Direktoratet for e-helse

Høring:
Innspill til kommende stortingsmelding om helseberedskap

Tema: Digital sikkerhet

IE-1101

Publikasjonens tittel:
Høring: Innspill til kommende stortingsmelding om helseberedskap – Digital sikkerhet

Rapportnummer
IE-1101

Utgitt:
9. juni 2022

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:
www.ehelse.no

Forord

I dette dokumentet gir Direktoratet for e-helse på oppdrag fra Helse- og omsorgsdepartementet sine innspill innen området digital sikkerhet til arbeidet med ny stortingsmelding om helseberedskap. Meldingen skal legges frem våren 2023. Den skal ta for seg fem scenarier - hvor digitale trusler er ett av dem.

Våre innspill bygger på det tidligere arbeidet med en strategi for digital sikkerhet i helse- og omsorgssektoren. Utarbeidelse av strategien var et oppdrag i fjorårets tildelingsbrev til direktoratet, i samarbeid med Helsedirektoratet, Helsetilsynet, Norsk helsenett SF, de regionale helseforetakene og kommunesektoren/KS. I arbeidet har sektoren blitt involvert gjennom bl.a. arbeidsmøter og drøftinger i nasjonal styringsmodell.[1] Det har også vært dialog med fagmyndigheter i og utenfor sektoren. Strategiprosessen gir derfor et godt grunnlag for innspill til den kommende stortingsmeldingen.

Arbeidet med strategi for digital sikkerhet i helse- og omsorgssektoren var planlagt fullført høsten 2022. For å få mest oppmerksomhet og rask utvikling på området og for å minske antall dokumenter å forholde seg til, har departementet vurdert det som hensiktsmessig å innarbeide strategi for digital sikkerhet i helse- og omsorgssektoren i den kommende stortingsmeldingen om helseberedskap. I strategiarbeidet var det fokus på nye tiltak. I en stortingsmelding er det også sentralt å presentere status på området i dag. I dette høringsutkastet er det innarbeidet et nytt kapittel 2 «Hva gjøres i sektoren i dag». I tillegg er det i Vedlegg A en liste over eksisterende tiltak i sektoren som er en oppfølging av Nasjonal strategi for digital sikkerhet og en oppsummert sammenstilling av relevante tiltak fra de regionale handlingsplanene for arbeidet med informasjonssikkerhet. Dette er med for å gi departementet god innsikt i pågående arbeid med digital sikkerhet i sektoren, men vil neppe bli et vedlegg til stortingsmeldingen.

For å forankre og forbedre faktabeskrivelser og anbefalinger, gjennomføres det nå en bred høring. Vi imøteser innspill og ser gjerne at de er konkrete, se høringsbrev og høringsskjema.

Direktoratet for e-helse skal styrke digitaliseringen i helse- og omsorgssektoren for å understøtte effektive og sammenhengende helse- og omsorgstjenester, og har som myndighet et hovedansvar for å tydeliggjøre rammebetingelsene for informasjonssikkerhet i digitaliseringsarbeidet i sektoren. Digital sikkerhet er en forutsetning for å lykkes med digitalisering. Vårt mål med innspillet er å beskrive sentrale innsatsområder som vil være viktige for forebyggende sikkerhet og helseberedskap, samtidig som de vil understøtte digitaliseringen i helse- og omsorgssektoren.

Mariann Hornnes, direktør

Oslo, juni 2022

[1] *Direktoratet for e-helse, Nasjonal styringsmodell, 2021*

Innhold

1. Innledning

Helse- og omsorgssektoren er i økende grad avhengig av digitale løsninger. Dette er en ønsket utvikling som gir oss mer effektive tjenester til daglig og når krisen treffer oss. Digitalisering og bruk av ny teknologi er derfor en utvikling som med stor sannsynlighet vil forsterkes fremover.

I takt med digitaliseringen av samfunnet blir det også stadig mer komplekst og krevende å beskytte Norge mot alvorlige trusler. Trusselbildet i det digitale rom er i endring og gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner blir større. Antallet cyberangrep mot norske mål har hatt en markant økning de siste årene. Nasjonal sikkerhetsmyndighet (NSM) beskriver risikoen for alvorlige cyberoperasjoner som høy og økende for virksomheter innen en rekke sektorer, der helse- og omsorgssektoren nevnes spesifikt. For å motvirke en slik utvikling er det avgjørende at virksomheter i sektoren øker sin sikkerhet, årvåkenhet og evne til å forebygge og håndtere hendelser.[2]

Den stadig mer spente sikkerhetspolitiske situasjonen i Europa synliggjør behovet for styrket beredskap. Risikoen for hendelser i det digitale domenet har økt betraktelig, og norske mål er utsatt både direkte og indirekte. Det er derfor avgjørende at virksomheter i helse- og omsorgssektoren tilegner seg nødvendig kunnskap og holder oversikt over endringer i risikobildet. De må jobbe kontinuerlig med forebygging og beredskap for å forhindre og håndtere hendelser, kriser og katastrofer. Videre må virksomhetene i sektoren evne å gjenopprette funksjoner under og i etterkant av slike hendelser, samt legge til rette for å lære av erfaring fra både reelle hendelser og øvelser.

Befolkningen skal ha tillit til at helse- og omsorgssektoren kan levere sine tjenester, og at helseopplysninger blir behandlet på en trygg måte. Det innebærer at de ikke kommer på avveie, er riktige, oppdaterte, og tilgjengelige for både helsepersonell og pasienter ved behov. Befolkningen må også kunne stole på at sektoren er rustet til å håndtere en eventuell krisesituasjon. Dette krever at arbeidet med digital sikkerhet og beredskap i helse- og omsorgssektoren er helhetlig og møter risikoen virksomhetene står overfor.

Helse- og omsorgsdepartementet (HOD) har det strategiske ansvaret for IKT-utviklingen i helse- og omsorgssektoren, og har overordnet ansvar for at befolkningen har tilgang til gode og likeverdige helse- og omsorgstjenester og folkehelseområdet – inkludert beredskap og sikkerhet.

HOD har nasjonalt ansvar for helseberedskapen. Departementet forvalter ansvaret ved regulering av kommunal, statlig og privat virksomhet gjennom regelverk, tilsyn, budsjett og tilskuddsforvaltning, ledelse, organisering og styring av forvaltningen og RHF-ene. Statsforvalteren er regional helseforvaltning og bindeledd mellom nasjonalt og lokalt nivå.

HOD har det overordnede ansvaret for IKT-sikkerheten i spesialisthelsetjenesten. HODs underliggende etater ivaretar rollen som forvalter av IKT-løsninger, registre og sektorens felleskomponenter. Å ivareta digital sikkerhet er imidlertid først og fremst et virksomhetsansvar. Ledelsen i virksomhetene er ansvarlig for at risikovurderinger gjennomføres, og at det på bakgrunn av dette iverksettes egnede tiltak. Nødvendig sikkerhetsstyring bør være integrert i ordinær virksomhetsstyring. Den som har ansvar for et fagområde eller en tjeneste i en

[2] *Nasjonal sikkerhetsmyndighet, Risiko 2022, 2022*

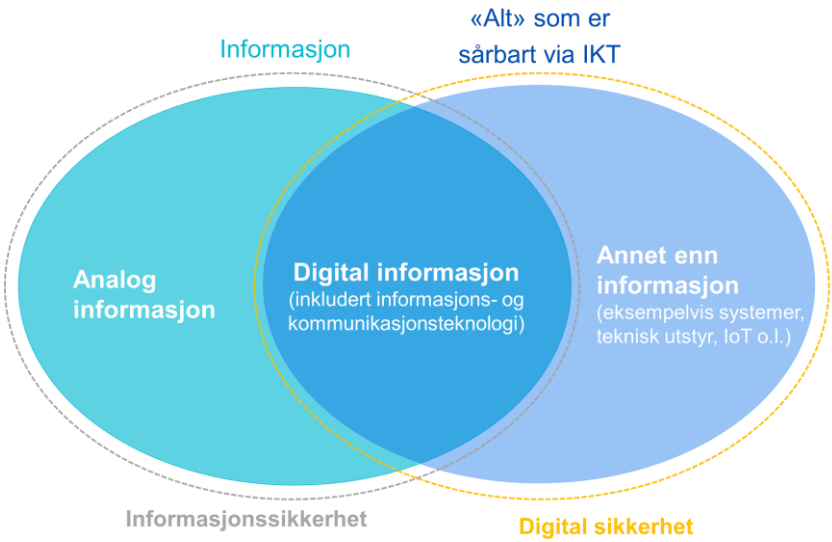
normalsituasjon, har også ansvaret for nødvendige beredskapsforberedelser og håndtering av ekstraordinære hendelser på sitt område.

Koronapandemien har utfordret oss på mange måter og synliggjort behovet for god helseberedskap. Pandemien har akselerert innføringen av nye digitale løsninger som gir store muligheter til å utvikle helse- og omsorgstjenesten til det beste for pasienter, helsepersonell og innbyggere. Samtidig introduserer digitalisering avhengigheter og nye sårbarheter gjennom stadig mer komplekse og integrerte systemer. Pandemien har også fremhevet virksomheters avhengigheter og verdikjeder. Når virksomheter som har roller i nasjonal beredskap og krisehåndtering er avhengige av sårbare leverandørkjeder som strekker seg ut av landet, har det betydning for Norges krisehåndteringsevne.[3]

Norge er blant de fremste landene i verden til å ta i bruk ny teknologi. Ved å møte digitale sikkerhetsutfordringer på en god måte og være forberedt på å håndtere fremtidige hendelser, kan helse- og omsorgssektoren få enda større utbytte av de positive mulighetene som følger av digitaliseringen.

Oppfølging av Nasjonal strategi for digital sikkerhet

Nasjonal strategi for digital sikkerhet (2019) definerer digital sikkerhet som beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte er avhengig av informasjons- og kommunikasjonsteknologi (IKT). Figuren under illustrerer hva som inngår i digital sikkerhet, samt avgrensningen mot begrepet informasjonssikkerhet.



Figur 1. *Illustrasjon av digital sikkerhet. Digital sikkerhet overlapper med informasjonssikkerhet der informasjonen er digitalt lagret og tilgjengelig via IKT. I tillegg tar digital sikkerhet for seg sikring av alt annet som er basert på, koblet til eller avhengig av informasjons- og kommunikasjonsteknologi. For helse- og omsorgssektoren vil dette for eksempel gjelde medisinsk utstyr og velferdsteknologi, som blir stadig tettere integrert i den øvrige IKT-infrastrukturen.*

[3] *Nasjonal sikkerhetsmyndighet,* Risiko 2021, *2021*

Daværende regjering ville med Nasjonal strategi for digital sikkerhet oppnå et felles grunnlag for håndtering av digitale sikkerhetsutfordringer som følger av en rask og gjennomgående digitalisering av det norske samfunnet. Strategien angir mål og prioriteringer som skal ligge til grunn for myndighetenes arbeid med digital sikkerhet. I strategien pekes det på følgende fem prioriterte områder med tilhørende overordnet mål:

- **Forebyggende digital sikkerhet** - Norske virksomheter digitaliserer på en sikker og tillitvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser
- **Digital sikkerhet i kritiske samfunnsfunksjoner** - Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur
- **Kompetanse** - Styrket digital sikkerhetskompetanse i tråd med samfunnets behov
- **Avdekke og håndtere digitale angrep** - Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep
- **Bekjempe data- og IKT-relatert kriminalitet** - Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.

Nasjonal strategi for digital sikkerhet understreker at det er i samspillet mellom en robust digital infrastruktur, evnen til å håndtere digitale angrep, bekjempelsen av data- og IKT-relatert kriminalitet og tilstrekkelig digital sikkerhetskompetanse at vi oppnår en helhetlig beskyttelse mot digitale hendelser. I helse- og omsorgssektoren er det i dag en rekke tiltak som følger opp de prioriterte områdene i den nasjonale strategien. En oversikt over disse er gitt i vedlegg A. De overordnede målsetningene har videre vært sentrale i utformingen av de foreslåtte innsatsområdene for arbeidet med digital sikkerhet i den nasjonale helseberedskapen.

Offentlige aktører med roller innen digital sikkerhet

Det er et virksomhetsansvar å ivareta den digitale sikkerheten, se omtale av roller og ansvar innen digital sikkerhet i kap. 3. Under følger en kort beskrivelse av utvalgte relevante nasjonale aktører som har påvirkning for arbeidet med digital sikkerhet for store deler av sektoren gjennom styringslinjer, tjenesteleveranser, veiledning eller lignende.

Helse- og omsorgsdepartementet (HOD) har det strategiske ansvaret for IKT-utviklingen i helse- og omsorgssektoren og har et overordnet ansvar for at befolkningen har tilgang til gode og likeverdige helse- og omsorgstjenester. HOD har det overordnede ansvaret for IKT-sikkerheten i spesialisthelsetjenesten. HODs underliggende etater ivaretar rollen som forvalter av IKT-løsninger, registre og sektorens felleskomponenter.

Helsedirektoratet har ansvar for å iverksette vedtatt politikk, samt forvalte lov og regelverk innenfor helse- og omsorgssektoren. Helsedirektoratet har også ansvar for den nasjonale beredskapen i sektoren.

Direktoratet for e-helse skal styrke digitaliseringen i helse- og omsorgssektoren for å understøtte effektive og sammenhengende helse- og omsorgstjenester. Direktoratet for e-helse har som myndighet et hovedansvar for å tydeliggjøre rammebetingelsene for informasjonssikkerhet i digitaliseringsarbeidet i sektoren, og er sekretariat for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

Helsetilsynet (Statens helsetilsyn) er øverste tilsynsmyndighet og har det overordnede faglige tilsynet med helse- og sosialtjenestene. Tilsyn og rådgivning skal medvirke til at befolkningens behov for sosiale tjenester og helsetjenester ivaretas, at tjenestene drives på en faglig forsvarlig måte, at svikt i tjenesteytingen forebygges og at ressursene brukes på en forsvarlig og effektiv måte. Statens helsetilsyn skal føre tilsyn med IKT-tjenestene i sektoren.

Norsk helsenett SF (NHN) er ansvarlig for utvikling, drift og forvaltning av nasjonale e-helseløsninger som ivaretar krav til sikkerhet og personvern. Gjennom Helsenettet fasiliterer NHN en trygg kommunikasjonsarena som muliggjør sikker utveksling av helsedata på tvers av foretak og behandlingsnivåer i sektoren.

HelseCERT (NHN) er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. De har som oppgave å øke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser. HelseCERT skal spre kunnskap om IKT-trusler og beskyttelsesmekanismer og kontinuerlig monitorere trafikken i Helsenettet.

Statens legemiddelverk (SLV) er fag- og tilsynsmyndighet for legemidler og medisinsk utstyr. De har oppgaver knyttet til forvaltning, tilsyn og overvåking, informasjon og veiledning.

Direktoratet for strålevern og atomtryggleik (DSA) er fag- og forvaltningsmyndighet på området strålevern, atomsikkerhet og ikke-spredning, radioaktiv forurensning og radioaktivt avfall.

Justis- og beredskapsdepartementet har samordningsansvaret for digital sikkerhet for sivil side av samfunnet. Ansvaret inkluderer blant annet å utarbeide og følge opp nasjonale strategier, identifisere sektorovergripende spørsmål og bidra til at ansvaret blir plassert og oppgaver blir håndtert på en god måte.

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og er det nasjonale fagmiljøet for IKT-sikkerhet. Nasjonalt cybersikkerhetssenter er etablert som en del av NSM og bidrar til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep.

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal ha oversikt over risiko og sårbarhet i samfunnet. De skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, og skal sørge for god beredskap og effektiv ulykkes- og krisehåndtering.

Kommunal- og distriktsdepartementet har ansvaret for politikkutforming og forvaltning innenfor en rekke sentrale samfunnsområder. Deres ansvarsområder inkluderer forvaltningspolitikk, modernisering, IKT-politikk og digitalisering av offentlig sektor, næringsrettet IKT, Digital21 og ressurser til IKT-forskning.

Datatilsynet er både tilsyn og ombud. Deres oppgave er å føre kontroll med at personvernregelverket etterleves og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Digitaliseringsdirektoratet (Digdir) skal bidra til utvikling og gjennomføring av regjeringen sin IKT-politikk. Digdir samordner og er pådriver i offentlig sektor sitt arbeid med forebyggende informasjonssikkerhet.

