene har og burde ha. De er gitt et ansvar for sikkerheten i den regionale infrastrukturen (regionalt nettverk og maskinpark), men har ikke kontroll med alt som er koblet til denne. Lokale sikkerhetsbrudd kan utgjøre en risiko for regionen som helhet, og de regionale IKT-leverandørene mener manglende avklaringer gjør det tidkrevende å rydde opp i kjente svakheter. Blant annet oppleves dette som en utfordring der det må ryddes i det helseforetakene drifter selv (inkludert forholdene tatt opp i kapittel 6.3.3), og der det er vanskelig å gjennomføre oppdatering av programvare for eldre utstyr og systemer ute i helseforetakene.

Gjennomgangen av de tekniske sikkerhetstiltakene i kapittel 5 viser at det gjennomgående er slik at utstyr og systemer som helseforetakene drifter selv har svakere tilgangskontroller, oppdateres sjeldnere, og i mindre grad er sikret. Flere av helseforetakene i disse regionene uttrykker et behov

[144] Notat til RSR i Helse Sør-Øst, «Forhold rundt lokale domener». I oppfølgingsintervju med Helse Nord har det ifølge Helse Nord IKT nylig pågått en diskusjon om opprettelse av nye domener til helseforetakene, for eksempel for å koble til skytjenester.
[145] I Helse Sør-Øst var det f. eks. tidligere ikke avklart hvem som skulle ha ansvar for opprydding i lagrede personopplysninger. I etterkant av våre tekniske kontroller har det blitt besluttet at helseforetakene, som eiere av dataene, har ansvar for oppryddingen. Sykehuspartner opplyser at de på sin side har skjerpet kontrollen med opprettelse av lagringsmuligheter. Opplyst i oppfølgingsmøte med Sykehuspartner 27. mai 2020.
[146] Vedtekter og instrukser for styret og administrerende direktør ved de regionale IKT-leverandørene, herunder stiftelsesprotokoll, styreinstruks, samt instruks for administrerende direktør kan også ha betydning. Helse Nord IKT trekker fram dette i svar på spørrebrev.
[147] 14 av 23 spurte helseforetak og IKT-leverandører.
[148] Helseforetakene gir i svarbrev uttrykk for at myndighet, ansvar og arbeidsoppgaver mellom dem og RHFet er klart regulert i helseforetaksloven.
[149] Hemit, Helse Nord-Trøndelag HF, Helse Nord IKT HF, UNN HF, Sykehuspartner HF, Sykehuset i Vestfold HF. [redacted]
[150] Helse Vest IKT uttaler at det må være en avklart fordeling av ansvar for IKT-infrastruktur og system/applikasjon for å kunne følge opp informasjonssikkerheten.

for/ønske om en viss grad av lokal kontroll, og at helseforetakene kan miste kompetanse ved å sentralisere IKT-drift og -sikkerhetsarbeid. Dette mener helseforetakene kan påvirke deres mulighet til å ivareta ansvaret de har i henhold til helseforetaksloven og personvernlovgivningen.[151] Selv om flere oppgaver ivaretas regionalt eller nasjonalt, må helseforetakene ha kompetanse til å stille krav til informasjonssikkerhet overfor regional IKT-leverandør.[152] Noen helseforetak mener overføring av oppgaver og/eller myndighet til regional IKT-leverandør kan innebære at sistnevnte tar stilling til hva slags utstyr og systemer som benyttes, noe som skal være fagmiljøenes oppgave.[153]

Uenighetene om oppgave- og ansvarsfordeling mellom helseforetak og regional IKT-leverandør har vært størst i Helse Sør-Øst og Helse Nord. Det er foretatt avklaringer om ansvar og oppgaver i begge regioner de siste årene. Helse Sør-Øst RHF har gitt Sykehuspartner et utvidet mandat i oppdragsbrevene for 2019 og 2020, bl.a. til å stoppe informasjonssystemer og nettverk som medfører en vesentlig sikkerhetsrisiko for foretaksgruppen som helhet. I Helse Nord har Helse Nord IKT bedt det regionale helseforetaket om å evaluere regionens IKT-styringsmodell og klargjøre ansvar- og myndighetsforholdene på området, og å tydeliggjøre Helse Nord IKTs ansvar og myndighet for IKT-infrastrukturen, med særlig vekt på ivaretakelse av informasjonssikkerhet. Se nærmere omtale av situasjonen i hver enkelt region i Vedlegg 5.

I noen tilfeller kan uklarheter om oppgave- og ansvarsfordeling skyldes manglende klarhet eller detaljeringsnivå i avtaleverk. Dette kan forklares med at avtaler ikke oppdateres ofte nok. Uklarheter i databehandleravtaler, tjenesteavtaler og andre avtaler (f. eks. avtale om felles journal) om hvem som har det formelle ansvaret og hvem som skal utføre oppgaver, kan i sum bidra til en uklar rolleforståelse.[154]

Spørsmål om regional fordeling av ansvar og oppgaver på informasjonssikkerhetsområdet kompliseres av ny personvernlovgivning. Som dataansvarlige har helseforetakene det juridiske ansvaret for behandlingen av helse- og persondata overfor sine pasienter,[155] mens de regionale IKT-leverandørene - som databehandlere - har et ansvar for behandlingen av data overfor dataansvarlig. Når det gjelder regionale IKT-løsninger med flere dataansvarlige, har det særlig vært uklart for helseregionene hvem som er ansvarlige ved sikkerhetsbrudd.[156] Svar fra helseregionene viser at de nå i hovedsak mener at lovverket er klart, men at det gjenstår noen uklarheter.

Ettersom det i hovedsak er de regionale helseforetakene som initierer regionale IKT-løsninger, har det blitt stilt spørsmål ved om regelverket tillater at dataansvaret deles mellom helseforetak og regionalt helseforetak, eventuelt at regionalt helsefortak kan ha et slikt ansvar alene. Helse Sør-Øst påpekte uklarheter senest i sitt innspill til *Prop. 65 L (2019-2020) Lov om e-helse (e-helseloven)*. Der et helseforetak som dataansvarlig vurderer at informasjonssikkerheten i en IKT-løsning ikke er innenfor akseptabel risiko, men likevel er lovpålagt ut ifra helselovgivning å gjøre løsningen tilgjengelig i virksomheten, mener Helse Sør-Øst RHF at det er utydelig hvordan ansvaret for risikoreduserende tiltak og restrisiko skal håndteres.

Undersøkelsen viser videre at det er flere problemstillinger som ikke krever avklaring av lovverket, men der regionene prøver å finne praktiske innretninger på den regionale ansvars- og oppgavefordelingen som også er i tråd med personvernlovgivningen. I Helse Vest er det for eksempel regional IKT-leverandør som - på vegne av foretakene - inngår databehandleravtaler med underleverandører for felles IKT-systemer. I Helse Nord har RHFet stilt krav i oppdragsdokumentet for

[151] Helse Nord-Trøndelag HF (HNT) og Sykehuset i Vestfold HF (SiV HF) påpeker dette i sine skriftlige svar på spørrebrev. Helse Nord-Trøndelag skriver at regional og nasjonal sentralisering av oppgaver som f.eks. IT-funksjoner og innkjøpsfunksjoner har vanskeliggjort helseforetakenes mulighet til å ivareta sitt ansvar etter helseforetaksloven og personvernlovgivningen.

[redacted]

[152] Informasjonssikkerhetsledere i Helse Vest IKT og Helse Midt-Norge IKT trakk også fram at det kunne være en utfordring at helseforetakene hadde begrensede ressurser på informasjonssikkerhetsområdet gitt størrelsen på virksomhetene. Bl.a. fordi dette i mindre grad satte dem i stand til å stille krav. I Helse Vest ble Helse Førde trukket fram som eksempel; de har 2500 ansatte og en informasjonssikkerhetsleder i 50 prosent stilling.
[153] Intervju med administrerende direktør Helse Nord RHF
[154] Avsluttende møte Sykehuspartner, Helse Nord RHFs svar av 29. september 2020 gjennom Helse- og omsorgsdepartementets kommentarer til rapporten..
[155] Dette ansvaret innebærer blant annet et ansvar for å sikre de registrertes rettigheter, gjennomføre risikovurderinger, og etablere og dokumentere tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå.
[156] Direktoratet for e-helse (2017) *Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten*,

2018 og 2019 om at IKT-leverandøren skal inngå databehandleravtale på vegne av helseforetakene for systemer hvor Helse Nord IKT HF har driftsansvar. Flere helseforetak i regionen mener imidlertid dette ikke er i tråd med personvernlovgivningen, fordi dette vil føre til at helseforetakene ikke får entydig kontroll over dataansvaret. De mener dette skaper utfordringer når det gjelder håndtering av avvik, leverandøroppfølging samt oversikt over protokoll over behandlingsaktiviteter for helse og personopplysninger de har ansvaret for.[157]

### 6.4.2 Uklarheter om ansvaret for ivaretakelse av sikkerheten i medisinsk-teknisk utstyr

Hvordan ansvaret skal fordeles for sikkerheten i medisinsk-teknisk utstyr (MTU), er en problemstilling i alle helseregionene. MTU har blitt stadig mer integrert i IKT-området ved at en større andel av utstyret i praksis er datamaskiner med egne lagringsenheter og oppkobling mot nettverk. Noe av utstyret kommuniserer også med regionale journalsystemer. Det har vært et skille mellom de medisinsk-tekniske avdelingene i helseforetakene på den ene siden, og IKT-ressurser i helseforetakene og ved de regionale IKT-leverandørene på den andre. Fagmiljøene har arbeidet parallelt med blant annet informasjonssikkerhet.[158] MTU er underlagt egen lov.[159]

Riksrevisjonen har tidligere tatt opp at det har vært uklare ansvarsforhold for informasjonssikkerhet i MTU, både internt i helseforetakene og mellom helseforetakene og de regionale IKT-leverandørene.[160] Selv om tre av helseregionene iverksatte tiltak i etterkant av undersøkelsen[161] for å sikre bedre samordning mellom fagmiljøer for IKT og MTU, er det ikke foretatt vesentlige organisasjonsmessige endringer, og det er fortsatt uklarheter i ansvarsfordelingen. Alle de regionale IKT-leverandørene og mange helseforetak trekker fram dette som en utfordring.[162]

De regionale styringssystemene omtaler ikke nærmere hvordan sikkerheten skal ivaretas i MTU, hva slags rolle medisinsk-tekniske avdelinger ute i helseforetakene skal ha på informasjonssikkerhetsområdet eller hvordan ansvaret skal fordeles mellom helseforetak og regionale IKT-leverandører.[163] Det framgår heller ikke tydelig hvordan helseforetakene skal forholde seg til krav til teknisk sikkerhet i styringssystemene[164] ved lokal drift av slikt utstyr, ut over at det i noen tilfeller presiseres at det er regional IKT-leverandør som skal tildele lokale administrasjonsrettigheter.[165]

## Faktaboks 5 Sikkerhetsfunksjonalitet og -oppdatering av medisinsk-teknisk utstyr

- Det er en utfordring med eldre utstyr og systemer der det er vanskelig eller umulig å gjennomføre sikkerhetsoppdateringer. Dette gjelder i stor grad medisinsk-teknisk utstyr (MTU) (jf. omtale i punkt 5.5.1), som har lengre levetid enn det som er vanlig for IKT-utstyr.
- I noen tilfeller kan man ved forsøk på programvareoppdateringer av medisinsk-teknisk utstyr risikere å påføre utstyret feil som potensielt kan gi pasientskader. I andre tilfeller støttes ikke programvaren lenger av leverandøren og det tilbys derfor ikke sikkerhetsoppdateringer.[166]

---

[157] Helgelandssykehusets svar på spørrebrev av 28. juni 2019 og Finnmarksykehuset HF sitt svar på spørrebrev av 1. juli 2019
[158] Universitetssykehuset i Nord-Norge HF (UNN) og Oslo Universitetssykehus HF (OUS) trekker i svar på spørrebrev fram at MTU blir mer og mer integrert med journalsystemer.
[159] Lov om medisinsk utstyr LOV-2020-05-07-37 erstatter LOV 1995-01-12-6.
[160] Dokument 3:2 (2015-2016) Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2014, Sak 3: Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr.
[161] Helse Sør-Øst RHF, Helse Midt-Norge RHF og Helse Vest rapporterte om tiltak i årlig melding for 2016. Helse Nord RHF rapporterer i årlig melding for dette året at de vil avvente resultatene fra arbeidet som pågår i Helse Sør-Øst.
[162] Svarbrev fra Helse Vest IKT AS, Helse Nord IKT HF, Sykehuspartner HF, Helse Bergen HF, Helse Stavanger HF, Helse Fonna HF, Universitetssykehuset i Nord-Norge HF (UNN), Ahus HF og Oslo Universitetssykehus HF. Ut over dette ble det også trukket fram i intervjuer i alle de utvalgte helseforetakene.
[163] Eventuell omtale av sikring av MTU er på mer overordnet nivå. F. eks. står det i Helse Sør-Østs sikkerhetsstrategi at strategien gjelder «*uavhengig av hvor opplysningene oppstår, inkludert i medisinsk- teknisk utstyr og annet teknisk utstyr*». Enkelte informasjonssikkerhetsledere uttalte at medisinsk-teknisk avdeling forhold seg til Normens Veileder i personvern og informasjonssikkerhet i medisinsk utstyr: https://ehelse.no/normen/veiledere/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr
[164] F. eks. krav til sikker konfigurasjon, sikkerhetsoppdateringer, tilgangskontroller og overvåking.
[165] F. eks. presiseres det i *Sikkerhetsstrategi for Helse Sør-Øst* at det er Sykehuspartner som skal godkjenne alle lokale administrasjonsrettigheter. Tilgangsstyring for MTU er i liten grad omtalt i styringssystemene - det rettes i stor grad mot IKT-systemene.
[166] For eksempel er en del medisinsk-teknisk utstyr basert på operativsystemet Microsoft XP, som ble lansert i 2001 og som ikke lenger støttes av Microsoft. Kilder: Intervju med administrerende direktør ved Helse Vest IKT 17. januar 2020. Helsedirektoratet: Overordnet risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren.

- Produsenter av MTU har i utgangspunktet ansvar for at utstyret fungerer etter hensikten, og hvis helseforetak gjør egne modifikasjoner vil dette innebære å påta seg produsentansvaret for utstyret. Dette innebærer at sikkerhetsoppdateringer må gjøres i samråd med leverandør / produsent.[167]
- MTU har ofte lav modenhetsgrad både med hensyn til sikkerhetsoppdatering, endepunktssikring, logging/sporbarhet og tilgangsstyring.[168] Det pekes på at enkelte leverandører av medisinsk-teknisk utstyr, selv enkelte store internasjonale leverandører, ikke forholder seg ikke til Microsofts oppdateringsregime.[169]
- Et moment som tas opp i stortingsmeldingen om IKT-sikkerhet[170] er at det (i anskaffelsesprosessen) må stilles større krav til leverandørene knyttet til informasjonssikkerhet i de systemer og utstyr de leverer. HelseCert gir i intervju uttrykk for at det har skjedd en endring på området, ved at helseregionene begynner å utfordre MTU-leverandørene mer.[171]

De regionale IKT-leverandørene har et begrenset ansvar for sikkerheten i slikt utstyr. Det er helseforetakene som anskaffer og er eier av utstyret.[172] De regionale IKT-leverandørene er i mindre grad involvert i drift av enheter (PCer, servere, mm.) og applikasjoner som understøtter utstyret. Dette er i stor grad ivaretatt av medisinsk-tekniske avdelinger ved helseforetakene, som dermed også har ansvar for IKT-sikkerhetsrutiner.[173] Den praktiske oppgavefordelingen varierer mye, både mellom regioner og mellom helseforetak i samme region:

- Helseforetakene i Helse Vest har et større driftsansvar for medisinsk-teknisk utstyr (MTU) enn helseforetak i de tre andre regionene. [redacted]. Det er de medisinsk-tekniske miljøene/avdelingene i helseforetakene som har ansvar for dette.[174] Helse Vest IKT står imidlertid for sikring av nettverket utstyret står i, samt tilganger som gis til utstyret fra eksterne leverandører. Dette innebærer at Helse Vest IKT har mindre kontroll over sikkerheten i MTU enn de regionale IKT-leverandørene i de andre regionene.
- I Helse Sør-Øst har de to utvalgte helseforetakene i undersøkelsen, [redacted] har større ansvar for å drifte MTU selv.[175]

Et dilemma som trekkes fram når det gjelder fordeling av arbeidsoppgaver mellom helseforetak og regionale IKT-leverandører, handler om at helseforetakene trenger utstyr som fungerer til enhver tid. For dem er det derfor viktig med en viss lokal kontroll, slik at eventuelle feil kan rettes så raskt som mulig.[176] På den annen side påpekes det − også av helseforetakene − at mindre avdelinger for

[167] Direktoratet for e-helse; Veileder i Personvern og informasjonssikkerhet - medisinsk utstyr, versjon 1.1.
[168] Brev fra Sykehuspartner til Riksrevisjonen 1. mars 2019.
[169] Brev fra Sykehuspartner til Riksrevisjonen 1. mars 2019, intervju med driftsansvarlig Hemit 20. november 2019, intervju med leder i HelseCert 29. mai 2020.
[170] Meld. St. 38 (2016–2017) IKT-sikkerhet — Et felles ansvar og Innst. 187 S (2017–2018)
[171] Intervju med leder i HelseCert.
[172] I de fleste tilfeller har de ansvaret for oppkoblingsløsning for leverandører ved fjernaksess, og drift av kliniske systemer som utstyret kommuniserer med, eksempelvis radiologi- (RIS/PACS) og laboratorieløsninger. I tillegg har de et ansvar for å opprette egne sikkerhetssoner for MTU i helseregionenes nettverk
[173] Typegodkjenningen ble tidligere gjort av Direktoratet for sikkerhet og beredskap (DSB), men gjøres nå av Legemiddelverket jf Forskrift om håndtering av medisinsk utstyr og elektromedisinsk utstyr som er ethvert medisinsk utstyr, inkludert systemløsninger, som er avhengig av en elektrisk energikilde for å fungere.
[174] [redacted]
[175] [redacted]
[176] Ifølge medisinsk-teknisk avdeling ved [redacted] har teknikerne også noen ganger behov for utvidede rettigheter for å drifte utstyret optimalt. Hvis f. eks. en PC svikter på en operasjonsstue, er det viktig at avdelingen har rettigheter til å kunne installere det som trengs av programvare på en ny PC, og å sette den inn i nettverket. Kilder: Intervju med tekniker, seksjonsleder og avdelingsleder ved medisinsk-teknisk avdeling.

medisinsk-teknisk utstyr ikke nødvendigvis har samme kompetanse på IKT-sikkerhet som de regionale IKT-leverandørene.[177]

I alle de fem utvalgte helseforetakene er det på ulike måter tatt initiativ til nærmere samarbeid mellom IKT-miljøet/informasjonssikkerhetsleder og medisinsk-tekniske avdelinger internt.

I alle fire helseregioner er det også tatt nye initiativer for å klargjøre ansvarsfordelingen mellom helseforetakene og de regionale IKT-leverandørene.[178] Helse Sør-Øst var kommet lengst i arbeidet på undersøkelsestidspunktet. Her ble det gjennomført et prosjekt i regi av det regionale helseforetaket, som så på samhandlingsløsninger for ulike grupper av MTU. Utgangspunktet var at flest mulig IKT-oppgaver knyttet til MTU skal kunne utføres av Sykehuspartner på oppdrag fra det enkelte helseforetak, og at fordelingen av ansvar for drift skal være den samme for alle helseforetakene i regionen.[179]

Det er også utfordringer knyttet til anskaffelser av medisinsk-teknisk utstyr fordi helseforetakene og IKT-leverandørene kan ha ulike prioriteringer og vektlegge ulike elementer/egenskaper. For lokale anskaffelser peker to av de regionale IKT-leverandørene for eksempel på at utstyr som driftes på gammel programvare er billig å kjøpe for helseforetakene, men dyrt å drifte for IKT-leverandørene. Flere av informantene mener det burde gjøres avklaringer i tjenesteavtalene mellom partene om dette, slik at man i avtalene ser innskjøppris og driftskostnader i sammenheng.

## 6.5 Svakheter i sikkerhetsatferden til de ansatte i helseforetakene og hos IKT-leverandørene

### 6.5.1 Sikkerhetsatferd blant de ansatte bidrar til å svekke IKT-sikkerheten

Atferden til de ansatte, både i helseforetakene og særlig hos IKT-leverandørene, påvirker en angripers sjanser til å lykkes med å få «fotfeste» i infrastrukturen i helseregionene. Den påvirker også hvilke potensielle konsekvenser et dataangrep kan få.

Intervjudata, avviksmeldinger, svar på spørrebrev og funn fra angrepssimuleringen tyder samlet sett på at mange ansatte hos IKT-leverandørene og i helseforetakene har en praksis som bidrar til å svekke IKT-sikkerheten. Uheldig praksis er spesielt knyttet til:

- **Valg av enkle passord**. [redacted].
- **Praksis med unntak fra krav i styringssystemet**. I noen sammenhenger stilles det klare krav i styringssystemet, men sikkerheten svekkes ved at det åpnes for unntak. Dette gjelder for eksempel at det i varierende omfang tillates bruk av felleskontoer (jf. punkt 5.3.5). [redacted].
- **Deling av tilganger**. Det ikke er uvanlig med deling av tilganger på arbeidsstasjonene og PCene, det vil si at brukere ikke logger ut/inn med egen brukeridentitet, men deler på brukernavn og passord.

[177] [redacted]

[178] [redacted]

[179] Helse Sør-Østs Virksomhetsplan for avdeling for teknologi og e-helse 2018. Status for prosjektet Samhandlingsmodell for MTU/IKT - presentasjon til direktørmøtet i Helse Sør-Øst 6. juni 2019. Intervju med administrerende direktør i Helse Sør-Øst RHF.

- **Svak tilgangsstyring**. Det gis tilgang til mer enn tjenstlig behov tilsier. For eksempel er det gitt utvidede rettigheter til en del ordinære brukerkontoer.
- **Ulik håndtering av sensitive opplysninger**. Ulik praksis i avdelingene kan føre til at sensitiv informasjon kommer ut. For eksempel vil en økonomiavdeling være avhengig av opplysninger om pasienten og behandlingen som er utført for å fakturere pasienten, mens en medisinsk avdeling nødig vil gi fra seg tilsvarende opplysninger.
- [redacted].
- [redacted].
- **Uautorisert fysisk tilgang**. Sykehusene skal generelt være åpne for publikum, men det forekommer at uvedkommende beveger inn i soner som er ment å være skjermet.
- **Slurv og bruk av snarveier**. Ansatte slurver, tar snarveier eller er uoppmerksomme. Flere sikkerhetshendelser viser at ikke anbefalt prosedyre er fulgt.

I intervju framhever IKT-leverandørene at sikkerhetsatferden hos egne ansatte er en av hovedårsakene til funnene i de kontrollen av de tekniske sikkerhetstiltakene (presentert i kapittel 5). De jobber med å bygge sikkerhetskultur og integrere informasjonssikkerhet i arbeidsprosesser, slik at sikkerhet ikke skal være noe «som kommer i tillegg». De uttaler at sikkerhetskulturen er i gradvis bedring.

Også i sykehusene viser intervjuene at mange ansatte er bevisst sikkerhetsutfordringene, men etterlevelsen av krav og anbefalinger er ulik. Flere av lederne i helseforetakene, som de administrerende direktørene i [redacted], anser at de ansattes atferd er avgjørende for informasjonssikkerheten, men erkjenner at det ikke er jobbet nok med å utvikle sikkerhetskulturen. Det krever både ressurser og tid å jobbe med sikkerhetskultur, og begge deler er knappe faktorer i et sykehus.

HelseCert, som kjenner godt til IKT-driftsmiljøene hos IKT-leverandørene, mener det generelt er en økt bevissthet om IKT-sikkerhet. De påpeker at det er de som drifter systemene som har størst påvirkning på sikkerheten i løsningene, og at sikkerhetskultur her dermed er svært viktig.[180] Flere av inntrengingstestene HelseCert har gjennomført mot IKT-leverandørene, og de mottatte revisjonene, viser imidlertid at vedtatte rutiner og retningslinjer ikke alltid følges av de ansatte.[181]

**Tilbøyelighet blant ansatte i helseforetakene til å klikke på e-postlenker**

Ifølge Nasjonal sikkerhetsmyndighet starter det store flertallet av alvorlige registrerte IKT-hendelser rettet mot nasjonal kritisk IKT-infrastruktur med en forfalsket e-post som har til hensikt å lure bruker til å åpne et vedlegg med ondsinnet programvare, eller klikke på en lenke som fører til infeksjon av maskinen.

Medarbeidere som er særlig eksponert for phishing oppgir i intervju at de opplever hyppige svindelforsøk. Dette har gjort dem mer oppmerksomme. Men flere gir uttrykk for at svindel-e-postene blir stadig mer avanserte, slik at de før eller senere vil kunne la seg lure.

