Direktoratet for e-helse

Strategi for digital sikkerhet i helse- og omsorgssektoren

Vurdering av behov og innretning

IE-1064

Publikasjonens tittel:
Strategi for digital sikkerhet i helse- og omsorgssektoren
– Vurdering av behov og innretning

Rapportnummer
IE-1064

Utgitt:
15.10.2020

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

Sammendrag

Direktoratet for e-helse anbefaler at det utarbeides en egen strategi for digital sikkerhet i helse- og omsorgssektoren.

Denne strategien må være kort, poengtert og handlingsrettet. Den bør bygge videre på *Nasjonal strategi for digital sikkerhet* og målene i denne, men tilpasses og utdypes i tråd med sektorens særtrekk og behov. Strategien må være fremtidsrettet, og dekke hele sektoren.

For å oppnå ønsket effekt bør strategien inneholde konkrete mål og reelle strategiske virkemidler. Det er ikke behov for ny kartlegging av totalsituasjonen i sektoren, men på enkelte områder kan det være nødvendig å innhente mer kunnskap. Formålene med strategien vil være å tydeliggjøre sikkerhetsbehov, tydeliggjøre roller og ansvar og identifisere relevante strategiske virkemidler og tiltak, for å løfte arbeidet med digital sikkerhet i hele sektoren.

Direktoratet for e-helse har på oppdrag fra Helse- og omsorgsdepartementet (HOD), i samarbeid med Norsk helsenett SF (NHN), gjennomført et arbeid for å *vurdere behov og eventuell innretning for en strategi for digital sikkerhet i helse- og omsorgssektoren.* I arbeidet har det vært vektlagt bred involvering av en rekke aktører, både i og utenfor sektoren. Arbeidet har resultert i følgende vurderinger:

Det er støtte til, og et tydelig behov for, en egen strategi for digital sikkerhet i sektoren. I helse- og omsorgssektoren rapporteres det om mange av de samme utfordringene som i andre samfunnskritiske sektorer, og samfunnet for øvrig. Samtidig har helsesektoren et spesielt sterkt behov for tilgjengelighet og integritet for å understøtte både pasientsikkerhet og samfunnets helseberedskap. Omfanget av, og sensitiviteten til, personopplysningene som blir behandlet er betydelig..

Formålet med strategien bør være å:

- Tydeliggjøre sikkerhetsbehov
- Tydeliggjøre roller og ansvar
- Identifisere relevante strategiske virkemidler og tiltak

Underveis i arbeidet har vi mottatt spørsmål om det hadde vært mer hensiktsmessig med en handlingsplan enn en strategi. Direktoratet mener at en strategi er bedre egnet til å berede grunnen for nye strategiske virkemidler i sektoren, samt å tydeliggjøre roller og ansvar. Videre er det viktig at digital sikkerhet løftes opp på strategisk nivå i sektoren.. Samtidig understreker dette behovet for at strategien er tydelig og handlingsorientert, og at den faktisk bidrar til å forenkle og styrke sikkerhetsarbeidet i sektoren.

Strategien bør bygge på nasjonale føringer, spesielt den nasjonale strategien for digital sikkerhet. Det er gjort et omfattende arbeid med å utvikle Nasjonal strategi for digital sikkerhet (2019). Den nasjonale strategien skal dekke hele samfunnet og er med vilje lagt på et generelt nivå, slik at den kan være relevant for alle sektorer. En egen strategi for helse- og omsorgssektoren må konkretisere hvordan målene og tiltakene i den nasjonale strategien skal nås i sektoren. Strategien må i tillegg sees i sammenheng med arbeidet som gjøres på sikkerhetsområdet i andre sektorer med tette sammenkoblinger med helse- og omsorgssektoren, eksempelvis i kommunesektoren.

Strategien må ta hensyn til sektorens utfordringer, ambisjoner, mål og særegne behov. Samtidig som de nasjonale føringene setter rammen for arbeidet, har helse- og omsorgssektoren en rekke særtrekk og sektorspesifikke utfordringer som må adresseres i en eventuell strategi. Dette innebærer at strategien må ta hensyn til:

- Trussel- og risikobildet i sektoren
- Sikkerhetsbehov som følger av teknologisk utvikling og digitalisering i sektoren
- Forutsetninger og særtrekk ved sektoren

I tillegg til den nasjonale strategien for digital sikkerhet, er det flere sektorspesifikke føringer som det må tas hensyn til i en strategi for digital sikkerhet i helse- og omsorgssektoren. Nasjonal helse- og sykehusplan 2020-2023 slår fast at «*befolkningen skal ha tillit til at helsetjenesten både ivaretar deres personvern og tar i bruk de mulighetene teknologien gir for å utvikle bedre tjenester*». Videre har Nasjonal e-helsestrategi for 2017-2022, satt som mål at vi skal ha «*en digitalisert, samlet helse- og omsorgstjeneste som oppleves enklere, bedre og mer helhetlig for innbyggerne*».

Strategien bør inneholde følgende sektorspesifikke temaer:

- *Sikker samhandling:* Det er stort behov for løsninger for sikker deling av data, og for sikre fellesløsninger for identitetshåndtering, autentisering og autorisasjon. Økt samhandling medfører også behov for styrkede kontrollmekanismer på sikkerhetsområdet
- *Sikker digital hjemmeoppfølging:* Pasientbehandling flyttes hjem til innbyggerne, og sårbarheter i medisinsk utstyr kan medføre store konsekvenser. Konfidensialitet, tilgjengelighet og integritet må ivaretas for både pasienter og personell. Det kan oppstå uklare ansvarsforhold på sikkerhetsområdet når flere aktører er involvert.
- *Sikkerhet i leverandørkjeden:* Sikkerhet i sektoren bør sees på som en helhet. Både leverandører og anskaffere etterlyser tydeligere og standardiserte sikkerhetskrav og nasjonale føringer for risikoaksept i anskaffelser. Behandling av data hos tredjepart medfører økt kompleksitet i leverandørkontroll, og det er viktig at sikring av medisinsk utstyr ivaretas i hele utstyrets livsløp.

Strategien må være fremtidsrettet. En strategi for digital sikkerhet kan ikke kun fokusere på situasjonen slik den er i dag. Digitaliseringen går i et svært raskt tempo, og en god strategi må også være rettet mot fremtidig utvikling og de sikkerhetsmessige behov denne medfører. Som det kommer frem av Nasjonal helse- og sykehusplan 2020-2023 vil fremtidens helsetjeneste kreve store endringer i hvordan hele sektoren samhandler og kommuniserer, både i og på tvers av sektoren og med pasienter. Sikkerhet er ett av hensynene som må ivaretas som en del av denne utviklingen.

Strategien bør dekke hele sektoren. Aktørbildet i helse- og omsorgssektoren er omfattende og komplekst, og består av over 17.000 private og offentlige virksomheter. Det digitale landskapet er fragmentert, med stor variasjon av modenhet på sikkerhetsområdet. Selv om størrelse og risikonivå varierer mellom ulike aktører, står hele sektoren overfor det samme trusselbildet. Sektoren utgjør en samlet eksponeringsflate inn mot felles verdier. Særlig de mindre virksomhetene, som mangler kapasitet til å opprettholde et tilstrekkelig sikkerhetsnivå, har behov for felles virkemidler. Strategien bør derfor dekke hele sektoren, men det bør differensieres basert på ansvar og risiko. En sentral ambisjon for strategien bør være å angi en felles retning, og tydelige prioriteringer fra myndighetenes side i et forståelig språk, til alle de ulike aktørene.

Strategien bør inneholde konkrete mål og strategiske virkemidler. Et gjentakende tema fra workshopene og møtene har vært behovet for målbare mål og konkrete virkemidler for å sikre en vellykket implementering. En rekke aktører har etterlyst målinger/ evalueringer/revisjoner, for dermed å sikre prioritet og etterlevelse i en sektor som fra før av har mange oppgaver som skal utføres med begrensede ressurser. For at hele sektoren skal ønske, og ha mulighet til å implementere strategien, bør det også vurderes behov og mulighet for økonomiske og andre virkemidler/insentiver.

Det er ikke behov for ny kartlegging av totalsituasjonen i sektoren, men på enkelte områder kan det være nødvendig å innhente mer kunnskap. Vi har spurt en rekke aktører om det er nødvendig å gjennomføre en full kartlegging av nåsituasjon på sikkerhetsområdet i hele sektoren. Selv om mange har spilt inn at de vet for lite om nåsituasjonen på digital sikkerhet, oppfatter vi at dette er knyttet til situasjonen i hver enkelt virksomhet og ikke sektoren som helhet. Vi oppfatter det derimot slik at man gjennom bl.a. Lysne-utvalgets rapport, Situasjonsbildet utgitt av NHN og andre rapporter som beskriver risiko og sårbarheter i sektoren, har en tilfredsstillende oversikt over situasjonen som utgangspunkt for et strategiarbeid.

Det kan likevel være behov for noe videre kartlegging på enkeltområder. Et eksempel kan være kartlegging av kompetansebehov. I kommunesektoren har blant annet Digitaliseringsdirektoratet, i samarbeid med KS, fått i oppdrag fra Kommunal og moderniseringsdepartementet (KMD) om å få frem et kunnskapsgrunnlag om arbeidet med informasjonssikkerhet i kommunene.

Innhold

1 Sikkerhet i en digital helse- og omsorgssektor

Digitalisering er et sentralt virkemiddel for å effektivisere og videreutvikle helse- og omsorgstjenesten, og den skjer i et stadig økende tempo. En avgjørende forutsetning for vellykket digitalisering er at behovet for sikkerhet blir tilstrekkelig ivaretatt.

Direktoratet for e-helse har i tildelingsbrevet for 2020 fått følgende oppdrag av Helse- og omsorgsdepartementet (HOD): «*Foreslå innretning på mulig strategi for informasjonssikkerhet for helse- og omsorgssektoren innen 15. oktober 2020, jf. risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren. Arbeidet skal gjøres i samarbeid med Norsk Helsenett SF og i dialog med departementet».* Det ble i innledende fase av arbeidet[1] presisert at anbefalingen til HOD skal gjelde innretning av en mulig strategi for *digital sikkerhet*, ikke kun informasjonssikkerhet.

Denne rapporten svarer ut oppdraget gitt av HOD. Den inneholder en analyse av behovet for en egen strategi for digital sikkerhet i helse- og omsorgssektoren, og en anbefaling om innretningen på en mulig strategi. Rapporten vil danne grunnlaget for å finne svar på følgende problemstilling:

*Er det **behov** for en egen strategi for digital sikkerhet i helse- og omsorgssektoren, og hvordan bør denne i så fall **innrettes**?*

I kapittel 2 presenteres nåsituasjonen, fremtidige sikkerhetsutfordringer og behovet for en egen strategi for digital sikkerhet i helse- og omsorgssektoren. I kapittel 3 presenteres mulige innretninger for en strategi, inkludert viktige hensyn, temaområder, innhold og omfang og hvordan arbeidet med en eventuell strategi kan innrettes. I kapittel 4 har vi oppsummert direktoratets anbefaling.