Nasjonal kommunikasjonsmyndighet (Nkom) er en tilsyns- og forvaltningsmyndighet for tjenester innenfor post og elektronisk kommunikasjon i Norge. Nkom er underlagt Kommunal- og distriktsdepartementet (KDD).

2. Hva gjøres i sektoren i dag

Det har lenge vært krav til ivaretakelse av informasjonssikkerhet når helse- og omsorgssektoren behandler helseopplysninger. I helseregisterloven av 2001 ble det stilt krav om sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet. Dette var også et poeng i statlig tiltaksplan for elektronisk samhandling i helse- og sosialsektoren 2001-2003, som fremhever at integriteten og sikkerheten til sensitive helsedata må ivaretas.[4] I takt med digitalisering i samfunnet og i sektoren, utvikling av lovverk på området, nasjonale og internasjonale sikkerhetshendelser, og økt avhengighet til teknologi har oppmerksomheten rundt digital sikkerhet i helse- og omsorgssektoren vært sterkt økende.

Arbeidet med digital sikkerhet i sektoren må skje som en del av en kontinuerlig forbedring, og det er sentralt å øke og ivareta modenhet innen digital sikkerhet over tid. Dette krever fokus fra sektoren fremover, og det skjer stadig utvikling både i de enkelte virksomhetene og ved felles innsats og virkemidler.

Sentrale virkemidler som HelseCERT og Normen har lenge vært viktige for sektoren, og bidrar til at sektorens totale beredskapsevne styrkes. I det følgende beskrives disse virkemidlene, samt en rekke andre pågående aktiviteter, virkemidler og annet arbeid som representerer bredden av det som i dag gjøres i sektoren innen digital sikkerhet. Dette er ikke en uttømmende oversikt, men har til hensikt å trekke frem noen viktige pågående aktiviteter, virkemidler og annet relevant arbeid.

HelseCERT

HelseCERTs formål er å gjøre helsesektoren sikrere.

En grunnleggende forutsetning for digitaliseringsarbeidet i helsetjenesten er at informasjonssikkerhet ivaretas. Riksrevisjonen har gjennomført en revisjon av helseforetakenes forebygging av angrep mot sine IKT-systemer, jf. Dokument 3:2 (2020–2021). Riksrevisjonens undersøkelse tydeliggjør behovet for å styrke arbeidet med informasjonssikkerhet i helse- og omsorgssektoren.

Norge har innført en modell med sektorvise responsmiljøer (SRM) for å styrke sikkerhetsarbeidet innenfor ulike samfunnsviktige sektorer. Formålet med et sektorvist responsmiljø er å bistå sin sektor med sikkerhetskompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå.[5] Det nasjonale cybersikkerhetskoordineringssentret (NCSC) er den nasjonale toppnoden i denne modellen. Under NCSC har man i Norge etablert en rekke SRM-funksjoner som samarbeider tett med NCSC.

HelseCERT er helsesektorens SRM, og ble etablert som en funksjon i Norsk helsenett SF på oppdrag fra Helse- og omsorgsdepartementet i 2011.

I grovt bistår et SRM sin sektor med å forebygge, oppdage og håndtere sikkerhetshendelser.

---

[4] *Sosial- og helsedepartementet, Si @!" elektronisk samhandling i helse- og sosialsektoren: statlig tiltaksplan 2001-2003*
[5] Tiltaksoversikt – Nasjonal strategi for digital sikkerhet, Departementene

- I det forebyggende sikkerhetsarbeidet har SRM-miljøene ansvar for å dele informasjon om trusler og sårbarheter, og å bistå med råd om effektive sikringstiltak. Denne informasjonen kan tilknyttede virksomheter bruke aktivt for å styrke sin egenbeskyttelse mot digitale angrep.
- Sikkerhetshendelser kan oppdages på ulike måter. Gjennom SRM-samarbeidet kan hendelser som har rammet én sektor koordineres, slik at andre sektorer kan forberede seg på og oppdage tilsvarende hendelse. Dersom en virksomhet oppdager en hendelse og varsler sitt SRM, kan SRM-funksjonen koordinere mot øvrige virksomheter i sektoren der det er relevant. Gjennom god informasjonsdeling og godt samarbeid blir SRM-modellen en muliggjører for å styrke både sektorer og samfunnet.
- Dersom en sikkerhetshendelse har inntruffet vil den rammede virksomheten kunne ha behov for støtte og rådgivning i hendelseshåndteringen. Slik støtte kan de få fra sitt SRM-miljø.

For å løse oppdraget som et SRM, og for å løse oppgavene over, har HelseCERT etablert Nasjonal Beskyttelsesprogram (NBP) for helsesektoren. I NBP er det etablert en rekke tjenester som til enhver tid er under videreutvikling for å løse oppdraget fra HOD, og samtidig tilby mest mulig verdi til helsesektoren og øke den nasjonale beredskapsevnen knyttet til IKT-sikkerhet. Alle tjenestene ligger innenfor spekteret av å forebygge, oppdage og håndtere sikkerhetshendelser.

- Gjennom et godt nettverk både nasjonalt og internasjonalt, med øvrige SRM-miljøer og andre, sitter HelseCERT med et godt og oppdatert trusselbilde. Informasjon om trusler og sårbarheter varsles til medlemmene i NBP, som regel med forslag til tiltak, slik at virksomhetene kan gjøre nødvendige grep for å forebygge sikkerhetshendelser. HelseCERT har etablert tjenester for å oppdage sårbarheter og svakheter i den internetteksponerte digitale infrastrukturen til virksomhetene i NBP. Som følge av kontinuerlig sårbarhetsskanning og at HelseCERT varsler virksomhetene om identifiserte sårbarheter, kan virksomhetene jobbe forebyggende med å lukke sårbarhetene før de utnyttes av en trusselaktør.
- Sikkerhetshendelser kan oppdages på mange ulike måter. HelseCERT har etablert en sensorplattform som kan bidra til å oppdage trusselaktører i den digitale infrastrukturen. I tillegg er HelseCERTs rike nettverk med andre sikkerhetsmiljøer en kilde til å oppdage sikkerhetshendelser hos tilknyttede virksomheter. HelseCERT varsler virksomheter fortløpende når det er tydelige indikasjoner på at de er rammet av en sikkerhetshendelse.
- Når en hendelse har oppstått står HelseCERT klar til å bistå den berørte virksomheten, eller de berørte virksomhetene, med råd og veiledning til hendelseshåndteringen.

Denne listen er ikke uttømmende, men illustrerende for oppgavene HelseCERT jobber med. NBP er et program som er utviklet for helsesektoren i stort. Medlemmene i NBP inkluderer hele spesialisthelsetjenesten, 95% av landets kommuner, og et par hundretalls små og store private virksomheter som leverer tjenester i Helsenettet.

HelseCERT legger NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser til grunn for arbeidet med håndtering av IKT-sikkerhetshendelser i, og mellom virksomheter.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen)

Normen[6] er en bransjenorm som er utarbeidet og forvaltes av organisasjoner og virksomheter i helse- og omsorgssektoren. Kravene i Normen er et omforent kravsett basert på norsk lov og beste praksis, og inneholder en rekke krav til helsevirksomhetene innen personvern og

[6] *Normen, Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, versjon 6.0*

informasjonssikkerhet. Normen gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge den. Dette skjer blant annet ved medlemskap i Helsenettet. I tillegg bruker mange virksomheter Normen som grunnlag for å stille krav til sine kunder/leverandører. Direktoratet for e-helse stiller med sekretariat for arbeidet til Normens styringsgruppe, med fast deltakelse fra NHN.

Normens aktiviteter består i tillegg til selve kravsettet for informasjonssikkerhet og personvern av veiledningsmateriell til Normens krav og er en arena for kompetanseheving og nettverksbygging for sektoren. Veiledningsmateriellet i Normen utbedres og suppleres kontinuerlig i tråd med utviklingen og behovene i sektoren. Som en følge av hyppigere hendelser og mer komplekse verdikjeder, har Normen blant annet nylig oppdatert sitt veiledningsmateriell innen internkontroll og risikostyring. Normens handlingsplan for 2022 omfatter blant annet veiledning tilknyttet etterlevelse («Normsjekk på nett»), leverandørhåndtering, og sikkerhetshendelser (deteksjon og respons).

Normen driver utstrakt utadrettet aktivitet. Sekretariatet for Normen holder løpende foredrag, kurs og webinarer for sektoren. Normens webinarserie er åpen for alle, og holdes enten av sekretariatets medlemmer, eller av foredragsholdere fra sektoren. Sektoren bidrar aktivt med å etterspørre temaer for fremtidige webinarer. Normen har utviklet tre kurs som holdes jevnlig og på forespørsel: Et grunnleggende introkurs til Normen, samt to modulbaserte kurs for henholdsvis teknisk personell og kommuner. Normen har også etablert seg som en fysisk møteplass gjennom den årlige Normkonferansen som arrangeres over to dager.

I NOU 2018:13 Digital sårbarhet - sikkert samfunn skrev Lysne-utvalget at de *observerer at «Normen er ønsket velkommen av sektoren, og at den i all hovedsak fungerer bra. Normen gjør at helseforetakene tør å stille krav, og leverandørene blir mer oppmerksomme på temaet ved anskaffelser. Prosessen med å utvikle Normen har hatt en god effekt i seg selv og økt kompetansen i bransjen.»*

Helsetilsynets tilsyn på digitale områder

Helsetilsynet har siden 2019 arbeidet med tilsyn med IKT i tjenestene. Hovedfokuset har vært IKT-systemers betydning for pasientsikkerheten. Helsetilsynets arbeid i perioden fra 2019 er oppsummert og publisert i tre rapporter. To kartlegginger handler om i hvilken grad norske sykehus var forberedt på å yte forsvarlig helsehjelp ved bortfall av IKT.[7] Kartleggingene viste at det var uklare ansvarsforhold mellom helseforetak og IKT-driftsleverandører, samt mangelfulle risikovurderinger før innføring og endring av IKT-systemer. Det er også kritiske utfordringer knyttet til legemiddelinformasjon. I flere regioner så tilsynet at det ikke legges tilstrekkelig vekt på å sikre at data er fullstendige og korrekte i ulike system. Praksisen med dobbeltregistrering i flere system strider mot kravet om at journalen skal gi en samlet framstilling av pasientens helsetilstand. Dette medfører også ekstra arbeid og risiko for feil og uforsvarlig pasientbehandling.

Helsetilsynet har også kartlagt hvor de største risikoene er for svikt i pasientbehandlingen, tilknyttet IKT.[8] Tilsynet identifiserte der ni spesifikke risikoer ved bruk av IKT, som kunne få negativ betydning for pasientbehandlingen. Formålet var både å prioritere framtidig

[7] *Helsetilsynet, Forsvarlig pasientbehandling uten IKT?, 2021*
[8] *Helsetilsynet, Hvor har feil og mangler ved bruk av IKT-systemer størst konsekvenser for pasientsikkerheten? En risikoanalyse, 2021*

tilsynsaktivitet, men også å gi en retning for hvordan man kan prioritere digitalisering med virkning på pasientsikkerheten.

Framover vil Helsetilsynet blant annet prioritere tilsyn med IKT-systemer for legemiddelinformasjon i spesialisthelsetjenesten og ha fokus på bruk av medisinsk utstyr. Helsetilsynet vil se på bruk av velferdsteknologi i kommunal helse- og omsorgstjeneste og bistå inn i koordineringsprosjektet «Bedre bruk av kunstig intelligens» som har fokus på trygg og sikker innføring av denne typen medisinsk utstyr.

Aktiviteter i kommunene

Digitaliseringstakten i kommunene og deres helsetjenester er høy, og det pågår en rekke aktiviteter rettet mot sikkerhet og beredskap både nasjonalt i regi av KS og i interkommunale samarbeid.[9] Det er bred enighet i kommunesektoren om at digitalisering og smart bruk av teknologi er sentrale virkemidler for å heve pasientsikkerheten, sikre bedre samhandling, få økt kapasitet, og videreutvikle helse- og omsorgstjenesten. Stat og kommune er enige om at sektoren som helhet bør arbeide sammen om de store fremtidige utfordringene. Målet er å skape løsninger i felleskap, og ikke hver for seg.

I samarbeid med medlemmene og samstyringsstrukturen for digitalisering i kommunal sektor, arbeider KS med å bidra til sterkere standardisering av programvare og komponenter. Dette vil gjøre at kommuner med mindre ressurser lettere kan ta disse i bruk på en trygg og sikker måte. Det er blant annet satt i gang et arbeid med rammeverk innen sikkerhet: Rammeverk for Trygg Digitalisering (RTD). Målgruppen for RTD er først og fremst små og mellomstore kommuner, slik at disse har en enkel veiledning og metodeverk som kan hjelpe med å digitalisere trygt, sikkert og raskere. Det utvikles også en referansearkitektur for informasjonssikkerhet, digital beredskap og personvern for kommunal sektor (RSB), som vil gjøre det enklere å stille krav til utvikling, innføring og forvaltning av kommune e-helseløsninger. I tillegg er det planlagt å etablere tverrsektorielle regler for sertifisering og godkjenning av leverandører som leverer teknologi i kommunal helse- og omsorgssektor, og det er opprettet en ressursbank for risiko og tiltak som kan bidra til å redusere ressursbruk ifm. risikovurderinger.

Kommunal sektor har en rekke arenaer for å sikre kunnskapsutvikling og -deling. Strategisk nettverk for informasjonssikkerhets- og personvernansvarlige (SNIP-nettverket) skal bidra til å gjøre kommunene mer robuste med hensyn til sikkerhetsutfordringene de står overfor. Fagråd for informasjonssikkerhet og personvern bidrar med faglige råd og kvalitetssikring av nye felles prosjekter for kommunal sektor. Regionale digitaliseringsnettverk bidrar til å samordne digitaliseringsarbeidet, og Foreningen kommunal informasjonssikkerhet (KiNS) driver aktiviteter for å bidra til å økt informasjonssikkerhet og personvern i kommuner og fylkeskommuner.

Regjeringen fremmet gjennom proposisjon 78 S (2021-2022)[10] forslag om økt bevilgning på 40 millioner kroner i 2022 for å tilrettelegge for at kommunene kan knytte seg til et cybersikkerhetssamarbeid (CERT eller tilsvarende). Videre ble det foreslått i proposisjonen en ordning for å styrke kommunenes kompetanse og kapasitet til å forebygge og håndtere digitale hendelser med en ramme på 10 millioner kroner. Bevilgningene er vedtatt i Stortinget. Proposisjonen peker på at det er et særskilt behov for å styrke den digitale sikkerheten i kommunal forvaltning, men at særlig små og mellomstore kommuner har faglige og økonomiske utfordringer med å ivareta dette ansvaret. Det pågår dialog mellom Kommunal- og

[9] Se *Digitalisering i helse- og omsorgsektoren (e-helse) - KS*
[10] *Prop. 78 S Endringer i Statsbudsjettet 2022*

distriktsdepartementet og KS om utformingen av ordningen. For å gjennomføre tiltakene vil KS etablere et Nasjonalt program for informasjonssikkerhet for kommunal sektor – NPISK.

Digital sikkerhet i helse- og sosialfaglig utdanning

Justis- og beredskapsdepartementet har i samarbeid med Kunnskapsdepartementet utarbeidet en nasjonal strategi for digital sikkerhetskompetanse.[11] Strategien peker på at kompetansebehovet i ulike yrker endrer seg hurtig, i møte med teknologisk utvikling. Det understrekes at digitalisering påvirker risikobildet, og at dette krever at også de ansvarlige for ulike yrkes- og profesjonsutdanninger må vurdere hvordan digital sikkerhet kan integreres i utdanningene.

Det er opprettet et prosjekt (DigSam) for utvikling av en åpen læringsressurs for sikkerhetsopplæring innen helsefaglige utdanninger. Prosjektet er et samarbeid mellom UiT - Norges arktiske universitet, NTNU - Norges teknisk-naturvitenskapelige universitet, HVL - Høgskulen på Vestlandet, USN – Universitetet i Sør-Øst Norge og OsloMet. Tiltaket er en del av føringen som ligger i Forskrift om felles rammeplan for helse- og sosialfagutdanninger. Det fremgår av forskriftens § 2 om felles læringsutbytte at "kandidaten kan vurdere risiko for uønskede hendelser og kjenner til metoder for å følge opp dette systematisk, samt at kandidaten har digital kompetanse og kan bistå i utviklingen av og bruke egnet teknologi både på individ- og systemnivå. DigSam-prosjektet utvikler, utprøver og evaluerer undervisnings- og vurderingsressurser til studenter om digital sikkerhet for å sikre at kandidatene i helse- og sosialfaglige utdanninger kan sørge for digital sikkerhet i egen yrkesutøvelse for å møte samfunnets behov for trygge digitale løsninger.