For å undersøke i hvilken grad helsepersonell lar seg lure av falske e-poster, ble en såkalt phishing-e-post sendt til et utvalg ansatte ved de utvalgte helseforetakene. De falske e-postene var tilpasset en antatt situasjon ved de ulike sykehusene og handlet om parkering eller avhending av gamle PCer. De

[180] Intervju med HelseCert 29. mai 2020.
[181] I alt 14 internrevisjoner eller revisjoner som er utført av eksterne pluss ni inntrengningstester gjennomført overfor IKT-leverandørene

ansatte ble bedt å registrere sitt behov/ønske om dette.[182] For detaljer om innholdet i testen, se faktaboks 13.

### Faktaboks 6 Phishingtesten

Riksrevisjonens phishiingtest ble utformet som en e-post med en lenke. Det ble registrert hvor mange som klikket på denne. De som klikket på lenken ble sendt videre til et skjema der de ble bedt om å oppgi informasjon, for å angi henholdsvis behov for parkeringsplass eller interesse for gratis PC. De ble også gitt mulighet til å laste ned et parkeringskart eller informasjon om PCene. De som prøvde å laste ned eksternt innhold fikk en feilmelding.

E-posten var med hensikt konstruert slik at den ansatte kunne oppdage at den var falsk. Blant annet ville mottaker ved å holde musepekeren over lenken kunne se at adressen var gal, og avsenderen var heller ikke en reell ansatt.

Sykehusansatte benytter e-post på ulik måte og i varierende grad. Noen sykehusansatte benytter ikke e-post i det hele tatt, som for eksempel enkelte ansatte i avdeling for medisinsk service. For andre ansatte, som ledere, og medarbeiderne i økonomiavdelinger, er e-post et sentralt verktøy i arbeidshverdagen.

Hvor mange som lar seg lure av phishing-tester, er avhengig av flere forhold - blant annet hvor sofistikerte e-postene er, karakteristika ved mottakers «hverdag» (travelhet, skjermeksponering etc.), om testen er varslet på forhånd, og i hvilken grad virksomheten nylig har gjennomført tiltak for å øke de ansattes kunnskap og oppmerksomhet.

Hvorvidt et angrep lykkes avhenger også av hvilke sikkerhetstiltak som er iverksatt. Alle helseregionene har spamfiltre og verktøy som skal avsløre og stanse falske e-poster og reklame. I tilllegg har helsenettet egne brannmurer.

Resultatene av testen viser at mange ansatte med stor sannsynlighet vil klikke på lenker i phishing-eposter (se tabell 11). Phishing-epost er en vanlig metode for angripere som ønsker å etablere et innledende fotfeste i en virksomhets IKT-systemer. I hvilken grad dette gir innpass i sykehusets systemer avhenger blant annet av hvilke tilganger PCens bruker har, og av tekniske sikkerhetstiltak. Testen omfattet ikke kontroll med tekniske tiltak som kan bidra til å stoppe slike e-poster før de kommer fram til de ansatte, eller hindrer at enkelte typer filer lastes ned.

### Tabell 2 Andel ansatte som responderte på falsk e-post

| Helseforetak | Utsendte e-poster | Klikket på lenke | Ga opplysninger | Lastet ned fil |
|---|---|---|---|---|
| [redacted] | 475 | 246 (52%) | 162 (34%) | **87 (18%)** |
| [redacted] | 475 | 210 (44%) | 144 (30%) | **87 (18%)** |
| [redacted] | 450 | 174 (39%) | 98 (22%) | **32 (7%)** |
| [redacted] | 450 | 128 (28%) | 97 (22%) | **42 (9%)** |
| [redacted] | 450 | 135 (30%) | 64 (14%) | **29 (6%)** |
| **Totalt** | 2300 | 893 (39 %) | 565 (25 %) | 277 (12 %) |

[182] [redacted]

Kilde: Riksrevisjonens utsendelse av falske e-poster og registrering av respons

Tabellen viser at det totalt var 39 prosent som klikket på lenken i e-posten de mottok. Blant helseforetakene varierte klikkprosenten mellom 52 som høyeste og 28 som laveste. [redacted] hadde den høyeste klikkraten, mens [redacted] hadde den laveste. Totalt 25 prosent av respondentene fylte ut opplysningerog sendte disse inn og 12 prosent lastet ned den eksterne informasjonen, altså kart/informasjon om PCene.

[redacted].[183] [redacted].

Det er viktig at ansatte rapporterer om mistenkelige e-poster, fordi det kan sette IKT- eller informasjonssikkerhetspersonell på sporet av et eventuelt dataangrep. Ved alle de fem sykehusene opplyste informasjonssikkerhetslederne at enkelte ansatte hadde varslet dem om vår epost. Slik varsling kan være viktig for å avdekke angrepsforsøk.

Fra dybdeintervjuene framkommer det at de ansatte ikke alltid er sikre på hvordan de skal håndtere mistenkelig e-post. Noen sletter slike e-poster umiddelbart, andre tar skjermdump og sender til for eksempel informasjonssikkerhetsleder, mens enkelte melder ifra til regional IKT-leverandør. Flere viser til at det ikke foreligger noen rutine for hvordan slike e-poster skal håndteres, mens andre igjen oppgir at de har dette.

**Mulige årsaker til uheldig sikkerhetsatferd**

Årsakene til uheldig sikkerhetsatferd er sammensatte, og tekniske og organisatoriske forhold spiller inn. Analysen viser at særlig noen forhold knyttet til sikkerhetskultur bidrar til å forklare den uheldige sikkerhetsatferden. Intervjuer med IKT-leverandørene og helseforetakene tyder på at blant annet følgende forhold har betydning:

- **Mangelfull kunnskap om sikker atferd**. Flere opplever at det ikke har vært nok opplæring og oppmerksomhet om falske e-poster og øvrige IKT-farer man kan bli utsatt for. Endel kjenner heller ikke til om det finnes rutiner for hvordan mistenkelig e-post skal håndteres, eller er usikre på om den enkelte ansatte kjenner innholdet i rutinene.

- Når det gjelder lagring av sensitiv informasjon på fellesområder vet mange ansatte ikke forskjell på fellesområder og lokalt område på sin PC. De forstår ikke hvor informasjonen de lagrer havner eller hvem som har tilgang til filområdene. En del er videre usikre på hvordan tilgangssystemet fungerer og hvilke tilganger som bør tildeles. Passordpraksisen tyder på at mange ikke vet hva som kjennetegner et sterkt passord og ikke i tilstrekkelig grad forstår viktigheten av å bruke slike.

- **Tungvinte systemer og andre hindringer** gjør at ansatte lager seg egne snarveier og måter å gjøre ting på, særlig når hverdagen er hektisk. En del oppgir at det tar lang tid å logge seg av og på systemene de benytter, at man kan glemme å logge seg ut om man blir tilkalt til en annen oppgave, og at det derfor kan være enklere å dele tilganger. Det er heller ikke alltid slik at bruker logges automatisk ut etter en tids inaktivitet. Ansatte opplever at det er mange passord å huske på og de skiftes ofte, noe som bidrar til at passordene som velges er svake, og dessuten til dels gjenbrukes.

[183] [redacted]

- **Konflikt med andre hensyn**. Krav til informasjonssikkerhet vil i noen tilfeller måtte vike fordi det kommer i konflikt med andre hensyn, som pasientsikkerhet.

### 6.5.2 Opplæring og bevisstgjøring består hovedsakelig av generelle e-læringskurs og intranettoppslag

#### Opplæring og informasjonsdeling hos IKT-leverandørene

Alle de fire IKT-leverandørene har opplæring av sine ansatte om IKT-sikkerhet. Kjernen i opplæringen er obligatoriske e-læringskurs i informasjonssikkerhet og personvern. Dette er en del av opplæringen av nyansatte. Det varierer hvor ofte disse kursene må gjentas.

I Sykehuspartner HF og Helse Vest IKT er kravet at det skal tas henholdsvis årlig og hvert tredje år. Hemit oppgir at deres kurs framover skal tas årlig, mens Helse Nord IKT ikke har stilt tilsvarende krav.

Opplæringen hos IKT-leverandørene er i noen grad differensiert mellom ulike grupper ansatte/stillingsnivåer. Det gis enkelte steder ytterligere kursing til ledere og/eller til visse typer ansatte, som systemforvaltere, prosjektledere, testere, utviklere og jurister. Helse Nord IKT har hittil benyttet Helse Nord RHF sitt generelle e-læringskurs, men ønsker seg på sikt et kurs som er mer tilpasset deres rolle og ansvar.[184]

Utover e-læringskursene har IKT-leverandørene valgt ulike aktiviteter og arenaer for å lære opp og informere sine ansatte. Eksempler på dette er nyhetsbrev og intranettartikler, sporadisk deltagelse på Nasjonal sikkerhetsmåned, møter der IKT-sikkerhet er temaet og eksterne kurs og konferanser.

#### Opplæring og informasjonsdeling i helseforetakene

Alle helseforetakene, med et par unntak[185] har en form for grunnopplæring av sine ansatte i informasjonssikkerhet. Mange helseforetak praktiserer at nyansatte må signere en sikkerhetsinstruks, datakontrakt eller lignende, som angir hovedreglene de ansatte må forholde seg til. Alle de fire regionale helseforetakene har utviklet et grunnleggende e-læringskurs som kan brukes i helseforetakene. I de fleste helseforetakene er dette kurset obligatorisk, men ikke i alle. Det er også ulike krav til hvor ofte kurset må tas, både mellom helseforetakene i samme region og mellom regionene. Det varierer også både mellom og innad i helseregionene om ledelsen følger opp om e-læringskurset gjennomføres.

Oppfattelsen av hvorvidt e-læringskursene er nyttige varierer. Noen ansatte gir i intervju uttrykk for at kurset var lærerikt og har gitt økt bevissthet. Andre igjen synes nytten er begrenset - at kurset i hovedsak inneholder selvfølgeligheter, tar for lang tid og i for liten grad er praktisk innrettet. Videre viser endel til at det er mange e-læringskurs, som kurs i brannvern, katastrofehåndtering, hygiene, journalsystem, ernæringsscreening osv., som kan gjøre at den ansatte mister oversikten over hva som er gjennomført og i liten grad klarer å ta inn innholdet.

Flere ansatte ønsker også at opplæringen hadde et annet format - en mer interaktiv opplæring med mulighet for å stille spørsmål og diskutere problemstillingene ut ifra egen jobbhverdag.

Utover e-læringskurs er det få faste, jevnlige opplæringstiltak, og det er ingen enhetlig praksis mellom helseforetakene. Opplæring i god atferd og riktig bruk av systemer foregår for øvrig i den enkelte avdeling og enhet, og kvalitet og omfang vil følgelig ha stort spenn. Flere helseforetak har imidlertid noe opplæring før det gis tilgang til pasientjournalsystemer eller i forbindelse med bruk av medisinsk-teknisk utstyr.

Sykehuset Telemark utmerker seg positivt ved at informasjonssikkerhetsleder og personvernombud i mange år har gjennomført klasseromsundervisning med alle nye ansatte. Dette helseforetaket oppgir

[184] Intervju med Helse Nord Ikt HF
[185] [redacted]

også at de i tillegg til generell og overordnet bevisstgjøring, blant annet har fagdager for superbrukere med spesialiserte temaer og egne temamøter i linjen, og i andre fora.

Undersøkelsen viser at opplæringen i informasjonssikkerhet i liten grad er differensiert.[186] Det vil si at det i hovedsak er det samme opplæringstilbudet til alle ansatte, uavhengig av om de er ledere eller medarbeidere, om de er nyansatte, vikarer eller medarbeidere med lengre ansiennitet, om de har mye eller lite befatning med IKT-systemer, om de er særlig utsatt for eksempel svindelforsøk eller håndterer spesielt sensitiv informasjon. Flere av lederne som er intervjuet, både i de regionale og de utvalgte helseforetakene, gir uttrykk for å ha sett behovet for en større differensiering i helseforetakenes opplæringstiltak, men slike opplæringstiltak er i liten grad gjennomført.

**Løpende informasjon om IKT-sikkerhetsforhold,** som aktuelle hendelser og trusler, supplerer den etablerte opplæringen. Av helseforetakenes skriftlige svar går det fram at langt de fleste benytter intranett til informasjonsdeling om IKT-sikkerhet, men omfang og type informasjon varierer. Oppslagene på intranett handler oftest om mulige trusler mot IKT-sikkerhet og aktuelle hendelser, men intranett brukes også til å spre temaartikler og dele løpende IKT-driftsmeldinger. Det er også eksempler på helseforetak som har endret praksis og i liten grad benytter intranettoppslag etter at å ha fått tilbakemeldinger fra de ansatte om at meldinger kom så ofte at de etter hvert ble ignorert.

I hovedsak er det helseforetakets informasjonssikkerhetsleder som står for innholdet i oppslagene, men informasjonen kan også komme fra IKT-leverandøren, gjerne i samarbeid med HelseCert.

Også når det gjelder bruk av e-post og møter som informasjonskanal, varierer praksis blant helseforetakene. E-post benyttes enkelte steder til å sende ut nyhetsbrev og faktaartikler, eller oppsummere møteinformasjon, men som oftest benyttes e-post bare til å varsle ansatte som er en del av beredskapslinja om konkrete IKT-sikkerhetshendelser.

Mangel på gode kommunikasjonsstrategier og -planer antydes av enkelte som en forklaring på svakheter ved sikkerhetskulturen. I [redacted] påpekes det i tillegg at intranettet er gammelt og anses å være lite egnet for å spre informasjon. Flere nevner at det generelt er en utfordring å nå ut med informasjon. Helseforetakene har mange ansatte, de er fordelt på ulike turnuser, og ikke alle er innom intranett og e-post jevnlig.

Å bygge en sterkere sikkerhetskultur fordrer at det jobbes med *atferden*, ikke bare oppmerksomheten, til hver enkelt ansatt i virksomheten. Forskning tyder på at å endre adferd krever innsats over tid, og at det må benyttes en *kombinasjon* av ulike virkemidler. Med andre ord har enkeltstående aktiviteter som interne phishing-e-poster, e-læringskurs, artikler på intranettet og treningssesjoner sannsynligvis begrenset effekt på atferd.[187]

## 6.6 Det gjennomføres risiko- og sårbarhetsanalyser av IKT-løsninger, men de følges ikke opp systematisk

### 6.6.1 Det gjennomføres ROS-analyser ved innføring og endring av helseforetakenes IKT-systemer

Alle regioner har utarbeidet prosedyrer for gjennomføring av risiko- og sårbarhetsanalyser (ROS-analyser)[188] ved innføring og endring av IKT-løsninger.[189] Slike risikovurderinger er svært viktige når IKT-løsninger blir stadig mer integrert, og en endring i ett system kan påvirke informasjonssikkerheten

[186] Skriftlige svar på spørsmål/spørrebrev og intervjudata
[187] https://www.magma.no/nar-ansatte-er-et-mal-for-cyberkriminelle
[188] Risiko- og sårbarhetsanalyser skal beskrive sannsynlighet for at uønskede hendelser oppstår som følger av innføring eller endring av en løsning, mulige konsekvenser dersom disse hendelsene oppstår, og tiltak for å redusere denne risikoen. Analysene omfatter ikke bare den tekniske sikkerheten, men også de tilhørende prosessene. Det kan dreie seg om krav til passord, pålogging, tilganger og lagring av opplysninger.
[189] Helse Midt-Norge: Risikovurdering av IT-sikkerhet. Helse Sør-Øst: Risikovurdering ved nye og endrede IKT-løsninger og databehandlinger. Helse Nord: «Risikovurdering og risikostyring». Helse Vest IKT HF M05 - Plan for risikovurdering der det anbefales at ROS-analysene oppdateres hvert tredje år.

i andre systemer. Enhver endring kan medføre «nedetid» som følger av at systemer ikke støtter endringen som gjøres. Dette kan innebære manglende tilgjengelighet til systemer og/eller informasjon.

En gjennomgang av 430 konkrete ROS-analyser tilsendt fra helseregionene,[190] samt intervjuer, viser at det er de regionale IKT-leverandørene som gjennomfører brorparten av ROS-analysene. De gjennomfører slike for felles IKT-løsninger i regionen, og bistår også i varierende grad helseforetakene i tilfeller der lokale IKT-løsninger skal innføres eller endres.

Helseforetakene opplyser at det ikke er gjennomført risiko- og sårbarhetsanalyser for alle lokale behandlingsaktiviteter (IKT-løsninger, medisinsk teknisk utstyr, registre og prosjekter), slik det i utgangspunktet skal etter personvernlovgivningen og prosedyrer i helseregionenes styringssystemer for informasjonssikkerhet og personvern.[191] Flere helseforetak skriver at de jobber med å få oversikt over gjennomførte risikoanalyser i forbindelse med arbeid med protokoll over behandlingsaktiviteter (se kapittel 6.3.2).[192]

Selv om det fortsatt er slik at noe utstyr og systemer ikke er risikovurdert[193] har det vært en klar forbedring på området siden Riksrevisjonens foregående undersøkelser, hvor det var gjennomført få ROS-analyser.[194] De regionale IKT-leverandørene har de siste årene forbedret egen metodikk for gjennomføring av ROS-analyser, og satt av dedikerte ressurser til arbeid med slike analyser.

Av de 430 ROS-analysene av innføring eller endring av IKT-systemer som helseforetak og regionale IKT-leverandører har oversendt, er det gjort en nærmere gjennomgang av et tilfeldig utvalg på 10 prosent (43 ROS-analyser).[195] Det er mange gjennomarbeidede risikoanalyser, hvor det klart framkommer vurdering av risikonivå (lav, middels eller høy risiko), sannsynlighet og konsekvens, konkrete utbedringstiltak, hvem som har ansvaret for tiltakene, og tidsfrist for når disse skal gjennomføres.

Gjennomgangen viser imidlertid at en del av dem mangler nærmere omtale av tiltakene som skal iverksettes, hvem som har ansvaret for å gjennomføre tiltakene, og/eller frist for når tiltaket skal være gjennomført.[196] Informasjonssikkerhetsledere ved helseforetak og regionale IKT-leverandører i alle regioner peker på at det ikke alltid er avklart hvem som skal følge opp tiltakene.

Flere informasjonssikkerhetsledere i helseforetakene peker på at de ikke har oversikt over hvordan tiltak helseforetakene har ansvar for har blitt fulgt opp ute i klinikker og avdelinger. Informasjonssikkerhetsledere oppgir at de heller ikke får beskjed fra regional IKT-leverandør om hvordan tiltakene sistnevnte har ansvar for er fulgt opp.

**Ressursbruk på ROS-analyser**

Sykehusinnkjøp og flere av informantene ved helseforetak og regionale IKT-leverandører peker på at gjenbruk av ROS-analyser kan være ressursbesparende, men at dette i svært liten grad gjøres − hverken innad i regionene eller på tvers av regioner.[197] Ett estimat er at en enkel ROS-vurdering av IKT-systemer og -utstyr i spesialisthelsetjenesten tar ca. 150-200 timer.[198]

Det gjøres ofte like omfattende ROS-analyser selv om systemet eller utstyret allerede er tatt i bruk ved andre helseforetak. Informanter viser til konkrete tilfeller der dette har blitt gjort selv om et helseforetak kjøpte identisk medisinsk teknisk utstyr som de allerede hadde.

---

[190] Det framgår av risikovurderingene hvem som har utarbeidet dem.
[191] Det er også obligatorisk med personvernkonsekvensvurdering når det er sannsynlig at behandlingen vil medføre en høy risiko for fysiske personers rettigheter og friheter. Dette er også omtalt i styringssystemene til Helse Sør-Øst, Helse Nord og Helse Vest. og Hemit
[192] For eksempel oppgir Sykehuset Innlandet og Sykehuset Vestfold dette. Sykehuset i Vestfold HF skriver i svarbrev at de lager en utvidet protokoll med blant annet oversikt over løsningsdesign og risikovurderinger.
[193] En del systemer og utstyr risikovurderes i etterkant av anskaffelsen i det de skal kobles til nettverket
[194] Dokument 3:2 (2014-2015) Helseforetakenes beredskap innen ikt, vann og strøm og Dokument 3:2 (2015-2016) Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr.
[195] Alle helseregionene er representert i utvalget.
[196] Eks: Helse Nord felles risikovurdering av Funksjonell bruk av ComPACS. Feltene for ansvarlig og frist er ikke fylt ut. Ref Finnmarksykehuset HF
[197] [redacted]
[198] https://www.dagensmedisin.no/artikler/2020/05/06/sunnaas-har-utviklet-losning-som-automatiserer-risikovurderinger/

I Helse Sør-Øst framhevet informasjonssikkerhetslederne i de utvalgte helseforetakene at dette kunne være et forsinkende ledd for dem. Sykehuspartner gjennomfører risikoanalyser på bestilling fra helseforetakene. Grunnet manglende kapasitet kan helseforetakene i noen tilfeller måtte vente opptil et år på få risikovurdert utstyr som er klart til å settes i drift.[199]

### 6.6.2 Ulike vurderinger av risiko mellom helseforetakene

I henhold til personvernlovgivningen må alle dataansvarlige ta stilling til og eventuelt akseptere risikoen i IKT-løsninger, og i informasjonsbehandlingsaktiviteter for øvrig.

Informanter i alle helseregionene påpeker at helseforetakene har ulike vurderinger av risiko på informasjonssikkerhetsområdet.[200] Det gjøres dermed ulike vurderinger av risiko for samme type systemer og utstyr.

Sykehusinnkjøp påpeker at dette kan føre til at det tar uforholdsmessig lang tid å oppnå konsensus om en kravspesifikasjon. For de regionale- og lokale anskaffelsene medfører en ulik tolkning også at leverandørene kan oppfylle kravspesifikasjon i helseforetak i én region, mens de ikke gjør det i helseforetak i en annen region. Det kan også gjøres ulike vurderinger/tolkinger av kravspesifikasjonen mellom helseforetak innen samme region[201]. Ulike vurderinger kan også skyldes lokale forhold og hvor store deler av IKT-systemet/løsningen som er tatt i bruk.

Hvis forutsetninger for bruk av utstyr og systemer er ulike, kan det imidlertid være gode grunner for at helseforetak foretar ulike risikovurderinger. F. eks. vil det være forskjeller mellom et stort sykehus, og et lite sykehus som gjør at det må gjøres lokale vurderinger.

I Helse Sør-Øst har det spesielt vært en forskjell mellom hva Oslo Universitetssykehus HF (OUS) og de andre helseforetakene har vært villige til å akseptere av risiko[202]. En medvirkende årsak til at det kan være vanskeligere å oppnå en felles risikoforståelse i regionen, er at OUS i hovedsak har egen infrastruktur og eget domene, og dermed ikke er del av den regionale plattformen SIKT.[203] Av styremøte i Sykehuspartner HF 1. april 2020 framgår det at ulike oppfatninger om sikkerhetsnivået internt i regionen og de tre sikkerhetsdomenene fram til nå har vært til hinder for tjenesteleveranser og informasjonsdeling i regionen.[204]

## Faktaboks 7 Eksempler på ulik vurdering av risiko i helseforetakene

**Anskaffelse av felles EKG-løsning** [redacted]

I [redacted] ble det diskusjoner om risiko under innføringen av et felles system for innsamling, analyse, arkivering og deling av informasjon fra EKG-utstyr (elektro-kardiogram) i 2017. Det var enighet i alle helseforetakene i regionen om at informasjonssikkerheten i løsningen ikke var tilfredsstillende, og at det var behov for å iverksette ytterligere tiltak slik at tilfredsstillende informasjonssikkerhet kunne oppnås.

Helseforetakene hadde imidlertid ulik vurdering av hvilke konsekvens en eventuell stopp av systemet kunne medføre. Flere av helseforetakene vurderte at pasientsikkerhetskonsekvensen ved å stanse løsningen var høyere enn risikoen ved at den ble opprettholdt, under forutsetning at tiltak ble iverksatt for å håndtere avdekkede risikoer.

---

[199] [redacted]

[200] Intervju med adm dir Helse Sør-Øst 24. juni 2019, intervju med adm dir Helse Nord 9 september 2019, intervju med adm dir Helse Midt-Norge 15. november 2019, intervju med adm dir Helse Vest 6. januar 2020, intervju med adm.dir Helse Vest IKT AS 17. januar 2020

[201] Intervju med Sykehusinnkjøp HF

[202] Intervju med adm.dir. Helse Sør-Øst

[203] Av styremøte i Sykehuspartner HF 1. april 2020, styresak 27-2020, framgår det at Helse Sør-Øst har tre plattformer; OUS, AHUS og SIKT, med to sikkerhetssoner; OUS og SIKT. Disse tre plattformene er ikke standardiserte, og det uttales at det har vært gjennomført omfattende tiltak for å bedre informasjonssikkerheten på plattformene, i hovedsak gjennom programmet ISOP.

[204] Styresak 027-2020 Sykehuspartner HF

Kun ett av helseforetakene ønsket å stanse løsningen. Ulik vurdering av konsekvensen ved å stoppe løsningen hadde blant annet sammenheng med ulik utbredelse og bruk av løsningen for innsamling, analyse, arkivering og deling av EKG.[205]

**Nasjonal anskaffelse av insulinpumper til barn**

I [redacted] vises det til den nasjonale anskaffelsen av insulinpumper til barn, som ble forsinket i over to år grunnet uavklarte spørsmål tilknyttet informasjonssikkerhet og personvern.