1.1 Avgrensninger og forutsetninger for oppdraget

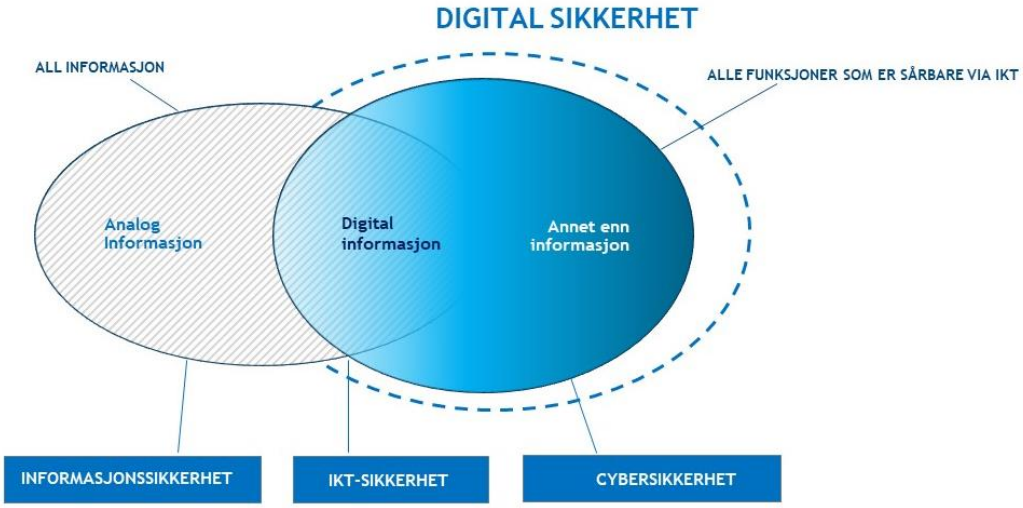
Direktoratet for e-helse fremlegger med denne rapporten sin vurdering av behovet for en eventuell strategi, samt en anbefaling til HOD om hvorvidt, og hvordan, utarbeidelsen av en egen strategi for digital sikkerhet i sektoren bør gjennomføres. Rapporten har fokus på problembeskrivelse og behov, for dermed å kunne gi en kvalifisert anbefaling til HOD. Selve strategiarbeidet er ikke påbegynt.

Digital sikkerhet er en forutsetning for pasientsikkerhet. Dette innebærer alt fra ivaretagelse av personvern til tilgjengeliggjøring av informasjon og tjenester. Denne rapporten er avgrenset til å omhandle de sikkerhetsmessige forholdene relatert til disse temaene.

[1] Oppstartsmøte med HOD 27. mai 2020.

1.2 Hva er digital sikkerhet?

Direktoratet for e-helse har, i samråd med Norsk helsenett SF (NHN) og HOD, besluttet å justere den opprinnelige formuleringen fra tildelingsbrevet fra «informasjonssikkerhet» til «digital sikkerhet». Begrepet digital sikkerhet er i den nasjonale strategien for digital sikkerhet, lansert av regjeringen i 2019, definert som «*beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi».*[2] Den samme definisjonen legges til grunn her.[3]



Figur 1: Digital sikkerhet. Basert på figur publisert av NVE i deres rapport «Regulering av IKT-sikkerhet - Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor».

IKT-sikkerhet, informasjonssikkerhet og cybersikkerhet er elementer med overlappende definisjoner, som alle inngår i begrepet digital sikkerhet. Digital sikkerhet favner bredere enn kun informasjonssikkerhet, samtidig er det deler av informasjonssikkerhet som ikke er dekket av begrepet. Analog informasjon er en del av informasjonssikkerhet, men er ikke inkludert i begrepet digital sikkerhet. Samtidig er det en rekke andre funksjoner som er sårbare via IKT som er inkludert i begrepet digital sikkerhet.

I begrepet digital sikkerhet ligger behovet for å ivareta både konfidensialitet, integritet og tilgjengelighet til informasjon og systemer, sett opp mot både interne og eksterne trusler. I tillegg til behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet, handler det om at selve systemene som behandler og lagrer informasjonen er tilgjengelige/funksjonelle og ikke manipulert av uvedkommende. I helse- og omsorgssektoren er dette eksempelvis spesielt kritisk når det kommer til medisinsk utstyr, som pacemakere og insulinpumper. Konfidensialitet, integritet og tilgjengelighet betyr at informasjonen og systemer skal 1) beskyttes mot uvedkommende, 2) ikke bli endret utilsiktet eller av uvedkommende, og 3) være tilgjengelig ved behov.[4]

[2] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet.*
[3] Det er et poeng i seg selv at en strategi for helse- og omsorgssektoren bruker samme begrep som den nasjonale strategien.
[4] Vi har her lagt til grunn definisjonen til Digitaliseringsdirektoratet.

1.3 Gjennomføring, involvering og metode

Arbeidet med å svare ut oppdraget fra HOD er organisert som et prosjekt med en styringsgruppe med representanter fra Direktoratet for e-helse og NHN, samt en arbeidsgruppe med fageksperter fra Direktoratet for e-helse og bistand fra BDO AS.

Det empiriske grunnlaget for vurderingene i denne rapporten inkluderer både styrende dokumenter og planverk for sektoren, offentlige utredninger og nasjonale strategier og risikoanalyser. En strategi for digital sikkerhet for helse- og omsorgsektoren forutsetter samtidig bred involvering av sektoren, interesseorganisasjoner og leverandører. Det er derfor gjennomført fire workshoper med representanter fra sektoren for å innhente relevant informasjon[5]. Hensikten med workshopene har vært å 1) sørge for tidlig involvering av sektoren, 2) innhente god og oppdatert situasjonsforståelse, samt 3) sikre bred forankring rundt felles utfordringer.

1. I den første workshopen deltok et begrenset antall nøkkelpersoner fra helse- og omsorgssektoren. Hovedtemaer var vurdering av behovet for en strategi, planlegging av arbeidet, aktuelle tema og involvering av sektoren.
2. Den andre workshopen hadde bredere deltakelse, med representanter fra en rekke offentlige og private virksomheter i både primær- og spesialisthelsetjenesten, fra leverandørsiden og fra interesseorganisasjoner. Her var hovedtemaene nåsituasjonen, samt hva man ønsket å oppnå med en eventuell strategi.
3. Den tredje workshopen ble gjennomført i samarbeid med KiNS[6], og hadde bred deltagelse fra kommuner og fylkeskommuner, samt Kommune-CSIRT, KS og enkelte regionale IKT-foretak. Hovedtemaene var utfordringsbildet sett fra kommunal sektor, viktige temaområder og mulig innretning av strategien.
4. Den fjerde workshopen hadde bred deltagelse fra hele sektoren. Her var hovedtemaene mulig innretning av strategien og arbeidet med utformingen av den, samt viktige temaområder.

Utover de konkrete workshopene har arbeidsgruppen orientert om oppdraget, fremdriftsplan og status, samt drøftet behov, temaer og mulige innretninger for en eventuell strategi med NUFA og NUIT. Det har også vært orientert om saken i Nasjonalt e-helsestyre og gjennomført møter med Justis- og beredskapsdepartementet (JD), Nasjonal sikkerhetsmyndighet (NSM), Helsetilsynet, Datatilsynet og interne fagmiljøer. Se ellers Vedlegg 1 Gjennomførte møter for en liste over gjennomført møter.

[5] Se vedlegg 1.
[6] Foreningen Kommunal Informasjonssikkerhet.

2 Behovet for en egen strategi for digital sikkerhet i helse- og omsorgssektoren

For å sikre bedre kvalitet, økt pasientsikkerhet og bedre ressursbruk, er det nødvendig å utnytte mulighetene som kommer av den teknologiske utviklingen. I *Prop. 65 L (2019–2020) Forslag til lov om e-helse (e-helseloven)* slås det fast at digitalisering skal understøtte nødvendig samhandling i sektoren, til nytte for innbyggerne, pasienter og helsepersonell, styring, statistikk og vitenskapelige formål. Digitalisering bidrar til å heve kvalitet, tjenestetilbud og effektivitet på en bærekraftig måte.[7]

I Nasjonal helse og sykehusplan 2020-2023, påpekes det at «*befolkningen skal ha tillit til at helsetjenesten både ivaretar deres personvern og tar i bruk de mulighetene teknologien gir for å utvikle bedre tjenester»*.[8] Planen inneholder tiltak og eksempler på ny bruk av teknologi i helsesektoren som skal bidra til at sektoren oppnår helsepolitiske mål.

På samme måte som for resten av samfunnet, medfører denne raske og omfattende digitalisering også sikkerhetsutfordringer i sektoren. Digital sikkerhet er en helt avgjørende forutsetning for både ***pasientsikkerhet*** og ***personvern*** for innbyggere og helsepersonell, samt helt sentralt for å legge til rette for god ***helseberedskap.*** Pasienter må ha tillit til at teknologi og informasjon er beskyttet, riktig og tilgjengelig, slik at de trygt kan ta i bruk nye digitale løsninger. Helseopplysninger skal være tilgjengelige for helsepersonell, slik at de kan ta riktige beslutninger og yte den beste helsehjelpen, men samtidig beskyttes mot uvedkommende, både interne og eksterne. Velferdsteknologi, medisinsk utstyr, journalsystemer og fagsystemer skal fungere uten å kunne bli manipulert av uvedkommende. Pasienter og helsepersonell må sikres sin lovfestede rett til personvern. Tilstrekkelig sikkerhet er også avgjørende for å ivareta en god helseberedskap. Helse- og omsorgssektoren er avhengig av tilgjengelige og sikre informasjons- og kommunikasjonssystemer, også i krisesituasjoner.

2.1 Kjente sikkerhetsutfordringer ved digitalisering

Nasjonale sikkerhetsmyndigheter har i flere år skrevet om digitale trusler og sårbarheter som en av de største risikoene det norske samfunnet står ovenfor. På nasjonalt nivå ble det i 2019 gjort et omfattende arbeid for å kartlegge utfordringsbildet, samt lage en helhetlig strategi for digital sikkerhet, for dermed på best mulig måte å møte dette komplekse utfordringsbildet. Både blant fageksperter og på politisk nivå er det enighet om at dette er et viktig nasjonalt fokusområde fremover.

Det digitale risikobildet endres raskt. Tilgjengeliggjøring av tjenester i det digitale rom medfører også potensielle sårbarheter, som kan utnyttes av en rekke trusselaktører. Sårbarhetene skyldes både menneskelige, teknologiske og organisatoriske forhold, eller – som oftest er tilfelle - en kombinasjon av disse. NSM skriver i sin rapport *Risiko 2020* at: «*en stor del av trusselaktiviteten mot Norge skjer i det digitale rom».*[9] I sin nyeste rapport, Helhetlig digitalt risikobilde 2020, påpeker NSM at stadig flere virksomheter prioriterer IKT-sikkerhetsarbeidet. Samtidig finnes det betydelige digitale sårbarheter i samfunnet og hos norske virksomheter. NSM har i flere år rapportert om at kjente sårbarheter benyttes for å gi

[7] Helse- og omsorgsdepartementet. 2020. *Forslag til lov om e-helse (e-helseloven)*. Prop. 65 L (2019–2020).
[8] Helse- og omsorgsdepartementet. 2019. *Nasjonal helse- og sykehusplan 2020 – 2023*. Meld. St. 7 (2019–2020)
[9] Nasjonal Sikkerhetsmyndighet. 2020. *Risiko 2020*

uautorisert tilgang til systemer og nettverk. Det digitale risikobildet preges fremdeles av dette. «*NSM observerer ulike typer digitale operasjoner mot norske mål, inkludert mot virksomheter som ivaretar viktige samfunnsfunksjoner».*[10] Ifølge NSM er en gjennomgående erfaring at digitale angrep blir mer og mer sofistikerte og komplekse, og at hendelseshåndtering er tid- og ressurskrevende.