Regionale handlingsplaner

De regionale helseforetakene har på oppdrag fra HOD utarbeidet regionale handlingsplaner for arbeidet med informasjonssikkerhet. Oppdraget ble gitt til som oppfølging av Riksrevisjonens funn fra deres gjennomgang av helseforetakenes forebygging av angrep i sine IKT-systemer.[12] Tiltakene i handlingsplanene dreier seg blant annet om roller og ansvar, oversikt, rapportering og oppfølging, kompetanse, informasjonssikkerhet i anskaffelser, applikasjoner, infrastruktur og teknisk sikkerhet og kontinuerlig forbedring. De regionale handlingsplanene for arbeidet med informasjonssikkerhet er nærmere omtalt i Vedlegg A. Handlingsplanene følges opp i helseregionene.

Implementering av sikkerhetsloven

Lov om nasjonal sikkerhet, med underliggende forskrifter, ble gjort gjeldende fra 1. januar 2019. Lovens formål er å trygge nasjonale sikkerhetsinteresser ved å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Departementet er ansvarlig for det forebyggende sikkerhetsarbeidet innenfor eget ansvarsområde og skal identifisere og holde oversikt over hva som skal beskyttes. Helse- og omsorgsdepartementet skal ha oversikt over grunnleggende

[11] *Justis- og beredskapsdepartementet og Kunnskapsdepartementet, Nasjonal strategi for digital sikkerhetskompetanse, 2019*
[12] *https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer/*

nasjonale funksjoner, virksomheter som er av vesentlig betydning for disse, virksomheter som er underlagt loven, og verdier som skal beskyttes, og melde inn til NSM, som skal ha den samlede oversikten. Departementet skal også se til at virksomheter i sektoren har sikkerhetsstyringssystem.

Gitt krav i loven har Helse- og omsorgsdepartementet utpekt grunnleggende nasjonale funksjoner (GNF) i helse- og omsorgssektoren. Dvs. tjenester, produksjon og andre former for virksomhet der helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser. HOD har identifisert GNF-ene *helseberedskap* og *trygg vannforsyning* innenfor eget myndighetsområde, samt en felles departemental GNF.

Departementet har identifisert og holder oversikt over virksomheter som har vesentlig betydning for disse funksjonene, samt virksomheter som behandler sikkerhetsgradert informasjon, råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, og/eller driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, og fattet vedtak etter sikkerhetsloven § 1-3 første ledd om at loven helt eller delvis skal gjelde for virksomheten.

Departementet har identifisert virksomheter i sektoren som omfattes av loven. Av lovens § 1-2 fremgår det at sikkerhetsloven gjelder statlige, fylkeskommunale og kommunale organer. Det vil si alle virksomheter i helse- og omsorgssektoren, inkl. RHF, HF og NHN SF da de regnes som «statlige, fylkeskommunale og kommunale organer» etter s-loven § 1-2.

Departementet har fattet vedtak etter lovens § 1-3 om at andre avgjørende virksomheter omfattes av loven. HOD vedtok høsten 2021 med hjemmel i s-loven § 1-3 første ledd bokstav b at Helse Vest IKT AS og Helseplattformen AS omfattes av loven fordi de "råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for GNF". HOD har meldt de to til NSM og sendt brev til Helseplattformen og Helse Vest IKT med varsel om vedtak om at «virksomheten» vil bli omfattet av sikkerhetsloven. HOD har mottatt svar fra begge. Endelig vedtak er planlagt sendt før sommeren 2022.

Virksomheter i helsesektoren har utarbeidet skadevurderinger, som grunnlag for å identifisere virksomheter av vesentlig og avgjørende betydning for GNF-ene, samt for å peke ut og klassifisere skjermingsverdige verdier (informasjon, informasjonssystem, infrastruktur og objekter). Når de skjermingsverdige verdiene er pekt ut og klassifisert, skal virksomheten som råder over dem gjennomføre risikoanalyser og, gjennom sin risikostyring identifisere behov for sikringstiltak, avhengigheter til andre virksomheter og sørge for nødvendig sikring.

Innføring av NIS-direktivet i norsk lov

NIS-direktivet er Europaparlamentets og Rådets direktiv (EU) om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU. Direktivet pålegger medlemsstatene å sørge for et visst nivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser.[13]

Bakgrunnen for NIS-direktivet var at det innen EU ikke har vært implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverk og informasjonssystemer

[13] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/

som er særlig viktige for det indre markeds funksjon. Direktivet setter krav til medlemslandenes arbeid med digital sikkerhet, til virksomheter som leverer tjenester som er essensielle for det indre markeds samfunnsmessige og økonomiske aktiviteter og til tilbydere av enkelte digitale tjenester. Virksomhetene faller i to kategorier. For det første tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. For det andre tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.[14]

Personvernforordningen (GDPR)

Lov om behandling av personopplysninger (personopplysningsloven)[15] gjennomfører EUs personvernforordning (GDPR) i norsk lov. Forordningen er et sett regler som gjelder for alle EU/EØS-land, som sammen med nasjonal særlovgivning om personvern på enkelte områder, utgjør det norske personvernregelverket. Personvernforordningen regulerer behandling av personopplysninger og pålegger virksomhetene, også i helse- og omsorgssektoren, en rekke plikter. Samtidig gir den enkeltpersoner (de registrerte) en rekke rettigheter.

Særlig relevant i denne sammenheng er forordningens artikkel 32[16], som beskriver virksomhetenes plikt til å ivareta personopplysningssikkerheten, blant annet ved å gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Videre er det relevant å trekke frem kravene til overføring av personopplysninger til tredjeland, herunder bruk av skytjenester. Slik overføring krever et særskilt grunnlag for å være lovlig. Den såkalte Schrems II-avgjørelsen har medført endringer i dette grunnlaget for overføringer til blant annet USA. Krav ved overføring til tredjeland er et område i stadig utvikling, og den enkelte virksomhet må gjøre vurderinger av hvorvidt tredjelandet gir like god beskyttelse av personopplysningene som innen EØS.[17]

Helseopplysninger er beskrevet i personvernforordningens artikkel 9[18] som en særlig kategori av personopplysninger, og krever derfor at spesifikke vilkår oppfylles før det er lov å behandle disse. For helse- og omsorgssektoren er dette i all hovedsak regulert i norsk helselovgivning.

Helselovgivningen

God informasjonssikkerhet er viktig for å kunne utøve forsvarlige helsetjenester. Helselovgivningen setter derfor også særskilte krav til informasjonssikkerhet. I helse- og omsorgssektoren behandles det store mengder opplysninger som grunnlag for gode helse- og omsorgstjenester, helseregistre, forskning og innovasjon. Opplysningene må behandles slik at helse- og omsorgstjenester kan tilbys på en forsvarlig måte og samtidig ivaretar innbyggernes tillit til sektoren.

Det er flere helselover og forskrifter som direkte eller indirekte stiller krav av betydning for digital sikkerhet. Særlig kan lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven)[19] nevnes. Loven regulerer virksomheters plikter ved behandling av helseopplysninger. Lovens § 22 fremhever at virksomheter skal gjennomføre tekniske og

---

[14] Justis- og beredskapsdepartementet, *Meld. St. 5 - Samfunnssikkerhet i en usikker verden, 2020, s. 86*
[15] Justis- og beredskapsdepartementet, *Lov om behandling av personopplysninger, 2018*
[16] Justis- og beredskapsdepartementet, *Lov om behandling av personopplysninger, 2018, art. 32*
[17] Datatilsynet, *Tilleggskrav (Schrems II), sist endret 04.11.2021*
[18] Justis- og beredskapsdepartementet, *Lov om behandling av personopplysninger, 2018, art. 9*
[19] Helse- og omsorgsdepartementet, *Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten, 2016*

organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, og viser til personvernforordningens artikkel 32. Videre beskriver forskrift for ledelse og kvalitetsforbedring i helse- og omsorgstjenesten[20] at virksomheten plikter å etablere systematisk styring og ha oversikt over risiko i virksomheten og hvordan man kan minimalisere denne. Dette skal bidra til faglig forsvarlige helse- og omsorgstjenester, kvalitetsforbedring og pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves.

Det finnes en god oversikt over krav til informasjonssikkerhet og personvern i helse- og omsorgssektoren i Normen,[21] (se omtale ovenfor).

Foreslått EU-forordning: European Health Data Space (EHDS)

EUs overordnede digitaliserings- og datastrategi fra 2020[22] slår fast at Europa ønsker å ta en sterkere og mer ledende rolle i den datadrevne økonomien globalt, og at den europeiske dataøkonomien skal være fundert på felles regelverk grunnleggende europeiske verdier. En viktig oppgave i realiseringen av datastrategiens mål er å få på plass et rammeverk for ni europeiske dataområder (European Data Spaces). I kjølvannet av koronapandemien har EU-kommisjonen løftet frem helse som et prioritert område for utvikling av et europeisk fellesområde for data – European Health Data Space (EHDS)[23].

Målet med EHDS er å fremme sikker tilgang til og utveksling av helsedata på tvers av landegrenser i EU og skape et indre marked for data, og foreligger på nåværende tidspunkt som forslag til en forordning[24]. Som hovedmål fremheves i forordningen å gi innbyggere tilgang til og kontroll på sine egne helsedata; å fremme et indre marked for digitale helsetjenester- og produkter; og tilrettelegge for en sikker og effektiv ramme for bruk av helsedata til forskning, innovasjon, politikkutforming og regulering.

Det er blant annet foreslått obligatoriske krav til interoperabilitet, sikkerhet og personvern for deling av helsedata mellom ytere av helsetjenester; en selvdeklareringsordning for leverandører av EPJ-systemer ut fra disse kravene; frivillig merking av helseapper for å sikre interoperabilitet med EPJ og dataportabilitet; og at innbyggere skal ha elektronisk tilgang til sine helsedata, på et felles europeisk format som man kan med seg og vise også i andre land. EHDS-forordningen skal være harmonisert med og komplementær til personvernforordningen (GDPR).[25]

[20] Helse- og omsorgsdepartementet, *Lov om behandling av helseopplysninger ved ytelse av helsehjelp, 2014*
[21] *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), versjon 6.0*
[22] EU-kommisjonen, *A European Strategy for Data*
[23] EU-kommisjonen, *European Health Data Space*
[24] EU-kommisjonen, *Proposal for a regulation – The European Health Data Space, COM(2022) 197/2*
[25] EU-kommisjonen, *Proposal for a regulation – The European Health Data Space, COM(2022) 197/2*

Relevante rapporter:

- *Direktoratet for e-helse, Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren, 2019*
- *Norsk helsenett, Situasjonsbilde 2021, 2021*
- *Helse- og omsorgsdepartementet, Nasjonal helseberedskapsplan, 2018*
- *NOU 2015: 13 Digital sårbarhet – sikkert samfunn (Lysneutvalget), 2015*
- *Meld. St. 38 (2016-2017), IKT-sikkerhet – Et felles ansvar, 2017*
- *Utenriksdepartementet, Internasjonal cyberstrategi for Norge, 2017*
- *Justis- og beredskapsdepartementet og Kunnskapsdepartementet, Nasjonal strategi for digital sikkerhetskompetanse, 2019*
- *NOU 2018: 14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet, 2018*
- *Direktoratet for samfunnssikkerhet og beredskap, Risikostyring i digitale verdikjeder, 2020*
- *Forsvarets forskningsinstitutt (FFI), Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene – en vurdering, 2020*
- NSMs årlige trussel- og risikovurderinger

3. Utfordringsbildet

Utfordringer knyttet til digital sikkerhet

Helse- og omsorgssektoren kjennetegnes ved et omfattende og komplekst aktørbilde. Sektoren er unik når det kommer til omfanget av beskyttelsesverdige data i form av helseopplysninger. Helsedata har høy verdi, og er særlig utsatt for misbruk og uautorisert spredning. Behovet for å sikre konfidensialitet, tilgjengelighet og integritet til både informasjon og systemer er særlig sterkt, fordi det er evnen til å gi forsvarlig helsehjelp og ivareta pasientsikkerheten som står på spill. Å sørge for robusthet der helsedata behandles er grunnleggende for å opprettholde tillit til helsevesenet.[26] Teknologi og systemer kan være sårbare for digitale trusler, og det inkluderer ikke bare systemer knyttet direkte til pasientbehandling. Systemer og tjenester for leveranser av varer og tjenester til helsetjenesten, produksjon og distribusjon av legemidler og vaksiner og lignende er også viktig å beskytte i et beredskapsperspektiv. Dette er viktige virkemidler ikke bare for å yte helse- og omsorgstjenester, men også for folkehelsen.

Sektoren står overfor et skjerpet digitalt trusselbilde
Det har vært en markant økning i antall alvorlige cyberangrep, og både i Norge og internasjonalt er det flere eksempler på hendelser som har rammet sektoren. Nasjonale etterretnings- og sikkerhetsmyndigheter har i sine åpne vurderinger trukket frem helse- og omsorgssektoren som risikoutsatt. Et trussel- og risikobilde i stadig endring vil i stor grad påvirke hvordan sektoren skal dimensjonere sikkerhetsarbeidet i tiden fremover.

Truslene sektoren står overfor spenner bredt, fra kriminelle aktører med intensjon om økonomisk vinning til statlige aktører som innhenter informasjon med etterretningsverdi. HelseCERT har vurdert det som meget sannsynlig at avanserte trusselaktører forsøker å tilegne seg forskningsdata og helseopplysninger.[27] Destruktive angrep som løsepengevirus og sabotasje kan få store konsekvenser ved at kritiske systemer og tjenester gjøres utilgjengelige, eller at sensitiv informasjon kommer på avveie med trusler om offentliggjøring hvis løsepengekrav ikke imøtekommes.

Et komplekst systemlandskap og mangelfull implementering av grunnleggende sikkerhetstiltak
Sektoren har et stort og komplekst landskap av systemer, og det er stor variasjon i implementering av sikkerhetstiltak. NSM erfarer at det ofte er de samme feilene som gjøres, både i offentlige og private bedrifter, og at de fleste cyberhendelser hadde vært avverget eller fått begrenset skadeomfang om NSMs grunnprinsipper hadde vært fulgt.[28] Helse- og omsorgssektorens størrelse og kompleksitet tilsier at denne beskrivelsen er treffende også her. Dette bekreftes av tilbakemeldinger som har blitt gitt av aktører i sektoren i dette arbeidet.

I Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer trekkes det frem at det er svakheter i grunnleggende sikkerhetstiltak. Dette omfatter blant annet kontroll med enheter, programvare, brukerkontoer og tilgangsrettigheter, samt sårbarhetsstyring av IKT-utstyr og programvare, og logging og overvåking. Utdaterte tekniske løsninger står i noen tilfeller i veien for god sikkerhet, og innføring av nye løsninger prioriteres

[26] Dette innebærer at virksomheter, systemer og tjenester tåler endringer og ytre påvirkninger, samtidig som at personvernprinsipper og de registrertes rettigheter og friheter ivaretas.
[27] Norsk helsenett, *Situasjonsbilde 2021, 2021*
[28] Nasjonal sikkerhetsmyndighet, *Risiko 2022, 2022, s.37*

uten at gamle, usikre løsninger fases ut. Omfang av utstyr, systemer og programvare i sektoren gjør at utbedring av kjente svakheter kan ta lang tid[29].

Udekket kompetansebehov
De ansatte i sektoren blir stadig mer avhengig av digitale løsninger og systemer for å utføre sine arbeidsoppgaver. Det trengs et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra virksomhetens øverste ledelse til den enkelte ansatte.[30] Det er en utfordring at digital sikkerhet stort sett ligger langt unna de ansattes kjernekompetanse.

Uheldig sikkerhetsatferd bidrar til å svekke den digitale sikkerheten, og kan utgjøre en vei inn i systemene for trusselaktører. Ifølge NSM er det mange eksempler på styrer og ledere som tar store, strategiske avgjørelser uten å kjenne til virksomhetens digitale sikkerhetstilstand. Slike feilgrep fører ofte til store og kostbare opprydningsjobber, og de bunner i mange tilfeller i manglende kunnskap og forståelse hos toppledelsen, så vel som hos fagpersonell.[31] For eksempel kan manglende informasjonsgrunnlag og forståelse for digital sikkerhet hos beslutningstakere medføre feilprioriteringer eller nedprioritering av nødvendige sikkerhetstiltak.