Da man skulle ta i bruk løsningen ble det stilt spørsmål om hvorvidt hvert enkelt HF skulle gjøre egne risikovurderinger. Det var samtidig uklart hvem som hadde ansvar for å sikre informasjonen som skulle lagres i skytjenesten til den valgte insulinpumpeløsningen, og det ble stilt spørsmål om hvem som hadde ansvaret for de krav som gikk utover den akseptable risikoen som helseforetaket har satt.

Et av helseforetakene ønsket først ikke å ta i bruk løsningen, men snudde etter oppfordring fra [redacted] og press fra pasientgruppene. Helseforetaket la ved et informasjonsskriv ved utlevering av pumpene der de gjorde oppmerksom på at løsningen/utstyret ikke var risikovurdert, men at helseforetaket vurderte hensynet til pasientsikkerheten og behandlingskvaliteten tyngre enn hensynet til informasjonssikkerheten.

Kilder:
[redacted]

Tre av helseregionene har i den senere tid sett behov for nye tiltak for å skape en felles forståelse mellom helseforetakene av hva som skal være kriteriene for å godkjenne sikkerheten i løsninger.[206]

### 6.6.3 Uklarheter om beslutningslinjene for akseptering av risiko i IKT-løsninger og utstyr

De fleste ROS-analysene som gjennomføres ved endring eller innføring av IKT-løsninger og -utstyr, blir gjenstand for felles behandling og diskusjon i regionale sikkerhetsutvalg/råd (se faktaboks ovenfor) hvor de regionale IKT-leverandørene og helseforetakene er representert. Utvalgene tilstreber å oppnå konsensus om en anbefaling for den enkelte risikovurdering. Informasjonssikkerhetslederne i sikkerhetsutvalgene skal ikke ta avgjørelser om hva slags risiko helseforetakene skal akseptere; de er avhengige av at beslutningen tas av ledere på riktig nivå i virksomheten.[207]

Flere av informasjonssikkerhetsledere i helseforetakene og hos IKT-leverandørene gir uttrykk for at de med et særlig ansvar for IKT-løsningene internt i helseforetakene ikke alltid er bevisst sitt ansvar. Flere informanter nevner at mange ikke vet hva det innebærer å være systemeier, som for eksempel det å vurdere risikoen i og rundt systemet.[208] De har ofte heller ikke nok kunnskap om risikoen. Videre nevnes det at det i mange tilfeller er uklart hvem som skal akseptere risikoen.

Uklarheter i beslutningslinjer er problemstillinger som har vært kjent over lengre tid, og som blant annet ble belyst i Direktoratet for eHelses rapport om *Informasjonssikkerhet ved bruk av private leverandører*.[209] Denne rapporten ble gitt ut i kjølvannet av «outsourcing-saken» i Helse Sør-Øst, der ni helseforetak fikk bot fra Datatilsynet.[210] Datatilsynet mente at de dataansvarlige hverken hadde hatt

[205] [redacted]

[206] Helse Sør-Øst RHF opplyser at regionen har hatt en felles gjennomgang av hva som skal være risikoakseptkriteriene på informasjonssikkerhetsområdet og konsensus i foretaksgruppen om hva risikoakseptkriteriene skal være. Det er i den forbindelse utarbeidet et eget dokument som beskriver dette.
I Helse Midt-Norge har man hatt et felles sett med risikoakseptkriterier, Risikoakseptkriteriene skal gjennomgås i forbindelse med oppdatering av styringssystemet, for å sikre at regionen er omforente om hva som er kriteriene og at alle har et eierskap til disse. Helse Nord har innført et møtepunkt for de dataansvarlige. Der helseforetakene eventuelt er uenige om akseptabelt risikonivå, skal problemstillingen løftes opp til et møte mellom de fire sykehusdirektørene i regionen.

[207] Det skal i utgangspunktet være oppnevnt en ansvarlig for behandlingsaktiviteter (inkludert IKT-løsninger) internt ved helseforetakene − en dataansvarlig eller systemeier.

[208] Flere av informasjonssikkerhetslederne har vært inne på dette. DIFI definerer en systemeier som en leder som er ansvarlig for å utvikle, forvalte og drifte et informasjonssystem. Dette vil ofte i større eller noen grad være basert på IKT. Systemeier benytter ofte en utpekt systemforvalter som operativt ansvarlig for de oppgaver systemeier har ansvaret for. En risikoeier vil normalt være systemeier for de informasjonssystem som kun benyttes innen eget ansvarsområde.

[209] Datert 1. desember 2017

[210] Styret i Helse Sør-Øst RHF besluttet å inngå kontrakt med en ekstern partner for å gjennomføre IKT-infrastrukturmodernisering - Styremøte 8. september 2016 (sak 069-2016)

god nok oversikt over risikobildet eller god nok kontroll med behandling av opplysninger.[211] Tre av helseregionene har sett behov for nye tiltak de siste årene for å bedre beslutningsprosessene gjennom bedre forankring i helseforetakene og på et høyere ledelsesnivå.[212] Mens i Helse Vest har konfliktsaker blitt løftet opp til det regionale direktørmøtet hvor alle direktørene fra helseforetakene møtes.

## 6.7 Økt ledelsesoppmerksomhet, men mangelfullt informasjonsgrunnlag

### 6.7.1 Informasjonssikkerhet er tema for styrene i de regionale helseforetakene og helseforetakene

En gjennomgang av styremøtereferater fra de fire helseregionene viser at informasjonssikkerhet har vært tema i styremøter i helseforetak og regionale helseforetak i perioden 2017 til 2019. Sakene knytter seg som regel til innføring av nye krav eller konkrete hendelser. Gjennomgangen av styredokumentene viser at det særlig har vært tre hendelser (se faktaboks 15) som har ført til at informasjonssikkerhet har blitt satt på agendaen.

**Faktaboks 8 Tre aktuelle hendelser**

- «Outsourcingssaken» i Helse Sør-Øst våren 2017 der ni helseforetak fikk bot av Datatilsynet for å ha forsømt sitt dataansvar. Hendelsen har ført til økt oppmerksomhet i helseforetakene om ansvaret de har for informasjonssikkerheten som dataansvarlige.
- Innføring av EUs personvernforordning (GDPR) i 2017-2018, som har stilt flere konkrete krav til informasjonssikkerhetsarbeidet i spesialisthelsetjenesten. Dette er en av årsakene til at regionene har gjennomført større oppdateringer av de regionale styringssystemene.
- Dataangrepet på Helse Sør-Øst i januar 2018. Angrep mot andre virksomheter, som Norsk Hydro ASA, har også vært tema på flere styremøter.

Større prosjekter som helt eller delvis har som formål å bedre informasjonssikkerheten (STIM, ASK og ISOP i Helse Sør-Øst, HIS i Helse Nord), er også behandlet i styremøter i de regionene der dette er gjennomført.

De administrerende direktørene som er intervjuet i helseregionene, gir alle uttrykk for at ledelsen og styrene i økende grad har blitt opptatt av informasjonssikkerhet. Dette skyldes delvis de tre ovennevnte sakene. I tillegg viser de til at det gradvis har kommet større forventninger og mer spesifikke krav «ovenfra». Helse- og omsorgsdepartementet har stilt flere krav til informasjonssikkerhetsarbeidet til de regionale helseforetakene, som igjen har stilt flere krav til helseforetakene og de regionale IKT-leverandørene.[213]

### 6.7.2 Det varierer hvorvidt informasjonssikkerhet er tema i «ledelsens gjennomgang»

Ledelsens gjennomgang er et sentralt verktøy for helseforetakene, de regionale IKT-leverandørene og de regionale helseforetakene sin virksomhetsstyring (se faktaboks 16). Det er flere områder som skal gjennomgås årlig, og informasjonssikkerhet er ett av disse.

[211] Helseforetakene fikk bøtene blant annet gitt på grunnlag av at helseforetakene bl.a. ikke hadde foretatt tilstrekkelig risikovurderinger før beslutning om it-tjenestene for foretakene skulle outsources, at ledelsen i foretakene ikke var tilstrekkelig involvert i beslutninger som ble fattet og at personopplysningene ikke var tilstrekkelig sikret - Datatilsynet Varsel om vedtak 24. oktober 2017 [redacted]
[212] Intervju med de fire regionale helseforetakene
[213] Det er også andre forhold som har hatt betydning for at informasjonssikkerhetstemaet har kommet mer på dagsordenen. Gode samarbeidsfora og rekruttering av enkeltansatte med særskilt kompetanse og engasjement for emnet i sentrale posisjoner er eksempler på slike forhold.

## Faktaboks 9 Ledelsens gjennomgang

Virksomhetens øverste ledelse skal gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst én gang i året. Ledelsen skal blant annet gjennomgå risikovurderinger, revisjoner og oversikter over rapporterte avvik. Dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar.

Ledelsens gjennomgang er som oftest grunnlag for rapporteringen i helseforetakenes årlige meldinger, som er viktig styringsinformasjon for de regionale helseforetakene.

Kilde: Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenestene § 8 og Norm for informasjonssikkerhet versjon 6.0

Ledelsens gjennomgang for samtlige helseforetak er gjennomgått i undersøkelsen. Alle helseforetakene har presisert i sine styringssystemer for informasjonssikkerhet og personvern at informasjonssikkerhetsområdet skal gjennomgås årlig, i tråd med kravet i Normen. De fleste helseforetakene gjennomfører ledelsens gjennomgang én til to ganger i året.

Helseforetakene gjennomfører som regel en felles gjennomgang for mange virksomhetsområder, der informasjonssikkerhet og personvern er ett av flere obligatoriske områder ledelsen skal behandle. En analyse av helseforetakenes gjennomganger for 2017 og 2018 viser at enkelte helseforetak ikke har hatt informasjonssikkerhet som tema disse årene.[214] Helseforetakene i Helse Nord, samt Helse Bergen HF, skiller seg ut her ved at de har en egen ledelsens gjennomgang viet til temaet informasjonssikkerhet.

Det er varierende hvor mye informasjon ledelsen får presentert i gjennomgangene, når de skal vurdere sikkerhetstilstanden i helseforetakene. Helse Bergen HF har de mest omfattende gjennomgangene, og tar opp temaer som sikkerhetsmål og sikkerhetsstrategi, oversikt over behandling av helse- og personopplysninger, sikkerhetsrevisjoner og tilsyn, risikovurderinger, avvik (både statistikk og enkeltavvik), opplæring, beredskap og trusselbilde.[215] Sykehuset Østfold HF har også detaljerte gjennomganger med faste punkter som gjennomgås. Ved de fleste andre helseforetakene gjennomgås hovedsakelig temaer knyttet til aktuelle hendelser eller innføring av GDPR. Det vil si at ledelsen ikke nødvendigvis får informasjon om sikkerhetstilstanden i eget foretak.

Tilsendt dokumentasjon viser at alle de regionale IKT-leverandørene har behandlet informasjonssikkerhet i ledelsens gjennomgang, og at temaet behandles mer inngående enn i helseforetakene. Ledere i disse virksomhetene får også løpende rapportering om sikkerhetstilstanden.

### 6.7.3 Sammenstilling av risiko på virksomhetsnivå blir ikke gjennomført

For at ledelsen i virksomhetene og helseregionene skal kunne få et godt bilde av sikkerhetstilstanden og treffe informerte beslutninger om hvilke tiltak som burde prioriteres, er det et krav å ha oversikt over områder i virksomheten hvor det er risiko for svikt eller mangel på etterlevelse av myndighetskrav.[216] Undersøkelsen viser oppsummert at foretakene får en del informasjon om risiko, men dette blir ikke sammenstilt i overordnet risikoanalyse på virksomhetsnivå.

En gjennomgang av tilsendt dokumentasjon viser at det sjelden gjennomføres risiko- og sårbarhetsanalyser (ROS) av sikkerheten i selve IKT-infrastrukturen, eller av andre informasjonssikkerhetsrelaterte temaer på mer overordnet nivå.[217] Risikoanalyser som omtaler risiko for de avvik som den tekniske revisjonen avdekket, foreligger i liten grad. For eksempel har ingen av de mottatte risikoanalysene en omtale av risikoen for ekstern inntrenging ved fysisk oppmøte i et helseforetak. Det er heller ikke utarbeidet ROS-analyser som sammenstiller eksisterende kunnskap

[214] Sykehuset i Vestfold HF gjennomførte ikke ledelsens gjennomgang i 2018. Helse Møre og Romsdal HF, Ahus HF og Helse Førde HF gjennomførte ledelsens gjennomgang begge år, uten at informasjonssikkerhet var tema. Ved Vestre Viken HF og St. Olavs hospital HF var informasjonssikkerhet tema i 2017, men ikke i 2018.
[215] Helse Bergen HF Ledelsens årlige gjennomgang 2018 Informasjonssikkerhet og personvern
[216] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 6
[217] Helseforetak og regionale IKT-leverandører har oversendt 430 konkrete risikovurderinger; samtlige gjelder endring eller innføring av IKT-løsninger eller andre informasjonsbehandlingsaktiviteter. Mer overordnede analyser er etterspurt ved intervjuer i dybdeundersøkelsen i alle de fire helseregionene.

om kjente risikoer på informasjonssikkerhetsområdet i den enkelte virksomhet eller i regionene som helhet.

Det er gjennomført enkelte andre analyser som kan gi et overordnet bilde av risikoen på området:

- Helse Nord RHF har utarbeidet en regional handlingsplan på informasjonssikkerhetsområdet, der ulike overordnede risikoforhold trekkes fram (sikkerhetskultur, tilgangsstyring og medisinsk teknisk utstyr).[218]
- I Helse Sør-Øst gjennomførte Sykehuspartner HF en overordnet risikoanalyse av tjenesteutsetting av infrastrukturen i 2018.
- Helse Midt-Norge RHF har utarbeidet en egen «ti på topp»-liste over risikoer, hvor én av risikoene er informasjonssikkerhet. Det er også gjennomført mange risikovurderinger i forbindelse med innføring av Helseplattformen,[219] inkludert av infrastrukturen som Helseplattformen skal inngå i.
- Helse Vest RHF opplyser at det ikke er laget noen overordnet risikovurdering. Regionen opplyser at å følge det ytre trusselbildet er Helse Vest IKTs ansvar/oppgave[220]. Helse Vest IKT opplyser at administrerende direktør i Helse Vest RHF, som styreleder i HV IKT, er godt orientert om risikoene på dette området.[221]
- Alle helseregionene har i tillegg bidratt til rapportene fra Helsedirektoratet: Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren - rapport IS 2635 av 26. juni 2017 og overordnet risiko- og sårbarhetsvurderinger for nasjonal beredskap i helse- og omsorgssektoren av 21. juni 2019.[222]

Tiltak som regionene har satt i gang, viser imidlertid at de også er klar over flere av risikoene selv om de ikke er beskrevet på et mer overordnet nivå. (se kapittel 6.5.1). De regionale IKT-leverandørene har også mye informasjon om sikkerhetstilstanden i regionen; bl.a. får de informasjon gjennom HelseCerts inntrengingstester,[223] og sårbarhetsskanning de selv gjennomfører. De regionale IKT-leverandørene har også felles møter med HelseCert, der det utveksles informasjon på tvers av regionene.[224]

Informasjonssikkerhetslederne som er intervjuet, oppgir at de regionale IKT-leverandørene er en viktig kilde til informasjon om sikkerhetstilstanden i helseforetakene. De påpeker at helseforetakene regelmessig mottar informasjon bl.a. om avdekkede sårbarheter på eget utstyr og egne systemer, trusler og hendelser som har vært i regionen, avvik[225] som er fanget opp av regional IKT-leverandør, samt resultater av inntrengingstester.[226] Det utveksles stadig mer informasjon,[227] men flere helseforetak gir uttrykk for at de trenger mer informasjon for å kunne vurdere sikkerhetstilstanden på en tilfredsstillende måte.[228]

Det er ikke nødvendigvis slik at all relevant informasjon om sikkerhetstilstanden tilflyter ledelsen i det enkelte helseforetak. For eksempel vil ikke ledelsen i helseforetakene nødvendigvis ha informasjon om sikkerhetstilstanden hos sin IKT-leverandør. Det er imidlertid eksempler på at ledelsen hos IKT-leverandørene har informert styret og ledelsen i helseforetakene og RHFene om sikkerhetstilstanden

---

[218] I etterkant av Riksrevisjonens tekniske kontroller ba styret i Helse Nord IKT HF administrasjonen om å legge fram en beskrivelse av det helhetlige risikobildet for informasjonssikkerhet for styret.Styremøte i Helse Nord IKT HF, styresak 058-2019. Dette ble gjentatt i styresak 036-2020 (22. juni 2020).
[219] Intervju med administrerende direktør Helse Midt-Norge RHF
[220] Intervju med Helse Vest RHF.
[221] Intervju med Helse Vest IKT
[222] Det kom ikke klart fram i intervjuet med Direktoratet fo e-helse om helseregionene også har bidratt til Direktoratet for e-hHelses rapport Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren fra juni 2019, som sammenstiller kunnskap om kjente risikoer.

[223] Informasjonssikkerhetsledere i helseforetakene oppgir også at de mottar informasjon fra HelseCert gjennom nyhetsbrev.
[224] Intervju med leder av HelseCert 29. mai 2020.
[225] Avvikene kan handle om feil på IKT-systemer internt ved regional IKT-leverandør. Kundesentrene mottar imidlertid også henvendelser fra helsepersonell, som kan registreres som sikkerhetsavvik.
[226] HelseCert gjennomfører inntrengingstester mot helseregionene. I tillegg gjennomfører alle helseregionene inntrengningstester av nye systemer og utstyr, her leier man gjerne inn private leverandører.
[227] Dette skjer gjennom de regionale sikkerhetsutvalgene. I Helse Nord er det i tillegg nylig opprettet et forum for «sikkerhetskoordinatorer» i helseforetak og regional IKT-leverandør. Disse har månedlige møter, der Helse Nord IKT HF presenterer statusoppdateringer på sårbarheter, trusler og hendelser som har vært i regionen. Hovedmålet med dette å koordinere arbeidet med sårbarheter som Helse Nord IKT har avdekket på utstyr og systemer de ikke har driftsansvar for.
[228] Helseforetakene skriver likevel i svar på spørrebrev at de ønsker mer informasjon fra Sykehuspartner om sistnevntes oppfølging av sårbarhetene, og om oppfølging av risikoreduserende tiltak som er iverksatt. (Sykehuset Innlandet HF, Sykehuset Vestfold HF, Sunnaas sykehus HF, Sykehuset i Østfold HF, Vestre Viken HF, Ahus)

fra deres perspektiv. Særlig i Helse Vest mottar ledelsen og styrene mye informasjon på denne måten.[229] Styrene og ledelsen i Helse Sør-Øst mottok mye informasjon i etterkant av «Outsourcing-saken» i 2017/2018 og dataangrepet i 2018. Direktoratet for e-helse uttaler i intervju at de har observert at det gjøres mange risikoanalyser av enkeltsystemer og utstyr i helseregionene, men at det i mindre grad lages oversikter over risiko på området. Erfaringen fra helseforetak er at det blir mange små risikovurderinger med mange tiltak, og man mister oversikten.[230]

### 6.7.4 Få sikkerhetsrevisjoner, kontroller og sikkerhetsøvelser

En viktig kilde for å si noe om sikkerhetstilstanden i helseforetakene er sikkerhetsrevisjoner[231] og andre kontroller[232]. Alle de fire IKT-leverandørene har gjennomført sikkerhetsrevisjoner og sikkerhetsøvelser[233] med tema informasjonssikkerhet i 2017 og 2018. Det er ikke innhentet informasjon om det er gjennomført revisjoner og sikkerhetsøvelser i 2019 og hittil i 2020.

Imidlertid er det ingen av *de regionale IKT-leverandørene* som har gjennomført den type teknisk kontroll som er utført i denne undersøkelsen.
[redacted].[234] Dette gjør at ledelsen ikke har fått et helhetlig bilde av sikkerhetstilstanden.

Innhentet informasjon fra samtlige helseforetak viser at det gjennomføres få revisjoner og sikkerhetsøvelser der informasjonssikkerhet er tema. De sikkerhetsrevisjonene og sikkerhetsøvelsene som er gjennomført varierer også i omfang og innhold. Enkelte helseforetak har imidlertid gjennomført flere typer revisjoner om informasjonssikkerhet, f. eks. Sykehuset Østfold HF og Sykehuset Telemark HF. Når det gjelder sikkerhetsøvelser er det få eksempler på at det er øvet på dataangrep som scenario.[235]

Med unntak av gjennomførte inntrengingstester fra HelseCerts side og enkelte revisjoner av tilgangsstyring[236] er det ikke gjennomført sikkerhetsrevisjoner eller kontrolltiltak som direkte berører de avvik Riksrevisjonen har avdekket gjennom denne revisjonen (se kapittel 4 og 5).

**Tabell 3 Helseforetak som har gjennomført sikkerhetsrevisjoner og -øvelser i 2017 og 2018**

| Kontroll | Helse Sør-Øst | Helse Nord | Helse Midt-Norge | Helse Vest |
|---|---|---|---|---|
| Helseforetak som har gjennomført sikkerhetsrevisjoner i 2017 | 3 av 9 | 4 av 4[237] | Ingen | 1 av 4 |
| Helseforetak som har gjennomført sikkerhetsøvelser i 2018 | 2 av 9 | Ingen | Ingen | 1 av 4 |

[229] I Helse Vest har administrerende direktør i Helse Vest IKT AS orientert alle styrene i Helse Vest om dette. De administrerende direktørene i RHFet og HFene i regionen sitter også i styret i Helse Vest IKT, og mottar informasjon om sikkerhetstilstanden i styremøter. Hvert år legges det fram en sak for styret i Helse Vest IKT HF, der risikoen knyttet til IKT-infrastrukturen legges fram. Presentasjonen sendes i etterkant til alle HF i Helse Vest.
[230] Intervju med direktoratet for e-helse
[231] Dette kan være revisjoner initiert av IKT-avdelingen (innleid bistand), internrevisjonen i foretaket eller konsernrevisjonen i regionen, ekstern revisor eller Riksrevisjonen
[232] Kontroller initiert av ledelsen i helseforetaket (internkontrolltiltak), fra tilsynsmyndigheter som Datatilsynet og Statens helsetilsyn. Det kan også være tester utført av HelseCert
[233] Anbefalinger i rapport fra Direktoratet for e-helse, Nasjonal e-helsemonitor - informasjonssikkerhet i helse og omsorgssektoren 2019: «Helseforetakene, i samarbeid med de regionale helseforetakene og IKT-tjenesteleverandør, bør gjennomføre minst én årlig øvelse i informasjonssikkerhet.» «Regionene bør søke å samarbeide om et felles rullerende øvelsesopplegg for informasjonssikkerhet, for å trekke ut felles lærdommer, beste praksis og løfte de som ligger etter i beredskapsplanlegging og -øvelser.»
[234] Intervju med HelseCert 29.mai 2020.
[235] Dataangrep var scenariet i øvelsen i 2019 for de administrerende direktører ved helseforetakene i Helse Sør-Øst. OUS gjennomførte en «skrivebordsøvelse» om cyberangrep i 2016 hvor ulike relevante scenarier ble vurdert. Finnmarksykehuset HF har gjennomført en skrivebordsøvelse hvor scenariet var at datasystemene ved Kirkenes sykehus måtte tas ned på grunn av «jamming» fra grensen mot Russland. (Jamming» er betegnelsen på en måte å ødelegge et signal på. Rett og slett å sende ut et signal som overskygger et annet signal. På denne måten kan kommunikasjons- og navigasjonssystemer bli slått ut, og miste sin funksjon.)
[236] Sykehuspartner HF - Revisjon av tilgangsstyring og Revisjon av tilgang til admin servere
[237] To av revisjonene har informasjonssikkerhet som en mindre del av selve revisjonen

Kilde: Helseforetakenes svar til Riksrevisjonen

Som det framgår av tabellen, har ingen av helseforetakene i Helse Midt-Norge gjennomført revisjoner eller sikkerhetsøvelser knyttet til informasjonssikkerhet i perioden.

Helseforetakene har også gjennom tjeneste- og databehandleravtaler hjemmel til å foreta egne kontroller eller benytte en tredjepart til å kontrollere informasjonssikkerheten hos sine leverandører. Selv om helseforetakene mottar mye informasjon fra de regionale IKT-leverandørene, er det kun to helseforetak som har gjennomført kontroller mot databehandler,[238] engasjert en tredjepart for kontroll eller bedt om kopi av kontroller som er gjort av eksterne revisorer rettet mot databehandler/ leverandøren.

Videre er det få helseforetak eller regionale IKT-leverandører som oppgir i svar på spørrebrev at de har gjennomført systematiske undersøkelser av sikkerhetskulturen i sin virksomhet. Unntakene er Sykehuset Østfold HF og Oslo Universitetssykehus HF, som gjennomfører spørreundersøkelser til de ansatte annethvert år, for å kartlegge informasjonssikkerhetskulturen i virksomhetene.[239] [redacted] har også nylig gjennomført en phishingtest (falske e-poster) rettet mot ledere i egen virksomhet, som ligner testen som er gjennomført i denne undersøkelsen (se kapittel 6.5.1).[240]

I en spørreundersøkelse[241] gjennomført av Direktoratet for e-helse i 2019 er det flere ledere som svarer at de har gjennomført undersøkelser rettet mot sikkerhetskultur. På spørsmål om ledelsen har kartlagt eller målt sikkerhetskultur i eget foretak/virksomhet de siste tre årene, svarer et av fire regionale helseforetak, fem av elleve helseforetak som er spurt, og tre av de fire regionale IKT-leverandørene ja på dette spørsmålet.[242] At flere svarer dette i spørreundersøkelsen kan skyldes at noen helseforetak har gjennomført en form for undersøkelse, men ikke oppgitt dette i svarbrev til Riksrevisjonen, eller at undersøkelser er mindre systematiske og ikke dokumentert.