Et fokusområde i årets rapport er bruk av skytjenester. NSM er positive til at virksomheter benytter skytjenester så lenge virksomheten har gjort gode og riktige vurderinger rundt dette. Økt bruk av skytjenester bringer samtidig med seg nye sårbarheter og økt risiko utover virksomhetens eget domene. *«NSM er bekymret for den samlede nasjonale avhengigheten av utenlandske skytjenesteleverandører, og hvordan denne avhengigheten kan spille ut i hele krisespennet».*[11]

I Nasjonal trusselvurdering 2020 rapporterer PST at datanettverksoperasjoner utgjør en vedvarende og langsiktig trussel mot Norge. Andre lands etterretningstjenester vil videreføre kartleggingsoperasjoner for å avdekke funksjoner og sårbarheter innen norsk kritisk infrastruktur, krisehåndtering og sikkerhet og beredskap. PST vurderer at «*med stor grad av anonymitet og mulighet for benektelse, kan sensitiv informasjon stjeles eller manipuleres, og kritisk infrastruktur forstyrres eller ødelegges».*[12]

Den gjentatte rapporteringen om digitale sikkerhetsutfordringer fra NSM og andre, viser med stor sikkerhet at samfunnet er sårbart, og at sikkerhet fortsatt ikke blir tilstrekkelig ivaretatt som en grunnleggende del av digitaliseringen.

2.1.1 Komplekse digitale avhengigheter

Den digitale utviklingen fører til lange verdikjeder med stadig flere involverte aktører og en forskyvning av kompleksitet utover i verdikjeden. Dette gjør det vanskeligere å holde oversikt og kontroll over eventuelle avhengigheter og hvilke konsekvenser som kan oppstå, og kan dermed medføre en pulverisering av ansvar. Helse- og omsorgssektoren er i dag avhengig av en rekke understøttende funksjoner for å levere sine tjenester. Eksempelvis leverer NHN tjenester og fasiliterer løsninger for hele helse- og omsorgssektoren. Dette har gjort det mulig å standardisere felles tjenester og sikkerhetsregimer i sektoren, men samtidig er Helsenettets funksjon helt avhengig av tredjeparter i ekomsektoren, noe brukerne av Helsenettet ikke nødvendigvis tar innover seg i sine vurderinger.

Nettopp denne sammenvevingen på tvers av sektorer er en av hovedtrekkene med de nye digitale avhengighetene. Der tjenesteleverandører tidligere hadde tilnærmet full kontroll over verdikjeden, er bildet i dag langt mer fragmentert.[13] I sin rapport, Risiko 2020 understreker NSM blant annet at: «*Innen de fleste samfunnssektorer er funksjoner og tjenester del av digitale verdikjeder, og avhengighetene på tvers er store og mange».*[14] I likhet med de andre sektorene gjennomgår helse- og omsorgssektoren en gjennomgripende digitalisering som fører til komplekse digitale verdikjeder. Utviklingen i det digitale tjenestetilbud skjer raskt, noe som gjør verdikjedene svært dynamiske. Denne kompleksiteten gjør det utfordrende å få oversikt over de totale sårbarhetene.[15] Direktoratet for samfunnssikkerhet og beredskap (DSB) vurderte i 2014 i hvilken grad kritiske samfunnsfunksjoner vil påvirkes av et bortfall av

[10] Nasjonal Sikkerhetsmyndighet. 2020. *Helhetlig digitalt risikobilde 2020*.
[11] Ibid
[12] Politiets sikkerhetstjeneste. 2020. *Nasjonal trusselvurdering 2020*.
[13] Justis- og beredskapsdepartementet. 2015. *Digital sårbarhet – sikkert samfunn*. NOU 2015: 13. Side 15.
[14] Nasjonal Sikkerhetsmyndighet. 2020. *Risiko 2020*.
[15] Ibid

elektronisk kommunikasjon[16]. Vurderingen viser at sektorene som vil bli rammet hardest er transport (særlig jernbanetrafikken og luftfarten), finansielle tjenester, helse og omsorg og styring og kriseledelse.[17]

Samtidig som Helse- og omsorgssektoren er avhengig av andre aktører spiller sektoren også en svært viktig rolle i å understøtte en rekke andre samfunnskritiske funksjoner. Ifølge DSBs liste over kritiske samfunnsfunksjoner og kapabiliteter[18] er følgende aktører fra helse- og omsorgssektoren sentrale i både egen og andre sektorer:

	Samfunnskritisk funksjon	Ansvar og involverte i helsesektoren
	Styring og kriseledelse	
1.1	Konstitusjonelle organer og forvaltningen	HOD, Hdir
1.2	Beredskap og kriseledelse	Hdir, kommunene
	Forsvar	
2.2	Forebyggende sikkerhet	HOD, Hdir, Helsetilsynet Direktoratet for e-helse
2.3	Militær respons (Totalforsvaret)	HOD
	Lov og orden	
3.6	Fengsels- og institusjonssikkerhet. Tvungent psykisk helsevern og omsorg	HOD, RHF, HF
	Helse og omsorg	
4.1	Helsetjenester	HOD, Hdir, FHI, SLV, RHF, HF, NHN, kommunene, apotek, Statens helsetilsyn og Statens strålevern
4.2	Omsorgstjenester	HOD, Hdir, HF, kommunene, Statens helsetilsyn,
4.3	Folkehelsetiltak	HOD, Hdir, FHI, Statens strålevern, kommunene
4.4	Atomberedskap	HOD, Hdir, Statens strålevern
	Redningstjeneste	
5.1	Redningsberedskap	HOD, Hdir, RHF, HF, kommunene, luftambulansetjenesten
5.4	Kjemikalie- og eksplosivberedskap	HOD, Hdir, FHI, HF, Statens strålevern, kommunene
	IKT-sikkerhet i sivil sektor	
6.1	Sikre registre, arkiver mv.	HOD, systemeiere
6.2	Personvern	Systemeiere
6.3	Hendelseshåndtering i IKT-systemer	Hdir, HelseCERT, systemeiere
	Natur og miljø	
7.1	Forurensningsberedskap	HOD, Hdir, kommuner
	Forsyningssikkerhet	
8.1	Matforsyning	HOD, kommunene
	Vann og avløp	
9.1	Drikkevannsforsyning	HOD, FHI, Statens strålevern, kommunene

Tabell 1: Utdrag fra tabell i DSB sin rapport «Samfunnets kritiske funksjoner». Tabellen inneholder alle samfunnskritiske funksjoner hvor virksomheter i helse- og omsorgssektoren har ansvar eller er involvert.

Digital sårbarhet i helse- og omsorgssektoren kan altså medføre store samfunnskonsekvenser. Dette understøtter viktigheten av at sektoren som helhet og hver virksomhet, tar ansvar for å ha et forsvarlig sikkerhetsnivå, vet hvilke tjenester de selv er

[16] Scenariet som ligger til grunn for vurderingen er at transportnettet for ekom settes ut av drift i en femdagersperiode.
[17] Direktoratet for samfunnssikkerhet og beredskap. 2014. *Risikoanalyse av cyberangrep mot ekom-infrastruktur.*
[18] Direktoratet for samfunnssikkerhet og beredskap. 2016. *Samfunnets kritiske funksjoner*. Side 10-18.

avhengig av, og hvilke mulige konsekvenser hendelser i egen digital infrastruktur kan ha for andre.

2.2 Særlige sikkerhetsutfordringer for en digital helse- og omsorgssektor

I helse- og omsorgssektoren rapporteres det om mange av de samme sikkerhetsutfordringene som gjelder i andre samfunnskritiske sektorer, og i samfunnet generelt. Samtidig har sektoren en rekke sikkerhetsutfordringer som en egen strategi for digital sikkerhet for helse- og omsorgssektoren kan bidra til å løse:

- Trussel- og risikobildet i sektoren,
- Sikkerhetsbehov som følger av teknologisk utvikling og digitalisering i sektoren, og
- Forutsetninger og særtrekk ved sektoren.

Helse- og omsorgssektoren har de siste årene opplevd flere sikkerhetshendelser som har bidratt til å sette søkelyset på utfordringer knyttet til alt fra teknologiske sårbarheter til feil behandling av helseopplysninger og mangelfull sikkerhetskompetanse hos helsepersonell. Slike sårbarheter kan få store konsekvenser, både ved utilsiktede hendelser og når de blir utnyttet av trusselaktører.

Mangfoldet av virksomheter, tette koblinger og lange verdikjeder i helse- og omsorgssektoren gjør at alt fra enkeltstående hackere til organiserte kriminelle og statlige etterretningstjenester er en del av det digitale trusselbildet. Mangelfull sikkerhet kan medføre en rekke negative konsekvenser, slik som nedetid på kritiske systemer, feilbehandling av pasienter, sensitiv informasjon på avveie og at publikum vegrer seg for å gi fra seg nødvendig informasjon grunnet manglende tillit til at informasjonen behandles forsvarlig.

HelseCERT - helse- og omsorgssektorens nasjonale senter for operativ informasjonssikkerhet - erfarer at det er krevende for virksomheter i helse- og omsorgssektoren å ha en komplett oversikt over egne systemer og mulige sårbarheter. HelseCERT sine erfaringer gjennom teknisk sikkerhetstesting (penetrasjonstesting) i sektoren viser at systemer koblet til internett, som sentralt driftsovervåkningsanlegg (SD-anlegg), medisinsk utstyr og ulike typer velferdsteknologi kan utnyttes for å komme seg inn i et ellers godt sikret nett. I rapport «Situasjonsbilde 2018» skriver de at truslene de ser mest av i helsesektoren nå er digital kriminalitet som «fisking» etter sensitiv informasjon, såkalt phishing, direktørsvindel, løsepengevirus og tjenestenektangrep.[19]

Direktoratet for e-helse utarbeidet i 2019 en overordnet ROS-vurdering for IKT i helse- og omsorgssektoren.[20] I denne ble det pekt på en rekke sårbarheter som er vurdert til å utgjøre stor risiko sett opp mot dagens trusselbilde. Disse inkluderer blant annet:

- Lange, komplekse og uoversiktlige verdikjeder
- Manglende IKT-sikkerhetskompetanse
- Mangelfull implementering av tekniske sikkerhetstiltak
- Utdatert programvare og utstyr som ikke oppdateres
- Mangel på og mangelfull etterlevelse av styringssystem for informasjonssikkerhet
- Manglende planverk og trening i håndtering av IKT-hendelser.

[19] HelseCERT. 2018. *Situasjonsbilde 2018*.
[20] Direktoratet for e-helse. 2019. *Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren*.

Det er få sektorer som er i nærheten av helse- og omsorgssektoren når det gjelder omfanget av og sensitiviteten til personopplysningene som blir behandlet. Hensynet til konfidensialitet har derfor hatt høy prioritet i arbeidet med digital sikkerhet i sektoren. Samtidig har helse- og omsorgssektoren et spesielt sterkt behov for tilgjengelighet og integritet av informasjon og systemer for å understøtte pasientsikkerhet og samfunnets helseberedskap. I tillegg har sektoren andre behov som må ivaretas, for eksempel må sykehus være åpne for både pasienter og publikum. Dette medfører begrensninger på hvilke fysiske tiltak som kan implementeres for å beskytte digital infrastruktur.

Gjennom workshops, møter og skriftlige innspillsrunder har en rekke aktører vært involvert i arbeidet med denne rapporten. Et viktig poeng med å involvere så mange, var å avdekke hva som er de største sikkerhetsutfordringene, og om det finnes utfordringer som ikke er tilstrekkelig adressert i ovennevnte rapporter og vurderinger.

Basert på tilbakemeldinger følger nedenfor tre hovedtemaer som vi mener bør inkluderes i en eventuell strategi for digital sikkerhet i helse- og omsorgssektoren. Disse tre temaområdene blir utdypet i mer detalj i kapittel 3.2.