Det er tidligere pekt på at digital sikkerhet bør styrkes i helsefaglige utdanninger.[32] I forskrift om felles rammeplan for helse- og sosialfagutdanninger heter det at kandidatene skal ha digital kompetanse, og skal kunne bistå i utviklingen av og bruke egnet teknologi både på individ- og systemnivå[33]. Det pågår initiativer for å inkludere mer digital kompetanse i helseutdanningene, men det er fortsatt potensial for å øke fokuset på digital sikkerhet.

I tillegg er det knapphet på ekspertkompetanse knyttet til digital sikkerhet både nasjonalt og internasjonalt. Dette gjør det krevende å rekruttere, utvikle og beholde tilstrekkelig kompetente fagressurser. Konkurransen om slike ressurser forsterkes av at de etterspørres i alle sektorer.

Varierende oppfølging av digital sikkerhet i verdikjeder
Utfordringer knyttet til kravstilling og risikostyring gjør seg gjeldende både for bestillere og leverandører. Særlig de mindre virksomhetene opplever det utfordrende og tidkrevende å utøve sikkerhetsstyring, samt å gjennomføre gode risikovurderinger og leverandørkontroll. Leverandøroppfølging omtales også som en utfordring av de større virksomhetene – det er krevende for den enkelte virksomhet å skaffe oversikt over hvilke avhengigheter en tjeneste har og hvilke sårbarheter man eksponeres for i andre ledd av verdikjeden. Manglende oversikt over verdikjeder har innvirkning på digital sikkerhet. Cyberoperasjoner rammer virksomheter som leverer tjenester til en lang rekke andre virksomheter med viktige samfunnsfunksjoner. Uoversiktlige verdikjeder og avhengigheter på tvers av samfunnsfunksjoner gjør at hendelser kan innvirke både på samfunnssikkerheten og statssikkerheten.[34] Når virksomheter som har roller i nasjonal beredskap og krisehåndtering er avhengige av sårbare leverandørkjeder som strekker seg ut av landet, har det betydning for Norges krisehåndteringsevne.[35] I dialogen med sektor har sikkerhet i leverandørkjeden blitt fremhevet som et tema det ønskes fokus på.

---

[29] Riksrevisjonen, *Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer, 2020*
[30] Nasjonal sikkerhetsmyndighet, *Risiko 2022, 2022, s. 9*
[31] Direktoratet for e-helse, *Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren, 2019, s. 22*
[32] Justis- og beredskapsdepartementet og Kunnskapsdepartementet, *Nasjonal strategi for digital sikkerhetskompetanse, 2019, s.24*
[33] Kunnskapsdepartementet, *Forskrift om felles rammeplan for helse- og sosialfagutdanninger, § 2-12*
[34] Nasjonal sikkerhetsmyndighet, *Risiko 2022, 2022, s. 20*
[35] Nasjonal sikkerhetsmyndighet *Risiko 2021*

Definisjon av digital verdikjede: *En digital verdikjede er en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware. En oversikt over en digital verdikjede består derfor i en oversikt over en fysisk infrastruktur, samt hvem som eier, vedlikeholder og opererer de forskjellige delene av denne. Videre vil den bestå av en oversikt over hvilke digitale tjenester som utveksles mellom de forskjellige delene, samt hvilken hardware og software som inngår.*
Direktoratet for samfunnssikkerhet og beredskap, Risikostyring i digitale verdikjeder 2020

Sektorens aktører beskriver at det er stor variasjon i kravstilling til og oppfølging av leverandører.[36] Ulik tolkning av krav og mangelfull kontroll av etterlevelse medfører lite effektive anskaffelser og reduserer sektorens evne til å ta i bruk ny teknologi. I rapporten *Samarbeid med næringslivet på e-helseområdet* beskrives det at leverandørene uttrykker frustrasjon over det som fremstår som manglende kompetanse om standarder, kvalitet og retningslinjer hos kunder. De regulatoriske rammene oppleves ikke å være godt nok forstått på innkjøpssiden, og kundene sliter dermed med å veilede leverandørene på hvilke standarder og regulatoriske krav de må tilpasse sine produkter og tjenester til. Det pekes på at faren for å bli tatt i å gjøre feil, eller at data kan komme på avveie, bidrar til et stort behov for å sikre seg. Leverandører forteller at denne berøringsangsten begrenser innovasjonstakten. Der det er gode normer for samspill mellom aktørene er gjennomføringsevnen til gjengjeld høy.[37]

Teknologiskifter og nye samhandlingsformer og leveransemodeller for helsehjelp
I det tidligere arbeidet med å vurdere innretting og behov for en sektorstrategi for digital sikkerhet, var sektoren særlig opptatt av at sikkerhet i leverandørkjeden, sikker samhandling og sikker digital hjemmeoppfølging måtte trekkes frem som sektorspesifikke temaer. Dette er eksempler på ny teknologi som gir store muligheter, men som også bringer med seg viktige sikkerhetsaspekter. Andre eksempler er kunstig intelligens, økt bruk av helsedata, persontilpasset medisin, bruk av skytjenester og økt samhandling gjennom data- og dokumentdeling.

For å lykkes med teknologiskiftet og nyttiggjøre teknologien er evnen til å identifisere og håndtere risiko i innføring og bruk av ny teknologi en kritisk suksessfaktor. Vurdering av risiko, sårbarheter og personvernkonsekvenser knyttet til ny teknologi og nye tjenester er ressurs- og kompetansekrevende. Ofte utføres tilnærmet identiske vurderinger av hver enkelt virksomhet.[38]

Medisinsk utstyr[39] og velferdsteknologi blir stadig tettere integrert i den øvrige IKT-infrastrukturen. Slikt utstyr kan ha egne lagringsenheter, nettverksoppkobling og kommunikasjon med andre systemer og skytjenester. Medisinsk utstyr kan også omfatte programvare. Dette introduserer nye utfordringer, blant annet knyttet til nye leveransemodeller, sårbarheter og endrede krav til bestiller- og brukerkompetanse. Samtidig har utstyret ofte lang levetid, og er utfordrende å holde oppdatert og sikre.[40] Utstyr plasseres i delvis ukontrollerte omgivelser, for eksempel i pasientens hjem, og det er mange involverte aktører.

[36] Direktoratet for e-helse, *Oppsummering av innspill gitt i arbeidsmøter med helse- og omsorgssektoren, 2021-2022*
[37] Direktoratet for e-helse, *Samarbeid med næringslivet på e-helseområdet, 2021*
[38] Direktoratet for e-helse, *Oppsummering av innspill gitt i arbeidsmøter med helse- og omsorgssektoren, 2021-2022*
[39] Se definisjon i lov om medisinsk utstyr, § 3
[40] Se Direktoratet for e-helse, *Veileder personvern og informasjonssikkerhet – medisinsk utstyr, 2021*

Roller og ansvar innen digital sikkerhet

Roller og ansvar innen digital sikkerhet må være tydelige, kjente og ivaretatt av sektorens virksomheter for at den digitale sikkerheten kan ivaretas på en effektiv måte. I dag peker mange aktører i sektoren på uklare roller og ansvar som en av de sentrale utfordringene knyttet til arbeidet med digital sikkerhet. Dette er derfor et viktig område å adressere i arbeidet med digital sikkerhet i helseberedskapen.

Hver enkelt aktør har ansvar for den digitale sikkerheten i sin virksomhet. Dette følger av ansvarsprinsippet, som innebærer at den som har et ansvar for en virksomhet, også har et ansvar for nødvendig forebyggende sikkerhet, beredskapsforberedelser og håndtering ved hendelser i en krisesituasjon. Dette er et ledelsesansvar, og det er sentralt at hver virksomhet ivaretar sitt ansvar gjennom nødvendig styring og kontroll, risikostyring, tekniske sikkerhetstiltak, prosesser, rutiner, planverk, nødvendig kompetanse og sikkerhetskultur.

Ved hendelser som angår flere virksomheter fungerer HelseCERT som et nav som koordinerer innsats og informasjonsdeling på tvers, og samarbeider med NSM og andre relevante myndighetsaktører.

Helse- og omsorgssektoren består av mange tusen virksomheter med ulike rammebetingelser og oppgaver. Nye samhandlingsformer bidrar til at sektoren blir stadig mer digitalisert og integrert. Sårbarheter kan oppstå når flere virksomheter deler ansvar for sikkerheten, der man legger andres risikovurderinger til grunn eller der man antar at sikkerheten blir ivaretatt av andre. Ved digital samhandling med utveksling av helseopplysninger er det særlig viktig at partenes ansvar og oppgaver er klart definert for å unngå ansvarspulverisering og at sikkerheten ikke blir ivaretatt på en forsvarlig måte.

I det følgende omtales utfordringer med roller og ansvar for aktører som yter helsehjelp, samt noen særskilte områder hvor det er behov for at roller og ansvar avklares.

Primærhelsetjenesten
Etter lov om kommunale helse- og omsorgstjenester skal hver kommune sørge for at personer som oppholder seg i kommunen, tilbys nødvendige helse- og omsorgstjenester. Tjenestene ytes av kommunene selv eller ved at kommunen inngår avtale med andre offentlige eller private tjenesteytere.[41] Eksempelvis har kommunene inngått avtaler med over 5000 fastleger.

Når kommunene yter tjenestene selv, er kommunen dataansvarlig og ansvarlig for å ivareta digital sikkerhet. Når kommunen har inngått avtale med andre ytere av helsehjelp, vil den enkelte tjenesteyter ha ansvaret for digital sikkerhet i sin virksomhet og normalt også være dataansvarlig.

Kommunens ansvar innebærer også plikt til å legge til rette for samhandling mellom ulike deltjenester innad i kommunene og med andre tjenesteytere. Kommunene skal samarbeide med fylkeskommune, regionalt helseforetak og stat slik at helse- og omsorgstjenesten i landet best mulig kan virke som en enhet.[42]

Kommunenes oppgaver er tverrsektorielle og den digitale sikkerhet knyttet til utøvelse av helsehjelp har avhengigheter til den helhetlige håndteringen av digital sikkerhet i kommunen. Kommunene opplever høyt digitaliseringstrykk, og deres sikkerhetsutfordringer strekker seg på tvers av sektorer, med mange initiativer, aktører og veiledninger å forholde seg til. Kommunene

[41] Lov om kommunale helse- og omsorgstjenester § 3-1 Kommunens overordnede ansvar for helse- og omsorgstjenester
[42] Lov om kommunale helse- og omsorgstjenester § 3-4 Kommunens plikt til samhandling og samarbeid

har også ansvar for å beskytte befolkningens helse og forebygge sykdom og skade ved å sørge for smittevern, miljørettet helsevern, trygt drikkevann og strålevern. Digitale trusler kan også påvirke kommunenes evne til å yte tjenester innenfor disse områdene.

Primærhelsetjenesten består av mange små tjenesteytere. De har ytelse av helsehjelp som sitt fagfelt og mindre kompetanse på sikkerhet og digitalisering. Mange kommuner er små og har begrenset kapasitet og kompetanse innen digital sikkerhet. Kommunene kan sette ut oppgaver, også innen sikkerhet, men ikke delegere lovpålagt ansvar. Kommunene ser kravstilling til og oppfølging av leverandører av tjenester og utstyr som særlig utfordrende. Digital hjemmeoppfølging er et område som introduserer nye problemstillinger der mange aktører med ulike roller er involvert.

Spesialisthelsetjenesten
Etter spesialisthelsetjenesteloven skal hvert regionale helseforetak sørge for at personer med fast bopel eller oppholdssted innen helseregionen tilbys spesialisthelsetjenester. Tjenestene kan ytes av de regionale helseforetakene selv, gjennom helseforetak de eier, eller ved at de inngår avtale med andre tjenesteytere.[43] I hver helseregion er det en regional IKT-leverandør av IKT-infrastruktur og tjenester.

Riksrevisjonen påpekte at rolle- og ansvarsfordelingen mellom aktørene i den enkelte region bare defineres i noen grad i styringssystemene for informasjonssikkerhet. Det fremkommer at det gjenstår praktiske avklaringer mellom regional IKT-leverandør og helseforetak når det kommer til om myndighet, ansvar og arbeidsoppgaver i deres helseregion er klart fordelt. Dette oppgis som en av de største utfordringene knyttet til avdekking og håndtering av dataangrep. Riksrevisjonen pekte spesielt på uklare ansvarsforhold knyttet til å ivareta sikkerheten i medisinsk-teknisk utstyr (MTU), både internt i helseforetakene og mellom helseforetak og regional IKT-leverandør. De regionale helseforetakene har adressert utfordringen gjennom sine handlingsplaner.[44]

Det vil normalt være helseforetakene som er dataansvarlig for sin behandling av helseopplysninger. Helseforetak kan inngå samarbeid i henhold til pasientjournalloven § 9[45] og da avtale hvordan dataansvaret skal være. Departementet kan i forskrift eller enkeltvedtak fastsette vilkår for slikt samarbeid. Tjenesteytere det er inngått avtale med vil ha selvstendig ansvar for digital sikkerhet i sin virksomhet og normalt også ha dataansvar.

De regionale helseforetakene har også ansvar for å legge til rette for nødvendig samarbeid mellom ulike helseforetak innad i det regionale helseforetaket, med andre regionale helseforetak, fylkeskommuner, kommuner eller andre tjenesteytere om å tilby spesialisthelsetjenester.[46]

Dataansvar
Ved all behandling av helseopplysninger skal det være en eller flere dataansvarlige.[47] Dataansvar er regulert i personvernforordningen og dataansvarlig er den/de som bestemmer formålet og midlene med behandlingen av opplysningene. Dataansvaret plasseres ut fra de faktiske forhold, basert på en konkret vurdering. Når formålet med og midlene for behandlingen er fastsatt i nasjonal rett, kan den dataansvarlige eller kriterier for utpeking av denne, fastsettes i nasjonal

[43] Lov om spesialisthelsetjenesten § 2-1 a. De regionale helseforetakenes ansvar for spesialisthelsetjenester.
[44] Alle de regionale helseforetakene har utarbeidet egne handlingsplaner for oppfølging av funnene i Riksrevisjonsrapporten, se omtale i Vedlegg A.
[45] Pasientjournalloven § 9 Samarbeid mellom virksomheter om behandlingsrettede helseregistre.
[46] Lov om spesialisthelsetjenesten § 2-1 e. Samhandling og samarbeid.
[47] Dataansvarlig er begrepet som benyttes i helselovgivningen og er det samme som behandlingsansvarlig etter personvernforordningen, jf. eksempelvis pasientjournalloven § 2 e.

rett. Dette er tilfellet for bl.a. nasjonal kjernejournal og e-resept, hvor Norsk helsenett SF er dataansvarlig.

Dataansvarlig har ansvaret for personvernet ved behandling av helseopplysningene. Dataansvarlig har plikter og ansvar av både prosessuell og materiell karakter. Sentrale plikter og ansvar er å sørge for at all behandling av personopplysninger har lovlig behandlingsgrunnlag, sørge for egnet informasjonssikkerhet og etablere internkontroll, sørge for tilgangsstyring, ivareta de registreres rettigheter og gjennomføre personvernkonsekvensvurderinger (DPIA).

Ved samhandling og deling av helseopplysninger er det viktig å ha full klarhet i hvem som har dataansvar på hvert steg i dataflyten. Deling av helseopplysninger for helsehjelpsformål må skje innenfor rammene av helsepersonells taushetsplikt. Etter pasientjournalloven § 19 skal den dataansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige, og er ansvarlig for at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten. Det er en utfordring ved digital samhandling å komme frem til avtaler med en hensiktsmessig oppgavefordeling knyttet til tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Leverandøroppfølging og verdikjeder
Sektoren har et komplekst aktørbilde der ansvaret for ulike løsninger, produkter og verdikjeder er delvis fragmentert og noe uoversiktlig. Ansvaret for drift og forvaltning er plassert hos ulike driftsleverandører både på kommunalt nivå, i spesialisthelsetjenesten og i den sentrale helseforvaltningen, samt hos private virksomheter og leverandører. Dette gjør det utfordrende å ha oversikt over alle avhengigheter, samt sikre effektiv hendelseshåndtering og god styring av risiko og sårbarhet for de ulike nivåene i sektoren.