### 6.7.5 Ledelsen og styrene i helseforetakene og de regionale helseforetakene får lite informasjon om informasjonssikkerhetsavvik

I Norm for informasjonssikkerhet stilles det krav om avviksbehandling, og de regionale styringssystemene for informasjonssikkerhet inneholder også retningslinjer og rutiner for avviksrapportering og avviksbehandling.[243]Alle helseforetakene har elektroniske avvikssystemer hvor ansatte kan melde om alle typer avvik, inkludert informasjonssikkerhetsavvik. I tilknytning til de elektroniske avvikssystemene er det egne retningslinjer og rutiner for å avviksmelding og -behandling. Det er opprettet ulike kategorier og underkategorier av avvik, inkludert kategorier for avvik knyttet til informasjonssikkerhet.

Dokumentanalysen[244] viser at ledelsen og styrene ved *helseforetakene* i liten grad får presentert systematiske analyser av informasjonssikkerhetsavvik. Alle helseforetakene utarbeider oversikter over antall informasjonssikkerhetsavvik per år. Disse rapporteres i de fleste tilfeller til ledelsen i forbindelse med ledelsens gjennomgang. Det er imidlertid få helseforetak som gjør systematiske analyser av avvikene, f. eks. ved å kategorisere avvikene etter type eller avdeling der avviket skjer, eller ved å vise utvikling over tid.

---

[238] OUS og Sykehuset Østfold HF har revidert databehandler i løpet av de siste to årene.
[239] Svar på spørrebrev fra helseforetak og regionale IKT-leverandører.
[240] [redacted]
[241] Nasjonal e-helsemonitor-Informasjonssikkerhet i helse- og omsorgssektoren 2019. Det ble sendt ut spørreskjema til ledelsen i RHF, utvalgte HF, de regionale IKT-tjenesteleverandørene og NHN. Svarene ble samlet inn og aggregert opp av Direktoratet for e-helse. Besvarelsene var delvis fra virksomhetsledelse og delvis fra fagansvarlige innenfor informasjonssikkerhet.
[242] Nasjonal e-helsemonitor: Informasjonssikkerhet i helse- og omsorgssektoren 2019, side 27.
[243] I Helse Midt-Norge har Hemit et eget prosedyredokument som inneholder momenter i vurderingen av om melding om avvik skal registreres, definisjoner av avvik med gradering, ansvarsforhold ved melding av avvik og en arbeidsbeskrivelse. I Helse Sør-Øst har Sykehuspartner HF utarbeidet en beskrivelse for bruk av mal for varsling og en beskrivelse av mal for rapportering av avvik eller bekymringsmeldinger knyttet til informasjonssikkerhet. Helse Nord har en retningslinje for behandling av avvik gjeldende informasjonssikkerhet. I Helse Vest er avviksbehandling og avviksrapportering omtalt flere steder i Håndbok Informasjonssikkerhet.
[244] Gjennomgang av AD-møter, ledelsens gjennomgang og styredokumenter i perioden 2017 -2019

Når det gjelder *de regionale helseforetakene,* viser en gjennomgang av de årlige meldingene for 2017-2019 at det som presenteres om avvik her i hovedsak er statistikk over avvik knyttet til pasientsikkerhet.[245]

## Faktaboks 10 Eksempler på systematiske analyser av informasjonssikkerhetsavvik

[redacted] fordeler saker etter hendelsestype, med et kort sammendrag av noen av de viktigste sakene, og belyser trender i avviksrapporteringen. I tillegg innarbeider de i grunnlaget for ledelsens gjennomgang en oversikt over saker helseforetaket har meldt til Datatilsynet, omtaler av antall avvik og eksempler på slike rapportert fra Helse Vest IKT. Avvikene som registreres ved Helse Vest IKT og de andre regionale IKT-leverandørene kan dreie seg om brudd på retningslinjer for bruk av systemer og utstyr som benyttes av helseforetakene, som f. eks. fanges opp av kundesenter/brukerstøtte. Det er i alle regioner slik at helseforetakene mottar informasjon om avvik fra de regionale IKT-leverandørene.

Kilde: Ledelsens gjennomgang

### Det meldes få informasjonssikkerhetsavvik, ut over brudd på taushetsplikt og personvern

I 2017 og 2018 ble det totalt i helseforetakene meldt inn hhv 1773 og 1730 informasjonssikkerhetsavvik. Det er ingen tydelig sammenheng mellom størrelsen på helseforetakene og antall meldte avvik. I 2018 meldte for eksempel [redacted] 232 avvik og [redacted]123 avvik, mens tilsvarende tall for [redacted]var 47. Til sammenlikning meldte mindre foretak som [redacted] og [redacted] henholdsvis 97 og 83 avvik i 2018. Dette kan tyde på at variasjonen skyldes også andre forhold enn bare forskjeller i antall reelle avvik, som ulikheter i meldepraksis.

Når det gjelder IKT-leverandørene, er det [redacted] som meldte flest informasjonssikkerhetsavvik i både 2017 og 2018 (henholdsvis 115 og 152). Til sammenlikning har antall meldte avvik i [redacted] vært langt lavere[246], mens [redacted] har meldt noe mer.[247] [redacted] rapporterer at det er meldt inn 285 informasjonssikkerhetsavvik de siste syv månedene i 2018.[248]

For å få en oversikt over hvilke type informasjonsavvik som meldes, har de fem utvalgte helseforetakene sendt de 20 siste informasjonssikkerhetsavvik som er meldt inn. Tabellen nedenfor viser hvordan disse fordeler seg på informasjonssikkerhetsområdet.

## Tabell 4 Informasjonssikkerhetsavvik i utvalgte helseforetak fordelt etter hendelsestype

| Type avvik | Antall meldinger |
|---|---|
| **Brudd på personvern og taushetsplikt[249]** | **52** |
| **Feil på utstyr eller i systemer eller feil bruk[250]** | **18** |
| **Svakheter ved tilgangsstyringen[251]** | **11** |
| **Manglende fysisk sikring** | **5** |
| **Manglende kommunikasjon og informasjon[252]** | **6** |

[245] Jf analyse av RHFenes årlige meldinger i NVIVO
[246] 20 avvik i 2017 og 23 avvik i 2018
[247] 91 avvik i 2017 og 73 avvik i 2018
[248] I perioden før juni 2018 ble avvik I Sykehuspartner håndtert i et annet system, og disse er ikke overført til avvikssystemet.
[249] Flere av disse avvikene er forklart med manglende opplæring/ manglende beskrivelse av oppgaver/arbeidsbeskrivelser eller menneskelig svikt.
[250] Dette forklares med systemfeil eller mangelfull dokumentasjon av systemer og prosedyrer/utdatert dokumentasjon
[251] Deling av brukernavn og passord, feil tilganger, svake passord
[252] Spesielt knyttet til prosedyreopplæring

| | |
|---|---|
| **Manglende tilgjengelighet til systemer** | **6** |
| **Lagring av filer på fellesområder** | **2** |
| **Mangelfull testing** | **2** |
| **Totalt antall avviksmeldinger om informasjonssikkerhet** | **102** |

Kilde: Riksrevisjonens analyse av enkeltavvik. Kategoriene er utarbeidet av Riksrevisjonen med bakgrunn i avviksmeldingenes innhold.

Tabell 13 viser at halvparten av informasjonsavvikene dreier seg om brudd på personvern og taushetsplikt. Det varierer mellom foretakene i hvor stor grad de melder om andre typer avvik. [redacted] utmerker seg ved at 15 av 20 avviksmeldinger er i kategorien brudd på personvern og taushetsplikt. De andre helseforetakene har en større bredde i hva som meldes av avvik. [redacted] har størst bredde i hva de rapporterer. Når det gjelder feil på utstyr, systemer eller feil bruk, ble 14 av de 18 avvikene meldt av [redacted]

Det at brudd på personvern og taushetsplikt utgjør en så stor prosentandel kan skyldes at det er denne type avvik helsepersonell hyppigst blir eksponert for, og har blitt lært opp til å melde om. Det kan imidlertid også skyldes underrapportering av de andre kategoriene. [redacted] Dette understøttes også av informanter som er intervjuet. Både de utvalgte helseforetakene, IKT-leverandørene og de regionale helseforetakene oppgir at det er underrapportering av informasjonssikkerhetshendelser.

Det er ikke innhentet enkeltavvik fra de regionale IKT-leverandørene. Informasjon fra intervjuer med ledere ved Helse Nord IKT, Helse Vest IKT, Hemit og Sykehuspartner indikerer imidlertid at det i større grad meldes om andre forhold enn brudd på taushetsplikt og personvern her, og i større grad om f. eks. avvik knyttet til mangelfull tilgangsstyring eller feil på utstyr/systemer.

## 6.8 De regionale helseforetakene bruker ikke alle sine virkemidler til å styre og følge opp informasjonssikkerhetsarbeidet

### 6.8.1 RHFene har stilt få egne krav til helseforetak og regionale IKT-leverandører

De regionale helseforetakene (RHF) i alle regioner har stilt krav overfor helseforetak og regionale IKT-leverandører gjennom flere krav til informasjonssikkerhet i perioden 2015-2019 i oppdragsdokumentene (Oppdrag og bestilling). I stor grad har RHFene videreformidlet kravene som departementet har stilt i foretaksmøter. RHFene har stilt få egne krav ut over disse til helseforetakene.[253]

De regionale IKT-leverandørene, som RHFene ser på som viktige virkemidler i informasjonssikkerhetsarbeidet i regionene, har fått noen få ytterligere krav. [254] Helse Sør-Øst RHF stilte en del særskilte krav til Sykehuspartner i 2018 og 2019, etter «Outsourcing-saken» i regionen i 2017/2018 og dataangrepet mot Helse Sør-Øst i 2018.[255] [256]

Som vist i kapittel 6.2, har Helse Sør-Øst, Helse Vest og Helse Nord i perioden 2018-2020 utviklet eller oppdatert regionale styringssystemer for informasjonssikkerhet som skal gjelde for alle virksomhetene i regionene, mens Helse Midt-Norge har kommet kortere i dette arbeidet. Det er i alle regioner enten etablert nye regionale fora for samarbeid, eller arbeidet med oppdatering av mandatet til eksisterende fora.

[253] Alle de fire helseregionene har fulgt opp at informasjonssikkerhet skal bygge på vurderinger av risiko- og sårbarhet. Det samme gjelder kravet om å videreutvikling og implementering av styringssystemene for informasjonssikkerhet. De mer overordnede kravene fra HOD har helseregionene i noen grad nedfelt i mer detaljerte krav til helseforetakene. Detaljeringsgraden i kravene varierer noe mellom regionene.
[254] Hemit er en avdeling i Helse Midt-Norge RHF. De mottar et oppdragsbrev, som tilsvarer Oppdrag og bestilling for de øvrige regionale IKT-leverandørene.
[255] Oppdrag og bestilling 2018 for Sykehuspartner HF av 14. februar 2018
[256] Oppdrag og bestilling 2019 for Sykehuspartner HF av 13. februar 2019

Alle RHFene har mål om å sentralisere driften av IKT-løsninger til de regionale IKT-leverandørene, innføre flere felles IKT-systemer i regionene, og standardisere arbeidsprosesser knyttet til bruk av løsningene. Slike endringer av IKT-forvaltningen kan indirekte bidra til å forenkle informasjonssikkerhetsarbeidet, som vist i kapittel 6.3.2.

### 6.8.2 Det er få formelle samarbeidsarenaer om informasjonssikkerhet på tvers av helseregionene

Det har vært få formelle samarbeidsfora der regionene samarbeider om IKT- og informasjonssikkerhet. Per i dag er det hovedsakelig to slike:

- Det ble i 2020 etablert et *Interregionalt IKT-direktørmøte* (nivået under administrerende direktør) mellom de fire regionale IKT-leverandørene, der direktørene møtes månedlig. Ifølge departementet er det regionale IKT-leverandørene som selv har tatt initiativ til dette, og IKT-sikkerhet er et av temaene. Ifølge departementet ble det opprettet bl.a. som en konsekvens av at helseregionenes felleseide selskap Nasjonal IKT HF ble nedlagt. Direktøren i Norsk Helsenett SF er også i dette møtet. Helse- og omsorgsdepartementet skal kobles på ved konkrete hendelser.
- Informasjonssikkerhetslederne i de fire regionale IKT-leverandørene har også felles møter med HelseCert hver sjette uke. Dette er et forum hvor ikke bare HelseCert gir tilbakemeldinger om f. eks. avdekkede sårbarheter, men der også de andre kan løfte problemstillinger.[257]

Det er i tillegg en mer uformell dialog mellom helseregionene knyttet til temaet informasjonssikkerhet på ledernivå. Det er også uformell kontakt mellom ansatte som jobber med sikkerhetsspørsmål som informasjonssikkerhetsledere/rådgivere på tvers av regionsgrensene.
De fire regionene er også representert i styringsgruppen som har ansvaret for å videreutvikle og forvalte Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Ut over dette møtes representanter for helseregionene i enkelte nasjonale kompetansefora, som Nasjonalt kompetanseforum for IKT-sikkerhet i helse- og omsorgssektoren.

Nasjonal IKT HF ble stiftet 1. januar 2014, som et helseforetak eid i felleskap av de fire regionale helseforetakene. Selskapet skulle være «spesialisthelsetjenestens hovedarena for samhandling innenfor informasjons- og kommunikasjonsteknologi».[258] Flere av prosjektene de har jobbet med har hatt elementer av informasjonssikkerhet i seg, men prosjektet om identitets- og tilgangsstyring[259] og mønstergjenkjenningsprosjektet er informasjonssikkerhet mer sentralt.[260] I foretaksmøtene 11. og 12. juni 2019 ble de regionale helseforetakene enige om at selskapet avvikles. Begrunnelsen for avviklingen var de store endringene i organiseringen av e-helseområdet de siste årene har medført færre oppgaver til Nasjonal IKT HF.[261]

### 6.8.3 Felleseide Sykehusinnkjøp HF har ikke ansvar for informasjonssikkerhetskrav

Ett område som det er mulig for helseregionene å samarbeide om er på anskaffelsesområdet hvor det er mulighet for en mer samordnet styring og kravsetting knyttet til anskaffelse av systemer og utstyr.[262] Sykehusinnkjøp HF, som eies i felleskap av de fire regionale helseforetakene, gjennomfører anskaffelser på vegne av alle helseforetakene. Ved opprettelsen fikk ikke selskapet noe definert oppdrag om å samordne krav og stille spesifikke krav til informasjonssikkerhet i system og utstyr som anskaffes. Selskapet har heller ikke ressurser som jobber dedikert med informasjonssikkerhet, utover et personvernombud for egen virksomhet.

---

[257] Intervju med leder i HelseCert 29. mai 2020
[258] Stiftelsesprotokoll for Nasjonal IKT HF - styrene i RHFene ga sin tilslutning i ulike styremøter i november 2013
[259] Nasjonal IKT HF - felles IKT-portefølje. Prosjektet skal i sin helhet (1) lage løsninger for forenklet og automatisert tilgangsadministrasjon og (2) tilrettelegging og innføring av én brukeridentitet (single sign on)
[260] Etablering av nasjonal metode og rammeverk for statistisk analyse av logger fra oppslag i behandlingsrettede helseregistre.
[261] Foretaksmøte 11. og 12. juni 2019. Helse- og omsorgsdepartementet ba i foretaksmøte i januar samme år om at de regionale helseforetakene vurderte
[262] I Digitaliseringsdirektoratets prosjektveiviser legges det vekt på informasjonssikkerhet og personvern i prosjektleveransene må følges opp helt fra prosjektstart og gjennom alle fasene i prosjektet, inkludert kravspesifikasjonsfasen i en anskaffelse: https://www.prosjektveiviseren.no/god-praksis/viktige-tema-i-alle-faser/informasjonssikkerhet-og-personvern

Sykehusinnkjøp HF  oppfatter selv at de har et ansvar for å ivareta informasjonssikkerhet der dette er en viktig del av anskaffelsen, og at de sammen med de regionale helseforetakene skal stille krav til sikkerheten i utstyr og systemer som anskaffes via dem, både nasjonalt og regionalt. I anskaffelsesprosesser er de imidlertid avhengige av å innhente informasjonssikkerhetskompetanse fra regionene. Ifølge ledelsen ved Sykehusinnkjøp HF har det vært en utfordring i noen anskaffelser å få inn den kompetansen som kreves for å ivareta kravene til informasjonssikkerhet.[263]

### Faktaboks 11 Sykehusinnkjøp HFs rolle

- Helse- og omsorgsdepartementet ba i 2015 helseregionene om at det ble etablert et felles eid helseforetak (Sykehusinnkjøp HF) for samordning av innkjøp innen 1. januar 2016.
- Sykehusinnkjøp HF får innmeldt innkjøpsbehov fra helseforetakene, og selskapets oppgave er å omsette behovene i avtaler gjennom anskaffelser.
- Sykehusinnkjøp har ulike anskaffelsesnivåer, lokale anskaffelser for det enkelte helseforetak, regionale anskaffelser som typisk omfatter en helseregion, og nasjonale anskaffelser som omfatter i hovedsak alle fire helseregioner.
- Sykehusinnkjøp har seks divisjoner: Divisjon nasjonale tjenester, divisjon legemidler, divisjon Nord, divisjon Midt-Norge, divisjon Sør-Øst og divisjon Vest.

Kilde: Protokoll fra foretaksmøte 7. januar 2015, intervju med divisjonsleder i Sykehusinnkjøp, Sykehusinnkjøps hjemmeside: https://sykehusinnkjop.no/om-oss

Sykehusinnkjøp HF uttaler at det ikke er etablert faste strukturer med de regionale helseforetakene for å styrke informasjonssikkerhet i de nasjonale anskaffelsene.[264] Ifølge Sykehusinnkjøp HF er det også en tendens til at de nasjonale avtalene får mest oppmerksomhet fra ulike interessenter. Det synes derfor ifølge dem som om det ikke har vært like stor oppmerksomhet om informasjonssikkerhet og personvern i de regionale anskaffelsene.

Arbeidet med å håndtere informasjonssikkerhetsrisiko i innkjøpsprosjekter er organisert ulikt i hver av Sykehusinnkjøps fire regionale divisjoner, noe som ifølge ledelsen skyldes at praksisen «henger igjen» fra tiden da disse var innkjøpsavdelinger underlagt det enkelte regionale helseforetak. Sykehusinnkjøp HF oppgir at samarbeidet om informasjonssikkerhet med region Midt-Norge har kommet lenger enn samarbeidet med de øvrige regionene, jf. kapittel 6.4.3.[265]

Det er etablert en ordning der det regionale informasjonssikkerhetsforumet (RIF) i Midt-Norge gjennomgår innkjøpsplanen til Sykehusinnkjøp HF sammen med dem, og peker ut de prosjektene som har særskilt behov for kompetanse innenfor informasjonssikkerhet. Deretter må anskaffelsesprosjektene be om ressurser fra HFene (inkl. fra IKT-leverandøren). I tillegg har de i felleskap utarbeidet et faktaark med krav til informasjonssikkerhet i alt medisinsk-teknisk utstyr (MTU) som anskaffes gjennom Sykehusinnkjøp HF i Region Midt-Norge.

Sykehusinnkjøp HF har ikke tilsvarende samarbeid med de andre regionene. Hemit (ved ISL) uttrykker at dette er en stor forbedring fra tidligere, men stiller spørsmål ved om Sykehusinnkjøp også burde ha noe kompetanse på informasjonssikkerhet selv. Et helseforetak i Helse Midt-Norge skriver likevel i sitt svar til Riksrevisjonen at det er nødvendig å få på plass enda bedre og tydeligere rutiner mellom helseforetakene, RHF og Sykehusinnkjøp HF.[266]

**Det er ikke samarbeid mellom regionene om tjenesteavtaler**

[263] Intervju med divisjonsdirektør i Sykehusinnkjøp HF.
[264] Intervju med Sykehusinnkjøp HF  Alle helseregioner jobber med å få bedre rutiner og faste strukturer for å styrke informasjonssikkerheten i nasjonale ansakffelser.
[265] I Helse Sør-Øst er det også utarbeidet en kravspesifikasjon for IKT- tjenester og Informasjonssikkerhet for MTU. Dokumentet benyttes til evaluering/vurdering av leverandørens tilbudte løsning innenfor områdene IKT- og Informasjonssikkerhet.
[266] Helse Nord-Trøndelags svar til Riksrevisjonen av 18. oktober 2019

Et annet område der det hadde vært mulig for regionene å samordne seg, er avtalene som brukes for kjøp av IKT-tjenester. De regionale IKT-leverandørene inngår tjenesteavtaler med sine underleverandører og/eller med helseforetakene. Helseforetakene kan også selv inngå tjenesteavtaler eller databehandleravtaler med sine egne underleverandører og dette er spesielt vanlig knyttet til MTU.

Som del av undersøkelsen har vi gjennomgått tjenesteavtaler fra IKT-leverandører og helseforetak i Helse Vest og Helse Nord i forbindelse med den tekniske kontrollen. Gjennomgangen viser at tjenesteavtalene er ulikt utformet både innad i helseforetak, mellom helseforetak og mellom regionene. Krav til informasjonssikkerhet i avtalene er ulike, og med varierende detaljeringsgrad.

Helse- og omsorgsdepartementet påpeker at de har observert at tjenesteavtalene i helseregionene er ulik utformet. Det er nå vedtatt at helseregionen skal benytte Statens standardavtaler (SSA),[267] som er kontraktsmaler for kjøp av IKT- og konsulenttjenester.[268] Disse malene inneholder en del generelle krav om informasjonssikkerhet og personvern. For eksempel inneholder den generelle avtaleteksten for Driftsavtalen krav knyttet til informasjonssikkerhet og personopplysninger. Det må likevel gjøres konkrete vurderinger av krav om sikkerhet i hver anskaffelse, og de relevante kravene må beskrives i kravspesifikasjoner/bilag til avtalen.

[267] Driftsavtalen - Avtale om kjøp av driftstjenester kap 9.2 og 9.3 Statens standardavtaler for IT-anskaffelser SSA-D
[268] Intervju med Helse- og omsorgsdepartementet

# 7 Helse- og omsorgsdepartementets oppfølging og virkemiddelbruk på IKT-sikkerhetsområdet i spesialisthelsetjenesten

## 7.1 Sammendrag

Dette kapittelet viser at Helse- og omsorgsdepartementet ikke utnytter alle tilgjengelige virkemidler for å ivareta informasjonssikkerheten. Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren og HelseCert er begge sentrale virkemidler i arbeidet med å styrke IKT-sikkerheten. Undersøkelsen viser at det er behov for å styrke den rollen HelseCert har når det gjelder å overvåke og teste IKT-sikkerheten i helseregionene. Direktoratet for e-helse har få oppgaver knyttet til informasjonssikkerhet utover Normen.

Helse- og omsorgsdepartementet har i fortaksmøtene stilt krav om informasjonssikkerhet. De regionale helseforetakene har i all hovedsak ikke rapportert konkret tilbake og departementet har heller ikke etterspurt denne informasjonen. Departementet har imidlertid fått informasjon om status gjennom uformell dialog med de regionale helseforetakene og ved å ta initiativ til statusrapporter på utvalgte områder.

## 7.2 Departementet utnytter ikke potensialet i virkemidlene for å ivareta informasjonssikkerheten

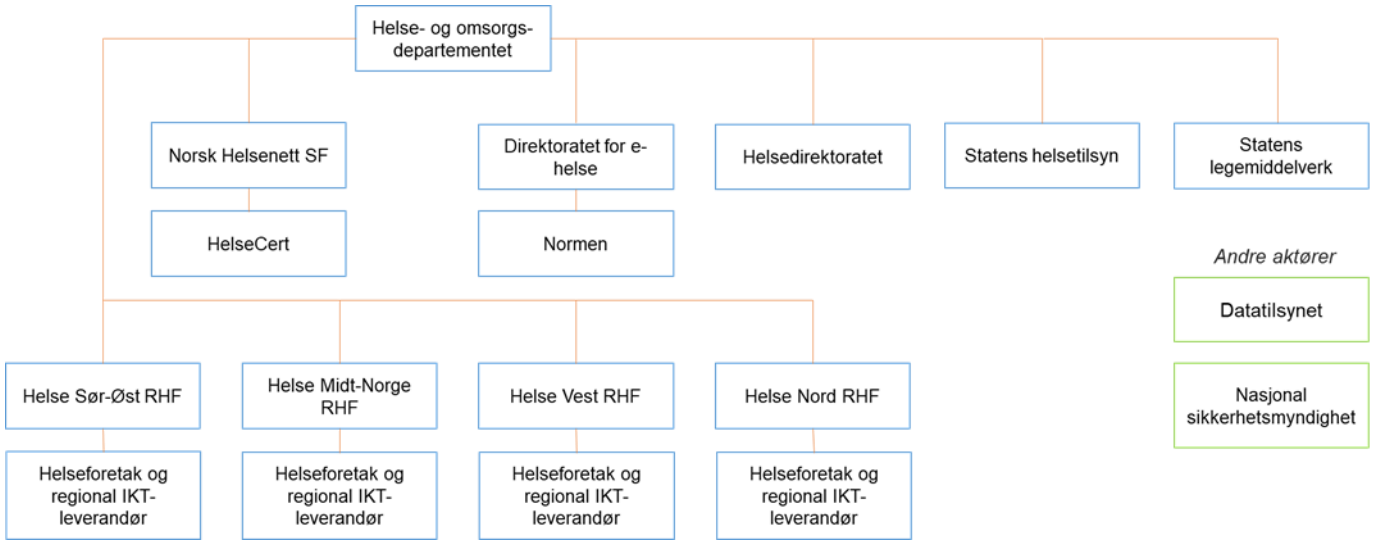
### 7.2.1 Mange aktører har oppgaver knyttet til å ivareta IKT-sikkerheten i helseregionene

Departementet skal gi de nødvendige rammebetingelsene samt legge til rette og følge opp at spesialisthelsetjenesten arbeider systematisk med IKT-sikkerhet.[269]

Området er i stor grad regulert av lover og forskrifter som foretakene må forholde seg til i sitt arbeid. Ut over juridiske virkemidler har departementet valgt å bruke foretaksmøtene med de regionale helseforetakene til å stille krav om informasjonssikkerheten i helseregionene når dette vurderes å være aktuelt.