- *Sikker samhandling:* Det er stort behov for løsninger for sikker deling av data, og for sikre fellesløsninger for identitetshåndtering, autentisering og autorisasjon. Økt samhandling medfører også behov for styrkede kontrollmekanismer på sikkerhetsområdet
- *Sikker digital hjemmeoppfølging:* Pasientbehandling flyttes hjem til innbyggerne, og sårbarheter i medisinsk utstyr kan medføre store konsekvenser. Konfidensialitet, tilgjengelighet og integritet må ivaretas for både pasienter og personell. Det kan oppstå uklare ansvarsforhold på sikkerhetsområdet når flere aktører er involvert.
- *Sikkerhet i leverandørkjeden:* Sikkerhet i sektoren bør sees på som en helhet. Både leverandører og anskaffere etterlyser tydeligere og standardiserte sikkerhetskrav og nasjonale føringer for risikoaksept i anskaffelser. Behandling av data hos tredjepart medfører økt kompleksitet i leverandørkontroll, og det er viktig at sikring av medisinsk utstyr ivaretas i hele utstyrets livsløp.

2.2.1 En kompleks sektor med mange aktører

Aktørbildet i helse- og omsorgssektoren er omfattende og komplekst, og består av over 17.000 private og offentlige virksomheter. Det digitale landskapet er fragmentert, med stor variasjon av modenhet på sikkerhetsområdet. Gjennom lokale og regionale beslutninger er det skapt et fragmentert IKT-landskap, noe som gjør det krevende å sikre samordnet elektronisk informasjonsutveksling. I tillegg gjør ulike styringslinjer det utfordrende å få til en koordinert digitalisering av i sektoren. Denne utfordringen er ikke minst gjeldende på området digital sikkerhet.

Selv om størrelse og risikonivå varierer mellom ulike aktører, står hele sektoren overfor det samme trusselbildet. Sektoren utgjør en samlet eksponeringsflate inn mot felles verdier. Særlig de mindre virksomhetene, som mangler kapasitet til å opprettholde et tilstrekkelig sikkerhetsnivå, har behov for felles, nasjonale virkemidler. Strategien bør derfor dekke hele sektoren, men det bør differensieres basert på ansvar og risiko. En sentral ambisjon for strategien bør være å angi en felles retning, og tydelige prioriteringer fra myndighetenes side, i et forståelig språk, til alle de ulike aktørene.

Helse- og omsorgssektoren inneholder også et stort mangfold av leverandører. Dette gjelder ikke minst på digitalisering- og teknologiområdet. Den pågående digitaliseringen i sektoren er

avhengig av en markedssituasjon hvor en større del av de tekniske løsningene både utvikles av, og tilbys i, det private markedet. Det står blant annet i *Prop. 65 L (2019–2020) Forslag til lov om e-helse (e-helseloven)* at en større grad av innovasjon og et robust leverandørmarked er en forutsetning for vellykket digitalisering. «*Dette forutsetter at det foreligger tydelige rammebetingelser i form av mål og strategier som følges opp av krav og prinsipper for utvikling. Rammebetingelsene må sikre utvikling av tjenester og løsninger som enklere kan integreres med hverandre. […] Behovet for nasjonale veiledninger og retningslinjer og utredning av og krav til kodeverk, terminologi, standarder, arkitektur og informasjonssikkerhet, vil derfor øke».*[21]

Sektorens kompleksitet vanskeliggjør en helhetlig styring av området digital sikkerhet. I Nasjonal helse- og sykehusplan 2020–2023 (Meld. St. 7 (2019–2020) er det et mål om en tydeligere nasjonal styring og koordinering av IKT-utviklingen. Regjeringen synliggjør her at de vil ta større ansvar for å sette retning og rammer for IKT-utviklingen – både gjennom styring av etater og helseregioner, samarbeid med kommunesektoren, bruk av regulering og helsefaglig normering, og budsjettforslag. Det betyr ikke at alt skal bestemmes nasjonalt, men at rammen for det lokale handlingsrommet og oppdragene til både tjenesten og forvaltningen må bli tydeligere.[22]

Direktoratet for e-helse har i kraft av sin rolle som fagdirektorat på e-helseområdet ansvar for å fremme digital sikkerhet i helse- og omsorgsektoren. Direktoratet har nasjonal myndighet og premissgiverrolle på e-helseområdet. Direktoratet skal være en pådriver i utviklingen av digitale tjenester i helse- og omsorgssektoren. Dette inkluderer å utvikle, formidle og vedlikeholde nasjonale veiledere og retningslinjer, også for økt digital sikkerhet. Blant annet er Sekretariatet for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren[23] plassert i Direktoratet for e-helse.

NHN er leverandør av kritiske tjenester til helsesektoren og helseforvaltningen, og ivaretar sikkerheten i disse løsningene. HelseCERT er en del av NHN, og er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. HelseCERT har det siste tiåret spilt en viktig rolle som et nav for samhandling mellom operative sikkerhetsmiljøer i sektoren. Samtidig har HelseCERT vært en viktig to-veis kanal inn mot NSM i rollen som sektorens responsmiljø (SRM) innenfor rammeverk for håndtering av IKT-sikkerhetshendelser[24]. Ved hjelp av sensorer i Helsenettet oppdager HelseCERT uønskede hendelser og trafikk som de varsler om til berørte aktører. Som forebyggende tiltak utfører HelseCERT også inntrengingstesting for virksomheter i helse- og omsorgssektoren. HelseCERT drifter tjenesten Nasjonalt beskyttelsesprogram for helse- og omsorgssektoren (NBP), som er en gratis tjeneste for virksomheter i sektoren. Formålet med tjenesten er å gi IKT-driftspersonell verdifull informasjon om aktuelle trusler, sårbarheter og hendelser.

2.2.2 Kommunal sektor

Kommunene har oppgaver og ansvar på tvers av en rekke sektorer. Sikkerhetsutfordringene er derav også tverrsektorielle. Digital sikkerhet i helse- og omsorgssektoren er helt sentralt på kommunalt nivå, da innbyggernes helse, pasientsikkerhet og personvern er viktige hensyn som kommunen skal ivareta.

[21] Helse- og omsorgsdepartementet. 2020. *Forslag til lov om e-helse (e-helseloven)*. Prop. 65 L (2019–2020).
[22] Helse- og omsorgsdepartementet. 2019. *Nasjonal helse- og sykehusplan 2020 – 2023*. Meld. St. 7 (2019–2020).
[23] Se mer i kapittel 3.1.2.4
[24] Nasjonal Sikkerhetsmyndighet. 2017. *Rammeverk for håndtering av IKT-hendelser*.

Digitaliseringstrykket er stort i kommunene, blant annet innen velferdsteknologi, smarte byer, skole, vann og avløp. Mange kommuner inngår i ulike driftssamarbeid gjennom interkommunale selskaper (IKS). IKT-anskaffelser innen helse skjer ofte i samarbeid mellom helseetaten som gjør en bestilling og setter krav og en IT-avdeling eller driftsselskap som konkretiserer kravene og gjennomfører anskaffelsen.

Da mange av virksomhetene i helse- og omsorgssektoren er en del av kommunal sektor, er kommunesektorens egenart viktig å hensynta i en strategi for digital sikkerhet for helse- og omsorgssektoren. Den digitale sikkerheten i en kommune bør jobbes helhetlig med, og sees i sammenheng. Det er viktig at en strategi for digital sikkerhet i helse- og omsorgssektoren ikke skaper unødvendige overlapp, eller motstridende krav, for kommunale virksomheter. Både Digitaliseringsdirektoratet og Kommunesektorens organisasjon (KS) er aktører det er viktig å samarbeide med i denne sammenheng. I tillegg er Foreningen Kommunal Informasjonssikkerhet (KiNS), HelseCERT og KommuneCSIRT tre sikkerhetsmiljøer som kjenner kommunesektoren godt. På workshop med kommuner kom det frem at KommuneCSIRT har velferdsteknologi som et prioritert område, hvor de fremover vil bygge kompetanse på ulike sikkerhetsutfordringer og bidra med veiledning til kommuner.

2.3 Fremtidig utvikling og sikkerhetsmessige behov

En strategi for digital sikkerhet kan ikke fokusere kun på situasjonen slik den er i dag. Digitaliseringen går i et svært raskt tempo, og en god strategi må også være rettet mot fremtidig utvikling og de sikkerhetsmessige behov denne medfører. Vi kan allerede i dag se skissene av en rekke utviklingstrekk og kommende sikkerhetsmessige behov.

Mye samhandling i sektoren foregår i dag ved såkalt meldingsutveksling, for eksempel at henvisninger, epikriser og prøvesvar blir sendt fra virksomhet til virksomhet gjennom EDI[25]. Fremover vil stadig flere journalsystemer og tjenester ha behov for deling av data ved hjelp av åpne API-er. I den forbindelse er det sikkerhetsbehov som må løses for at systemet skal fungere uten å bli misbrukt. Direktoratet for e-helse har i 2019 anbefalt en tillitsmodell for data- og dokumentdeling for å svare på noen av disse utfordringene.[26]

Det er ikke bare behov for å dele data innad i helsevesenet. Det er vel så viktig at relevante helseopplysninger deles med pasienten. Erfaringer viser at pasienter ønsker å få informasjon etter behandling. Utsendelse av epikriser til pasientene fører til bedre tillitsforhold mellom pasient, lege og sykehus og til bedret pasienttilfredshet.[27] Dette er sensitiv informasjon som også må beskyttes. Det er viktig at kliniske hensyn blir godt ivaretatt både i design og implementasjon av løsninger for datadeling, samtidig som tilstrekkelig sikkerhet blir ivaretatt.

Norske helsedata er en betydelig samfunnsressurs. I fremtiden kan kunstig intelligens gjøre det mulig å utnytte våre felles helsedata til å tilby raskere og mer presis diagnostisering, bedre behandling og mer effektiv ressursbruk. Helsedata kan også brukes til kvalitetsforbedring, helseanalyse, ledelse, beredskap og forskning. Men dette fordrer effektiv tilgang til komplett, korrekt og oppdatert informasjon. Digitaliseringsdirektoratet har bygget flere nasjonale løsninger som kan brukes i utviklingen av offentlige digitale tjenester.[28] I fremtiden kan helsesektoren potensielt tilgjengeliggjøre mer data gjennom åpne API-er. De digitale løsningene for denne delingen må også ivareta sikkerhetsbehovet.

[25] Norsk Helsenett. *Elektronisk meldingsutveksling (EDI)*.
[26] Direktoratet for e-helse. 2019. *Anbefaling av tillitsmodell for data- og dokumentdeling*.
[27] Trumpy, Jens Hugo. 2002. *Bør pasientene automatisk få kopi av sin epikrise?*
[28] Digitaliseringsdirektoratet. *Oversikt over nasjonale fellesløsninger*.

2.4 Sammenlikning med andre sektorer og land

For å utrede behovet for en strategi for digital sikkerhet i helse- og omsorgssektoren, er det naturlig å se hen til hva som er gjort både i andre land og andre sektorer.

2.4.1 Andre sektorer med kritisk infrastruktur

Digitale sikkerhetsutfordringer i helse- og omsorgssektoren er på mange måter sammenfallende med andre sektorer i Norge. Angrepsvektorene og trusselaktørene er ikke veldig annerledes for helse- og omsorgssektoren enn for næringslivet og offentlig sektor. For eksempel har kraft- finans og telekomsektorene behov for høy grad av tilgjengelighet i systemer og infrastruktur, og NAV, Skatteetaten, Politiet og Domstolene har mange av de samme utfordringene med å hindre snoking i personopplysninger.