Sektorens virksomheter og de som er ansvarlige for nasjonale e-helseløsninger må sørge for at det opprettholdes en oversikt over sammenhengende komponenter og tjenester. Det er behov for en oversikt over kritisk infrastruktur. Beredskapsplaner må ta høyde for at håndtering av IKT-hendelser kan skje i verdikjeder der flere aktører er involvert. Dette er adressert i innsatsområdet planverk og øvelser.

Nasjonal IKT-helseberedskap
Nasjonal helseberedskapsplan[48] er et sentralt styringsdokument for håndtering av kriser i sektoren, og i dag inngår ikke IKT-beredskap som en del av planverket. Direktoratet for e-helse peker på at man gjennom øvelser og hendelser i sektoren har avdekket uklarheter rundt roller og tilhørende ansvar ved IKT-kriser, og at samhandling og kommunikasjon i disse tilfellene ikke er tydelig avklart.[49]

Helsedirektoratet har i de overordnede risiko- og sårbarhetsvurderingene for nasjonal beredskap i helse- og omsorgssektoren fra 2019[50] også pekt på at roller og ansvar knyttet til IKT-beredskap og nasjonal kriseledelse i sektoren må avklares nærmere. De anbefaler å utarbeide en egen nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan. Videre anbefaler de at det utvikles et kart for sektoren over myndighetsroller, systemeierskap og leverandører som skal være til bruk i beredskapsarbeidet.

[48] Helse- og omsorgsdepartementet, *Nasjonal helseberedskapsplan, 2018*
[49] Direktoratet for e-helse, *Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren, 2019, s. 26*
[50] Helsedirektoratet, *Overordnede risiko- og sårbarhetsvurderinger for nasjonal beredskap i helse- og omsorgssektoren, 2019*

4. Forslag til mål for digital sikkerhet og beredskap i helse- og omsorgssektoren

Alle virksomheter i helse- og omsorgssektoren må øke sin sikkerhet, forebygge digitale hendelser og være forberedt på å håndtere digitale sikkerhetshendelser i tillegg til å sikre fortsatt forsvarlig leveranse av helse- og omsorgstjenester, dersom slike hendelser oppstår.

Arbeidet med digital sikkerhet i sektoren må understøtte sektorens kjernevirksomhet. Dette inkluderer forsvarlig helsehjelp, evne til å beskytte befolkningens helse og forebygge sykdom og skade ved å sørge for smittevern, miljørettet helsevern, trygt drikkevann og strålevern, og helseberedskap. Digital sikkerhet er også en forutsetning for å lykkes med andre av sektorens oppgaver, som forskning. Sektoren må være i stand til å tilpasse seg teknologi, trusler og sårbarheter i kontinuerlig endring.

Med bakgrunn i utfordringene som sektoren står overfor foreslås følgende mål for arbeidet med digital sikkerhet. Disse adresserer felles og vedvarende utfordringer for sektoren, i tillegg til grunnleggende forutsetninger for å lykkes med sikker digitalisering.

Virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder.
Alle virksomheter har et ansvar for egen digital sikkerhet og helseberedskap. Gjennom en risikobasert tilnærming må det sørges for nødvendig egenevne til å overvåke, oppdage, håndtere og beskytte seg mot digitale hendelser. Samtidig er det mange likheter mellom virksomhetene i deres oppgaver og utfordringer knyttet til digital sikkerhet. Gode felles tjenester og ressurser kan gi gevinster både i kvalitet, kostnader og tidsbruk. Det totale potensialet er stort, fordi små forbedringer hos mange virksomheter til sammen vil ha stor effekt.

Ansvar og roller med betydning for digital sikkerhet i og mellom sektorens virksomheter er avklart, kjent og ivaretatt.
Mange av utfordringene som sektoren står overfor dreier seg om ulike former for uklarheter knyttet til roller og ansvar. At ansvar og roller er avklart, kjent og ivaretatt er en viktig forutsetning for å nå de øvrige målene.

Sektoren ivaretar sikkerhet i lange og komplekse digitale verdikjeder.
Innføring av nye løsninger og teknologi og økt integrasjon mellom systemer kan medføre lange og komplekse samhandlings- og leverandørkjeder. Avhengigheten til leverandører blir stadig større. Den digitale samhandlingen mellom sektorens virksomheter øker. Det helhetlige sikkerhetsnivået er derfor avhengig av sikkerhetshåndteringen både hos sektorens virksomheter og leverandører. For å ivareta egnet digital sikkerhet i hele verdikjeden må virksomheter ha tilstrekkelig styring og kontroll der blant annet nødvendig kompetanse, oversikt over avhengigheter og etterlevelse følges opp.

Det er høy tillit fra innbyggere og pasienter til hvordan sektoren ivaretar digital sikkerhet.
Godt og systematisk sikkerhetsarbeid i sektoren bidrar til å bygge tillit hos innbyggere og pasienter. Noen områder kan være av særlig betydning. Dette omfatter bl.a. håndtering av sikkerhetshendelser,

hvordan sikkerheten i digitale innbyggerløsninger framstår, og at det er tilstrekkelig åpenhet om sektorens arbeid med digital sikkerhet. Det er nødvendig at innbyggerne både har tillit til at helseopplysninger er sikret mot tilgang fra uvedkommende og at helseopplysningene er tilgjengelig for helsepersonell som trenger tilgang.

Virksomhetene evner å effektivt ta i bruk nye teknologier på en sikker måte og er robuste i møte med et risikobilde i endring.

Trusler, teknologi og relasjoner som sektorens virksomheter opererer i, endrer seg raskt. Trygg og effektiv innovasjon oppnås ved å sørge for god digital sikkerhet samtidig som en utnytter mulighetene teknologien gir for å utvikle bedre tjenester. Virksomheter må være i stand til å vurdere sikkerhet ved innføring og bruk av ny teknologi, noe som er krevende. Å være robust i møte med et risikobilde i endring innebærer at virksomheter må være i stand til å håndtere nye trusler. Dette innebærer blant annet innføring av nye og utfasing av gamle løsninger i henhold til egne behov og risikovurderinger.

Virksomhetene i sektoren har høy bevissthet om sårbarheter og trusler, og er forberedt og øvet på å avdekke og effektivt håndtere ekstraordinære IKT-hendelser.

Virksomhetene i sektoren må være i stand til å forebygge, avdekke, varsle og håndtere enhver form for IKT-hendelse som truer evnen til å levere helse- og omsorgstjenester, pasientsikkerheten og skjerming av sensitiv helseinformasjon. Det er nødvendig med gode risikovurderinger, tiltak for å avdekke, begrense og stanse alvorlige IKT-sikkerhetshendelser, samt evne til å gjenopprette sikker tilstand for berørte systemer etter hendelser. Egnede beredskapsplaner, velutviklet kompetanse, god kapasitet, forberedte tiltak, trening samt systematisk gjennomføring og læring fra øvelser, er sentrale virkemidler.


Gudmund
Nordby

5. Forslag til innsatsområder i arbeidet med digital sikkerhet

Direktoratet for e-helse foreslår seks innsatsområder i arbeidet med digital sikkerhet i den nasjonale helseberedskapen. Innsatsområdene gjelder både forebygging og håndtering av uønskede digitale hendelser og adresserer de områdene der sektoren har felles og vedvarende utfordringer og behov. Innsatsområdene fokuserer på at virkemidler og tiltak som fungerer godt i dag må videreføres og styrkes, samtidig som det trengs nye tiltak på områder der sektoren har et potensial for forbedring og utvikling.

De foreslåtte innsatsområdene er:

- **Videreutvikling av eksisterende nasjonale virkemidler**
  Arbeidet med digital sikkerhet i sektoren må være del av en kontinuerlig forbedring, og felles virkemidler som HelseCERT og Normen er helt sentrale bidragsytere til dette forbedringsarbeidet. For å bidra til at sektorens totale beredskapsevne styrkes, må også disse eksisterende virkemidlene videreføres og videreutvikles.
- **Kompetanse og sikkerhetskultur**
  Digitaliseringen stiller nye krav til kompetanse for å ivareta sikkerheten i sektoren. Økt kompetanse om digital sikkerhet og god sikkerhetskultur, fra virksomhetens øverste ledelse og til den enkelte ansatte, vil redusere risikoen for uønskede digitale hendelser.
- **Planverk og øvelser**
  Alle sektorens virksomheter må være forberedt på å håndtere digitale sikkerhetshendelser og sikre fortsatt forsvarlig leveranse av helsetjenester. For å oppnå dette må det blant annet gjennomføres flere øvelser i sektoren, både nasjonalt, regionalt og lokalt.
- **Etterlevelse og oppfølging**
  NSM erfarer at de fleste cyberhendelser gjøres mulig av manglende implementering av grunnleggende sikkerhetstiltak. Økt etterlevelse av sikkerhetskrav og implementering av grunnleggende tiltak vil redusere risikoen for uønskede hendelser, og det er viktig at etterlevelsen følges opp. Dette er et viktig område i den strategiske ledelsen og risikostyring av virksomhetene.
- **Ny teknologi og digitale verdikjeder**
  Ny teknologi vil ha stor betydning for den fremtidige helsetjenesten, men skaper også større avhengighet til leverandører og gir lange og komplekse digitale verdikjeder. Å ivareta god beredskap i slike verdikjeder stiller nye krav til sektorens virksomheter, og arbeidet må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring.
- **Støtte til mindre virksomheter**
  For å øke sektorens totale beredskapsevne, må den digitale sikkerheten styrkes også i de mindre virksomhetene. Ofte har disse begrenset tilgang på kompetanse og kapasitet innen digital sikkerhet, med få muligheter til å bruke mer tid på ikke-kliniske oppgaver. Det er nødvendig med skreddersydde tiltak for å styrke beredskapsevnen i disse virksomhetene.

Videreutvikling av eksisterende nasjonale virkemidler

Oppmerksomheten rundt digital sikkerhet i helse- og omsorgssektoren øker, og det skjer stadig utvikling på området både i de enkelte virksomhetene og ved felles virkemidler som treffer på tvers. Det er sentralt at arbeidet med digital sikkerhet i sektoren skjer som en del av en kontinuerlig forbedring, og felles virkemidler som HelseCERT og Normen er helt sentrale bidragsytere til dette forbedringsarbeidet.

For å bidra til at sektorens totale beredskapsevne styrkes, må eksisterende virkemidler som bidrar på tvers av hele sektoren videreføres og videreutvikles. Viktige momenter for videreutvikling av både HelseCERT og Normen beskrives i det følgende.

Videreutvikling av HelseCERT

Regjeringen styrker HelseCERT, helsetjenestenes kompetansemiljø for operativ informasjonssikkerhet, i Norsk helsenett SF. HelseCERT skal sikre økt kapasitet til å gjennomføre sikkerhetstesting av aktørene i sektoren, overvåke sikkerhetssituasjonen og drive aktiv kommunikasjon og bistand til aktørene i helse- og omsorgssektoren. Samtidig vil HelseCERTs kapasitet til å inngå i nasjonalt IKT-beredskapsarbeid styrkes. Den interne sikkerhetsmonitoreringen i helseregionene og Norsk helsenett SF forsterkes, og arbeidet gjøres i samarbeid med de regionale helseforetakene, slik at HelseCERT bygger monitoreringstjenester som treffer de regionale helseforetakenes behov. Trusselbildet og sårbarhetene for digitale angrep er i endring og styrking av arbeidet med informasjonssikkerhet er viktig for å sikre at sensitive opplysninger ikke kommer på avveie.

HelseCERT har siden 2011 videreutviklet Nasjonalt beskyttelsesprogram (NBP) til helse- og omsorgs-tjenesten for å styrke den operative sikkerheten. Det er etablert løsninger for sikkerhetsmonitorering som kan oppdage cyberangrep og tekniske sårbarheter. Over 400 virksomheter deltar i beskyttelsesprogrammet per juni 2021. Dette inkluderer 335 kommuner, etater underlagt Helse- og omsorgsdepartementet, spesialisthelsetjenesten og en rekke leverandører tilknyttet Helsenettet. HelseCERT deler viktig kunnskap og innsikt som virksomhetene i sektoren kan bruke i egne risikovurderinger. Digital beskyttelse i dybden (DBD) er et program som ble utviklet og etablert i 2020. Målet er at virksomhetene i helsesektoren, sammen med HelseCERT, aktivt kan forsvare seg mot og oppdage cyberangrep som skjer i infrastrukturen internt i den enkelte virksomhet.

HelseCERT jobber kontinuerlig med utviklingen av sitt tjenestetilbud, innenfor rammen av å være et sektorvist responsmiljø, for å sikre at tjenestene på best mulig måte møter behov som følger av et digitalt trusselbilde i endring. Slik gjør HelseCERT helsetjenesten sikrere, og styrker den nasjonale helseberedskapen.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren – et verktøy for styrket beredskap

Sektorens kjennskap og forpliktelse til Normen som kravsett gjør at en videreutvikling av Normen vil være et sentralt og effektivt virkemiddel for å nå frem med viktige føringer og krav innen digital sikkerhet. Normen skal – gjennom en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet – bidra til gode helsetjenester, god pasientsikkerhet, kvalitetssikring, helsepersonellets læring, godt personvern og til å realisere pasientenes helsetjeneste. Dette danner grunnlaget for god beredskap overfor sikkerhetshendelser, også i forbindelse med krise og krig. Det økte trusselnivået som også treffer helse- og omsorgssektoren, samt tempoet i utviklingen, fordrer at det investeres videre i allerede sterke fagmiljøer. Normen som etablert bransjenorm er et slikt miljø, som i henhold til sitt mandat bidrar med relevant, nødvendig og

tilpasset veiledning på fagområdet informasjonssikkerhet og personvern til helse- og omsorgssektoren.

Styringsformen til Normen innebærer bred sektorforankring og involvering av andre relevante miljøer. Det gjør at forutsetningene er gode for et stadig oppdatert situasjonsbilde og god kjennskap til hvilke behov sektoren har innen informasjonssikkerhet og personvern, herunder hva som kan påvirke sektorens beredskapsevne. Normens styringsgruppe vedtar strategi og årlige handlingsplaner for Normens arbeid. Inneværende strategi gjelder ut 2022.

Forespeilede nytteeffekter av Normens strategi for perioden 2019-2022:

- Gjør det enklere for virksomhetene å få på plass egnede informasjonssikkerhets- og personverntiltak
- Bidrar til økt tillit til at sektoren behandler helse- og personopplysninger på en trygg måte
- Bidrar til et harmonisert sikkerhetsnivå i sektoren
- Bidrar til at sektoren har et godt kravstillingsverktøy til informasjonssikkerhet og personvern ved anskaffelser

Det utarbeides i år en ny strategi for Normen som skal gjelde for perioden 2023-2025.

Forslag til tiltak:

- Videreutvikle HelseCERT
- Videreutvikle Normen

Kompetanse og sikkerhetskultur

Kompetanse om digital sikkerhet er en forutsetning for å kunne beskytte verdier mot uønskede digitale hendelser. Styrket digital sikkerhetskompetanse bidrar til økt bevissthet, som er nødvendig for å bygge en god sikkerhetskultur. Fokus på kompetanse og sikkerhetskultur kan ha en positiv effekt på tilliten fra befolkning, helsepersonell og mellom virksomheter.

Ifølge NSM er det nødvendig med et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra virksomhetenes øverste ledelse til den enkelte ansatte.[51] En god sikkerhetskultur bidrar til at virksomhetenes sikkerhetstiltak ivaretas av medarbeiderne. Dersom medarbeiderne vet hva som er forventet av dem, tar ansvar for egne handlinger og har en forståelse for hvorfor sikkerhetstiltak eksisterer, vil de også sørge for å melde fra om sikkerhetsmessige forhold som virksomheten bør vite om.[52] Helse- og omsorgssektoren kjennetegnes i utgangspunktet av en sterk sikkerhetskultur,[53] men digital sikkerhet inngår ikke uten videre i denne.

Virksomhetenes arbeid med digital sikkerhet omfatter både teknologi, prosesser og kompetanse, og årvåkenhet blant ansatte er med på å styrke den totale sikkerheten. NSM peker på at lav digital sikkerhetskompetanse i sektoren utgjør en sårbarhet. I tillegg kan det føre til svakheter i prosesser der digital sikkerhet inngår som en del av vurderingen, for eksempel ved anskaffelse, introduksjon og bruk av ny teknologi og etterlevelse av sikkerhetskrav.