Helse- og omsorgsdepartementet har også det overordnede ansvaret for at de underliggende etatene og Norsk helsenett SF gjennomfører aktiviteter i samsvar med målene i Stortingets vedtak og forutsetninger.

## Figur 4 Aktører i informasjonssikkerhetsarbeidet i spesialisthelsetjenesten




**Norsk Helsenett SF** skal blant annet legge til rette for og være en pådriver for sikker elektronisk samhandling, sørge for at det foreligger en hensiktsmessig og sikker infrastruktur for effektiv samhandling mellom alle deler av helse- og omsorgstjenestene og bidra til kvalitetssikring av elektroniske tjenester til beste for pasienter og befolkningen for øvrig.[270] Norsk Helsenett ivaretar informasjonssikkerheten i den nasjonale IKT-infrastrukturen (Helsenettet), ved den interne enheten HelseCert (*Computer Emergency Response Team*), som er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet.

**Direktoratet for e-helse** er departementets fag- og myndighetsorgan innen digitalisering. Direktoratet er sekretariat for *Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren* (Normen), som er et sett av krav til informasjonssikkerhet basert på lover og regelverk på området. Direktoratet skal videre bidra til å spre kunnskap om informasjonssikkerhet (og personvern) i sektoren.[271] Direktoratet har også fram til 1. januar 2020 vært dataansvarlig for Nasjonal kjernejournal og e-resept, som benyttes av både spesialisthelsetjenesten og primærhelsetjenesten.[272]

**Helsedirektoratet** har ansvar for den nasjonale beredskapen på IKT-området.

Ut over dette har departementet gitt tilskudd til en utdanningsinstitusjon som jobber med IKT-sikkerhet.[273]

**Statens helsetilsyn** (Helsetilsynet) og **Datatilsynet** kan kontrollere den enkelte virksomhets etterlevelse av krav til behandling av personopplysninger i lovverket. Ved brudd på personopplysningssikkerheten skal den dataansvarlige (ansvarlig for behandling av helseopplysninger) uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet.[274] Helsetilsynet har per dags dato kun gjennomført tilsyn med bruk av pasientjournaler.[275] I henhold til Prop. 1S (2019–2020) vil Helsetilsynet få ansvar for tilsyn i henhold til ny sikkerhetslov.

**Statens legemiddelverk** (Legemiddelverket) skal sikre at alle *legemidler* som brukes i Norge har god kvalitet, er trygge å bruke og har ønsket virkning. Det er Statens legemiddelverk som forvalter og fører tilsyn med produktregelverket for medisinsk utstyr. Dette regelverket er harmonisert innenfor EØS-

[270] Norsk Helsenett SFs Vedtekter §3 Sist endret 20. juni 2019
[271] Tildelingsbrev 2019 til Direktoratet for e-helse 21. desember 2018
[272] Prop. 65 L (2019-2020) Lov om e-helse (e-helseloven)
[273] Departementet har gitt tilskudd på 2,1 millioner kroner både i 2019 og 2020 til Center for Cyber and Information Security (CCIS), som er et nasjonalt senter for forskning, utdanning og kompetansebygging innen cyber- og informasjonssikkerhet tilknyttet NTNU Gjøvik. Senterets mandat er å styrke samfunnets kompetanse og ferdigheter når det gjelder å beskytte mot, oppdage, respondere på og etterforske kriminelle handlinger som gjennomføres ved bruk av teknologi tilknyttet cyber og informasjonssikkerhet.
[274] Personopplysningsloven - Artikkel 33.Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten.
[275] Ifølge Prop. 1 S (2019-2020) bygger Statens helsetilsyn sin prioritering av områder for tilsyn på vurderinger av risiko og fare for svikt i tjenestene. virksomhetenes eget ansvar for sikkerhet og kontinuerlig forbedring.

området og kravene til informasjonssikkerhet innenfor dagens EØS-regelverk. Kravene i gjeldende EØS-regelverk om informasjonssikkerhet skal oppfylles av både produsenter, brukere og myndigheter.

**Nasjonal sikkerhetsmyndighet** (NSM) har utarbeidet grunnprinsipper for IKT-sikkerhet, og Helse- og omsorgsdepartementet stilte i foretaksmøtet i 2020 krav om at disse skal legges til grunn for informasjonssikkerhetsarbeidet i helseregionene. NSMs grunnprinsipper består av et sett med tekniske sikkerhetstiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenester mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene er utgangspunktet for Riksrevisjonens tekniske undersøkelser. Det nasjonale responsmiljøet NorCert, som håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon, er en del av NSM. HelseCert oppgir at de har et tett samarbeid med NorCert.[276]

I tillegg blir nasjonale øvelser innen helse og IKT gjennomført i samarbeid med **Direktoratet for samfunnssikkerhet og beredskap (DSB)**. Videre har **Digitaliseringsdirektoratet (Digdir)** veiledningsmateriell på informasjonssikkerhetsområdet som kan benyttes.[277]

Helse- og omsorgsdepartementet ba i foretaksmøtet i 2020 RHFene om å arbeide systematisk med innføring av NSMs grunnprinsipper for IKT-sikkerhet, HelseCerts anbefalte sikkerhetstiltak, og relevante deler av nasjonal strategi for digital sikkerhet. De ble også bedt om å, i samarbeid med Norsk Helsenett/HelseCert, inngå samarbeidsavtaler med NSM/NorCert knyttet til NorCerts nasjonale sensornettverk på Internett.

Helse- og omsorgsdepartementet oppfatter at det er en klar rolle- og ansvarsfordeling på informasjonssikkerhetsområdet internt i departementet, og mellom departementet og de regionale helseforetakene. Analysen viser at ingen av de regionale helseforetakene, regionale IKT-leverandørene eller helseforetakene mener det er behov for noen sterkere styring fra departementets side. Ledere som er intervjuet, mener gjennomgående at regelverket har blitt klarere og at de fleste utfordringene man står overfor kan løses innenfor dette.

Selv om hverken Helse- og omsorgsdepartementet eller helseregionene etterlyser noen overordnet klargjøring av roller og ansvar, viser undersøkelsen at det er usikkerhet knyttet til om regelverket tillater at dataansvaret deles mellom helseforetak og regionalt helseforetak når det gjelder hvem som har ansvaret ved et informasjonssikkerhetsbrudd. I forbindelse med fastsettelse av ny forskrift om pasientjournal (pasientjournalforskriften) i 2019 presiserte Helse- og omsorgsdepartementet at deres vurdering var at lovverket er åpent for delt dataansvar allerede. Hvordan dataansvaret i så fall skal fordeles må, i følge departementet, avgjøres i det konkrete tilfellet. Departementet opplyser i intervju at de ikke kjenner til eksempler på at et regionalt helsefortak er dataansvarlig alene, eller at helseforetak og regionalt helseforetak har et felles dataansvar.

For øvrig viser departementet i intervju til Nasjonal Helse- og sykehusplan (2020–2023) og Prop. 65 L (2019–2020) Lov om e-helse (e-helseloven), der det går fram at det er behov for å videreutvikle digital infrastruktur og arbeidet med IKT-sikkerhet.

### 7.2.2 Det er behov for ytterligere styrking av HelseCert

HelseCert skal blant annet bistå aktører i helsesektoren med håndtering av alvorlige hendelser, og spre kunnskap i sektoren om IKT-trusler og hvordan man kan beskytte seg mot dem. Av intervjuer med HelseCert framkommer det at det siste i stor grad skjer gjennom veiledning som gis i forbindelse med inntrengingstester og sårbarhetsskanning av tjenester som er eksponert på Internett og Helsenettet.[278]

[276] Intervju med leder i HelseCert.
[277] Direktoratet er pekt ut av Kommunal- og moderniseringsdepartementet til å gi anbefalinger på det systematiske arbeidet med informasjonssikkerhet etter eForvaltningsforskriften § 15
[278] Intervju med leder i HelseCert. 29. mai 2020. HelseCert har for øvrig laget en liste med anbefalte sikkerhetstiltak fra og med 2018. Den er publisert på nettsiden til Norsk Helsenett. HelseCert jobber kontinuerlig med å utvikle denne, og det skal publiseres en ny i løpet av sommeren 2020. De anbefalte sikkerhetstiltakene er ikke veldig ulike det som NSM anbefaler.

HelseCert er i dag organisert som en avdeling under sikkerhetsdivisjonen i Norsk Helsenett og har 12 ansatte.[279] Det er faste møter hver sjette uke med informasjonssikkerhetslederne i de fire regionale IKT-leverandørene, hvor HelseCert kan gi tilbakemeldinger, og IKT-leverandørene kan løfte problemstillinger. Utover de faste møtene er det løpende dialog på operativt og teknisk nivå med de regionale IKT-leverandørene. HelseCERT opplyser at de siden november 2019 gjennomført fire øvelser sammen med de regionale IKT-leverandørene for å forberede håndtering av dataangrep.[280]

Overfor helseregionene har HelseCert tre funksjoner som særlig gir informasjon om det tekniske IKT-sikkerhetsnivået i helseregionene[281]:

- Sårbarhetsskanning av enheter som står i Helsenettet
- Inntrengingstester rettet mot helseforetakene
- Overvåking av informasjonsflyten («trafikken») i den nasjonale IKT-strukturen (Helsenettet)

Alle de fire regionale IKT-leverandørene oppgir at HelseCerts sårbarhetsskanninger av Helsenettet[282] er en viktig kilde til informasjon om sårbarheter i maskinvare/klienter som er direkte eksponert mot Internett eller Helsenettet. De mener imidlertid at HelseCert med fordel kunne styrket seg på de to øvrige områdene:

- **Inntrengingstester.** I perioden 2013 til og med 2016 ble det gjennomført inntrengingstester mot alle fire regioner hvert år. I 2017 og 2018 ga Helse- og omsorgsdepartementet konkrete krav i oppdragsbrev om at det også skulle gjennomføres tester mot kommuner. Fra og med 2017 er omfanget av inntrengingstester mot helseregionene redusert ved at det gjennomføres inntrengningstester mot den enkelte helseregion annethvert år. Testene[283] gjennomføres både mot den regionale IKT-leverandøren og et utvalgt helseforetak.

  Alle de regionale IKT-leverandørene oppgir at inntrengningstestene er en viktig kilde til informasjon om svakheter i deres IKT-infrastruktur. De oppgir at de ønsker flere tester rettet mot sine regioner. Direktoratet for e-helses mener også at det er behov for flere slike tester. I rapporten *Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgstjenesten* fra 2019[284] står det at inntrengningstester er et effektivt virkemiddel for å oppdage sårbarheter i infrastrukturen i sektoren og at sektorens totale kapasitet for å gjennomføre slike tester regelmessig bør styrkes.

  HelseCert oppgir at de ikke har kapasitet til å møte etterspørselen fra regionene, fordi de har begrensede ressurser og også skal betjene primærhelsetjenesten. Testene er finansiert via tilskudd fra departementet, og gjøres altså uten kostnader for regionene.[285]

- **Trafikkovervåking.** Ved å overvåke blant annet mønstre i nett-trafikken, mengde trafikk og type informasjon som sendes via nettet, kan HelseCert fange opp «unormal» aktivitet, som kan være et tegn på at uvedkommende er inne i nettet. De overvåker imidlertid ikke trafikken i helseregionenes egne nettverk.

[redacted]

[279] HelseCert startet opp i 2011/2012 med 2-3 ansatte.
[280] Helse- og omsorgsdepartementets svarbrev av 29. september 2020.
[281] I tillegg har HelseCERT en rekke andre aktiviteter som arranggjør av nasjonalt kompetanseforum, gir råd og og anbefalinger, varsler om trusler og sårbarheter til medlemmer i Nasjonal beskyttelsesprogram. HelseCERT varsler også aktørene i sektor der det finnes informasjon om at brukernavn og passord har kommet på avveie.
[282] Dette innebærer at de kommuniserer med maskinvare (klienter og servere) som er koblet til nettet, for å finne sårbare enheter som kan utgjøre en sikkerhetsrisiko. Et eksempel på sårbarhet kan være at enhetene ikke har oppdatert programvare. Basert på dette utarbeider de sårbarhetsoversikter for virksomheter i helse og omsorgssektoren. Det er kun klienter og servere som er direkte eksponert mot Internett eller Helsenettet som omfattes av HelseCerts sårbarhetsskanning. Helseregionene må selv gjennomføre sårbarhetsskanning av enheter som bare er tilkoblet deres lokale/regionale nettverk.
[283] Testene gjennomføres i to steg. HelseCert starter med inntrengningstest fra Internett og Helsenettet, før de reiser ut til kontrollobjektet og gjennomfører tester av sikkerheten på innsiden av nettverket
[284] Rapport fra Direktoratet for e-helse 1. juli 2019
[285] Intervju med HelseCert

[redacted] Disse tre mener det vil kunne styrke sektorens felles IKT-sikkerhet om det ble etablert en nasjonal sikkerhetsovervåkingstjeneste i helse- og omsorgstjenesten.[286]

Også HelseCert ønsker å bygge opp tjenester for sikkerhetsovervåking av helseregionenes nettverk. I Helse Nord gjennomføres prøveprosjektet «Sikkerhetsmonitorering og analyse - sikkerhet i dybden» i samarbeid mellom Norsk Helsenett (NHN) og HelseCert. HelseCerts oppgave vil hovedsakelig være å oppdage og varsle om avanserte trusselaktører i deres systemer. [287] Dette skal være en kundefinansiert tjeneste.

HelseCert mener de selv må forbedre sin ordinære, nettverksbaserte overvåking og påpeker at mer kryptert trafikk gjør at man må utvikle mer avanserte sikkerhetsovervåkingsløsninger. De peker også på at flere tjenester blir flyttet til «skyen», noe som utfordrer dagens strategi for å oppdage angrep, på grunn av avtalemessige forhold med skytjenesteleverandørene og tilgang til data for nærmere overvåking og analyse.[288]

### 7.2.3 Direktoratet for e-helse har hatt en lite tydelige rolle på informasjonssikkerhetsområdet

Direktoratet for e-helses viktigste oppgaver på informasjonssikkerhetsområdet har vært å fungere som sekretariat for *Norm for informasjonssikkerhet og personvern for helse- og omsorgssektoren* (Normen), og å bidra til å spre kunnskap om informasjonssikkerhet og personvern i helsesektoren.[289]

Alle virksomheter som vil knytte seg til Helsenettet må forplikte seg til å følge Normen, som er et sett av krav til informasjonssikkerhet og personvern basert på lovverket.[290] Normen beskriver både tekniske og organisatoriske sikkerhetstiltak. Den første utgaven av Normen ble lansert i 2006, og i februar 2020 ble den sjette versjonen lansert. Det finnes ikke tilsvarende bransjenormer for andre offentlige sektorer.

Intervjuer med ledelse og informasjonsledere/-rådgivere viser at Normen har vært sentral for utviklingen av de regionale styringssystemene for informasjonssikkerhet og personvern.[291] Alle de fire regionene er representert i styringsgruppen som har ansvaret for å videreutvikle og forvalte Normen, og for å gjøre den kjent i sektoren.[292]

At Normen er et sentralt virkemiddel på området framgår også av Direktoratet for e-helses *Nasjonal e-helsemonitor: Informasjonssikkerhet i helse- og omsorgssektoren 2019* der en høy andel av respondenter fra utvalgte helseforetak, regionale IKT-leverandører og RHFene svarer at de i stor grad har benyttet Normen som utgangspunkt for utforming av krav innenfor informasjonssikkerhetsområdet.[293]

Fra og med 2020 har direktoratet fått som fast oppgave å utvikle, formidle og vedlikeholde nasjonale standarder, veiledere og retningslinjer om informasjonssikkerhet.[294]

---

[286] Administrerende direktør i Helse Nord RHF uttaler i intervju at: «Helse Nord RHF er av den oppfatning at det ikke er behov for en egen Cert-løsning mellom regionene, utover HelseCert. Det bør derimot vurderes å styrke HelseCert, ved å overføre oppgaver til Cert'en som i dag løses i den enkelte region.» Han trekker fram sikkerhetsovervåking som et konkret eksempel på dette.
[287] Intervju med HelseCert.
[288] Intervju med HelseCert.
[289] I Hovedinstruks for Direktoratet for e-helse av 2015 framgår det at direktoratet også har hatt ansvar for å forvalte, informere om og fortolke enkelte paragrafer i lover og forskrifter på informasjonssikkerhetsområdet. Dette gjelder blant annet Pasientjournalloven § 9 om samarbeid om journal, § 13 om nasjonal kjernejournal, § 21 om personopplysninger fra folkeregisteret og § 22 om informasjonssikkerhet.
[290] Lovgivningen har flere krav til informasjonssikkerhet, personvern og behandling av helse- og personopplysninger enn det som er hovedtema for Normen, for eksempel flere problemstillinger rundt bruk av helse- og personopplysninger for andre formål enn ytelse av helse- og omsorgstjenester, spesifikke krav til registre som har egne forskrifter, rettsgrunnlag for behandling av helse- og personopplysninger samt plikt til og krav til journalføring. (Normen, side 9).
[291] Dette gjelder også for styringssystemet til Hemit i Helse Midt-Norge. Det regionale styringssystemet som er under utvikling i regionen bygger også bl.a. på Normen.
[292] Foruten representanter fra helseregionene består styringsgruppen av representanter for Norsk Helsenett SF, Apotekforeningen, Den norske legeforening, Norsk fysioterapeutforbund, Helsedirektoratet, Norsk psykologforening, Norsk sykepleierforbund, Den norske tannlegeforening, Direktoratet for e-helse, Folkehelseinstituttet, KS, NAV, Norsk psykologforening, Norsk sykepleierforbund, Den norske tannlegeforening, Norges farmaceutiske forening, den offentlige tannhelsetjenesten og private laboratorier. Kilde: https://ehelse.no/normen/om-normen.
[293] Henholdsvis 100 prosent av RHFene, 82 prosent av HFene og 75 prosent av de regionale IKT-leverandørene. Resten svarer at de har brukt Normen i moderat grad. Spørsmålet som stilles til de regionale IKT-leverandørene er mer spesifikt enn spørsmålet til de andre. De er bedt om å oppgi i hvilken grad Normen benyttes som utgangspunkt for utforming av krav mot foretak, leverandører og andre. Nasjonal e-helsemonitor: Informasjonssikkerhet i helse- og omsorgssektoren 2019, side 21.
[294] Hovedinstruks av 2020.

Ut over dette har departementet ved enkelte anledninger stilt krav og gitt konkrete oppdrag til Direktoratet for e-helse gjennom tildelingsbrev:

- 2016 - *utvikle en nasjonal sikkerhetsinfrastruktur* for sikker digital kommunikasjon i helse- og omsorgstjenesten i samarbeid med Norsk Helsenett SF.[295] Dette innebar blant annet å utarbeide og implementere en nasjonal forvaltningsmodell for e-helsestandarder og fellestjenester for elektronisk samhandling i helse- og omsorgstjenesten.
- 2017 - gjennomgå informasjonssikkerheten ved bruk av private leverandører i helse- og omsorgssektoren og levere rapport.[296]
- 2019 - gjennomføre en *risiko- og sårbarhetsanalyse* for helse- og omsorgssektorens IKT-sårbarheter, med spesielt fokus på tiltak og oppfølging av disse.[297] Det ble presisert at arbeidet måtte gjøres i samarbeid med Norsk Helsenett SF og andre relevante aktører, i tillegg til Helsedirektoratet.[298]
- 2020 - *foreslå innretning på mulig strategi for informasjonssikkerhet* for helse- og omsorgssektoren, jf. risiko- og sårbarhetsvurderingen for IKT i helse- og omsorgssektoren som skulle utarbeides i 2019. Arbeidet skulle gjøres i samarbeid med Norsk Helsenett SF og i dialog med departementet. Direktoratet ble også bedt om å delta i planlegging og gjennomføring av et IKT-scenario under Helseøvelsen 2020.
- 2020 - utarbeide en felles standard databehandleravtale for behandling av helseopplysninger, som sektoren kan benytte ved inngåelse av slike avtaler.[299]

Oppdragene på informasjonssikkerhetsområdet har med andre ord dels handlet om gjennomføring av enkeltstående utviklingsprosjekter knyttet til nye og eksisterende nasjonale e-helseløsninger, og dels om strategiarbeid og arbeid med å sørge for et kunnskapsgrunnlag. Fra 1. januar 2020 er de konkrete utviklingsprosjektene overført til Norsk Helsenett. Den nye organiseringen skal forsterke myndighetsrollen til Direktoratet for e-helse, mens Norsk Helsenett skal fungere som nasjonal tjenesteleverandør for helsesektoren.

I forslag til ny Lov om e-helse, jf. Prop. 65 L (2019–2020), står det at direktoratet har en tydelig rolle som fagdirektorat på e-helseområdet. Direktoratet for e-helses oppgaver knyttet til informasjonssikkerhet trekkes fram som et godt eksempel på et område hvor en tydeligere rolle vil være et viktig virkemiddel.[300] Helse- og omsorgsdepartementet legger i intervju vekt på at direktoratet ble opprettet 1. januar 2016, og at det har tatt tid å meisle ut direktoratets rolle på informasjonssikkerhetsområdet.[301]

## 7.3 Departementet har ikke innhentet informasjon om hvordan kravene om IKT-sikkerhet til de regionale helseforetakene er fulgt opp

Helse- og omsorgsdepartementet får informasjon om helseregionenes informasjonssikkerhetsarbeid gjennom de regionale helseforetakenes årlige meldinger eller i egne møter. Disse bygger blant annet på helseforetakenes og de regionale IKT-leverandørenes [302] årlige meldinger til de regionale helseforetakene.[303]

En analyse av de årlige meldingene i perioden 2017–2019 viser at samtlige regionale helseforetak har rapportert om informasjonssikkerhet. Rapporteringen er imidlertid på et overordnet nivå, der det ikke

[295] I årsrapporten for 2018 framgår det at Felles grunnmur for digitale tjenester er en forutsetning for kostnadseffektiv, sikker og enklere utvikling, bruk og forvaltning av digitale samhandlingsløsninger. Direktoratet har i 2018 laget en plan for å utvikle Grunnmuren. I årsrapporten for 2019 framgår det at det er gjennomført flere grunnmurstiltak som linjeaktiviteter i Direktoratet for e-helse, for eksempel tiltak knyttet til meldingsutveksling, data- og dokumentdeling, grunndata, Normen, HelseID og arbeid med en modell for koordinert utvikling og forvaltning av grunnmuren.
[296] Tillegg til tildelingsbrev til Direktoratet for e-helse for 2017, datert 9.6.2017.
[297] Tildelingsbrev for 2019.
[298] Bakgrunnen for dette oppdraget var at Helsedirektoratet i sin rapport *Overordnede risiko- og sårbarhetsvurderinger for helse og omsorgssektoren* (utgitt i juni 2017) anbefalte å gjennomføre en særskilt ROS-analyse for hele helse- og omsorgssektorens IKT-sårbarheter, og at Direktoratet for e-helse burde lede dette arbeidet.
[299] Tildelingsbrev til Direktoratet for e-helse for 2020.
[300] Prop. 65 L (2019-2020). Departementet foreslår også at Direktoratet for e-helses rolle og sentrale oppgaver lovfestes. Direktoratet for e-helses rolle er i dag ikke forankret i lov. En tydeligere regulering av direktoratets oppgaver skal ifølge lovforslaget skape klarhet og bidra til økt gjennomsiktighet for markedsaktørene og innbyggerne.
[301] Intervju med Helse- og omsorgsdepartementet
[302] Hemit er en avdeling i Helse Midt-Norge RHF, og rapporterer ikke på samme måte som de andre regionale IKT-leverandørene.
[303] Intervju med Helse- og omsorgsdepartementet

framgår hva som konkret er gjort for å bedre informasjonssikkerheten. Rapporteringen inneholder typisk en kort beskrivelse av prosess med å utvikle regionale rammeverk/styringssystem og uttalelser om at informasjonssikkerhet er et område med stor oppmerksomhet.