Derimot er det større særegenheter når det kommer til det direkte skadepotensialet i helse- og omsorgssektoren. Konsekvensene med for eksempel brudd på tilgjengelighet er fort større i helse- og omsorgssektoren, når sektoren sammenliknes med samfunnet ellers. Brudd på tilgjengelighet i kritiske systemer kan direkte medføre fare for liv og helse.

I likhet med helse- og omsorgssektoren har for eksempel finanssektoren og telekom også en del kjernesystemer som bygger på utdatert teknologi og spesialisert maskinvare. Selv om disse utfordringene deles med andre sektorer, er de ikke behandlet spesielt i den nasjonale strategien utover krav og forventninger fra myndighetene til beskyttelse av kritisk infrastruktur. For helse og omsorgssektoren gjelder dette særlig medisinsk utstyr. Dette er en form for kritisk infrastruktur som har direkte betydning for folks liv og helse.

Kraftsektoren setter ulike krav til sikring av ulike anlegg utfra en klasseinndeling som er spesifisert i kraftberedskapsforskriften[29]. Interessant med denne tilnærmingen er at det er anleggets funksjon og ikke virksomhetens størrelse som skal være dimensjonerende for sikringstiltakene. En kunne se for seg tilsvarende nasjonal klassifisering i helse- og omsorgssektoren basert på ulike kriterier, for eksempel antall pasienter et system behandler, antall helsepersonellbrukere og hvilke livsviktige eller samfunnskritiske funksjoner systemet utøver. NVE utvikler veiledere for å bistå kraftselskapene med hvordan lov og forskrift skal tolkes, blant annet sjekkliste for IKT-sikkerhet ved anskaffelser[30].

2.4.2 Digital sikkerhet i helsesektoren i andre land

Det er indikasjoner på at digitaliseringstakten i norsk helsesektor er høyere enn i resten av verden. Dette er blant annet understøttet av tall fra Nasjonal e-helsemonitor om IKT-investeringskostnader for helseregionene.[31] En positiv bieffekt av digitalisering og fornying er at nyere IT-systemer generelt er sikrere enn eldre IT-systemer. Til en viss grad blir norske virksomheter derfor sikrere av å ta i bruk mer moderne systemer og rydde opp i de gamle. Det har i norsk helsesektor tradisjonelt vært fokusert mest på konfidensialitet, altså på skjerming av helseopplysninger mot uautorisert innsyn. Dette er ikke unikt for Norge, og forholdet underbygges blant annet av studier gjort i USA.[32] De siste årene har imidlertid vist at helsesektoren i likhet med resten av samfunnet er blitt mer avhengig av at IT-systemene fungerer for å kunne opprettholde normal drift.

[29] Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)
[30] Norges vassdrags- og energidirektorat. 2020. *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen*.
[31] Direktoratet for e-helse. 2020. *Nasjonal e-helsemonitor*.
[32] Independent Security Evaluators. 2016. *Securing Hospitals - A research study and blueprint*.

Helse- og omsorgssektoren er på verdensbasis utsatt for digitale angrep som lammer helseberedskapen hos de rammede virksomhetene. I 2019 ble 400 tannlegekontorer i USA rammet av et løsepengevirus.[33] Samme type hendelse rammet i 2020 amerikanske Universal Health Services, en sykehuskjede med over 90 tusen ansatte.[34] Tysk politi etterforsker nå et løsepengevirusangrep som et uaktsomt drap etter at en kvinne døde mens hun måtte fraktes til et annet sykehus da datasystemene på det nærmeste sykehuset var utilgjengelige.[35]

2.4.2.1 Den danske strategien for cyber- og informasjonssikkerhet

Et av landene det vil være naturlig for Norge å sammenligne seg med er Danmark. Danmark er lik Norge på flere måter, og står ovenfor mange av de samme sikkerhetsmessige utfordringene. De to landene har også valgt lignende tilnærminger til å håndtere disse. I likhet med Norge fikk Danmark i 2018 en nasjonal «cyber- og informationssikkerhedsstrategi». I motsetning til den norske strategien stiller imidlertid den danske strategien krav til at seks utpekte samfunnskritiske sektorer skal ha sin egen sektorspesifikke strategi for cyber- og informasjonssikkerhet. Helse- og omsorgssektoren (sundhedssektoren) er en av disse.

Den danske «Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022», kalt «En styrket, fælles indsats for cyber- og informationssikkerhed» ble lansert i 2019. De danske aktørene besøkte i forbindelse med utarbeidelsen av sin strategi blant annet norske helsemyndigheter. De fikk da en rekke innspill til sitt arbeid. Strategien legger ikke bare vekt på at det er viktig å ivareta konfidensialitet (i form av at opplysninger oppbevares forsvarlig og sikkert), men også at det er viktig å ivareta tilgjengelighet og integritet (i form av at de relevante opplysningene kan nås når det er behov for dem og at opplysningene er korrekte så behandling kan skje på riktig grunnlag). Det ble lagt vekt på at helse- og omsorgssektoren er karakterisert ved en rekke spesifikke forhold når det kommer til digital sikkerhet[36]:

- Sektoren har et meget høyt antall medarbeidere som håndterer sensitive personopplysninger
- Sektoren har et meget komplekst IT-landskap
- Sektoren inkluderer både store organisasjoner og små private virksomheter som alle skal ha et høyt sikkerhetsnivå

I lansering av strategien trakk de også frem noen konkrete områder der det er særlig viktig å iverksette tiltak:

- Medisinsk utstyr
- Leverandørstyring
- Gjensidige avhengigheter mellom aktørene i sektoren
- Cyber- og informasjonssikkerhetskompetansen hos medarbeiderne i sektoren

De spesifikke forholdene som er nevnt er langt på vei gjeldende også i Norge.

2.5 Drøfting og konklusjon om behov

Det digitale risikobildet i helse- og omsorgssektoren understøtter behovet for en egen strategi for digital sikkerhet. Det eksisterer flere forebyggende og reaktive virkemidler både nasjonalt og regionalt, f.eks. HelseCERT og Normen. Disse fungerer godt og har bred

[33] Collier, Kevin (CNN). 2019. *"Hundreds of dental offices crippled by ransomware attack"*.
[34] Newman, Lily Hay (Wired). 2020. *"A Ransomware Attack Has Struck a Major US Hospital Chain"*.
[35] Digi. 2020. «*Kvinne døde etter løsepengevirus-angrep»*.
[36] Sundhedsdatastyrelsen. 2018. *Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022*.

forankring i sektoren. Samtidig eksisterer det en rekke kjente sikkerhetsutfordringer, trusselbildet skjerpes, og forventningene til digitalisering og rask innføring av ny teknologi øker. Da vil det være hensiktsmessig med en strategi både for å styrke eksisterende innsats, men også for å beskrive nye tiltak og virkemidler på nasjonalt nivå.

Selv om svært mye allerede er behandlet i nasjonal strategi for digital sikkerhet, er det identifisert en rekke særskilte utfordringer i sektoren som ikke blir tilstrekkelig adressert i den nasjonale strategien. En overvekt av de involverte aktørene har også gitt sin støtte til behovet for en egen strategi i sektoren. Det pekes på behovet for en felles og samlet retning, med klare prioriteringer fra myndighetenes side.

I prosessen har arbeidsgruppen også mottatt innspill som stiller spørsmål ved om en egen strategi er nødvendig. Slik vi har forstått innspillene, er skepsisen i stor grad knyttet til bekymring for at sektoren ikke trenger nok et lite konkret dokument, uten reell effekt. I tillegg er det for noen aktører, f.eks. for kommunesektoren, vanskelig å forholde seg til flere sektorstrategier og ytterligere kompliserende føringer. Dette er viktig å hensynta i en strategi. Det understreker behovet for at en strategi for digital sikkerhet i helse- og omsorgssektoren er *kort, poengtert* og *handlingsorientert.* Hensikten må være at den faktisk bidrar til å forenkle og styrke sikkerhetsarbeidet i sektoren.

Videre kan en strategi legge til rette for sikker digitalisering for alle, blant annet gjennom å tydeliggjøre ansvar og roller, samt å kommunisere tydelig hvilke forventninger myndighetene har til sikkerhetsarbeidet i den enkelte virksomhet. Det er avdekket et klart behov for å konkretisere egne strategiske mål og tiltak for sektoren, som et supplement til de overordnede nasjonale målene og tilhørende tiltaksoversikt.

Konklusjon: Direktoratet for e-helse anbefaler at det utarbeides en egen strategi for digital sikkerhet i helse- og omsorgssektoren.

3 Innretning på strategi for digital sikkerhet i helse- og omsorgssektoren

I tillegg til å vurdere behovet for en egen strategi for digital sikkerhet i helse- og omsorgssektoren, har en viktig del av arbeidet vært å vurdere hvordan den bør innrettes. Vi har kartlagt hvilke elementer som bør hensyntas i arbeidet, samlet og presentert viktige temaer som strategien bør inneholde og vurdert mulige innretninger og omfanget av dette innholdet. Avslutningsvis presenteres det også en anbefaling for hvordan selve utarbeidelsen av en strategi for digital sikkerhet i helse- og omsorgssektoren bør innrettes.

3.1 Viktige hensyn

Verken sikkerhetsarbeid eller strategiarbeid bør gjennomføres i et vakuum. Det eksisterer allerede er en rekke føringer og reguleringer, både på nasjonalt nivå og for sektoren, som må hensyntas i dette arbeidet. Eksempler på dette er Nasjonal strategi for digital sikkerhet, flere offentlige utredninger på sikkerhetsområdet, og årlige trussel- og risikovurderinger fra sektorvise og nasjonale myndigheter.

Nasjonale lovverk legger også føringer på sikkerhetsområdet i sektoren. Dette inkluderer personvernforordningen, sikkerhetsloven, og i nær fremtid også NIS-direktivet. I tillegg berører flere sektorspesifikke lover området. Normen dekker på sin side mange, men ikke alle, lovkrav til informasjonssikkerhet, personvern og behandling av helse- og personopplysninger. Se Vedlegg 2 Relevante regulatoriske føringer for en kort beskrivelse av relevante regulatoriske føringer.

Helsetilsynet kontrollerer den enkelte virksomhets etterlevelse av en rekke lover for sektoren, som også inkluderer noen krav til sikkerhet. I Statsbudsjettet for 2019 fikk Helsetilsynet i oppdrag å etablere tilsyn også med IKT-løsningene i sektoren. En tilsynsfunksjon for IKT er under oppbygging i Statens Helsetilsyn. I tillegg fører Datatilsynet tilsyn etter personvernforordningen og NSM etter sikkerhetsloven.

Datatilsynet og Riksrevisjonen har de siste årene utført tilsyn og revisjoner som har involvert digital sikkerhet. Riksrevisjonen er i gang med en forvaltningsrevisjon av helseforetakenes evne til å forebygge angrep mot sine IKT-systemer. I tillegg gjennomfører flere kommuner forvaltningsrevisjoner hvor digital sikkerhet har vært på agendaen. Sentrale funn i slike revisjoner vil være viktige for innretning og innhold i en strategi for digital sikkerhet i sektoren.

3.1.1 Nasjonale føringer

Selv om helse- og omsorgssektoren har en rekke særtrekk og sektorspesifikke utfordringer er det viktig at arbeid som allerede er gjort på nasjonalt nivå, samt de politiske føringene som er gitt gjennom disse arbeidene, hensyntas i utarbeidelse av en strategi for digital sikkerhet i helse- og omsorgssektoren.