Arbeidet med å øke bevissthet og kompetanse innen digital sikkerhet i sektoren er preget av at den enkelte virksomhet utvikler og innfører kompetansetiltak hver for seg. Dette gir varierende kvalitet, ulik praksis og lite effektiv bruk av ressurser.

Det finnes gode virkemidler knyttet til kompetanseheving i sektoren i dag. Deling og gjenbruk av slike ressurser er en effektiv måte å heve kompetansenivået på. Det vil være hensiktsmessig å kartlegge og vurdere eksisterende kompetansetiltak, for å tilrettelegge for dette på tvers av sektoren. De regionale helseforetakenes kartlegging av sikkerhetskultur i egen organisasjon kan være et mulig utgangspunkt for en slik kartlegging.

Et mulig neste steg fra en kartlegging er å utvikle felles kompetanseressurser. Dette vil bidra til å styrke digital sikkerhetskompetanse og videreutvikle sikkerhetskultur på en effektiv måte. Det kan gi sektoren tilgang til gode verktøy med lavere samlet ressursinnsats enn om hver enkelt virksomhet skal utvikle alt innhold selv. En viktig forutsetning vil være at ressursene tilpasses sektorens ulike målgrupper og deres behov. Standardiserte, kvalitetssikrede opplæringsressurser bidrar til lik praksis, som kan lette samhandlingen mellom sektorens virksomheter, og i leverandørforhold.

Et annet grep for å styrke digital sikkerhetskompetanse er å legge til rette for at digital sikkerhetskompetanse integreres ytterligere i helsefaglige utdanninger. Dette setter helsearbeidere i bedre stand til å ivareta digital sikkerhet i en digitalisert arbeidshverdag. I tillegg til å innbefatte regulær helseutdanning, kan et slikt grep inkludere en styrking av etter- og videreutdanningstilbudet.

Forslag til tiltak

- Gjennomføre en kartlegging og vurdering av eksisterende kompetansetiltak, med formål om at virkemidler som fungerer godt kan deles og gjenbrukes i hele sektoren.

---

[51] Nasjonal sikkerhetsmyndighet, *Risiko 2022, 2022, s. 9*
[52] Nasjonal sikkerhetsmyndighet, *Grunnprinsipper for personellsikkerhet, 2020*
[53] For eksempel knyttet til å unngå uønskede hendelser i pasientbehandling.

- Basert på kartleggingen, vurdere behovet for en utredning av tiltak med formål å styrke kompetansen om digital sikkerhet hos helsepersonell.
- Bidra til økt oppmerksomhet på digital sikkerhetskompetanse i helsefaglige utdanninger.

Planverk og øvelser

Trusselbildet på IKT-området endrer seg raskt og alle sektorens virksomheter må være forberedt på å håndtere digitale sikkerhetshendelser og sikre fortsatt forsvarlig leveranse av helsetjenester. Den enkelte virksomhet har et selvstendig ansvar for å gjennomføre risikovurderinger, iverksette forebyggende tiltak, utarbeide kontinuitets- og beredskapsplaner, trene, øve og bygge kompetanse og gjennomføre nødvendige tiltak ved ekstraordinære hendelser og i en krisesituasjon.

I forbindelse med et arbeid med å videreutvikle Nasjonal helseberedskapsplan vil det være naturlig å vektlegge IKT-beredskap ytterligere. Som ledd i en slik revisjon vil det også være relevant å vurdere behovet for å tydeliggjøre roller, ansvar, informasjonsdeling og kommunikasjon ved hendelser som utløser behov for en nasjonalt, samordnet krisehåndtering. En slik plan bør være overordnet og danne grunnlag for å utforme planer lokalt og regionalt som baserer seg på de samme prinsipper for håndtering av IKT-hendelser og en omforent forståelse for ansvar, roller og begreper.

Gjennomføring av øvelser kan være et viktig virkemiddel for å forebygge IKT-hendelser, øke krisehåndteringsevnen, styrke samarbeidet med andre aktører, tydeliggjøre ansvar og roller og avdekke eventuelle sårbarheter samt styrke arbeidet med samfunnssikkerhet med fokus på digitale sikkerhetshendelser. Øvelser kan benyttes til å påvise effekt av gjennomførte tiltak og endringer som er implementert.

Et viktig moment i både beredskapsplaner og øvelser, er at disse aktivitetene tar høyde for at håndtering av uønskede digitale hendelser oftest må skje i nær samhandling med andre aktører i og utenfor sektor – offentlige og private.

I dag gjennomføres det fortsatt for få øvelser i sektoren der digital sikkerhet inngår som tema. I kommunene gjennomfører færre enn 13% en beredskapsøvelse på IKT-sikkerhetsområdet minst en gang per år[54,55].Tilsvarende har Riksrevisjonen i en undersøkelse av spesialisthelsetjenesten påpekt at det er gjennomført for få øvelser hos helseforetakene der informasjonssikkerhet inngår som tema.[56] Fordi øvelser er et viktig virkemiddel for å forsterke helseberedskapen for alvorlige IKT-hendelser både nasjonalt, regionalt og lokalt, bør det legges til rette for at øvelser med fokus på alvorlige IKT-hendelser gjennomføres regelmessig og systematisk. Det bør utarbeides en flerårig øvingsplan for å ivareta dette. En flerårig øvingsplan bør basere seg på en overordnet strategi eller rammeplan for øvelser, ses i sammenheng med det øvrige beredskapsarbeidet og koordineres med relevante samvirkeaktører. Det er viktig at planverk, ROS-analyser, krisescenarioer, trusselvurderinger og tidligere erfaringer ligger til grunn for øvingsplanleggingen.

Digital sikkerhet, beredskap og håndteringskompetanse kan øves særskilt, og som del av større øvelser, og det må tilrettelegges for at slike øvelser regelmessig gjennomføres både lokalt, regionalt og nasjonalt. Regelmessig gjennomføring av øvelser vil styrke virksomhetenes evne til å forebygge IKT-hendelser, øke bevissthet, styrke organisering og ferdigheter innen digital sikkerhet. Det skal tilrettelegges for samøvelser internt i sektoren, på både operativt og strategisk nivå. På nasjonalt nivå vil Helsedirektoratet innarbeide håndtering av digitale trusler og alvorlige hendelser som et ledd i sin helhetlige øvelsesvirksomhet. Helsedirektoratet vil i dette arbeidet involvere andre virksomheter i planlegging, gjennomføring og læring etter denne type øvelser, og da spesielt Norsk Helsenett/HelseCERT, Direktoratet for e-helse og de regionale

[54] Digitaliseringsdirektoratet (Digdir), *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner*, 2020, s. 19
[55] Statistisk sentralbyrå, *Befolkning*, 19. mai 2022
[56] Riksrevisjonen, *Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer*, 2020, s. 55

helseforetakene. Det skal også tilrettelegges for og/eller deltas i tverrsektorielle øvelser på området.

En sentral del av gevinstrealisering fra øvelser er at virksomhetene planlegger, gjennomfører og evaluerer øvelser, samt at de aktivt benytter erfaringer som del av sitt kontinuerlige forbedringsarbeid. Det overordnede målet er å sikre evnen til å levere forsvarlige helsetjenester og ivareta pasientsikkerheten også under krevende forutsetninger.

Generelt er det også behov for å tilrettelegge for forsterket, strukturert og styrt informasjons- og erfaringsdeling innen helse- og omsorgssektoren. Det vil bidra til å styrke sektorens samlede evne til å forebygge, avdekke og håndtere uønskede, og potensielt alvorlige hendelser.

Forslag til tiltak

- Utarbeide overordnet nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan for å danne et likt og generisk plangrunnlag regionalt og lokalt der tydelig ansvars- og varslingslinjer i håndtering av IKT-sikkerhetshendelse i sektoren fremkommer samt i samvirke med andre sektorer.
- Planverk på ulike nivåer må være omforent og bygge på overordnet planverk, felles begrepsbruk og forståelse.
- Det bør etableres felles møtearenaer eller samarbeidsfora for systematisk og kontinuerlig arbeid med og fokus på digital sikkerhet. Slike møtearenaer eller samarbeidsfora kan benyttes til samordning av planverk, kompetansebygging og dele erfaringer fra hendelser og øvelser samt bidra til å koordinere planlegging og deltakelse i øvelser.
- Etablere kart over myndighetsroller, systemeierskap og leverandører som skal være til bruk i beredskapsarbeidet.
- Etablere en nasjonal oversikt over kritisk infrastruktur i helse- og omsorgssektoren.
- Etablere en overordnet strategi eller rammeplan for øvelser som omfatter digital sikkerhet i helsesektoren med tydelige forventninger til systematisk arbeid med øvelser på nasjonalt nivå og i hver enkelt virksomhet. Dette vil kunne sikre regelmessige øvelser og bidra til helhetlig tilnærming, samsvar mellom mål og virkemiddel samt koordinering i egen sektor og med andre virksomheter i andre sektorer på flere nivå.
- Tilrettelegge for informasjonsdeling i forbindelse med dataangrep, og erfaringsutveksling fra etterfølgende evaluering, i tråd med NSMs grunnprinsipper.

Etterlevelse og oppfølging

Økt kontroll med digital risiko vil styrke den forebyggende sikkerheten og øke virksomhetenes evne til å motstå uønskede digitale hendelser. En forutsetning for å oppnå dette er etterlevelse av grunnleggende sikkerhetskrav og anbefalinger. Økt kontroll med digital risiko vil også gi fleksibilitet til raskere å ta i bruk nye løsninger på en trygg måte.

Det digitale landskapet i helse- og omsorgssektoren er fragmentert, og det er stor variasjon innen modenhet og utfordringer på området digital sikkerhet. NSM erfarer at de fleste cyberhendelser hadde vært avverget eller fått begrenset skadeomfang om NSMs grunnprinsipper hadde vært fulgt.[57] I spesialisthelsetjenesten viser Riksrevisjonens undersøkelse at det er svakheter i grunnleggende sikkerhetstiltak.[29] Dette omfatter bl.a. manglende kontroll på utstyr, systemer og programvare. Tekniske løsninger i bruk i sektoren kan være utdaterte og sårbare, og utbedring av kjente svakheter kan ta lang tid. Virksomhetene må ha en helhetlig tilnærming til sikkerhetsstyring og legge større vekt på etterlevelse og oppfølging. Kontroll av sikkerhetsarbeidet er nødvendig for å vurdere om sikkerhetstilstanden er forsvarlig, og danner grunnlag for forbedring.[58]

Det er viktig at grunnleggende sikkerhetskrav og -anbefalinger etterleves i sektoren, og at etterlevelsen følges opp.[59] Systematisk oppfølging gir virksomhetene bedre oversikt over egne risikoer og faktisk sikkerhetstilstand. Det er sentralt at nødvendig sikkerhetsstyring er integrert i ordinær virksomhetsstyring. Gjennom kunnskap om sikkerhetstilstanden settes den enkelte virksomheten i stand til å kontinuerlig forbedre sikkerhetsstyringen.

Ordninger for kontroll og dokumentasjon av sikkerhetsarbeid er effektivt, og en viktig komponent i slike ordninger er tilrettelegging for læring og kontinuerlig forbedring. Gjennom god oversikt over sikkerhetstilstanden i sektorens virksomheter dannes et godt grunnlag for transparens mellom samhandlende virksomheter. Arbeidet med kontroll og dokumentasjon kan gjøres med høyere kvalitet og effektivitet gjennom å støtte virksomhetene med veiledning og verktøy.[60]

Ved å måle effekten av sentralt iverksatte tiltak[61] legges det til rette for mer målrettede, konkrete og effektive tiltak i fremtiden. Tilsyn er også et sterkt virkemiddel for å bedre etterlevelse. Dette krever at nødvendig tilsynsgrunnlag og tilsynskompetanse er etablert. NIS-direktivet åpner for etablering av sektortilsyn innen informasjonssikkerhet.[62]

Forslag til tiltak

- Tydeligere forventing om at etterlevelse følges opp internt i den enkelte virksomhet, og at sikkerhetsstyring integreres i den ordinære virksomhetsstyringen.
- Forbedre ordninger for kontroll og dokumentasjon av sikkerhetsarbeid, samtidig som virksomhetene støttes gjennom veiledning og verktøy.
- Stille krav om at tiltakseiere på nasjonalt nivå skaffer oversikt over tiltakenes effekt.

---

[57] *Nasjonal sikkerhetsmyndighet, Risiko 2022, 2022, s. 37*
[58] I tråd med *Nasjonal sikkerhetsmyndighet, Grunnprinsipper for fysisk sikkerhet, personellsikkerhet og sikkerhetsstyring, 2020*
[59] Relevante krav og anbefalinger er Normen og NSMs grunnprinsipper for IKT-sikkerhet.
[60] Innen områder som eksempelvis compliance, benchmarking og modenhet.
[61] For eksempel bruk av Normen i sektoren.
[62] *EØS-notatbasen, NIS-direktivet, 2016*

Ny teknologi og digitale verdikjeder

Skytjenester, kunstig intelligens, maskinlæring og sensorteknologi er eksempler på ny teknologi som vil ha stor betydning for den fremtidige helsetjenesten. Denne typen teknologi vil bli viktig for å understøtte leveransen av helsetjenester, for eksempel ved digital hjemmeoppfølging og fjernkirurgi. Bruk av ny teknologi gir bedre og mer effektive løsninger, men fører også med seg nye sårbarheter.

Ny teknologi, tjenester og samhandlingsformer som tas i bruk i helse- og omsorgssektoren innebærer ofte at flere aktører og leverandører er involvert. Dette danner lange digitale verdikjeder. Å ivareta god beredskap i slike verdikjeder stiller nye krav til sektorens virksomheter, og beredskapsarbeidet må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring. Det oppstår avhengigheter mellom komponentene i kjeden, og disse kan det være vanskelig å ha oversikt over.[63] Det er derfor viktigere enn før å kontinuerlig følge opp leverandører, samhandlende virksomheter og tredjeparter, for å holde oversikt over avhengigheter og potensielle sårbarheter. Slik oversikt er viktig i en beredskapssammenheng – det har betydning både for forebyggende arbeid og i hendelseshåndtering. Behovet for oversikt over en digital verdikjede øker med kritikaliteten til den funksjonen den understøtter.

De digitale verdikjedenes kompleksitet, flyktighet og transnasjonale karakter, samt momentan propagering (umiddelbar spredning) ved svikt eller andre feil i slike kjeder, gjør at styring av risiko i slike kjeder er krevende både på virksomhets- og myndighetsnivå.[64] Kravstilling og evaluering ved anskaffelser, sikkerhetsstyring av leverandører og utføring av leverandørkontroll oppleves som utfordrende og tidkrevende. Både leverandører og de som bestiller vil ha nytte av styrket veiledning, standardiserte sikkerhetskrav, nødvendige avklaringer for bruk av ny teknologi og tydeliggjøring av ansvar for oppfølging av sikkerhetstiltak.

Styring av risiko ved bruk av ny teknologi, tjenester og samhandlingsformer krever gode rutiner for vurdering, innføring og oppfølging. Risikovurdering av digitale verdikjeder som går på tvers av virksomheter og landegrenser er kompetansekrevende, og virksomhetene i sektoren vil kunne ha nytte av støtte i dette arbeidet. Det ligger et stort potensial i samarbeid med relevante fag- og veiledningsmiljøer i og utenfor sektoren. Aktuelle virkemidler som kan fremkomme av slikt samarbeid er styrket veiledning, arenaer for ressursdeling[65] og sandkasser[66].

Også mellom virksomheter med like behov vil det være hensiktsmessig med økt samarbeid ved anskaffelser, kravstilling og oppfølging av leverandører. Økt samarbeid og støtte til virksomheter i anskaffelsesprosesser kan medføre mer effektiv tidsbruk og høyere kvalitet i anskaffelser og oppfølging av leverandører. Oppfølging av og samarbeid med leverandører kan styrkes ved at det etableres langsiktige relasjonskontrakter og strategiske samarbeid. Slike avtaler kan sikre tilgang til nødvendig ekspertise og kapasitet gjennom hele kontraktens levetid.

Forslag til tiltak

- Stille forventning om at sentralt og lokalt beredskapsplanverk må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring. Dette bør inkludere rutiner/systemer for varsling ved hendelser som berører andre i verdikjeden (særlig de som er avhengig av andres tjenesteleveranse).