Unntaket er de årlige meldingene fra Helse Sør-Øst RHF. I årlig melding for disse tre årene ble det rapportert om de to store informasjonssikkerhetshendelsene i regionen i 2017 og 2018 (se faktaboks 10), om mulige konsekvenser og svakheter som ble avdekket i den etterfølgende gjennomgangen (2017) og konkrete forbedringsprosjekter (2018). I årlig melding for 2019 viser Helse Sør-Øst blant annet til at evalueringen av dataangrepet mot dem er gjennomført og arbeidet er oppsummert i en evalueringsrapport. Det vises til konkrete funn og tilrådninger/forbedringspunkter.

Analysen viser videre at departementet har stilt styringskrav på konkrete områder, men at de har ikke har fått informasjon om aktiviterer og status på disse områdene i de påfølgende årlige meldingene. Det framkommer ikke om departementet har fulgt opp den manglende rapporteringen og tidligere styringskrav:

- I styringskravene for 2018 og 2019 la departementet blant annet vekt på menneskelige forhold og kultur for å bedre informasjonssikkerheten. Det framgår ikke i de årlige meldingene fra RHFene om regionene har kartlagt sikkerhetskulturen eller gjort tiltak for å utvikle denne . Det framkommer heller ikke om departementet har etterlyst dette i foretaksmøtet hvor den årlige meldingen behandles eller i tilleggsrapporteringene til årlig melding.[304]
- Ingen av de regionale helseforetakene har rapportert på kravene fra foretaksmøtet i 2017 om å utarbeide risiko- og sårbarhetsanalyser. Departementet ba i foretaksmøtet om at de regionale helseforetakene sørget for tilfredsstillende informasjonssikkerhet med utgangspunkt i vurdering av risiko og sårbarhet, og oppfølging gjennom internkontroll. RHFene rapporterte ikke hvordan de hadde arbeidet med dette i de årlige meldingene for 2017, men om andre forhold knyttet til temaet informasjonssikkerhet. I de årlige meldingene for dette året blir det kun referert til at de har gitt innspill til Helsedirektoratets rapport *Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren fra 2019*, der informasjonssikkerhet inngår som et av flere temaer. Heller ikke i de årlige meldingene for 2018 eller 2019 rapporteres det konkret om dette. Departementet har ikke bedt om tilleggesrapportering i den forbindelse.
- Helse- og omsorgsdepartementet ba i foretaksmøte i januar 2015 helseregionene om å lukke avvikene fra Riksrevisjonens tidligere undersøkelser på informasjonssikkerhetsområdet.[305] Den nye undersøkelsen viser at flere av merknadene som ble påpekt i disse undersøkelsene, fortsatt er utfordringer; som manglende oppfølging av logger og tilgangsstyring og at ansvarslinjene for informasjonssikkerhet i medisinsk-teknisk utstyr er uklare. Departementet har stilt krav i foretaksmøter om oppfølging av undersøkelsene, men det framgår ikke av de årlige meldingene fra RHFene hvordan helseregionene har arbeidet med disse problemstillingene.[306]

***Andre kilder til informasjon***

Departementet opplyser i intervju at de har fått informasjon om helseregionenes arbeid med informasjonssikkerhet gjennom flere andre kanaler enn de årlige meldingene. Ifølge departementet er det jevnlig dialog med de regionale helseforetakene, hvor ulike problemstillinger drøftes og hvor det er behov for informasjonsinnhenting ved spørsmål fra Stortinget, Riksrevisjonen, media og andre. Departementet har ingen praksis med referatføring fra disse møtene.

Departementet påpeker at det også har vært felles oppfølgingsmøter med de regionale helseforetakene hvor det er orientert om forbedringsarbeidet etter konkrete informasjonssikkerhetshendelser, eller etter publisering av rapporter om informasjonssikkerhet i spesialisthelsetjenesten. Departementet opplyser at særlig «Outsourcing-saken» og dataangrepet mot

[304] Departementet sender brev til de regionale helseforetakene hvert år for å be om tilleggsrapportering om enkelte forhold i årlig melding.
[305] Dok 3:2 (2014 - 2015) undersøkelsen om styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler i fire helseforetak og Helseforetakenes beredskap innen IKT, vann og strøm. Dokument 3:2 (2015-2016) om de regionale helseforetakenes og helseforetakenes ivaretakelse av informasjonssikkerheten i medisinsk teknisk utstyr
[306] Departementet ga en orientering om status for forbedringsarbeidet etter Riksrevisjonens rapport om informasjonssikkerhet i medisinsk- teknisk utstyr i brev til Riksrevisjonen av 5. april 2018.

Helse Sør-Øst, samt rapporter utarbeidet av Direktoratet for e-helse og Riksrevisjonen har vært drøftet på de felles oppfølgingsmøtene.[307] Departementet viser også til at temaet har blitt tatt opp ved to anledninger på de nasjonale direktørsamlingene, som arrangeres to ganger i året.

Departementet understreker at informasjonssikkerhet er et fagområde i utvikling, Dette preger styringen av området ved at departementet løpende må følge med på den teknologiske utviklingen og aktuelle hendelser.

Rapporter fra Direktoratet for e-helse er en viktig kilde for informasjon for departementet. Rapportene peker blant annet på risikoer og utfordringer departementet bør være oppmerksomt på. Direktoratet har utarbeidet tre rapporter de siste årene der informasjonssikkerhet er tema:

- Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten (desember 2017). Rapporten som ble utgitt på oppdrag fra departementet, kom i kjølvannet av «Outsourcing-saken» i Helse Sør-Øst. En anbefaling i rapporten er å utrede og avklare dataansvaret mellom helseforetak og regionale helseforetak, herunder om dataansvaret slik det er i dag er forenlig med strategier for etablering av fellesløsninger i helse- og omsorgssektoren. For øvrig anbefales det å oppdatere Norm for informasjonssikkerhet og personvern (ny utgave utgitt 4. februar 2020), å iverksette tiltak for å heve kompetansen innen IKT-sikkerhet og risikovurdering på styre- og ledelsesnivå, samt å etablere et forum for beste praksis i bransjen for kompetanseheving og sikkerhetskultur.

- Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren (juni 2019) er utarbeidet på oppdrag fra departementet på bakgrunn av behov som har framkommet i tidligere utredninger.308 Rapporten sammenstiller eksisterende dokumentasjon på nasjonalt nivå om informasjonssikkerhet i helse- og omsorgssektoren. Datagrunnlaget som både er tverrsektorielt og sektorspesifikt, bygger bl.a på stortingsmeldinger, rapporter, høringer og trusselvurderinger men ikke doklumentasjon utarbeidet av foretakene i spesialitshelsetjenesten. Rapporten konkluderer med at arbeidet med IKT-sikkerhet i helse- og omsorgssektoren må styrkes, og de største sårbarhetene vurderes til å være:
  - Lange, komplekse og uoversiktlige verdikjeder
  - Manglende IKT-sikkerhetskompetanse
  - Mangelfull implementering av tekniske sikkerhetstiltak
  - Utdatert programvare og utstyr som ikke oppdateres
  - Mangel på og mangelfull etterlevelse av styringssystem for informasjonssikkerhet
  - Manglende planverk og trening i håndtering av IKT-hendelser

- Flere av disse sårbarhetene er også avdekket i denne undersøkelsen. I rapporten som direktoratet har utarbeidet, er sårbarhetene imidlertid i liten grad konkretisert. Når det for eksempel gjelder tekniske sikkerhetstiltak, baserer konklusjonen seg kun på funn fra hendelser og tilsyn.

- I Nasjonal e-helsemonitor: Informasjonssikkerhet i Helse- og omsorgssektoren (desember 2019) har Direktoratet for e-helse kartlagt status på informasjonssikkerhet i helsesektoren ved å etablere sammenliknbare indikatorer som kan relateres til internasjonale forhold. Dette danner et utgangspunkt for å følge med på utviklingen av informasjonssikkerhet i helsesektotren. Undersøkelsen er basert på en spørreundersøkelse og «modenhetsmåling» rettet mot RHFene, HFene og de regionale IKT-leverandørene og omfatter temaer rundt styring og kontroll, risikostyring, beredskap og hendelseshåndtering sikkerhetskultur, og bruk av Normen i dette arbeidet. Undersøkelsen viser at respondentene innen helsesektoren skårer høyere enn statlige virksomheter som ble undersøkt av Difi i 2018. De regionale felles IKT-tjenesteleverandørene skårer høyere i modenhet innen informasjonssikkerhet enn helsesektoren globalt.309

[307] Intervju med Helse- og omsorgsdepartementet
[308] Overordnede risiko- og sårbarhetsvurderinger for helse- og omsorgssektoren 2017. Helsedirektoratet.
[309] Nasjonal e-helsemonitor - Informasjonssikkerhet i helse- og omsorgssektoren 2019 - 20. desember 2019

I tillegg har **Helsedirektoratet** gjennomført en overordnet risiko- og sårbarhetsanalyse for nasjonal beredskap i helse- og omsorgssektoren i 2019.[310] Ett av temaene er IKT-/informasjonssikkerhet, personvern og beredskap. Det foreslås flere tiltak som blant annet en sterkere styring av IKT-sikkerhet fra Helse- og omsorgsdepartementet ved å stille felles krav til hele sektoren.

Helse- og omsorgsdepartementet mottar også noe informasjon fra **Norsk Helsenett SF**, ved **HelseCert**. Departementet opplyser at de hovedsakelig mottar overordnet informasjon om svakheter som er avdekket gjennom inntrengingstester. De mottar årlig en rapport om sikkerhetsstatus ved slike tester, der generelle funn omtales. [redacted].[311] Departementet understreker imidlertid at Norsk Helsenett først og fremst rapporterer til virksomhetene som undersøkes, og ikke til departementet. Ved noen tilfeller er det imidlertid slik at Norsk Helsenett rapporterer til departementet, dersom de vurderer at funnene er så alvorlige at de mener departementet burde orienteres, eller at funn ikke følges opp over tid.

[310] Helsedirektoratet 21. juni 2019
[311] Senest i 2019. [redacted]

# 8 Vurderinger

Dagens moderne sykehus digitaliseres i økende grad, og informasjons- og kommunikasjonsteknologi (IKT) benyttes i de fleste sentrale oppgaver på et sykehus. Dette gir grunnlag for økt kvalitet i pasientbehandlingen. Samtidig fører det til at sårbarheten ved bortfall eller feil i IKT-tjenester øker. Pasienter og innbyggere skal kunne ha tillit til at opplysninger ikke kommer på avveie og at uvedkommende ikke får tilgang.

Undersøkelsen viser at det i alle helseregioners IKT-infrastruktur er vesentlige sårbarheter som kan utnyttes med metodene som er benyttet i Riksrevisjonens angrepssimulering. I tre av helseregionene førte vår angrepssimulering til at vi fikk høy grad av kontroll over viktige IKT-systemer, og derigjennom tilganger som kunne utnyttes til å volde stor skade.

Undersøkelsen har avdekket vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak i alle de fire helseregionene. Det varierer mellom regionene på hvilke områder svakhetene ligger, men alle steder kan de utnyttes av angripere. Undersøkelsen viser også at svakheter i tekniske sikkerhetstiltak henger sammen med helseregionenes sikkerhetsorganisering og -styring, og sikkerhetsatferden blant helse- og IKT-personell.

De fleste utfordringene kunne etter vår vurdering vært løst med dagens IKT-løsninger. Det er i alle regioner et etterslep av oppgaver på sikkerhetsområdet. Noen av de viktigste tiltakene krever systematisk arbeid over tid, og gode prioriteringer i den daglige driften.

Alle de fire helseregionene har problemer med å imøtekomme sentrale krav til informasjonssikkerhet stilt i lov og forskrift. Regionenes tekniske og organisatoriske tiltak er etter vår vurdering ikke tilstrekkelige for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Videre er sensitive opplysninger ikke tilstrekkelig sikret i henhold til kravene i helseregisterloven, helsepersonelloven og pasientjournalloven. De påviste svakhetene i styringen av området står heller ikke i samsvar med betydningen IKT har for sykehusdriften.

Et dataangrep kan få store konsekvenser for pasientbehandlingen og dermed true pasientsikkerheten. Selv om oppmerksomheten om informasjonssikkerhet har økt i helseregionene, og det er iverksatt flere tiltak de siste årene, er det mye arbeid som gjenstår før IKT-sikkerheten er betryggende.

## 8.1 De simulerte dataangrepene ga høy grad av kontroll over IKT-infrastrukturen i tre av fire helseregioner, og tilgang til store mengder sensitive pasientopplysninger i alle helseregioner

Helsepersonell som trenger informasjonen må få tilgang til den raskt og enkelt, og kunne stole på at opplysningene er korrekte, oppdaterte og fullstendige. Pasienter og innbyggere skal kunne ha tillit til at opplysninger ikke kommer på avveie og at uvedkommende ikke får tilgang.

Målet i angrepssimuleringen var å ta kontroll over mest mulig av den regionale IKT-infrastrukturen, samt å få tilgang til sensitive opplysninger. I [redacted] fikk vi en høy grad av kontroll over viktige IKT-systemer, og derigjennom tilganger som kunne utnyttes til å volde stor skade. Med de tilganger som vi oppnådde i disse tre helseregionenes systemer, kunne en reell angriper blant annet ha:

- stjålet store mengder sensitive helse- og personopplysninger
- slettet eller utilgjengeliggjort opplysninger som er nødvendige for pasientbehandlingen
- stoppet og utilgjengeliggjort systemer og utstyr som er kritisk for driften av sykehusene
- manipulert opplysninger om pasientene

I [redacted] fikk vi mindre grad av kontroll over IKT-systemene, men kontroll over mange av regionens PCer. Disse kan brukes for videre angrep.

De simulerte angrepene viser også at en angriper kan gjøre betydelig skade selv uten høy grad av kontroll over IKT-systemene. I alle helseregioner fant vi store mengder sensitive opplysninger som var tilgjengelige for alle ansatte.

Ett av formålene med simulering av dataangrep var å undersøke helseregionens evne til å oppdage aktiviteter i dataangrep. Det ble derfor ikke gjort forsøk på å skjule aktivitetene. Riksrevisjonen genererte mye nettverkstrafikk og la igjen kjente tegn på angrep, som burde kunne oppdages i regionenes overvåkning. Aktivitetene i angrepene ble i varierende grad oppdaget av helseregionene. [redacted] oppdaget flere av aktivitetene i angrepssimuleringen, mens de andre tre oppdaget mindre eller ingenting. En profesjonell angriper som går mer forsiktig fram vil redusere sannsynligheten for å bli oppdaget.

I simuleringen ble det brukt velkjente verktøy, som er tilgjengelige for alle på åpne nettsider. Angrepssimuleringen illustrerer dermed hva som er mulig for andre, som for eksempelvis misfornøyde pasienter eller ansatte med visse IKT-kunnskaper, eller enkeltstående hackere som ønsker å vise fram sine kunnskaper. Avanserte aktører - som etterretningstjenester og organiserte kriminelle - vil ha tilgang til et enda større utvalg av verktøy, de kan tillate seg å bruke mer tid på å skjule sine spor og kan ha muligheter til å utnytte sårbarheter som ikke er allment kjent. De kan dermed enklere skaffe seg kontroll med IKT-infrastrukturen med mindre risiko for å bli oppdaget.

[redacted]

[redacted]

Helseregionene har heller ikke gjort nok for å begrense angriperes mulighet til å gjøre skade dersom de først har lyktes med å komme inn, [redacted] «Skallet» som skal sikre mot angrep fra Internett, har blitt hardere de senere årene. Imidlertid har de tekniske sikkerhetstiltakene innenfor dette «skallet» fortsatt vesentlige svakheter.

Etter vår vurdering viser dette at helseregionenes IKT-systemer ikke er beskyttet godt nok mot vesentlige tap av helseopplysninger eller manipulasjon av systemer og utstyr. Dersom helseopplysninger eller IKT-systemer manipuleres eller gjøres utilgjengelige, kan det forårsake pasientskader. Helseopplysninger på avveie kan få alvorlige konsekvenser for helseforetak og pasienter i form av tapt tillit, uønsket eksponering, identitetstyveri, utpressing mm. Dataangrep kan også få betydelige økonomiske konsekvenser.

## 8.2 I alle fire helseregioner er det vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak som skal forebygge og oppdage dataangrep

Helseregionene skal gjennomføre tekniske sikkerhetstiltak for å oppnå en egnet sikring av sine IKT-systemer og opplysningene lagret i dem. Tekniske sikkerhetstiltak skal primært bidra til å forebygge at dataangrep lykkes, men man må også ha tiltak for å oppdage de angrep man ikke klarer å forebygge.

Resultatene av angrepssimuleringen viser at sentrale sikkerhetstiltak har vært utilstrekkelige for å forebygge og oppdage dataangrep i alle helseregioner. I undersøkelsen er seks sentrale

sikkerhetstiltak basert på blant annet Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet lagt til grunn. Resultatene fra kontrollen av sikkerhetstiltakene er som følger:

1. **Mangelfull kontroll med enheter og programvare**: Helseregionene mangler en fullgod oversikt over maskiner og programvare i egne nettverk, som er en forutsetning for å sikre disse. [redacted] Mangelfull kontroll med enheter og utstyr gjør det mulig for en angriper å kjøre programvare, inkludert angrepsverktøy, i helseregionenes nettverk fra angripers egen PC eller fra helseregionenes maskiner.

2. **Svak kontroll med brukerkontoer og tilgangsrettigheter:** Det brukes mange svake passord både i helseforetakene og hos IKT-leverandørene, som gjør det enkelt for en angriper å knekke passord og få mulighet til å logge inn som ulike brukere. Når mange brukerkontoer i tillegg gis mer rettigheter enn det som følger av tjenstlige behov, er det enklere for en angriper å få kontroll med systemer. Det er videre funnet flere tilfeller der personopplysninger, inkludert sensitiv informasjon om pasienter, er tilgjengelig for alle ansatte i en helseregion. Tofaktor-autentisering er en forbedring for å sikre kontroll med hvem som logger på IKT-infrastrukturen som er tatt i bruk i flere helseregioner, men dette dekker ikke alle situasjoner og den ønskede bedringen i sikkerhet oppnås dermed ikke i mange tilfeller.

3. **Mye utstyr og programvare er ikke sikkert konfigurert:** Mange av helseregionenes maskiner er ikke konfigurert på en sikker måte. Det kan for eksempel bety at usikre metoder for å kommunisere med maskinen ikke er fjernet, unødvendig programvare ikke er fjernet eller at kjente standardpassord ikke er endret. Maskiner med nyere programvare er noe bedre sikret, men størstedelen har vesentlige mangler. [redacted] Svakhetene kan utnyttes til å overta kontroll med maskiner og ulike typer utstyr på sykehusene.

4. **Mangelfull sårbarhetsstyring av IKT-utstyr og programvare:** Rask installasjon av sikkerhetsoppdateringer skal sikre at angripere ikke kan utnytte sårbarheter som oppdages i programvare. Undersøkelsen viser at helseregionene oppdaterer produkter fra [redacted] rimelig raskt i mange tilfeller, men at det går langt tregere for annen programvare. Det finnes også eldre programvare som ikke lenger kan oppdateres, ofte i sammenheng med medisinsk-teknisk utstyr. Kjente sårbarheter i programvare kan utnyttes til å ta kontroll over maskiner i helseregionene, noe vi viste i vår angrepssimulering.

5. [redacted]

6. **Mangelfull logging og overvåkning:** Det er mangler i datagrunnlag for å oppdage angrep ved at det logges mindre enn anbefalt og det mangler sensorer for å innhente supplerende data. Videre er det svakheter i analysene av data for å avdekke dataangrep. Dermed ble få av aktivitetene i vår angrepssimulering faktisk oppdaget av helseregionene.

Det er ikke lagt til grunn at helseregionene skal følge anbefalingene fra Nasjonal sikkerhetsmyndighet (NSM) fullt ut. Helseregionene må foreta prioriteringer av sikkerhetstiltak basert på akseptabel risiko og kostnader. Ettersom tiltakene er grunnleggende for å oppnå god IKT-sikkerhet, er det imidlertid viktig at anbefalingene i størst mulig grad følges.

Alle helseregionene har vesentlige svakheter i sikkerhetstiltakene som ble kontrollert. Disse kan utnyttes av en angriper til å få uautorisert tilgang til systemer og informasjon. Det er ulikheter mellom regionene på hvilke områder svakhetene ligger, men i sum er det vesentlige svakheter i alle de grunnleggende sikkerhetstiltakene i alle regioner.

Svakhetene i de forebyggende sikkerhetstiltakene (punkt 1 til 5) kan utnyttes i dataangrep, og gjorde det mulig å få høy grad av kontroll over tre av fire helseregioners IKT-infrastruktur med kun velkjente standardverktøy i angrepssimuleringen.

Noen dataangrep vil lykkes, og det er derfor viktig at virksomheter også har systemer og rutiner som gjør at de kan oppdage angrep (punkt 6). Dette legger igjen grunnlaget for at angrepet kan håndteres. Helse Sør-Øst, som oppdaget flest av aktivitetene i angrepssimuleringen, hadde kommet lenger enn de andre i arbeidet med å samle inn og analysere data for overvåking av nettverk og IKT-systemer. Dette øker sannsynligheten for at regionen vil kunne oppdage og håndtere reelle dataangrep.

Helseregionene fikk umiddelbart etter testingen informasjon om svakhetene i tekniske sikkerhetstiltak som ble oppdaget. Mange av de konkrete svakhetene som ble utnyttet i angrepssimuleringen og som framkom av analyser, er utbedret i etterkant. [redacted].En angriper vil kartlegge og utnytte de svake punkter som kan finnes. Selv om de fleste sårbarheter blir fjernet, kan en gjenværende vesentlig sårbarhet være nok til at en angriper kan få kontroll over IKT-systemene. For å oppnå tilfredsstillende sikkerhet er det derfor viktig med et systematisk arbeid for å fjerne svakheter.

Etter vår vurdering er det for store svakheter i grunnleggende tekniske sikkerhetstiltak. I alle helseregionene vil det ta tid å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

## 8.3 Helseregionene er på etterskudd i informasjonssikkerhetsarbeidet, og mangler oversikt over sikkerheten i IKT-infrastrukturen

### 8.3.1 Det er økt oppmerksomhet om informasjonssikkerhet i helseregionene, og det er iverksatt flere forbedringstiltak som vil kunne øke IKT-sikkerheten på sikt

Undersøkelsen viser at det er økt oppmerksomhet om IKT- og informasjonssikkerhet i helseforetakene og helseregionene, og at det gjøres mye godt sikkerhetsarbeid.

Undersøkelsen viser at spesielt tre konkrete hendelser («Outsourcingssaken» i Helse Sør-Øst våren 2017, innføring av GDPR og dataangrepet på Helse Sør-Øst i januar 2018) har ført til økt oppmerksomhet om informasjonssikkerhetsområdet i helseregionene. Det er satt i verk tiltak for å forbedre IKT- og informasjonssikkerheten på flere områder. De viktigste tiltakene er:

- styrking av tekniske sikkerhetstiltak:
  - Sykehuspartner HF har styrket overvåkingskapasiteten, mens de tre andre regionale IKT-leverandørene jobber med konkrete tiltak for å styrke overvåkingen.
  - Det stilles krav til sterkere passord for administratorkontoer.
  - Det er igangsatt sårbarhetsskanning i alle helseregioner.
  - Graden av automatiserte sikkerhetsoppdateringer har økt.

- oppdatering av styringssystemene for informasjonssikkerhet og personvern, som fungerer som et rammeverk for styring/ledelse og sikkerhetsorganisering i den enkelte virksomhet.

- styrket arbeid med risiko- og sårbarhetsanalyser (ROS-analyser) ved innføring og endring av IKT-løsninger. Sammenlignet med situasjonen ved Riksrevisjonens tidligere undersøkelser har det skjedd en tydelig forbedring på dette området.

- større fagmiljøer for IKT-sikkerhet ved de regionale IKT-leverandørene. I Helse Sør-Øst er det bygget opp et fagmiljø som jobber spesifikt med overvåking og deteksjon.

- flere stillinger i helseforetakene som er dedikert til informasjonssikkerhetsarbeid, som rapporterer direkte til ledelsen. Samtidig viser undersøkelsen at helseforetakenes oppgaveportefølje på

informasjonssikkerhetsområdet har økt i omfang og kompleksitet, og at helseforetakene har hatt lite ressurser på dette området i forhold til oppgavemengden.

- e-læringskurs i informasjonssikkerhet er blitt obligatorisk i alle regioner. Det er fortsatt ikke slik at alle har gjennomført kursene.

- etablering av nye, regionale samarbeidsfora på informasjonssikkerhetsområdet, og tydeliggjøring av mandatene til eksisterende fora.

Det er også etablert større, regionale forbedringsprosjekter i Helse Nord og Helse Sør-Øst som helt eller delvis har som formål å bedre informasjonssikkerheten. Prosjektene rettes mot særskilte utfordringer i disse regionene og tar også tak i noen av svakhetene som er avdekket i denne undersøkelsen. Noen av prosjektene har som målsetting å redusere porteføljen av systemer og programvare, og å få bedre oversikt over systemer og komponenter/eiendeler. I Helse Sør-Øst er det også et viktig mål å oppgradere regionens IKT-infrastruktur, samt å etablere en felles teknologisk plattform for hele regionen. Helse Vest og Helse Midt-Norge har ikke sett samme behov for større forbedringsprosjekter.