Eksempelvis nevnes følgende nasjonale føringer og initiativer (ikke uttømmende):

- Nasjonal strategi for digital sikkerhet
- Nasjonal strategi for digital sikkerhetskompetanse
- Andre nasjonale strategier som også omfatter digital sikkerhet, eksempelvis Nasjonal strategi for kunstig intelligens

- Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhet
- Grunnprinsipper for IKT-sikkerhet 2.0
- Grunnprinsipper for fysisk sikkerhet
- Grunnprinsipper for sikkerhetsstyring
- Grunnprinsipper for personellsikkerhet
- Andre relevante råd fra Nasjonal sikkerhetsmyndighet, eksempelvis deres råd for tjenesteutsetting og skytjenester
- Relevante rapporter fra EOS-tjenestene (E-tjenesten, PST og NSM)
- Kartlegging av sikkerhetstilstanden i kommunal sektor i regi av Digitaliseringsdirektoratet
- Sikkerhetsloven
- NIS-direktivet

Vi har i dette kapittelet valgt å utdype noen av disse.

3.1.1.1 Nasjonal strategi for digital sikkerhet

Nasjonal strategi for digital sikkerhet, publisert i 2019, er den fjerde i rekken av strategier norske myndigheter har lansert på området. Den forrige var Nasjonal strategi for informasjonssikkerhet, som ble lansert i 2012. Den nasjonale strategien dekker hele samfunnet, og er av generell karakter.

Den nasjonale strategien for digital sikkerhet er resultatet av et grundig arbeid over lengre tid. Arbeidet bygget på anerkjente NOUer og Stortingsmeldinger på området, og en rekke aktører fra både fra privat og offentlig sektor var involvert i arbeidet. Regjeringens ambisjon er at Nasjonal strategi for digital sikkerhet skal sette det norske samfunnet i stand til «*å møte utfordringene som følger av en rask og gjennomgående digitalisering».* Strategiens visjon er at: *«I Norge skal det være trygt å bruke digitale tjenester. Privatpersoner og virksomheter skal ha tillit til at den nasjonale sikkerheten, den enkeltes velferd og demokratiske rettigheter blir ivaretatt i et digitalisert samfunn».*[37]

Strategien har følgende mål:

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

Det enkelte departement er ansvarlig for at strategiens prioriteringer og foreslåtte tiltak blir fulgt opp innenfor sin sektor. Det er ikke gitt konkrete føringer om at egne sektorstrategier skal utarbeides, men dette er én måte å løse dette oppdraget på. Det som er spesifisert, er at departementet aktivt skal involvere berørte parter i privat sektor i utarbeidelsen av tiltak og følge opp effektiviteten av iverksatte tiltak i egen sektor.

3.1.1.2 Andre sentrale nasjonale strategier og utredninger

Digital sikkerhet har fått mye oppmerksomhet hele det siste tiåret. Både før, parallelt, og i etterkant av arbeidet med nasjonal strategi for digital sikkerhet, er det utarbeidet flere offentlige utredninger og strategier som er relevante for området.

[37] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*.

NOU 2015: 13 Digital sårbarhet – sikkert samfunn, var den første offentlige utredningen som omhandlet samfunnets digitale sårbarhet på nasjonalt nivå. Utvalget kom med en rekke anbefalinger for hvordan norske myndigheter og det norske samfunnet burde jobbe for å redusere sin digitale sårbarhet. Disse ble i stor grad videreført og videreutviklet med den nye nasjonale strategien for digital sikkerhet.[38]

Stortingsmelding St. 38 (2016–2017) IKT-sikkerhet — Et felles ansvar, var den første stortingsmeldingen om IKT-sikkerhet. Her ble det blant annet understreket at ingen sektorer, og få nasjoner, kan kontrollere sin digitale sårbarhet alene. Utfordringene i det digitale rommet er grenseoverskridende – på tvers av land, sektorer og virksomheter, og utviklingen går svært fort. For å sikre effektivisering gjennom økt digitalisering av det norske samfunnet, må IKT-løsninger og digitale tjenester være tilstrekkelig, sikre og pålitelige.[39]

NOU 2018: 14 - IKT-sikkerhet i alle ledd, tok for seg organisering og regulering av nasjonal IKT-sikkerhet. Utvalget anbefalte flere regulatoriske og organisatoriske tiltak for å styrke nasjonal IKT-sikkerhet. Dette inkluderte blant annet å etablere et nasjonalt IKT-sikkerhetssenter, og tydeligere styring og bedre koordinering av nasjonal IKT-sikkerhet.[40]

3.1.1.3 Sentrale nasjonale aktører, anbefalinger og vurderinger

Det er Justis- og beredskapsdepartementet som har samordningsansvaret for digital sikkerhet for den sivile delen av samfunnet. De har blant annet ansvaret for å utarbeide og følge opp nasjonale strategier, og identifisere sektorovergripende spørsmål. De er også styrende departement for NSM, som er det nasjonale fagmiljøet for IKT-sikkerhet. I slutten av 2019 styrket Regjeringen den nasjonale digitale sikkerheten med etableringen av Nasjonalt cybersikkerhetssenter (NCSC). Senteret er en del av NSM, og samler Forsvaret, andre offentlige virksomheter, samt en rekke private aktører på ett sted. Denne samlingen av kompetanse og kapasitet legger til rette for et felles risikobilde og situasjonsforståelse, og gir mulighet for koordinering av innsats hvis Norge skulle bli utsatt for et bredt dataangrep.

NSM har siden 2017 utarbeidet «Grunnprinsipper for IKT-sikkerhet»[41], som er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. NSM har også utviklet flere andre temarettede veiledere for sikring av ugraderte systemer, og i 2020 har de i tillegg publisert grunnprinsipper for flere andre områder.

Arbeid med sikkerhet krever god forståelse av risikobildet. Det gjennomføres jevnlig trussel- og risikovurderinger på nasjonalt nivå, av diverse myndighetsorganer. Både NSM, Direktoratet for samfunnssikkerhet og beredskap (DSB), Kripos, PST og Etterretningstjenesten publiserer årlig sine vurderinger, hvor digital risiko og digitale trusler får svært mye oppmerksomhet. Helse- og omsorgssektoren er i stor grad berørt av de samme truslene og risikoene som resten av samfunnet, og disse vurderingene er en viktig del av situasjonsbildet som utgangspunktet for en strategi for digital sikkerhet i sektoren.

3.1.2 Føringer i sektoren

For at en strategi for digital sikkerhet i helse- og omsorgssektoren skal bidra til å forenkle arbeidet med digital sikkerhet i sektoren, må utarbeidelsen koordineres med andre relevante styringsdokumenter og initiativer.

[38] Justis- og beredskapsdepartementet. 2015. *Digital sårbarhet – sikkert samfunn*. NOU 2015: 13.
[39] Justis- og beredskapsdepartementet. 2017. *IKT-sikkerhet — Et felles ansvar*. Meld. St. 38 (2016–2017).
[40] Justis- og beredskapsdepartementet. 2018. *IKT-sikkerhet i alle ledd*. NOU 2018: 14.
[41] Nasjonal Sikkerhetsmyndighet. 2020. *Grunnprinsipper for IKT-sikkerhet 2.0*.

Eksempelvis nevnes følgende føringer og initiativer i sektoren (ikke uttømmende):

- Prop. 65 L (2019–2020) Forslag til lov om e-helse (e-helseloven)
- Nasjonal e-helsestrategi 2017-2022, samt plan for arbeidet med ny strategi
- Nasjonal helse- og sykehusplan 2020-2023
- Helsedirektoratets overordnede ROS-vurderinger for nasjonal helseberedskap
- Diverse områdestrategier (eksempelvis strategi for innbyggertjenester, samhandling etc.)
- Plan for utvikling av Felles grunnmur for digitale tjenester i helse- og omsorgstjenesten
- Felles tillitsmodell for data og dokumentdeling
- Akson – felles kommunal journal
- Helhetlig samhandling
- Helsedataprogrammet
- Normen, både revidert mandat for styringsgruppen og forslag til ny forvaltningsmodell
- Pasientsikkerhetsprogrammet

Vi har i dette kapittelet valgt å utdype noen av disse.

3.1.2.1 Én innbygger – én journal

Gjennom stortingsmeldingen St. 9 (2012–2013) *Én innbygger – én journal – Digitale tjenester i helse- og omsorgssektoren*[42]*.* har Regjeringen satt tre overordnede mål for IKT-utviklingen i helse- og omsorgssektoren:

- *Helsepersonell skal ha enkel og sikker tilgang til pasient- og brukeropplysninger*
- *Innbyggerne skal ha tilgang på enkle og sikre digitale tjenester*
- *Data skal være tilgjengelig for kvalitetsforbedring, helseovervåking, styring og forskning*

3.1.2.2 Nasjonal e-helsestrategi

Nasjonal e-helsestrategi for 2017-2022, har mål om *en digitalisert, samlet helse- og omsorgstjeneste som oppleves enklere, bedre og mer helhetlig for innbyggerne*.[43] Norge er i dag kommet et stykke på veien for å nå ambisjonene om en effektiv, bærekraftig og papirløs helse- og omsorgstjeneste. De seks strategiske satsingsområdene i nasjonal e-helsestrategi er som følger:

- *Digitalisering av arbeidsprosesser*
- *Bedre sammenheng i pasientforløp*
- *Bedre bruk av helsedata*
- *Helsehjelp på nye måter*
- *Felles grunnmur for digitale tjenester*
- *Nasjonal styring av e-helse og økt gjennomføringsevne*

Plan for e-helse 2019-2022 er et vedlegg til Nasjonal e-helsestrategi, og beskriver innsatsen som er nødvendig for å realisere strategien. Planen inneholder 14 innsatsområder, som er sortert under de seks strategiske satsingsområdene. Et av disse 14 innsatsområdene er å: «*styrke arbeidet med beredskap, informasjonssikkerhet og personvern».*[44]

[42] Helse- og omsorgsdepartementet. 2012. *Én innbygger – én journal*. Meld. St. 9 (2012–2013).
[43] Direktoratet for e-helse. 2019. *Nasjonal e-helsestrategi og handlingsplan 2017-2022 (oppdatert 2019)*.
[44] Ibid

3.1.2.3 Nasjonal helse og sykehusplan

I Nasjonal helse og sykehusplan 2020-2023, påpekes det at «*befolkningen skal ha tillit til at helsetjenesten både ivaretar deres personvern og tar i bruk de mulighetene teknologien gir for å utvikle bedre tjenester»*.[45] Planen inneholder tiltak og eksempler på ny bruk av teknologi i helsesektoren som skal bidra til at sektoren oppnår helsepolitiske mål. Dette medfører også store endringer i hvordan hele sektoren samhandler og kommuniserer, både i og på tvers av sektoren og med pasienter.

Vellykket digitalisering krever god samhandling mellom mennesker og teknologi, og sikkerhet er et av hensynene som må ivaretas som en del av utviklingen. Flere av målene i Nasjonal helse- og sykehusplan er knyttet til sikker samhandling, og hvordan dette skal legge til rette for helsehjelp, innovasjon og forskning:

- Pasientene opplever sammenhengende tjenester på tvers av sykehus og kommuner. Digitale løsninger gjør arbeidshverdagen enklere, ikke vanskeligere.
- Pasienter opplever en sammenhengende akuttmedisinsk kjede der innsats settes tidlig inn, og informasjonen følger pasienten hele veien.
- Pasientene opplever at bruk av våre felles helsedata, ved hjelp av teknologi, gir bedre og mer presis helsehjelp. Pasientene føler seg trygge på at informasjonen om dem blir behandlet på forsvarlig måte.
- Helsepersonellet jobber i team rundt pasienten, utvikler tjenesten i tråd med kunnskap om hva som virker og utnytter mulighetene som teknologien gir.