---

[63] Mer om risiko knyttet til digitale verdikjeder i *Direktoratet for samfunnssikkerhet og beredskap, Risikostyring i digitale verdikjeder, 2020*, kap. 2
[64] *Direktoratet for samfunnssikkerhet og beredskap, Risikostyring i digitale verdikjeder, 2020, pkt. 1.2.3, s. 10*
[65] Dette kan for eksempel inkludere ROS- og DPIA-bank
[66] Se *Datatilsynets KI-sandkasse*

- Ta DSBs modell for risikostyring i digitale verdikjeder inn i veiledere til relevant sektorlovverk.[67]
- Legge til rette for bedre støtte til vurdering, innføring og utvikling av ny teknologi i samarbeid med relevante fag- og veiledningsmiljøer i og utenfor sektoren. Dette inkluderer utarbeidelse av veiledningsmateriell, opplæringsaktiviteter, etablering av sandkasser og lignende.
- Legge til rette for samarbeid ved anskaffelser, og ved kravstilling og oppfølging av leverandører. Nettverk og fagforum, interkommunale samarbeid, veiledning og utarbeidelse av felles kravspesifikasjoner kan være måter å gjøre dette på.

[67] *Direktoratet for samfunnssikkerhet og beredskap, Risikostyring i digitale verdikjeder, 2020*

Støtte til mindre virksomheter

For å øke sektorens totale beredskapsevne i et skjerpet trusselbilde må den digitale sikkerheten styrkes også i de mindre virksomhetene. I sektoren er det mange små og mellomstore virksomheter som legekontor, psykologpraksiser og tannlegekontor. Alle virksomheter har et ansvar for å ivareta sin egen digitale sikkerhet, og ofte har mindre virksomheter begrenset tilgang på kompetanse og kapasitet innen digital sikkerhet, og få muligheter til å bruke mer tid på ikke-kliniske oppgaver. Dette gir risiko for uønskede digitale hendelser samtidig som evnen til å avdekke og håndtere disse er begrenset. I en situasjon med økt samhandling og tettere knyttede digitale verdikjeder kan sikkerhetstilstanden i de mindre virksomhetene utgjøre en sårbarhet også for øvrige deler av sektoren.

Det er i liten grad lagt til rette for at mindre virksomheter samarbeider og lærer av hverandre for å løse sammenlignbare oppgaver. De mindre virksomhetene må hver for seg bruke tid og ressurser på å utføre sammenliknbare oppgaver innen digital sikkerhet. Dette inkluderer sikkerhetsstyring i egen virksomhet, gjennomføring av risikovurderinger og oppgaver knyttet til teknisk IKT-sikkerhet.[68]

Det er nødvendig med tiltak for å styrke beredskapsevnen i de små virksomhetene, og disse tiltakene må ta utgangspunkt i forutsetningene og rammebetingelsene i disse virksomhetene. Dette vil kunne redusere sannsynligheten for vellykkede angrep og legge til rette for bedre håndtering av hendelser. Tiltakene kan omfatte for eksempel tilrettelegging for økt samarbeid og etablering av felles ordninger og tjenester. Antallet mindre virksomheter i sektoren er høyt, og tiltak som gir effekt i den enkelte virksomhet kan ha stor samlet effekt for sektoren.

En kartlegging av sikkerhetstilstanden i mindre virksomheter vil gi et nødvendig kunnskapsgrunnlag for hvilke behov de har på området. Dette kan omfatte kartlegging av virksomhetenes kapasitet til å avdekke og håndtere sikkerhetshendelser, samt momenter som styringssystem for informasjonssikkerhet, hvem som utfører sikkerhets- og driftsoppgaver for mindre helsevirksomheter, kompetansebehov og vurdering av risiko.

Basert på en kartlegging av sikkerhetstilstanden i de mindre virksomhetene kan behovet for felles ordninger og tjenester utredes og relevante tiltak prioriteres. Områder som antas å gi stor verdi er felles utarbeidelse av vurderinger og kravspesifikasjoner, operativ støtte og tilbud om felles løsninger for å avdekke og håndtere digitale angrep.

Forslag til tiltak

- Kartlegge sikkerhetstilstanden og -behov i de mindre virksomhetene i sektoren.
- Utrede mulige felles ordninger og tjenester som vil gi verdi for bredden av mindre virksomheter.

[68] Dette avhenger av hvilken driftsmodell som benyttes (IKT-tjenester i egen regi, skytjenester, hybride løsninger etc.).

6. Vedlegg A: Eksisterende tiltak på digital sikkerhet i helse- og omsorgssektoren

Dette vedlegget gir en oversikt over eksisterende tiltak som er relevante for den digitale sikkerheten i helse- og omsorgssektoren i dag. Dette inkluderer enkelte tverrsektorielle tiltak. Oversikten har blitt utarbeidet som en oppfølging av Nasjonal strategi for digital sikkerhet og er kategorisert etter temaområdene i den nasjonale strategien.

Sikkerhet er en viktig del av alle små og store digitaliseringsinitiativ. Denne oversikten har fokus på tiltak med relevans for hele eller større deler av sektoren og et dedikert fokus på digital sikkerhet. Den inkluderer derfor ikke større tiltak der digital sikkerhet kun er en del av et større initiativ, eller tiltak som kun er relevant for enkeltvirksomheter.

Det er også hentet ut og sammenstilt relevante tiltak fra de regionale handlingsplanene for arbeidet med informasjonssikkerhet for å synliggjøre pågående initiativer i de regionale helseforetakene. Handlingsplanene er utarbeidet av de regionale helseforetakene på oppdrag fra HOD som oppfølging av Riksrevisjonens funn fra deres gjennomgang av helseforetakenes forebygging av angrep sine IKT-systemer. Disse følges opp i helseregionene.

Der det er relevant er det oppgitt status og videre plan for tiltakene.

Forebyggende digital sikkerhet

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren
Ansvarlig: Normens styringsgruppe
Relevant for: Hele sektoren
Beskrivelse: Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen – *www.normen.no*) er et sett av krav til informasjonssikkerhet og personvern basert på lovverket, med tilhørende veiledningsmateriell. Normen styres og forvaltes av en styringsgruppe sammensatt av representanter for sektoren. Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern hos den enkelte virksomhet, i felles systemer og infrastruktur, og i sektoren generelt. Videre skal Normen bidra til at virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. Sekretariatet for Normen i Direktoratet for e-helse har ansvar for forvaltning av Normen i henhold til styringsgruppens føringer basert på sektorens behov.
Status: Første versjon av Normen ble godkjent i 2006 og er innarbeidet og godt kjent i sektoren.
Plan: Normen har en strategi for å oppnå de overordnede og langsiktige målene for Normen. Strategien beskriver hvordan målene skal nås på mellomlang sikt og besluttes av Styringsgruppen. Strategien gjelder for tre til fire år om gangen, men kan oppdateres og endres årlig. For å gjennomføre strategien har Normen en handlingsplan. Handlingsplanen er et verktøy for styring av oppgaveporteføljen og skal beskrive konkrete tiltak. Planen besluttes av Styringsgruppen og gjelder for ett år om gangen. Styringsgruppen for Normen skal vedta strategi for 2023-2025 i år. Strategien blir utarbeidet på bakgrunn av behov som sektoren har. Handlingsplanen for 2022 fokuserer bl.a. på å ferdigstille arbeidet med oppdatering av veiledningsmateriell, temaet «forskning» i Normen, kunstig intelligens, data- og dokumentdeling og videreutvikling av kurs og kompetansehevingsaktiviteter. Normen starter i 2022 et større arbeid på området leverandøroppfølging og styring.

Videreutvikling av og opplæring gjennom Normen
Ansvarlig: Direktoratet for e-helse
Relevant for: Hele sektoren
Beskrivelse: Normen er en arena for kompetansebygging og erfaringsutveksling, gjennom blant annet *faste kurs, ukentlige webinarer, konferanser og andre kompetansehevingsaktiviteter.*
Status: Handlingsplanen til Normen prioriterer også i 2022 satsing på kompetanseheving.
Plan: I 2022 skal Normen satse på videreføring og utvikling av webinarer, videreutvikle og avholde introkurs Normen, kurs om informasjonssikkerhet og personvern medisinsk utstyr, basiskurs informasjonssikkerhet og personvern, lage nytt forskningskurs, avholde fysisk og

digital Normkonferanse, få på plass ny nettside samt se på mulighetene for å prøve å lage podcast.

Normkonferansen
Ansvarlig: Direktoratet for e-helse ved Normsekretariatet
Relevant for: Hele sektoren
Beskrivelse: Normsekretariatet viderefører Normkonferansen som en årlig møteplass og kompetansearena for aktører i helse- og omsorgssektoren.
Status: Sekretariatet er i gang med planlegging av Normkonferansen 2022 som skal være en fysisk og digital konferanse. I 2022 blir det viktig blant annet å ha fokus på at folk kan møtes, dele erfaring og diskutere.
Plan: Planlegging av konferansen er i gang.

HelseCERT og Nasjonalt Beskyttelsesprogram
Ansvarlig: NHN ved HelseCERT
Relevant for: Hele sektoren
Beskrivelse: HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. Deres oppgave er å styrke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser. HelseCERT skal spre kunnskap om IKT-trusler og beskyttelsesmekanismer og kontinuerlig monitorere trafikken i Helsenettet. Gjennom Nasjonalt Beskyttelsesprogram (NBP), som er en tjeneste som er inkludert for medlemmer av Helsenettet, utfører HelseCERT blant annet monitorering, informasjonsdeling og forebygging, bistand til hendelseshåndtering, sårbarhetsoversikt og inntrengningstesting. HelseCERT videreutvikler NBPs eksisterende sensorplattform, sårbarhetsskanning, øvrige tjenester og utvider kapasitet til sikkerhetstesting av aktører i sektoren i henhold til endringer i trusselbildet.

Monitorering av sikkerhetssituasjon og kommunikasjon
Ansvarlig: NHN
Relevant for: Hele sektoren
Beskrivelse: Norsk helsenett SF skal styrke HelseCERTs arbeid med monitorering og overvåkning av sikkerhetssituasjonen i sektoren, og videreutvikle arbeidet med kommunikasjon og bistand til sektoren.

Sikkerhetstesting
Ansvarlig: NHN
Relevant for: Hele sektoren
Beskrivelse: Norsk helsenett SF øker kapasiteten til å gjennomføre sikkerhetstesting av aktører i sektoren. Det skal tas hensyn til mangfoldet av aktører og behov ved utvelgelse av aktører som skal sikkerhetstestes.

VDI-samarbeid med nasjonale sikkerhetsmyndigheter
Ansvarlig: NSM og virksomheter med installerte VDI-sensorer
Relevant for: Virksomheter med installerte VDI-sensorer
Beskrivelse: Nasjonalt cybersikkerhetssenter (NCSC) drifter og organiserer et nasjonalt sensornettverk på internett; Varslingssystem for digital infrastruktur (VDI). Dette består av sensorer utplassert hos virksomheter som ansees som en del av kritisk infrastruktur i Norge, og benyttes til å analysere metadata fra nettverkstrafikken for å avdekke mistenkelig aktivitet.

Direktoratet for e-helse som fagmyndighet for sektoren
Ansvarlig: Direktoratet for e-helse
Relevant for: Hele sektoren
Beskrivelse: Som fagmyndighet har Direktoratet for e-helse et hovedansvar for å tydeliggjøre rammebetingelsene for informasjonssikkerhet i digitaliseringsarbeidet i sektoren. Direktoratet for e-helse er sekretariat for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, gjennomfører utrednings- og strategioppdrag innen fagområdet for HOD, og har ansvar for nasjonal e-helsemonitor som inkluderer enkelte aktiviteter innen informasjonssikkerhet. Direktoratet for e-helse vil utvikle og styrke sin fagmyndighetsrolle på området ytterligere.

Årlig rapportering om trusselbildet
Ansvarlig: NHN ved HelseCERT
Relevant for: Hele sektoren
Beskrivelse: NHN utgir en årlig rapport som bygger videre på nasjonale sikkerhetsmyndigheters trusselrapporter, og summerer opp konkret innsikt fra det operative sikkerhetsarbeidet i helse- og omsorgssektoren. Rapporten gir anbefalinger til tiltak.

Nasjonal e-helsemonitor
Ansvarlig: Direktoratet for e-helse

Relevant for: Hele sektoren
Beskrivelse: Direktoratet for e-helse skal gjennom Nasjonal e-helsemonitor følge med på IKT-utviklingen i helse- og omsorgssektoren i Norge og etablere et kunnskapsgrunnlag om bruk og effekter av IKT i sektoren. I 2018 startet Direktoratet et arbeid med å etablere indikatorer for informasjonssikkerhet i samarbeid med aktører fra helse- og omsorgssektoren med høy informasjonssikkerhetskompetanse og -erfaring. I 2019 publiserte direktoratet en undersøkelse av modenhet på informasjonssikkerhet blant RHF-ene og NHN. Det gjennomføres også innbygger- og helsepersonellundersøkelser som omfatter sikkerhetsrelaterte spørsmål som tillit til at informasjon er sikker og tilgjengelig. Arbeidet videreføres.
Status: Det har vært dialog med de regionale helseforetakene og NHN om gjennomføring av ny modenhetsundersøkelse.
Plan: En ny modenhetsundersøkelse planlegges gjennomført til høsten.

Felles sikkerhet i forvaltningen
Ansvarlig: Digitaliseringsdirektoratet
Relevant for: Offentlig forvaltningsstyring og kontroll av informasjonssikkerhet
Beskrivelse: Strategisk arbeid for å styrke informasjonssikkerhetsarbeidet i små- og mellomstore virksomheter.
Status: Konsept
Plan: Digitaliseringsdirektoratet anbefaler at det startes et arbeid for å utvikle en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter, som inkluderer styringsaktiviteter og sikkerhetstiltak. Kort oppsummert utforsker tiltaket muligheten for å lage en, “en bro”, mellom sikkerhetstiltak og veiledning på styring og kontroll. Tiltaket må sees på som et operativt hjelpemiddel som kan gi virksomhetene hjelp til å arbeide med informasjonssikkerhet, redusere omfanget av det som må gjøres i hver enkelt virksomhet og effektivisere arbeidet. Det vil for eksempel kunne gi virksomheter mulighet til å benytte en katalog over oppgaver og informasjonstyper som utgangspunkt for å få oversikt og dermed ha et felles utgangspunkt for vurderinger av konsekvensnivåer for disse oppgavene, og anbefalte minimumstiltak for å håndtere risiko.

Digital sikkerhet i kritiske samfunnsfunksjoner

Helsenettet
Ansvarlig: NHN
Relevant for: Alle virksomheter tilknyttet helsenettet
Beskrivelse: Helsenettet er en lukket og sikker kommunikasjons- og samhandlingsarena for aktørene i helse- og omsorgssektoren, og er en av sektorens viktigste sikkerhetsmekanismer. Helsenettet bidrar til å ivareta en sikkerhetsarkitektur, en juridisk konstruksjon som gjør deling og samhandling om helsedata på tvers av aktører mulig innenfor trygge rammer. Over Helsenettet tilbys en rekke tjenester som påvirker sikkerheten i den digitale samhandlingen i sektoren, slik som kjernejournal, elektronisk meldingsutveksling (EDI), e-resept og registertjenester, i tillegg til sikkerhetsrelaterte tjenester som HelseID (sikker autentisering) og tjenester fra HelseCERT med mer. NHN videreutvikler Helsenettet i takt med digitaliseringen i sektoren.

Oppfølging tilknyttet sikkerhetsloven
Ansvarlig: HOD
Relevant for: Virksomheter underlagt HOD
Beskrivelse: Ny sikkerhetslov med underliggende forskrifter ble gjort gjeldende fra 1. januar 2019. Lovens formål er å forebygge, avdekke og motvirke sikkerhetstruende hendelser. Helse- og omsorgsdepartementet jobber med identifisering av virksomheter og skjermingsverdige verdier (objekter, infrastruktur og informasjonssystemer) som understøtter grunnleggende nasjonale funksjoner (GNF), og vil stille krav om at alle underliggende etater og virksomheter etablerer oversikt over kritisk digital infrastruktur som er essensiell for å ivareta helse- og omsorgssektorens og nasjonalt beredskapsansvar.