De gjennomførte tiltakene er i hovedsak rettet mot forbedring av organisatoriske og tekniske forhold, og i mindre grad tiltak rettet mot utvikling av sikkerhetskulturen. Svakheter ved sikkerhetsatferden er nevnt av alle de regionale IKT-leverandørene som en av hovedårsakene til de tekniske sikkerhetsavvikene denne undersøkelsen har avdekket.

### 8.3.2 Helseregionene har ikke jobbet systematisk nok med opprydding og utfasing av eldre systemer og tilganger

For å imøtekomme de lovkrav som stilles til informasjonssikkerhet i helseforetakene, må helseregionene være ajour med sikkerhetstiltak.

Undersøkelsen viser at helseregionene har utfordringer som har sammenheng med ledelse og prioriteringer i den daglige driften. Der det innføres nye løsninger som i utgangspunktet skal heve IKT-sikkerhetsnivået, er det mange eksempler på at man enten ikke greier å fase ut de gamle løsningene, eller at man ikke greier å rydde opp i gamle løsninger som skal videreføres. Dermed får man en situasjon der nye, sikrere løsninger eksisterer parallelt med gamle, mindre sikre løsninger. Undersøkelsen viser at ingen av helseregionene har jobbet systematisk nok med å rydde i gamle løsninger:

- Brukerkontoer som ikke lenger er i bruk står fortsatt åpne
- Tilganger og tilgangsgrupper som ikke lenger er i bruk, fases ikke ut
- Eldre, lokale domener er i bruk i helseforetakene, selv om det er bestemt at de skal fases ut
- Det ryddes ikke fortløpende i sensitive pasientopplysninger, og i noen tilfeller er slike opplysninger tilgjengelige for ansatte uten tjenestlig behov

I angrepssimuleringen ga manglende opprydding på disse områdene oss mange veier videre inn i helseregionenes systemer, samt tilgang til sensitive person- og helseopplysninger.

Flere av de som er intervjuet peker på at endringsbehovet i sektoren generelt er drevet av ønsker om ny funksjonalitet, og at det derfor kan oppstå konflikt mellom innføring og administrering av nye løsninger, og rydding i gamle. Når rydding ikke prioriteres fortløpende, vil det være desto mer ressurskrevende når man går i gang.

I mange tilfeller er det helseforetakene som skal stå for opprydding. Undersøkelsen viser at helseforetakene kan ha mindre vilje til å prioritere ressurskrevende oppryddingsarbeid, blant annet fordi ressurser til slike oppgaver til enhver tid må veies opp mot andre oppgaver nærmere pasientbehandlingen. Kontrollen av de tekniske sikkerhetstiltakene viser at utstyr og systemer som helseforetakene drifter selv har svakere tilgangskontroller, oppdateres sjeldnere, og i mindre grad er sikret.

Ifølge helseregionene tar opprydding lang tid på grunn av det store omfanget av IKT-systemer, IKT-utstyr og programvare, samt begrensinger i eldre tekniske løsninger. Kompleksitet og omfang påvirker helseregionenes evne til å få oversikt over alt utstyr og programvare, og avhengigheter mellom disse. Manglende oversikt gjør det også vanskeligere å identifisere og gjennomføre viktige sikkerhetstiltak som sikkerhetsoppdateringer, sikker konfigurasjon av systemer og styring av tilgangsrettigheter. Helse Sør-Øst har en særlig kompleks og omfattende portefølje av utstyr, systemer og programvare.

Det er fortsatt mye arbeid som gjenstår for at helseregionene skal komme ajour med viktige sikkerhetstiltak. Manglende opprydding er en sentral årsak til tekniske funn i denne undersøkelsen. Etter vår vurdering bidrar dette til å svekke sikkerheten.

### 8.3.3 Uklare ansvarsforhold og oppgavefordeling i helseregionene vanskeliggjør forbedringsarbeidet

Ledelsen i de regionale helseforetakene, helseforetakene og de regionale IKT-leverandørene skal sørge for at det er tydelig hvem som har ansvar for hva på informasjonssikkerhetsområdet. Alle skal være kjent med hvilke oppgaver de har, i tillegg til å ha tilstrekkelig kunnskap om andres ansvar og oppgaver, og hvem som har myndighet til å ta beslutninger. De regionale helseforetakene må også sørge for samordning innad i helseregionene på IKT-sikkerhetsområdet, slik at hensyn til helheten og fellesskapet blir ivaretatt.

Undersøkelsen viser at det er uklarheter mellom IKT-leverandørene og helseforetakene om hvem som skal gjennomføre konkrete informasjonssikkerhetstiltak:

- Det er i mange tilfeller uklart hvem som skal gjøre nødvendig opprydding og forbedringstiltak.
- Det er uklart hvordan ansvaret for ivaretakelse av sikkerheten i medisinsk-teknisk utstyr skal fordeles

Opprydding og forbedringstiltak blir forsinket eller satt på vent fordi det ikke er avklart hvem som skal utføre oppgaven. I noen tilfeller er ansvaret delt mellom flere parter (helseforetak og regional IKT-leverandør), og arbeidet stopper opp fordi én av partene ikke tar sin del av ansvaret. Både helseforetakene og IKT-leverandørene påpeker at det gjenstår praktiske avklaringer om oppgavefordeling dem imellom.

I Helse Nord, Helse Midt-Norge og Helse Sør-Øst mener de regionale IKT-leverandørene at manglende avklaring av ansvar og oppgaver mellom helseforetakene og dem er en av hovedutfordringene i arbeidet med å forebygge og avdekke dataangrep. De er gitt et ansvar for sikkerheten i den regionale IKT-infrastrukturen, men har ikke kontroll med alt helseforetakene kobler til denne. Lokale sikkerhetsbrudd kan utgjøre en risiko for regionen som helhet, og de regionale IKT-leverandørene mener manglende avklaringer gjør det tidkrevende å rydde opp i kjente svakheter. Blant annet oppleves dette som en utfordring der det må ryddes i det helseforetakene drifter selv, og der det er vanskelig å gjennomføre oppdatering av programvare for eldre utstyr og systemer ute i helseforetakene. I Helse Vest framstår ansvaret for oppgavene som klarere.

I alle de fire regionene er det uklarheter rundt ansvaret for å ivareta sikkerheten i medisinsk-teknisk utstyr, som for eksempel røntgenutstyr eller måleinstrumenter. Medisinsk-teknisk utstyr har blitt stadig mer integrert i IKT-området ved at en større andel av utstyret i praksis er datamaskiner med egne lagringsenheter og oppkobling mot nettverk. Også Riksrevisjonens undersøkelse av informasjonssikkerhet i medisinsk-teknisk utstyr, som ble rapportert i Dokument 3:2 (2015-2016), viste at det var uklare ansvarslinjer for informasjonssikkerheten for slikt utstyr, både internt i helseforetakene og mellom helseforetakene og de regionale IKT-leverandørene.

Hvordan oppgavene er fordelt for slikt utstyr mellom regional IKT-leverandør og helseforetak varierer, både mellom regioner og mellom helseforetak i samme region. Helse Vest skiller seg ut ved at regional IKT-leverandør ikke er involvert i drift av regionens medisinsk-tekniske utstyr, og i liten grad i sikring av utstyret. Medisinsk-teknisk utstyr er plassert i et nettverk som er sikret av Helse Vest IKT, men for øvrig er det helseforetakene i regionen som ivaretar sikkerheten gjennom sikkert oppsett, sikkerhetsoppdateringer, tilgangskontroller og overvåking.

Etter vår vurdering er det ikke godt nok avklart innad i helseregionene hvem som har ansvaret for å gjennomføre nødvendige informasjonssikkerhetstiltak. I noen tilfeller må helseregionene klargjøre ansvar- og myndighetsforholdene i styringssystemene, i andre tilfeller må det gjøres presiseringer i databehandleravtaler, tjenesteavtaler og andre avtaler om hvem som har det formelle ansvaret og hvem skal utføre oppgaver. Konsekvensen av manglende avklaringer er at viktige tiltak for å forebygge dataangrep blir forsinket eller ikke gjennomført.

### 8.3.4 Ledelsen i både de regionale helseforetakene og underliggende foretakene har mangelfull informasjon om reell sikkerhetstilstand og sikkerhetsrisiko

Tilstrekkelig styringsinformasjon og forsvarlig beslutningsgrunnlag er en forutsetning for god styring og oppfølging. Det er et ledelsesansvar å håndtere risiko på en helhetlig måte og på bakgrunn av dette gjennomføre tilstrekkelige tiltak, styring og kontroll.

Undersøkelsen viser at ledere i helseregionene i varierende grad får informasjon om den reelle sikkerhetstilstanden:

- Ledelsen i både de regionale helseforetakene og helseforetakene mangler en helhetlig oversikt over informasjonssikkerhetsrisikoen, selv om det gjøres mange risiko- og sårbarhetsanalyser ved anskaffelser eller endringer av IKT-systemer eller -utstyr. Det gjennomføres sjeldent risikoanalyser av sikkerheten i selve IKT-infrastrukturen eller av andre informasjonssikkerhetsrelaterte temaer på et mer overordnet nivå. Risikoanalyser som omtaler risiko for tekniske sikkerhetssvakheter som denne undersøkelsen har avdekket, foreligger i liten grad.
- Helseforetakene gjennomfører få revisjoner, sikkerhetsøvelser og kontroller av blant annet IKT-leverandører. Videre har helseregionene i liten grad undersøkt sikkerhetskulturen og om de ansatte opptrer på en måte som ivaretar IKT- sikkerheten.
- Det er etablert systemer for å melde avvik i helseforetakene, men informasjonen som gis til ledelsen, er mangelfull. For det første rapporteres relativt få informasjonssikkerhetsavvik, noe som indikerer en underrapportering på dette området. For det andre analyseres de rapporterte hendelsene i liten grad. Det fratar organisasjonen muligheten for å lære av IKT-sikkerhetshendelser og sette i verk tiltak for å forebygge framtidige hendelser.

Undersøkelsen viser at helseregionene er klar over flere av risikoene. Det er imidlertid viktig at kunnskap om sikkerhetsrisikoen systematiseres, og inngår som en del av styringsgrunnlaget til styre og ledelse i helseregionene. Etter vår vurdering har ikke helseregionene et godt nok informasjonsgrunnlag til å kunne prioritere og iverksette nødvendige tiltak.

### 8.3.5 De regionale helseforetakene har ikke fulgt opp informasjonssikkerhetsarbeidet godt nok

De regionale helseforetakene har et tilsynsansvar overfor helseforetak de eier, som blant annet innebærer at de skal påse at helseforetakene håndterer helse- og personopplysninger i henhold til lover og regler. Tilsynsansvaret innebærer også å følge opp de krav Helse- og omsorgsdepartementet stiller til informasjonssikkerhetsarbeidet.

Undersøkelsen viser at de regionale helseforetakene har fulgt opp kravene fra departementet ved å videreformidle dem til helseforetakene og de regionale IKT-leverandørene, og ved at disse rapporterer om hvordan kravene er møtt. De regionale helseforetakene har i liten grad operasjonalisert kravene eller stilt ytterligere informasjonssikkerhetskrav ut ifra risikoen i den enkelte helseregionen.

At de regionale helseforetakene i liten grad stiller konkrete krav til informasjonssikkerhet kan ha sammenheng med at informasjonsgrunnlaget deres om tilstand og utfordringer ikke er tilstrekkelig. Undersøkelsen viser at oppfølgingen fra de regionale helseforetakene er blitt mer aktiv i etterkant av at omfattende regelendring, dataangrep og informasjonslekkasjer har kastet lys på brister i helseforetakenes informasjonssikkerhet. Dette tyder på at oppfølgingen på dette området har vært lite systematisk og proaktivt.

Undersøkelsen viser videre at de regionale helseforetakene heller ikke har fulgt godt nok opp at kravene de har stilt, har blitt innfridd av helseforetakene og IKT-leverandørene. Det gjør at

informasjonen de regionale helseforetakene videreformidler til departementet om tilstand og utfordringer på informasjonssikkerhetsområdet blir ufullstendig.

De regionale helseforetakene har ansvar for å samordne regionenes arbeid på IKT-området. Undersøkelsen viser at de regionale helseforetakene har lagt dårlig til rette for å samarbeide på tvers for å styrke informasjonssikkerheten i hele sektoren. Det er etablert få felles fora og organer der informasjonssikkerhetsutfordringer kan drøftes og løses i fellesskap.

Det felleseide selskapet Sykehusinnkjøp HF benyttes i liten grad til samordning for å sikre at det stilles samme informasjonssikkerhetskrav til like systemløsninger. Sykehusinnkjøp HF har begrenset kompetanse om IKT-sikkerhet, og de regionale helseforetakene har i liten grad bidratt til å styrke denne ved enten å stille til rådighet egen kompetanse eller stille krav til at Sykehusinnkjøp HF selv styrker kompetansen.

Nasjonal IKT HF ble opprettet av RHFene i 2014 som en hovedarena for samarbeid og samordning innen informasjons- og kommunikasjonsteknologi. De fikk imidlertid få definerte oppgaver innenfor informasjonssikkerhet og foretaket ble avviklet i 2019. I stedet er forumet regionalt direktørmøte etablert, men det kan stilles spørsmål ved om dette er tilstrekkelig for å styrke samordningen og samarbeidet innen informasjonssikkerhetsområdet.

Undersøkelsen viser at det er betydelige svakheter ved IKT-sikkerheten i helseregionene, og flere av svakhetene er påvist i tidligere undersøkelser. Samtidig har trusselen for dataangrep økt. Etter vår vurdering har ikke de regionale helseforetakene fulgt opp informasjonssikkerhetsarbeidet godt nok. De regionale helseforetakene har ikke innhentet nok informasjon om sikkerhetsnivået i egen region, det er fortsatt områder der ansvar og oppgavefordeling i helseregionene er uavklart, og samordningen på tvers av helseregionene har ikke vært god nok.

## 8.4 Atferden blant helse- og IKT-personell svekker IKT-sikkerheten

Foretakene har et ansvar for å utvikle en god sikkerhetskultur. Dette innebærer blant annet at ledelsen må sørge for at medarbeiderne har nødvendig kunnskap om informasjonssikkerhetstrusselen på det aktuelle fagfeltet, relevant regelverk, retningslinjer, veiledere og styringssystem, og at det legges til rette for at kravene kan etterleves. Undersøkelsen viser at en viktig årsak til at det har vært mulig å bryte seg inn i IKT-infrastrukturen er manglende etterlevelse av de retningslinjer og anbefalinger som foreligger.

Undersøkelsen viser at både enkelte IKT-personell og helsepersonell opptrer på en måte som svekker sikkerheten, ved for eksempel å sette svake passord, dele tilganger, gi tilgang til mer enn det som er nødvendig for å utføre oppgaver, og ved å slurve og ta snarveier. Selv når det er etablert retningslinjer som skal sørge for god IKT-sikkerhet, gjøres det i mange tilfeller unntak fra disse som svekker sikkerheten. Dette var en sentral årsak til at vi fikk kontroll over systemer og tilganger til sensitive opplysninger i angrepssimuleringen.
[redacted]
.

Mange dataangrep starter med en forfalsket e-post som har til hensikt å lure bruker til å åpne et vedlegg med ondsinnet programvare, eller klikke på en lenke som fører til infeksjon av maskinen. I denne undersøkelsen ble det gjennomført en phishing-test rettet mot ansatte i helseforetakene. Testen viser at en angriper med stor sannsynlighet ville fått ansatte til å trykke på lenker eller forsøke å laste ned filer med ondsinnet kode. Som testen illustrerer, er det vanskelig fullstendig å forhindre at enkelte ansatte klikker på falske e-poster, og det er derfor viktig å ha tekniske tiltak som kompenserer for dette. Undersøkelsen har ikke omfattet kontroll med tekniske tiltak som kan bidra til å stoppe slike e-poster før de kommer fram til de ansatte, eller hindrer at enkelte typer filer lastes ned.

Undersøkelsen viser videre at det meldes få informasjonssikkerhetsavvik i helseregionene, og at det gjøres få analyser av de avvik som meldes. Dette kan tyde på manglende oppmerksomhet rundt informasjonssikkerhet blant de ansatte.

Kompetanseoppbygging skal være kontinuerlig og tilpasset ulike roller og brukergrupper. Undersøkelsen viser at både helseforetakene og IKT- leverandørene har enkelte opplærings- og informasjonstiltak for å styrke kompetanse og sikkerhetsbevissthet. Informasjon til ansatte om informasjonssikkerhet formidles hovedsakelig som oppslag på intranettet. Opplæringstiltakene er for det meste e-læringskurs. Kursene er i liten grad tilpasset den enkeltes arbeidshverdag og utfordringer, og det er ikke alle som tar kursene selv om de nå er blitt obligatoriske. Opplæringen er noe mer differensiert hos de regionale IKT-leverandørene.

Undersøkelsen viser at sikkerhetskulturen i helseregionene ikke er tilfredsstillende, og at dette gir sårbarheter som kan utnyttes av angripere. Å bygge god sikkerhetskultur slik at sikkerhetsatferden bedres, krever etter vår vurdering ledelsens oppmerksomhet og innsats over tid. Informasjonssikkerhetsfeltet er i kontinuerlig endring, noe som gjør at det er behov for jevnlig og variert påfyll og gjenoppfriskning av kunnskap.

## 8.5 Helse- og omsorgsdepartementet har vært for passive i sin oppfølging av informasjonssikkerhetsarbeidet i helseregionene

Helse- og omsorgsdepartementet har det overordnede ansvaret for spesialisthelsetjenesten. Dette innebærer å sette de regionale helseforetakene i stand til å oppfylle sine plikter til å sørge for spesialisthelsetjeneste til befolkningen innen sine helseregioner. Departementet er videre ansvarlig for å fastsette de overordnede helsepolitiske målsettingene og for gi de regionale helseforetakene rammebetingelser som gjør det mulig for dem å nå disse målsettingene.

Undersøkelsen tyder på at departementets oppmerksomhet om informasjonssikkerhet har vært økende i kontrollperioden 2017-2019, og de har stilt relevante krav på området i denne perioden. Mange av kravene fra departementet tar utgangspunkt i konkrete hendelser, nye lovkrav eller resultater etter revisjoner/evalueringer.

Samtidig viser undersøkelsen at departementet ikke har innhentet tilstrekkelig informasjon om hvordan krav om IKT-sikkerhet til de regionale helseforetakene er ivaretatt og fulgt opp. For eksempel har departementet stilt krav om at det må jobbes med sikkerhetskultur, men det er ikke gitt svar i årlig melding på om dette kravet er møtt, og departementet har heller ikke etterspurt supplerende rapportering. Mange av svakhetene som ble avdekket i Riksrevisjonens revisjoner i 2014[312] og 2015[313], er fortsatt til stede.

Det er også iverksatt tiltak tidligere ved å etablere HelseCert og utvikle Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Samtidig er det etter Riksrevisjonens vurdering et potensial for å utnytte virkemiddelapparatet i Direktoratet for e-helse og Norsk Helsenett bedre for å styrke informasjonssikkerheten. Det er behov for å styrke den rollen HelseCert har når det gjelder å overvåke og teste IKT-sikkerheten i helseregionene. Direktoratet for e-helse har ansvar for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, men har hatt en lite tydelig rolle på området ut over dette.

Departementet skal holde seg orientert om foretakenes virksomhet, hvorvidt krav følges og iverksette tiltak ved behov. Undersøkelsen viser at departementet ikke i tilstrekkelig grad har sørget for å skaffe seg et godt nok informasjonsgrunnlag. De regionale helseforetakenes rapportering er på et overordnet nivå og gir ikke alltid svar på om stilte krav er innfridd. Utover rapporteringen i årlig melding fra de regionale helseforetakene, har departementet fått informasjon om status gjennom uformell dialog med de regionale helseforetakene og ved å be Direktoratet for eHelse utarbeide rapporter knyttet til

[312] Dokument 3:2 (2014-2015) undersøkelsen om styring og kontroll av tilgang til helseopplysninger i elektroniske pasientjournaler i fire helseforetak og Helseforetakenes beredskap innen IKT, vann og strøm.
[313] Dokument 3:2 (2015-2016) om de regionale helseforetakenes og helseforetakenes ivaretakelse av informasjonssikkerheten i medisinsk teknisk utstyr.

informasjonssikkerhet.  I tillegg mottar departementet årlig rapport fra Norsk Helsenett/HelseCert som inneholder informasjon om inntrengingstester i helseregionene.

Arbeidet med IKT-sikkerhet er en forutsetning for å sikre forsvarlig pasientbehandling og for å lykkes med økt digitalisering av helsektoren. Etter vår vurdering viser de påviste svakhetene i undersøkelsen at departementets oppfølging på dette området har vært for passiv. Styringen synes i stor grad å være hendelsesbasert og for lite proaktiv.

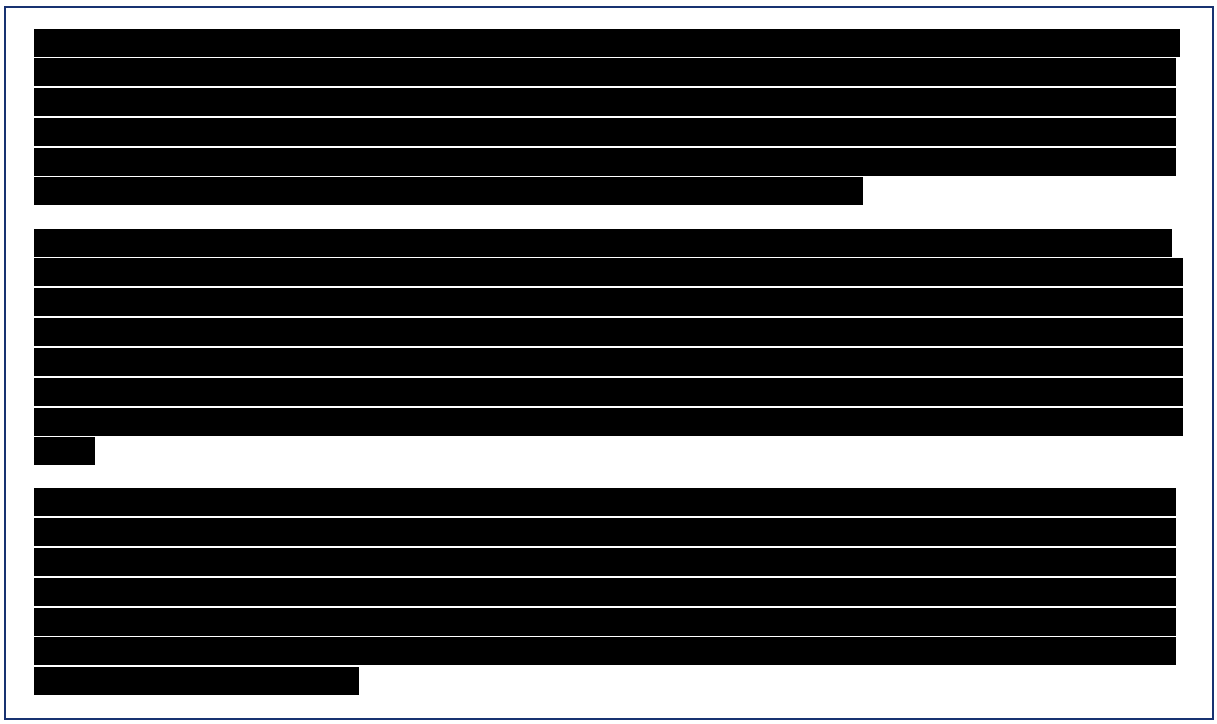
# 9 Ordforklaringer

| Begrep | Definisjon |
|---|---|
| Active Directory | Katalogtjeneste som benyttes i et *domene* hvor det blant annet defineres brukerkontoer, grupper, maskiner og tilgangsrettigheter. Brukeres tilgangsrettigheter defineres ofte ved medlemskap i en gruppe som gis rettigheter i et program. |
| Angrepssimulering | En metode som etterligner dataangrep hvor vi forsøker å omgå sikkerhetstiltak i applikasjoner, IKT-systemer eller nettverk. Formålet er å kontrollere om tiltakene fungerer etter hensikt og identifisere eventuelle svakheter som kan utnyttes i dataangrep. |
| Applikasjon | Programvare som benytter datamaskinens ressurser til en oppgave som brukeren ønsker utført, for eksempel tekstbehandling, regneark eller et pasientjournalsystem. En applikasjon kjøres på en eller flere servere eller PC-er. |
| Autentisering | Prosessen som gjennomføres for å bekrefte en påstått identitet, for eksempel ved å oppgi et passord. Vanligvis brukes begrepet når en brukers identitet skal bekreftes for tilgang til et IKT-system, men autentisering av en maskin er også aktuelt for kontroll med tilgang til for eksempel et nettverk. Se også tofaktor-autentisering. |
| Brukerkonto | Representerer en digital identitet og identifiserer hvem en person eller et system er. En ansatt vil ha en brukerkonto og oppgi for eksempel et passord for å bekrefte at vedkommende er den som brukerkontoen angir. |
| Dataangrep | Handlinger med hensikt å skade eller påvirke et IKT-system. Angrepet kan ha som mål å gjøre et system utilgjengelig for brukerne, stjele konfidensielle opplysninger eller endre opplysninger. Dataangrep kan potensielt skade pasienter ved å sette medisinsk utstyr ut av drift eller endre opplysninger som pleiepersonell legger til grunn for behandling. Dataangrep kan utføres av for eksempel fremmede makter, kriminelle grupper, misfornøyde pasienter eller egne ansatte. |
| Digitalisering | Transformasjon fra at IT er et støtteverktøy i virksomheten til at det er en del av dens DNA. Det betyr at forretningsmodell og -praksis samt organisasjon og prosesser er designet for å utnytte dagens og morgendagens teknologi (Sannes og Andersen, 2016) |
| Domene | Sammenkobling av flere systemer under én felles kontrollfunksjon, ofte kalt en domenekontroller. Gjennom domenekontrolleren defineres prosesser, tilganger og sikkerhetsnivå, og det er mot domenekontrolleren brukere autentiserer seg. I all hovedsak benyttes Microsoft Active Directory som katalogtjeneste i helseforetakenes domener. Domenet vil understøtte en infrastruktur som tilbyr IKT-tjenestene i et helseforetak, herunder ofte også medisinsk-teknisk og bygningsteknisk utstyr. |
| Enheter | Alt utstyr som kobles til et nettverk i en virksomhet. På et sykehus vil dette inkludere alt fra servere og PC-er til medisinsk-teknisk og bygnings-teknisk utstyr. Enheter kan være fysiske eller virtuelle. |
| Enveiskryptert passord | Ved lagring og overføring av passord benyttes som regel matematiske funksjoner for å beskytte passordet. Det lages da et enveis-kryptert passord (en «passordhash»). At det er enveis-kryptert innebærer at det ikke er mulig å finne tilbake til passordet med den matematiske funksjonen. Angripere bruker dermed rå datakraft og genererer tabeller med «passordhasher» ut fra millioner eller milliarder av mulige passord. Hvis angriperen får tak i en reell «passordhash», sammenlignes denne med alle genererte verdier. |
| Herding av maskiner og programvare | Sikker konfigurasjon av maskiner og programvare for å hindre eller redusere konsekvensen av dataangrep eller ubevisste feil. Jf. sikker konfigurasjon. |
| Konfigurasjon | Konfigurasjon er en samlebetegnelse for alle innstillinger som er gjort ved oppsett av en datamaskin (eller annet utstyr) og programvare som kjører på den. Se sikker konfigurasjon. |
| NAC-løsning | Løsning som krever at enheter som kobles til virksomhetens nettverk autentiseres seg ved for eksempel et kryptografisk signert sertifikat lagret på enheten (Network Access Control). Autentisering kan også gjennomføres på andre måter. |
| Nettfiske (Phishing) | Forsøk på svindel eller manipulasjon der bakmennene ved å sende en e-post forsøker lure brukeren til å oppgi sensitive opplysninger (f.eks. passord) eller klikke på lenker som laster ned skadevare. |
| Server | En server er en datamaskin som leverer tjenester til klienter (for eksempel PC-er) i et nettverk (jfr. klient/tjener-teknologi) slik at data og ressurser kan deles. En klient kan være for eksempel en PC eller smarttelefon. Typiske servere er for eksempel |