3.1.2.4 Normen

Norm for informasjonssikkerhet og personvern i helse og omsorgssektoren (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket.[46] Dette er en bransjenorm, som er utarbeidet og forvaltes av organisasjoner og virksomheter i helse- og omsorgssektoren. Den skal være et hjelpemiddel for den enkelte virksomhets arbeid med informasjonssikkerhet og personvern. Normen har også et populært kurs – og konferansetilbud til sektoren. I tillegg engasjeres sektoren i utarbeidelse av faktaark og veiledere gjennom referansegrupper, arbeidsseminar o.l. Til sammen utgjør disse aktivitetene en viktig arena kompetansebygging og erfaringsutveksling rundt digital sikkerhet i sektoren.

Normen dekker mange, men ikke alle, lovkrav til informasjonssikkerhet, personvern og behandling av helse- og personopplysninger. Den utdyper og supplerer gjeldende regelverk, og gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge den. I medlemsvilkårene til Helsenettet er det et vilkår at virksomheten må følge Normen. Det er imidlertid ingen funksjon som i dag kontrollerer disse virksomhetenes etterlevelse av Normen. Dette gjør at den enkelte virksomhet ikke får noen tilbakemelding på om kravene er godt nok ivaretatt. NHN har tidligere gjennomført slike kontroller, men de er blitt avviklet i senere tid.

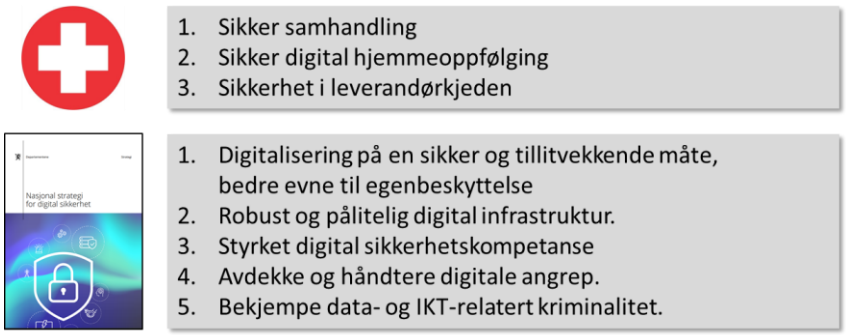
Normen er utarbeidet og forvaltes av en styringsgruppe fra helse- og omsorgstjenesten. Det er et pågående arbeid som nå reviderer mandat for Normens styringsgruppe, og utvikler ny forvaltningsmodell for Normens produkter.

[45] Helse- og omsorgsdepartementet. 2019. *Nasjonal helse- og sykehusplan 2020 – 2023*. Meld. St. 7 (2019–2020).
[46] Direktoratet for e-helse. 2020. *Normen*.

3.2 Temaområder

Sikkerhetsutfordringene ved digitalisering er i høyeste grad sektoroverskridende. Det er gjort et omfattende arbeid med å utvikle Nasjonal strategi for digital sikkerhet (2019). Det er dermed naturlig at den nasjonale strategien, og de politiske føringene som er gitt gjennom dette arbeidet, setter rammen for en strategi for digital sikkerhet i helse- og omsorgssektoren. Samtidig har helse- og omsorgssektoren, som skissert i kapitlene over, en rekke særtrekk og sektorspesifikke utfordringer som må adresseres i en strategi.

Totalt sett bør ambisjonen for en strategi for digital sikkerhet i helse- og omsorgssektoren dermed være å bidra til å realisere både de nasjonale målene for digital sikkerhet og de nasjonale målene for e-helse. I praksis betyr dette at en strategi for digital sikkerhet i helse- og omsorgssektoren både bør ta for seg hvordan målene fra den nasjonale strategien skal oppnås i helse- og omsorgssektoren, samt inkludere temaer som er særegne for sektoren. Basert på tilbakemeldingene vi har fått et det særlig tre hovedtemaer som bør inkluderes i en strategi for digital sikkerhet i helse- og omsorgssektoren: sikker samhandling, sikker digital hjemmeoppfølging og sikkerhet i leverandørkjeden.



Figur 2: Temaer som bør inkluderes i strategien.

3.2.1 Prioriterte områder fra den nasjonale strategien

Den nasjonale strategien legger vekt på at det er viktig å sørge for en helhetlig tilnærming til sikkerhetsutfordringene, enten det gjelder tilsiktede eller utilsiktede digitale hendelser. «*Det er i samspillet mellom de forebyggende tiltakene, 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».* [47] Under utarbeidelse av en sektorstrategi, bør målene og tiltakene fra den nasjonale strategien operasjonaliseres for helse- og omsorgssektoren.

3.2.1.1 Forebyggende digital sikkerhet

Overordnet mål: *Norske virksomheter digitaliserer på en sikker og tillitvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.*

Å ivareta digital sikkerhet er først og fremst et virksomhetsansvar. Virksomhetsledere er ansvarlig for å foreta risikovurderinger, og på bakgrunn av dette gjennomføre tilstrekkelige tiltak. Det mangler ikke på gode råd fra NSM, Datatilsynet, Digitaliseringsdirektoratet og Normen til hvordan virksomheter bør jobbe med sikkerhet for å beskytte seg og ivareta lovkrav. Likevel er det en utfordrende oppgave for enhver virksomhet å følge alle gode råd.

[47] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Side 11.

Det kan være behov for å kommunisere tydelig hvilke ansvar og roller som gjelder i helse- og omsorgssektoren, noe Helsedirektoratet har påpekt i ROS 2019.[48] I tillegg er det viktig at myndighetene legger til rette for at virksomheter både kan forebygge og håndtere uønskede digitale hendelser, både for å ivareta egen sikkerhet og for å øke samfunnets samlede robusthet. De siste årene har vist stadig større kostnader knyttet til gjenoppretting etter datainnbrudd. Sektoren forvalter offentlige midler og det er et selvstendig argument for forebyggende sikkerhet i sektoren at de økonomiske verdiene beskyttes slik at de kommer befolkningen til gode i form av helsehjelp.

3.2.1.2 Digital sikkerhet i kritiske samfunnsfunksjoner

Overordnet mål: *Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.*

Kritiske samfunnsfunksjoner er funksjoner som samfunnet må klare å opprettholde til enhver tid. Helse- og omsorgssektoren utøver flere kritiske samfunnsfunksjoner som bygger på både sentral og lokal infrastruktur. I tillegg til de direkte konsekvensene for liv og helse ved bortfall av disse funksjonene, er en rekke andre samfunnsfunksjoner avhengige av at de fungerer, jf. Tabell 1 i avsnitt 2.1.1. Helseberedskap er en helt sentral del av nasjonal beredskap.

Sektoren behandler personopplysninger om størstedelen av befolkningen og er dermed et attraktivt mål for avanserte trusselaktører som har motivasjon til å utføre kartlegging, ID-tyveri og påvirkingsoperasjoner med konsekvenser for nasjonal sikkerhet.

Helsemyndighetene må ha oversikt over kritisk digital infrastruktur i sektoren, stille krav til sikkerhet, og følge opp at sikkerheten er tilstrekkelig. Helsemyndighetene må på strategisk nivå sørge for at det finnes rammeverk og metoder for å identifisere kritisk digital infrastruktur sett opp mot grunnleggende nasjonale funksjoner (GNF).[49]

Rapporten *Risikostyring i digitale verdikjeder* ble publisert i januar 2020, og var en oppfølging av *NOU 2015:13 Digital sårbarhet – sikkert samfunn.* Direktoratet for samfunnssikkerhet og beredskap (DSB) nedsatte en arbeidsgruppe, ledet av professor Olav Lysne, som skulle foreslå et nasjonalt rammeverk for at myndighetene skal kunne ha en samlet oversikt over digitale verdikjeder, og en modell for at virksomhetene selv kan etablere oversikt over slike kjeder.[50] Dette bør danne grunnlag for hvordan sektoren skal jobbe med dette temaet, på strategisk nivå og på virksomhetsnivå.

3.2.1.3 Kompetanse

Overordnet mål: *Styrket digital sikkerhetskompetanse i tråd med samfunnets behov.*

Sikkerhetskompetanse er ansett for å være et spesielt viktig satsningsområde. Samtidig som den nasjonale strategien for digital sikkerhet ble det utarbeidet en egen strategi for digital sikkerhetskompetanse.[51] Behov for kompetanse har også i workshopene skilt seg ut som et tema som er viktig for sektoren, spesielt i skjæringspunktene mellom helsefag, teknologi og sikkerhetsfag. Det er mange aktører som sier at deres største utfordring innen digital sikkerhet er nettopp manglende kompetanse. Dette gjelder både ansatte og ledere, blant helsepersonell i IKT-miljøene og blant anskaffere.

[48] Helsedirektoratet. 2019. *Overordnede risiko- og sårbarhetsvurderinger for nasjonal beredskap i helse- og omsorgssektoren 2019 - Oversikt over tiltak.*
[49] Se avsnittet om Sikkerhetsloven i Vedlegg 2.
[50] Direktoratet for samfunnssikkerhet og beredskap. 2020. *Risikostyring i digitale verdikjeder*.
[51] Denne strategien ble utarbeidet av Justis- og beredskapsdepartementet i samarbeid med Kunnskapsdepartementet.

Ett tiltak fra den nasjonale strategien for digital sikkerhet som direkte treffer helse- og omsorgssektoren er en satsing på styrket digital sikkerhet i helsefagutdanningene.[52] Plan for e-helse 2019-2022 har også et mål om økt kunnskap og kompetanse om beredskap, informasjonssikkerhet og personvern gjennom kompetansehevende tiltak som er tilpasset ulike roller og brukergrupper. De kompetansehevende tiltakene omfatter blant annet basis- og bestillerkompetanse og innebygd personvern.

Sektoren har tradisjon for å dele informasjon om trusler og sårbarheter både gjennom Normkonferansen og gjennom operative aktiviteter i regi av NHN og HelseCERT. Et godt eksempel på pedagogisk opplæring for helsepersonell er kompetanseprogrammet KOMP-iS,[53] som ble utviklet av Helse Sør-Øst og som store deler av sektoren har fått glede av.

3.2.1.4 Avdekke og håndtere digitale angrep

Overordnet mål: *Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.*

Ifølge NSM forutsetter den kollektive evnen til å håndtere digital angrep at de ulike sektorene følger opp dette arbeidet og at de ulike sektorresponsmiljøene videreutvikles sammen med det nasjonale responsmiljøet. Evnen til å avdekke og håndtere digitale angrep varierer mellom store og små virksomheter i helse- og omsorgssektoren. HelseCERT favner bredt og fungerer som sektorresponsmiljø (SRM) [54] opp mot det nasjonale responsmiljøet, i tillegg til å bidra til kompetansedeling og operativt sikkerhetssamarbeid på tvers i sektoren.

Det er viktig å opprettholde det gode samarbeidet med nasjonale aktører som NSM. NSM skal videreutvikle nasjonale kapasiteter med blant annet kunstig intelligens og maskinlæring.[55]. Dette bør også ses i sammenheng med HelseCERT sin utvikling av ny sensorplattform i programmet Digital Beskyttelse i Dybden (DBD)[56]. Økt nasjonal kapasitet betyr større muligheter for tverrsektoriell samhandling som kan komme helsesektoren til gode hvis forholdene ligger til rette for det. Fremover blir det viktig å opprettholde evnen til å agere på råd fra NSM angående trusler og sårbarheter. Virksomhetene må ha en tilstrekkelig evne til egenbeskyttelse og håndteringskapasitet, samt etablerte kommunikasjonslinjer til nasjonale kapasiteter gjennom HelseCERT.