HelseID
Ansvarlig: NHN
Relevant for: Alle virksomheter tilknyttet helsenettet og brukere av nasjonale e-helsetjenester
Beskrivelse: HelseID er en felles påloggingsløsning for helse- og omsorgssektoren. Den legger til rette for enklere pålogging for helsepersonell, og styrket informasjonssikkerhet ved digital samhandling i sektoren. Dette skjer blant annet gjennom funksjonalitet for autentisering av brukere, systemer og virksomheter, samt beskyttelse av systemer.

Felles tillitstjenester
Ansvarlig: Norsk helsenett SF

Relevant for: Alle samhandlende virksomheter
Beskrivelse: Ifølge målbilde for felles tillitstjenester i Program digital samhandling trinn 1 skal Norsk Helsenett: • realisere felles tillitstjenester som støtter felles krav og retningslinjer til tilgangsstyring av data- og dokumentdelingstjenester • etablere et felles tillitsanker som en organisatorisk funksjon hos NHN og som håndterer avtaler/bruksvilkår og en felles ansvarsfordeling ved bruk av data- og dokumentdeling. • ta frem et felles rammeverk for håndtering av sikkerhetsvurderinger for å lette håndtering av sikkerhetsvurdering av data- og dokumentdelingsløsninger. • standardisere informasjonen som skal oversendes virksomheter som tilbyr tjenester og danne grunnlag for å ivareta deres forpliktelser som dataansvarlig. • etablere felles minimumskrav til tilgangsstyring ved bruk av data- og dokumentdeling. • sikre at nye autentiseringsløsninger som oppfyller krav til autentisering kan benyttes på tvers av virksomheter ved bruk av data- og dokumentdeling.

Kompetanse

Sikkerhetsopplæring innen helsefaglige utdanninger - DigSam
Ansvarlig: Utvikling av åpen læringsressurs. Ansvarlig: DigSam prosjektet (UiT, NTNU, HVL,USN OsloMet)
Relevant for: Primært grunnutdanninger innen helse- og sosialfag, men kan tilpasses alle virksomheter som yter helse- og sosialtjenester.
Beskrivelse: Tiltaket er en del av føringen som ligger i nasjonal forskrift for helse- og sosialfagutdanninger om digital kompetanse. Prosjektet utvikler, utprøver og evaluerer undervisnings- og vurderingsressurser til studenter om digital sikkerhet for å sikre at kandidatene i helse- og sosialfaglige utdanninger kan sørge for digital sikkerhet i egen yrkesutøvelse for å møte samfunnets behov for trygge digitale løsninger. DigSam-prosjektet presiserer at de ikke kan ta ansvar for hvordan innholdet i opplæringen som ligger der implementeres og drives i helse og omsorgssektoren, men det er mulighet for tilpasninger med følgende ansvar: Implementering og drift, eventuelle tilpasninger for helse og omsorgstjenesten.
Status: Prosjektet utvikler et digitalt kurs for undervisere i høyere utdanning om digital sikkerhet slikt at undervisere i høyere utdanning kan utvikle sin kompetanse på området.
Plan: DigSam prosjektet avsluttes i juni 2022.

Nasjonalt kompetanseforum for IKT-sikkerhet i helse- og omsorgssektoren
Ansvarlig: NHN ved HelseCERT

Relevant for: Store virksomheter
Beskrivelse: HelseCERT viderefører nasjonalt kompetanseforum for digital sikkerhet. Forumet er rettet mot cybersikkerhetsdomenet, med fokus på erfaringsutveksling, kompetansespredning og diskusjon rundt framtidige løsninger og bruk av felleskomponenter.

NTNU CCIS forskningsgruppe e-helse og velferdsteknologi (NTNU CCIS e-HWS)
Ansvarlig: NTNU Center for Cyber and Information Security (NTNU CCIS)
Relevant for: Hele sektoren
Beskrivelse: NTNU CCIS er et nasjonalt senter for forskning, utdanning og kompetansebygging innen cyber- og informasjonssikkerhet. Senteret er en nasjonal hovedleverandør av tidsrelevant kunnskap og kompetanse for å styre digital sikkerhet med nettverksarenaer og møteplasser for offentlig-privat, sivil-militært og internasjonalt samarbeid. Senterets forskningsgruppe for digital sikkerhet innen e-helse og velferdsteknologi (e-HWS) fokuserer på personvern- og informasjonssikkerhetsutfordringer relatert til områder innen e-helse og velferdsteknologi. En tildeling fra Helse- og omsorgsdepartementet til NTNU CCIS finansieres gruppens strategiske arbeid og forskningsinitiativer.
Status: Siden etableringen i 2016 har NTNU CCIS e-HWS bygd opp en betydelig forsknings- og utviklingsaktivitet. Gruppen er blant annet leder for IKTPLUSS prosjektet Health Democratization (Norges forskningsråd), ansvarlig for helse-demonstratoren i Senter for forskningsdrevet innovasjon Norwegian Center for Cyber Security in Critical Sectors (SFI NORCICS, Norges forskningsråd), deltager i IKTPLUSS prosjektet DigiRemote og deltager i ITN prosjektet Privacy Matters (EU Horizon 2020). Helsedemonstratoren i SFI NORCICS er tett knyttet til test-, trenings- og øvingsarenaen Norwegian Cyber Range (NCR). NCR er fremhevet som tiltak 27 i Nasjonal strategi for digital sikkerhet (2019). NTNU CCIS e-HWS står også bak spinn-off selskapet Biofy AS som leverer sikre og personvernbevarende skyløsninger for biometri. Videre har forskningsgruppen har også utredet et etter- og videreutdanningskonsept for digital sikkerhet i helse- og omsorgssektoren (2020).
Plan: NTNU CCIS e-HWS skal fortsette å være en aktiv forskningsgruppe på problem-stillinger knyttet til personvern- og informasjonssikkerhetsutfordringer relatert til områder innen e-helse og velferdsteknologi i samspill med relevante aktører i sektoren. Tiltaket skal sikre tilgjengeliggjøring av en relevant test-, trenings-, og øvingsarena for helse- og omsorgssektoren som en integrert del av Norwegian Cyber Range. Videre vil tiltaket medføre etablering av etter- og videreutdanningstilbud for digital sikkerhet i helse- og omsorgssektoren ved NTNU.

Avdekke og håndtere digitale angrep

HelseCERT som helsetjenestens sektorvis responsmiljø

Ansvarlig: NHN ved HelseCERT
Relevant for: Hele sektoren
Beskrivelse: HelseCERT er tilgjengelig for å støtte virksomheter i både primær- og spesialisthelsetjenesten med rådgivning og koordinering ved hendelser. HelseCERT har etablert relasjon med Nasjonalt cybersikkerhetssenter, som er den nasjonale responsfunksjonen og koordinerer de sektorvise responsmiljøene. Dette svarer ut krav til sektorvise responsmiljø i NIS-direktivet. Som oppfølging til nye krav som stilles gjennom NIS-direktivet styrkes HelseCERT til å være sektorens mottakspunkt for varsling av sikkerhetshendelser.

Digital beskyttelse i dybden
Ansvarlig: NHN og RHF-ene
Relevant for: Hele sektoren
Beskrivelse: Gjennom programmet Digital Beskyttelse i Dybden hjelper HelseCERT virksomheter i sektoren med å forebygge, oppdage og håndtere sikkerhetstruende hendelser internt i virksomhetenes infrastruktur. Norsk helsenett skal videreutvikle Digital sikkerhet i dybden i samarbeid med de regionale helseforetakene.
Status: Norsk helsenett har i tildelingsbrevet fra HOD for 2022 fått i oppdrag å videreutvikle programmet.

Kommune-CSIRT: Beredskap mot digitale hendelser
Ansvarlig: DSB
Relevant for: Kommunal sektor
Beskrivelse: Kommune-CSIRT er et nasjonalt senter for sikkerhet i kommunal sektor, og har medlemmer over hele landet. Virksomheten deltar også fullt ut i det sektorvise responsmiljøsamarbeidet (SRM) hvor NSM NCSC er vertskap. Finansieringen av senteret er per 1.4.22 basert på abonnementsavgift for medlemmers tilgang til tjenestene som leveres.
Status: Per 1.4.2022 har Kommune-CSIRT 50 medlemmer hvorav 2 fylkeskommuner, 2 vannverk og resten kommuner. Virksomheten leverer operativ, én-til-én rådgivning, trusseletterretning, støtte ved hendelser og informasjonsdeling til alle medlemmene.
Plan: Kommune-CSIRT har som ambisjon å få alle kommuner og fylkeskommuner som medlemmer - for å øke sikkerheten betydelig for kommunenorge.

Statistisk logganalyse
Ansvarlig: Helse Sør-Øst

Relevant for: Helse Sør-Øst på kort sikt, andre regioner på sikt.
Beskrivelse: Det har manglet et verktøy som gjør at helseforetakene systematisk kan etterkontrollere alle oppslag for å avdekke urettmessige oppslag. Prosjektet skal etablere teknisk løsning og rammeverk for kontroll av oppslagslogger i elektronisk pasientjournal. Løsningens formål er å identifisere uvanlige oppslag som videre må vurderes manuelt for avklaring av om oppslaget er i overensstemmelse med lovverket. Løsningen vil etableres for helseforetakene i Helse Sør-Øst, og skal også kunne skaleres opp som et tilbud til andre helseregioner. Drift av løsningen er derfor lagt til NHN. Utrulling til helseforetakene i Helse Sør-Øst er planlagt å starte i 2022, og skal etter planen være ferdigstilt første kvartal 2023.
Status: Helse Nord RHF har anskaffet lisenser, og vil samarbeide med Helse Sør-Øst om innføring av maskinell løsning for mønstergjenkjenning. Etablering av mønstergjenkjenning skal gjennomføres så snart løsning er anskaffet og utprøvd i Helse Sør-Øst

Bekjempe data- og IKT-relatert kriminalitet

Anmeldelse til politiet og rapportering til HelseCERT og øvrige sikkerhetsmyndigheter er et viktig tiltak som den enkelte virksomhet oppfordres til å gjøre ved hendelser. Utover dette pekes det ikke på noen spesifikke tiltak innen dette området for helse- og omsorgssektoren.

Relevante krav gitt i styringsdokumenter fra Helse- og omsorgsdepartementet 2022

Foretaksmøtet (jan 2022) ba de regionale helseforetakene om å:
Beskrivelse: Foretaksmøtet (jan 2022) ba de regionale helseforetakene om å: • rapportere på arbeidet med de regionale handlingsplanene for det systematiske arbeidet med å styrke informasjonssikkerheten og med å lukke de sårbarhetene som Riksrevisjonens undersøkelse avdekket innen utgangen av 2022. • utarbeide en årlig rapport i samarbeid med Norsk helsenett SF om trusler, trender, sårbarheter og relevante tiltak som spesialisthelsetjenesten kan benytte i sitt arbeid med risiko- og sårbarhetsvurderinger innen 1. juni hvert år. Erfaringer fra penetrasjonstesting og portskanningstester vil være relevant. • samarbeide med HelseCERT om regionale og nasjonale kapabiliteter for å oppdage og håndtere sikkerhetshendelser, og gjennom det sørge for at hensiktsmessige kapabiliteter blir etablert for å styrke egenbeskyttelsen og regionenes samlede evne til å oppdage digitale angrep.

Digital sikkerhet og beredskap. Foretaksmøtet ba Norsk helsenett SF om å:
• jobbe aktivt med videreutvikling av en god sikkerhetskultur som understøtter målene med sikkerhetsarbeidet

- videreutvikle Nasjonalt beskyttelsesprogram (NBP) i regi av HelseCERT for å styrke den operative sikkerheten i helsesektoren. Tjenestene i NBP skal bidra til å forebygge, oppdage og håndtere digitalt angrep i helse- og omsorgssektoren
- forberede etablering av mottaksapparat for å håndtere innrapportering av sikkerhetshendelser i sektoren, som følge av at NIS-direktivet gjennomføres i norsk rett - utarbeide en rapport innen 1. juni hvert år om trusler, trender, sårbarheter og relevante tiltak som sektoren kan benytte i sitt arbeid med risiko- og sårbarhetsvurderinger, og bistå de regionale helseforetakene i sitt arbeid med trusselvurderinger
- bidra til god beredskap gjennom godt forebyggende sikkerhetsarbeid og øvelser
- utøve en pådriverrolle i sektoren for nasjonal IKT-beredskap og yte bistand til Helsedirektoratet som leder arbeidet med nasjonal helseberedskap, inkludert utvikling av nasjonale IKT-beredskapsplaner og øvelsesgjennomføring.

De regionale handlingsplanene

Her gis en sammenstilling av relevante tiltak fra de regionale handlingsplanene. Det er ikke en direkte gjengivelse av alle tiltakene fra handlingsplanene, men en oppsummering for å trekke frem essensen fra handlingsplanene samlet sett.

Samhandling for medisinsk teknisk utstyr
Ansvarlig: De regionale helseforetakene
Relevant for: Foretaksgruppene
Beskrivelse: For medisinsk-teknisk utstyr (MTU) skal ansvarsforholdet mellom leverandør, helseforetak og IKT-leverandør være avklart.

Utarbeide og benytte trusselvurderinger
Ansvarlig: De regionale IKT-leverandørene
Relevant for: Foretaksgruppene
Beskrivelse: De regionale IKT-leverandørene skal sammen utarbeide/bidra inn i årlige trusselvurderinger i samarbeid med relevante aktører fra både privat og offentlig sektor. Helseforetakene skal benytte denne og andre kilder i sitt arbeid med informasjonssikkerhet.

Samarbeidsforum
Ansvarlig: De regionale helseforetakene, Direktoratet for e-helse og NHN SF
Relevant for: Spesialisthelsetjenesten
Beskrivelse: Det er opprettet et samarbeidsforum for å dele erfaringer mellom helseregionene, Direktoratet for e-helse og Norsk helsenett SF for å styrke erfaringsoverføring på tvers, og for å identifisere egnede nasjonale og interregionale tiltak for å styrke informasjonssikkerheten i helseforetakene og forebygge angrep mot IKT-systemene. Dette innebærer blant annet øvelser, revisjoner, sårbarhetsskanning og penetrasjonstesting.

Forumet skal gi anbefalinger til hvordan kriterier for å akseptere risiko innen informasjonssikkerhet bør utformes.

Forvaltning og oppfølging av leverandører
Ansvarlig: De regionale helseforetakene
Relevant for: Spesialisthelsetjenesten
Beskrivelse: For nasjonale anskaffelser kan det pekes på en region for å forvalte området som en anskaffelse omfatter, slik at arbeidet med risikoanalyser og oppfølging av leverandører blir mer effektivt etter anskaffelsen er gjennomført.

Grunnprinsipper for IKT-sikkerhet
Ansvarlig: Helseforetakene
Relevant for: Foretaksgruppene
Beskrivelse: Helseforetakene skal arbeide med systematisk innføring av Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet.

Tekniske sikkerhetstiltak i infrastrukturen
Ansvarlig: De regionale IKT-leverandørene
Relevant for: Foretaksgruppene
Beskrivelse: Infrastrukturmodernisering er et pågående og kontinuerlig arbeid. En viktig del av moderniseringen handler om å redusere kompleksitet i IKT-porteføljen og få mindre teknisk gjeld. Styrket kontroll med nettverk og styrket autentisering er to sentrale områder.

Måling av informasjonssikkerhetskultur
Ansvarlig: Sykehuspartner HF, Helse Vest RHF, Helse Midt-Norge RHF, Helse Nord RHF
Relevant for: Foretaksgruppene
Beskrivelse: Informasjonssikkerhetskulturen i foretaksgruppene skal måles og eventuelle tiltak iverksettes med bakgrunn i målingen.

Informasjonssikkerhetskompetanse i anskaffelser
Ansvarlig: De regionale helseforetakene
Relevant for: Spesialisthelsetjenesten

Beskrivelse: For bedre kravstilling og vurdering av informasjonssikkerhet i anskaffelser, skal Sykehusinnkjøp HF benytte kapasitet og kompetanse innen informasjonssikkerhet fra helseregionenes IKT-leverandører.

Status: De administrerende direktørene i de regionale helseforetakene har besluttet at behovet for informasjonssikkerhet i anskaffelser skal dekkes ved å benytte regionenes informasjonssikkerhetsmiljøer og at Sykehusinnkjøp HF ikke skal bygge opp et eget miljø innen informasjonssikkerhet. Det pågår et arbeid, ledet av regionenes IKT-direktører, med å detaljere hvordan informasjonssikkerhetsmiljøene skal involveres, og hvordan deltakelsen skal fordeles mellom regionene.

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt:
postmottak@ehelse.no