| | |
|---|---|
| | filservere, databaseservere, webservere og applikasjonsservere. Servere kan være virtuelle. |
| Servicekonto | En brukerkonto som anvendes av et system eller applikasjon som identifikasjon for å få tilgang til tjenester på en server. For eksempel vil et pasientjournalsystem oppgi en servicekonto for å få tilgang til databasen der pasientdata er lagret. |
| Sikker konfigurasjon | Et samling av innstillinger i et IKT-system som er tilpasset på en slik måte at de gir økt motstandsdyktighet mot dataangrep. For eksempel å fjerne unødvendig funksjonalitet og utdaterte teknologier fra en server for å minske dens angrepsflate. Jf. herding av maskiner og programvare. |
| Tofaktor-autentisering | Prosess der det kreves to separate bevis for identitet ved pålogging til et IKT-system. Dette er vanligvis en kombinasjon av noe man husker (for eksempel et passord) med noe man har (for eksempel et smartkort eller en applikasjon på mobiltelefon) eller er (for eksempel fingeravtrykk). Jf. autentisering |
| Tynne klienter | En maskin med lite eller ingen programvare og lagringsplass, og som derfor er avhengig av en sentral server (terminalserver) for å utføre oppgaver for en bruker. Det motsatte er PC-er (tykke klienter) hvor programmer kjøres lokalt og resultater kan lagres på PC-en. |
| Utvidede rettigheter | Høyt tilgangsnivå som gir mulighet til utføre mange funksjoner i et domene, på en maskin eller i et program. Øverste tilgangsnivå gir mulighet til å utføre alle funksjoner som ønskes. Utvidede rettigheter tildeles vanligvis administratorer i en IKT-leverandør ut fra tjenstlig behov, og bør ikke tildeles sluttbrukere. |

# 10 Vedlegg til rapport

### Vedlegg 1 Forskjeller mellom regionene med hensyn til sikkerhetsoppdateringer



Kilde: Analyse av uttrekk fra IKT-systemer

### Vedlegg 2 Fagmiljøer for IKT-sikkerhet ved de regionale IKT-leverandørene

- Sykehuspartner har en avdeling for strategisk sikkerhet med ca. 14 ansatte, og en avdeling for operativ sikkerhet (Sykehuspartner Cert) med ca. 22 ansatte.[314] Avdelingen er ledet av en informasjonssikkerhetsleder, som også har et ansvar for det totale sikkerhetsnivået overfor administrerende direktør.
- Helse Vest IKT har en seksjon for sikkerhet med ni ansatte, som ledes av en IKT-sikkerhetsleder og er organisert under avdeling for tjenesteproduksjon (driftsavdeling). De har også et driftssenter med noen funksjoner som inkluderer sikkerhet.
- Helse Nord IKT har en sikkerhetssjef og tre informasjonssikkerhetsrådgivere som er organisert i staben. Avdeling for tjenesteproduksjon (driftsavdeling) har også en informasjonssikkerhetsrådgiver som har ansvar for å koordinere de interne sikkerhetstiltakene i avdelingen, og en teknisk sikkerhetsressurs. Helse Nord IKT etablerte høsten 2019 et drifts- og overvåkingssenter med enkelte funksjoner innen sikkerhet, der det i etterkant er ansatt en dedikert sikkerhetsressurs.
- Hemit har to informasjonssikkerhetsrådgivere som er organisert i staben, og to sikkerhetskoordinator med et ansvar for operativ sikkerhet som er organisert under avdeling for drift. Hemit har lagt stor vekt på å ansvarliggjøre ledere ute i avdelingene, og å innarbeide rutiner for informasjonssikkerhetsarbeidet i organisasjonen.[315] Hemit har inngått avtale med tredje part om en sikkerhetsovervåkingsløsning.

[314] Informasjon om antall ansatte er hentet fra intervjuer med henholdsvis informasjonssikkerhetsleder og direktør for IKT-tjenester i Sykehuspartner.
[315] Kilder: Intervjuer med informasjonssikkerhetsledere i Sykehuspartner, Helse Vest IKT, Helse Nord IKT og Hemit.

## Vedlegg 3 Regionale forbedringsprosjekter for informasjonssikkerhet

Flere av regionene har iverksatt definerte prosjekter for å forbedre infrastrukturen og styrke informasjonssikkerheten.

***Helse Sør-Øst***

I Helse Sør-Øst er det satt i verk tre store programmer som vil kunne bidra til å styrke informasjonssikkerheten.

- **Prosjekt for applikasjonssanering, standardisering og konsolidering (ASK) 2017 - 2020[316].** Målet med prosjektet var å redusere HeIse Sør-Østs komplekse programvareportefølje ved å fjerne gamle servere og programvare, og ved like type systemer (dubletter) velge de beste og avvikle resten. Prosjektet omfatter sanering av både eldre servere og applikasjoner. Driftsmiljøer med kjente sårbarheter erstattes med standardiserte løsninger og sikkerhetsmekanismer.

- **Program for styrket informasjonssikkerhet, personvern og tilgangsstyring (ISOP).** Programmet inneholder en rekke tiltak på informasjonssikkerhetsområdet innenfor områdene teknologi, prosess, kultur og organisasjon. Opprettelsen av programmet ble besluttet etter «Outsourcing-saken» i 2017/2018,[317] og ble utvidet etter datainnbruddet i Helse Sør-Øst i 2018. Et av hovedprosjektene er «Styrket tilgangsstyring», som blant annet omfatter anskaffelse av nye systemer for tilgangsstyring.[318] Et annet hovedprosjekt har vært å etablere metodeverk for ny sikkerhetsarkitektur («Sikkerhetsplattform»). Dette delprosjektet ble avsluttet i 2019.To av delprosjektene melder om forsinkelser våren 2020.[319]

- **Program for standardisering og IKT-infrastrukturmodernisering (STIM)**. Prosjektet skal levere en standardisert, modernisert og sikker regional IKT-infrastruktur som blant annet å ivaretar krav til sikker og stabil drift. Det skal bl.a. innføres ny regional sikkerhetsarkitektur (som bygger på metodeverket utviklet gjennom ISOP-programmet) og ny domenestruktur, og implementeres ytterligere sikkerhets- og skillemekanismer som ivaretar krav til informasjonssikkerhet og personvern.[320] Innføring av Windows 10 i regionen er også en del av prosjektet. Programmet ble formelt etablert 21. januar 2019.[321]

***Helse Nord***

- **Felles innføring av kliniske systemer (FIKS).** Helse Nord gjennomførte programmet Felles innføring av kliniske systemer (FIKS) i perioden 2011 til 2016. Det ble innført felles kliniske systemer innen fagområdene elektronisk pasientjournal, lab, radiologi og patologi, samt felles pasientjournal. Programmet gjorde systemporteføljen mindre, men helseforetakene har fortsatt hatt høy grad av frihet til å anskaffe mindre applikasjoner.

- **Mobil digital klinisk arbeidsflyt (MODI)**. Programmet Mobil digital klinisk arbeidsflyt (MODI) skal levere fremtidig sikker arbeidsflate, oppgradering til Windows 10, administrasjon av mobile enheter og «disaster recovery»-løsning (DSDR) for Helse Nord.[322]

- **Prosjekt for Helhetlig Informasjonssikkerhet (HIS).** Prosjektet Helhetlig Informasjonssikkerhet (HIS)[323] ble etablert i november 2016. Prosjektet skulle i utgangspunktet ferdigstilles i 2019, men etter en prosjektrevisjon skal det pågå til i 2021. Per i dag handler de viktigste delprosjektene om å sikre kontroll på regionens nett, enhetene i nettet og forvaltningen av dem («Sikker produksjon»),[324] anskaffe og innføre nye løsninger for tilgangsstyring og sikker pålogging («Tilgangsstyring og sikker pålogging»), og nye løsninger for å sikre en mer automatisert IKT-overvåkingsfunksjon for regionen («Overvåking»).

***Helse Midt-Norge***

- **Helseplattformen.** I Helse Midt-Norge innføres ny, felles pasientjournal (PAS/EPJ) ved sykehus og kommuner i hele Midt-Norge. Det gjennomføres konkrete prosjekter under Helseplattformen som skal bidra til styrket informasjonssikkerhet på sikt.

---

[316] Applikasjonssanering, standardisering og konsolidering - ASK Mandat - 16. mars 2018
[317] Da Infrastrukturmoderniseringsprogrammet (IMOD) ble stilt i bero etter «outsourcing-saken», ble det besluttet at ISOP-programmet skulle etableres. Etter datainnbruddet i Helse Sør-Øst ble det besluttet umiddelbare tiltak som gikk inn i ISOP-programmet.
[318] F eks Tilgangsstyring av privilegerte tilganger i Active Directory, Privilegerte tilganger (PAM) og Styrket Autentisering i HSØ (SAiHSØ))
[319] Styresak HSØ 036/2020
[320] HSØ - Programmandat av 1. desember 2018
[321] Styresak helse Sør-Øst, sak 036-2020.
[322] Intervju med HNIKT-10. september 2019
[323] Helse Nord - Styresak 145-2013/3
[324] Dette inkluderer tiltak innenfor overvåking, segmentering av nettverk, kontroll over enheter (bl.a. ny NAC-løsning) og sikker konfigurasjon av servere.

***Helse Vest***

- Det gjennomføres mer løpende tiltak, og regionen har ikke definert noe eget prosjekt med formål å bedre informasjonssikkerheten.

## Vedlegg 4 Samarbeidsforum for informasjonssikkerhet i den enkelte region

**Helse Sør-Øst**

***Regionalt sikkerhetsfaglig råd (RSR)*** skal være en faglig ressurs for regionen og det enkelte helseforetak på informasjonssikkerhetsområdet. Rådet arbeider med overordnede spørsmål, som sikkerhetsmål og -strategi for de regionale tjenestene. RSR forvalter det regionale styringssystemet for informasjonssikkerhet og personvern. (Hent opp fra tidligere tekst i kapittel 6.8)

***Regionalt sikkerhetsvurderingsteam (RSV)*** er en arbeidsgruppe under RSR som behandler risikoanalyser av IKT-systemer og -utstyr. Informasjonssikkerhetsledere/-rådgivere fra alle helseforetakene i regionen deltar i teamet, som ledes av Sykehuspartner. Organet skal vurdere informasjonssikkerheten i regionale IKT-løsninger, og IKT-løsninger som berører to eller flere helseforetak. De tar stilling til risikoanalyser av slike systemer og kommer med en anbefaling til helseforetakene. Anbefalingen kan innebære at det må gjøres tiltak som reduserer risikoen.[1] RSV har eksistert i mange år; opprettelsen ble formalisert gjennom Sykehuspartners oppdragsbrev i 2013.

**Helse Midt-Norge**

***Regionalt informasjonssikkerhetsforum (RIF)*** er et regionalt fagforum for informasjonssikkerhet, som behandler risikoanalyser av IKT-systemer og -utstyr. Informasjonssikkerhetsledere/-rådgivere fra alle helseforetakene i regionen deltar i forumet, som ledes av Hemit.

***Regional eiergruppe for Informasjonssikkerhet og personvern*** er et samarbeidsforum i HMN som skal understøtte oppgaver gitt i oppdragsbrev til HF og Hemit. Gruppen skal, i samarbeid med Regionalt informasjonssikkerhetsforum (RIF), bidra til regional samordning og mer effektiv saksbehandling med tilstrekkelig kvalitet i arbeid med informasjonssikkerhet og personvern i HMN. Forumet ble opprettet i 2019.[325]

**Helse Vest**

***Regionalt IKT-sikkerhetsutvalg (SU)*** består av representanter fra de dataansvarlige, både fra helseforetakene og syv private leverandører som Helse Vest RHF har avtaler med om levering av helsetjenester. I tillegg er Helse Vest IKT AS representert inn i utvalget. Utvalget ledes av Helse Vest RHF. Gjennom utvalget forvalter RHFet, sammen med de nevnte virksomhetene det regionale styringssystemet for informasjonssikkerhet og personvern. RSU er et faglig rådgivende organ for virksomhetene i Helse Vest innenfor IKT-sikkerhet. Det er tilstedeværende møter hver 6. uke og elektroniske møter hver 14. dag.

**Helse Nord**

***Fagråd for informasjonssikkerhet (FRIS)*** er «et rådgivende organ som skal sikre en mest mulig enhetlig tilnærming til området informasjonssikkerhet» i Helse Nord. Hvert enkelt helseforetak i regionen (inkludert Helse Nord IKT) har en representant i FRIS. Helseforetakenes informasjonssikkerhetsledere/rådgiverne er de som er utpekt. Fagrådet ledes av informasjonssikkerhetsleder i det regionale helseforetaket.

***Møter mellom «sikkerhetskoordinatorer».*** Hvert helseforetak i Helse Nord har en sikkerhetskoordinator (som regel de samme som sitter i FRIS). Disse har månedlige møter med Helse Nord-IKT, der sistnevnte presenterer statusoppdateringer om sårbarheter, trusler og hendelser som har vært i regionen. Det blir også informert om spesifikke trusler i det enkelte foretak, og hvilke avdelinger risikoene gjelder for. Ifølge Helse Nord IKT er hovedmålet med dette å koordinere arbeidet med sårbarheter som Helse Nord IKT har avdekket på utstyr (og systemer) de ikke har driftsansvar for.[326]

***Partnermøte.*** Helse Nord har innført et møtepunkt for de dataansvarlige («Partnermøte»). Der helseforetakene eventuelt er uenige om akseptabelt risikonivå, skal problemstillingen løftes opp til et møte mellom de fire sykehusdirektørene i regionen. Ifølge Helse Nord RHF var EKG-saken den viktigste årsaken til at man valgte å innføre et slikt forum (se faktaboks 14).

[325] [redacted]

[326] Intervju med informasjonssikkerhetsleder i Helse Nord IKT HF.

## Vedlegg 5 Ansvarsforhold knyttet til IKT-infrastruktur i den enkelte region

**Helse Vest.** Styret i RHFet besluttet i mars 2018 at Helse Vest IKT både har «*ansvar og styringsmyndighet innenfor operative IKT-tjenester*»[327] og «*ansvar og styringsmyndighet for IKT-infrastrukturen*» i Helse Vest.[328] Styringsmyndigheten innebærer at Helse Vest IKT har mandat til å ta beslutninger om hvilke systemer, enheter og applikasjoner som kan stå i det regionale nettverket, og i siste instans hvilke som må oppdateres eller fases ut.[329] Imidlertid peker både Helse Vest IKT og helseforetak i regionen på at det gjenstår praktiske avklaringer om ansvarsfordelingen knyttet til sikkerheten i medisinsk-teknisk utstyr, som i Helse Vest står utenfor det regionale nettverket (se kapittel 6.4.2). Inntil nylig har det vært enighet om at Helse Vest IKT *ikke* skal spille noen rolle, men flere av helseforetakene i regionen peker på området som en sikkerhetsutfordring.

**Helse Midt-Norge.** Ifølge Hemit er det krevende å levere fellestjenester til virksomheter som har individuelt ansvar, fordi det krever mange konsensusprosesser som både er utfordrende og tidkrevende å få til. Selv om ansvarsfordelingen formelt er tydelig, mener Hemit at det i praksis kan være vanskelig å få et klart definert oppdrag med et klart definert ansvar. Dette gjelder særlig tilfeller der eksterne tjenester som er kjøpt av helseforetakene (skytjenester, medisinsk teknisk utstyr, etc.) skal integreres med øvrig IKT-infrastruktur.[330] Ifølge Hemit er det også stadig diskusjoner med helseforetakene om systemer eller utstyr som ikke lenger kan oppdateres/supporteres, og dermed kan utgjøre en sikkerhetsrisiko. Helseforetakene ber i mange tilfeller om at det gjøres unntak for spesifikke systemer eller utstyr. Hemit peker på at de ikke har myndighet til å bestemme at HFene må finne et alternativ til utstyr/systemer som ikke lenger kan oppdateres, slik Helse Vest IKT har.[331]

**Helse Sør-Øst.** Sykehuspartner har i henhold til regionens styringssystem et «helhetlig ansvar for informasjonssikkerhet i infrastrukturen.» Både Helse Sør-Øst RHF og Sykehuspartner mener at IKT-leverandøren ikke har hatt virkemidler til å håndheve dette i praksis.[332] Helse Sør-Øst RHF har gitt Sykehuspartner et utvidet mandat i 2019 og 2020. Sykehuspartner har nå fått myndighet til å kunne stoppe informasjonssystemer og nettverk som medfører en vesentlig informasjonssikkerhetsrisiko for foretaksgruppen som helhet. Dette vedtaket omfatter imidlertid bare systemer, enheter og applikasjoner som inngår i regional infrastruktur.[333] Sykehuspartner fikk også i resultatmål dette året å bidra til å redusere digitale sårbarheter innenfor infrastrukturområdet ved å redusere antallet gamle, lokale domener.

I *Oppdrag og bestilling* til helseforetakene for 2020 har RHFet stilt flere krav som handler om ansvarsforholdet mellom helseforetakene og Sykehuspartner på IKT-området, som går i retning av sentralisering på IKT- og informasjonssikkerhetsområdet.[334]

**Helse Nord.** Helse Nord IKT har bedt om en evaluering av styringsmodellen på IKT-området. Styret i Helse Nord IKT sluttet seg 16. mars 2020 til en anmodning til det regionale helseforetaket om å 1) evaluere IKT-styringsmodellen i Helse Nord, og herunder klargjøre ansvar- og myndighetsforhold, og 2) tydeliggjøre Helse Nord IKT HFs ansvar og myndighet for infrastrukturen, med særlig vekt på ivaretakelse av informasjonssikkerhet.[335]

Helse Nord IKT er gitt myndighet til å forvalte sikkerhetskravene til regionens IKT-infrastruktur.[336] Helse Nord IKT understreker at de ikke har myndighet til å pålegge helseforetak å følge kravene. De peker også på at helseforetak gjennomfører lokale systemanskaffelser uten at de er involvert, at de har manglende kontroll med enheter/komponenter som er koblet til den regionale infrastrukturen, og at de er avhengig av at helseforetakene prioriterer nødvendig vedlikehold, oppgradering mv. der de drifter selv. I tillegg eier helseforetakene PC-ene som Helse Nord IKT drifter. Når regionen for eksempel skal oppgradere til Windows 10 er Helse Nord IKT avhengig av at helseforetakene prioriterer å ta kostnaden knyttet til oppgraderingen.

---

[327] Operative tjenester omfatter applikasjonsdrift, meldingsutveksling, kundesenter, tilgangsstyring, på stedet-support, driftssenter, desktop, sykesignal, tele/video, server og lagring, datakommunikasjon og datahaller.
[328] Styresak 027/2018
[329] Intervju med administrerende direktør i Helse Vest IKT.
[330] Svar på spørrebrev fra Hemit.14. oktober 2019
[331] Intervju med avdelingsleder for basisdrift i Hemit.
[332] Intervju med administrerende direktør i Helse Sør-Øst RHF, svarbrev fra Sykehuspartner.
[333] Oppfølgingsmøte med Sykehuspartner 27. mai 2020
[334] Dersom helseforetakene skal beholde egne datarom, må de gjennomføre tiltak for å heve sikkerheten til akseptabelt nivå. Det stilles krav om at helseforetakene skal bidra aktivt til å sanere applikasjoner for å bidra til å lette overgangen til Windows 10 som operativsystem. Det presiseres at helseforetakene ikke skal «bygge opp eller inneha interne IKT-kapabiliteter (kompetanse og kapasitet) som naturlig hører hjemme hos Sykehuspartner HF».
[335] Brev fra Helse Nord IKT til Helse Nord RHF datert 23. mars 2020.
[336] Styret i Helse Nord RHF har i styresak 005-2017 «Beslutningsgang for IT infrastruktur og basistjenester» slått fast at Helse Nord IKT har ansvar for teknisk, merkantil og funksjonell forvaltning av IKT-infrastruktur og basistjenester. Infrastruktur er definert som all maskinvare (eksempelvis PC, nettverk, servere) og programvare for ikke-faglige systemer f. eks. for epost eller databaser, men ikke fagsystemer som f. eks. kurve eller innkjøp. I styresak 49/2019 «Myndighets- og ansvarsforhold på IKT-området i Helse Nord» er det gjort enkelte presiseringer.

IKT-leverandøren mener også dagens finansieringsmodell på IKT-området skaper unødig konflikt mellom dem og helseforetakene, og at den fører til treghet i gjennomføringen av viktige tekniske sikkerhetstiltak.[337] Helse Nord IKT fakturerer helseforetakene for kostnadene knyttet til de store, regionale forbedringsprosjektene. Helse Nord IKT mener dette kan oppfattes som kostnader som ikke er direkte knyttet til tjenester helseforetakene mottar. Til sammenligning mottar Sykehuspartner investeringsmidler fra Helse Sør-Øst til å gjennomføre tilsvarende regionale forbedringsprosjekter.

Helse Nord RHF påpeker at det de siste årene har vært stor uenighet i regionen om styringen av IKT-området, og at det fortsatt arbeides med hvordan man skal få dette til å fungere best mulig i praksis.[338] De mener Helse Nord IKT ønsker en utvidet rolle og ansvar for systemer og utstyr som det formelt enten er RHFet eller helseforetakene som har ansvaret for. RHFet understreker også at det er fagmiljøene som skal bestemme hva slags utstyr og systemer som skal benyttes, samtidig som helseforetakene ikke skal gjennomføre systemanskaffelser uten at Helse Nord IKT er involvert.[339]

[337] Helse Nord IKT fakturerer helseforetakene for kostnadene knyttet til de store, regionale forbedringsprosjektene. Helse Nord IKT mener dette kan oppfattes som kostnader som ikke er direkte knyttet til tjenester helseforetakene mottar. Til sammenligning mottar Sykehuspartner investeringsmidler fra Helse Sør-Øst til å gjennomføre tilsvarende regionale forbedringsprosjekter.
[338] Riksrevisjonen intervjuet administrerende direktør i Helse Nord RHF før Helse Nord IKT ba om en ny gjennomgang av IKT-styringsmodellen, og RHFet har per nå ikke tatt stilling til Helse Nord IKTs forespørsel.
[339] Intervju med administrerende direktør Helse Nord RHF 9. september 2019