Sektoren må i større grad gjennomføre beredskapsøvelser knyttet til bortfall av IKT og cyberangrepshendelser. Evaluering etter datainnbruddet i Helse Sør-Øst i 2018 er trukket frem i nasjonal strategi som et viktig tiltak.[57] Formålet med slike evalueringer er å identifisere læringspunkter, foreslå tiltak og påse at de følges opp.

3.2.1.5 Bekjempe data- og IKT-relatert kriminalitet

Overordnet mål: *Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.*

Overordnet mål, delmål og tiltak for det femte prioriterte området i nasjonal strategi er direkte rettet mot politiet. Det er likevel verdt å merke seg at strategien forteller om et større behov for samarbeid mellom politiet og andre aktører. Ingen kan ivareta sikkerheten alene. Det er nødvendig å legge til rette for effektivt operativt sikkerhetssamarbeid i sektoren for å håndtere digital kriminalitet i samarbeid med andre relevante myndigheter. For at politiet skal kunne bekjempe datakriminalitet er de helt avhengige av et godt samarbeid med

[52] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Tiltak 2.4.
[53] KS. 2020. *KOMP-iS-filmene*.
[54] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Tiltak 40.
[55] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Tiltak 1.
[56] Norsk Helsenett. 2019. *Årsrapport 2019*.
[57] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Tiltak 45.

virksomhetene som rammes. Helsesektoren med sine mange ansatte og store verdier, gir viktige bidrag til vårt kollektive forsvar. Det er naturlig at HelseCERT har operativ dialog med politiet, for eksempel gjennom Nasjonalt cyberkrimsenter (NC3),[58] NSM og Felles cyberkoordineringssenter (FCKS).[59]

3.2.2 Prioriterte områder fra Helse- og omsorgssektoren

De prioriterte områdene i nasjonal strategi for digital sikkerhet dekker mye av behovet for digital sikkerhet i helse- og omsorgssektoren. Samtidig er det områder som er viktig for sektoren, som den mer generelle nasjonale strategien ikke inkluderer i tilstrekkelig grad. De følgende tre avsnittene oppsummerer innspillene arbeidsgruppen har mottatt, blant annet gjennom workshoper med bred deltakelse fra sektoren.

3.2.2.1 Sikker samhandling

Samhandling er et høyt prioritert område i sektoren. Det vises blant annet til arbeidet med Felles grunnmur[60] og Felles tillitsmodell[61]. Strategi for digital sikkerhet bør adressere hvordan konfidensialitet, integritet og tilgjengelighet skal ivaretas i dette arbeidet. En rekke forhold innenfor temaet sikker samhandling bør derfor vurderes inkludert i en strategi for digital sikkerhet i helse- og omsorgssektoren, eksempelvis:

- Sikker samhandling skal legge til rette for *helsehjelp*, *innovasjon* og *forskning*. I Nasjonal helse- og sykehusplan 2020–2023 er flere av målene knyttet til dette.
- Felleskomponenter for identitetshåndtering, autentisering og autorisasjon skal bidra til økt sikkerhet i sektoren. Sikre fellesløsninger reduserer behovet for sikkerhetskompetanse hos den enkelte virksomhet, særlig for mindre virksomheter.
- Ved økt samhandling er det behov for styrkede mekanismer for å kontrollere sikkerheten hos samhandlende virksomheter. Tilsyn, selvevaluering og økonomiske insentiver er eksempler på kontrollmekanismer som kan fungere effektivt.
- Behandling og oppfølging av enkeltpasienter skjer på ulike tjenestenivåer og ved ulike virksomheter, både i primær – og spesialisthelsetjenesten. Ofte beveger pasienter seg på tvers av disse skillelinjene i løpet av et sykdomsforløp. Relevante og nødvendige opplysninger om pasienten må være tilgjengelige for helsepersonellet, og i enkelte tilfeller kan denne tilgjengeligheten handle om liv og død. Det medfører store behov til effektiv samhandling og sikker formidling av informasjon.

3.2.2.2 Sikker digital hjemmeoppfølging

I tråd med Nasjonal helse- og sykehusplan flyttes stadig mer pasientbehandling hjem til innbyggerne. Nettbasert behandling kan bidra til å redusere antall konsultasjoner som krever fysisk oppmøte. Ved avansert hjemmesykehus kan pasienter også motta behandling som normalt foregår på sykehuset, i hjemmet. Dette er både et ønske fra mange pasienter, og ressurseffektivt for de som leverer tjenestene. Covid-19 situasjon har tydeliggjort en rekke fordeler ved digital hjemmeoppfølging. Blant annet har helsevesenet hatt mulighet å gi forsvarlig helsehjelp til en rekke pasienter fra sårbare grupper som har hatt behov for å være i karantene eller av andre grunner kvier seg mot å omgå store menneskemengder.

[58] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Tiltak 4.
[59] Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Tiltak 43.
[60] Direktoratet for e-helse. 2019. *Plan for utvikling av felles grunnmur for digitale tjenester i helse- og omsorgstjenesten*.
[61] Direktoratet for e-helse. 2019. *Anbefaling av tillitsmodell for data- og dokumentdeling*.

Bruk av velferdsteknologi, medisinsk utstyr i hjemmebehandling, fjerndiagnostikk, etc., bringer med seg en rekke sikkerhetsutfordringer som må løses for at helsepersonell og pasienter skal ha tillit til teknologien. Medisinsk avstandsoppfølging innebærer lange, komplekse og uoversiktlige verdikjeder. En rekke forhold innenfor temaet *sikker digital hjemmeoppfølging* bør derfor vurderes inkludert i en strategi for digital sikkerhet i helse- og omsorgssektoren, eksempelvis:

- Digital hjemmeoppfølging innebærer teknologi som er plassert i pasientens hjem, som kan utgjøre et av de svakeste elementene i verdikjeden.
- Sikker autentisere av pasientene som til tider kan ha kognitiv svikt, eller andre lidelser som påvirker mulighetene de har til å autentisere seg, og sikker autentisering av utstyret må ivaretas.
- Sårbarheter i digitalt medisinsk utstyr kan medføre store konsekvenser. Både eksterne trusler, slik som hacking av pacemakere og insulinpumper, men også programvarefeil og teknisk svikt, kan potensielt ha dødelig utfall.
- Usikker infrastruktur i pasientens hjem kan også være en utfordring. Dersom utstyret har dårlig sikring, kan det medføre sårbarheter som gjør at dataene kan endres, noe som kan få fatale konsekvenser for pasienten. Samtidig må utstyret være enkelt å bruke for en brukergruppe som gjerne har begrenset kapasitet på området.
- Både fastlege, sykehjem og sykehus kan ha utstyr hjemme hos samme innbygger. Det vil da være behov for avklarte roller og enhetlig kommunikasjon til pasienten rundt ansvar knyttet til sikkerhet og personvern.
- Medisinsk utstyr har ofte særegne utfordringer knyttet til sikkerhet. Det er derfor nødvendig med tett samarbeid med leverandørene gjennom hele utstyrets levetid.
- En tilleggsutfordring med medisinsk utstyr hos innbygger er at helsepersonell har begrenset mulighet til å følge opp og at pasienten i større grad involveres i bruken.
- Digital dialog (eksempelvis videokonsultasjoner og nettbaserte behandlingsprogram) mellom pasient og helsevesen blir stadig mer utbredt. Konfidensialitet, integritet og tilgjengelighet må ivaretas både for pasienter og helsepersonell.
- Innrapporterte data fra pasienten og mellomlagring/ pre-prosessering hos leverandører lagres som oftest i leverandørenes dataservere i skyen. Flere underleverandører skaper lange og uoversiktlige verdikjeder. Dette stiller komplekse krav til dekkende databehandleravtaler, gjennomføring av dekkende risikovurderinger, rutiner for sletting av overskuddsdata, overføring av data utenfor EU/EØS, hva leverandører har tilgang til, og i de tilfeller leverandører tilbyr "add-ons" som virksomhetene (dataansvarlig) ikke har kontroll på. Det er videre viktig å sikre at data kan slettes/overføres hvis/når den leverandøren sitt system byttes ut, eller pasient/behandler ikke lenger bruker systemet.

3.2.2.3 Sikkerhet i leverandørkjeden

De fleste virksomhetene i sektoren er små og har begrensede muligheter til å utøve sikkerhetsstyring, inkludert gode risikovurderinger og leverandørkontroll. Leverandøroppfølging er også en utfordring for større virksomhetene. Leverandørene har selv løftet sin frustrasjon over store ulikheter i krav, og hvordan disse følges opp. Ulik tolking av krav og manglende tilsyn ser ut til å være problematisk for effektive anskaffelser og

innovasjon. En rekke forhold innenfor temaet *sikkerhet i leverandørkjeden* bør derfor vurderes inkludert i en strategi for digital sikkerhet i helse- og omsorgssektoren, eksempelvis:

- Sikkerhet i sektoren bør sees på som en helhet. Standardisering av sikkerhetskrav, og sentralisering av tjenester vil gjøre det enklere å vite hvem som har ansvar for ivaretagelsen av et forsvarlig høyt sikkerhetsnivå. En strategi bør legge til rette for at mindre aktører med begrenset kompetanse og ressurser kan oppnå god nok sikkerhet, f.eks. gjennom å ta i bruk sikre felles komponenter og godkjente løsninger.
- Et legekontor kan stille krav til deres journalleverandør at de skal følge Normen, men legekontoret har begrensede muligheter til å følge opp og kontrollere at sikkerhetskravene er fulgt. Denne problemstillingen kan løses ved hjelp av ordninger for tilsyn eller sertifisering av leverandører.
- Utvikling av flere regionale og nasjonale systemer gjør at mer informasjon samles i en kurv og stiller større krav til tilgjengelighet/oppetid. For å ivareta helseberedskapen blir det viktigere i fremtiden at den enkelte virksomhet kartlegger sine verdikjeder og stiller riktige krav og forventninger til samarbeidspartnere og tjenesteleverandører.
- Tilbakemeldinger fra flere aktører i sektoren viser at både leverandører og tjenestetilbydere i sektoren ønsker tydeligere standardiserte sikkerhetskrav for leverandører i sektoren. Det er likevel en utfordring for sektoren å skape felles forståelse for risiko knyttet til digitale løsninger, blant annet fordi ulike virksomheter må ha ulik risikoaksept. Flere i sektoren etterlyser likevel nasjonale føringer eller retningslinjer for risikoaksept i anskaffelser, blant annet for bruk av skytjenester[62].
- Sikring av medisinsk utstyr er et eget fagfelt og krever blant annet oppfølging og samarbeid med leverandører i utstyrets livsløp.
- Behandling av data hos tredjepart krever gode databehandleravtaler og leverandørkontroll. I tillegg til velferdsteknologi, er det flere som trekker frem nye problemstillinger og utfordringer knyttet til kunstig intelligens (KI)[63] og genetikk[64].

3.3 Innretning på innhold og omfang

3.3.1 Formål

I workshopene og møtene som har blitt gjennomført som en del av dette arbeidet, har interessenter i sektoren løftet en rekke relevante sikkerhetsutfordringer og innspill til hva som bør være formålet med en strategi for digital sikkerhet i helse- og omsorgssektoren. Tilbakemeldingene tyder på at disse formålene er viktige for hva som skal oppnås med en strategi, uavhengig av tema:

- Tydeliggjøre sikkerhetsbehov
- Tydeliggjøre roller og ansvar
- Identifisere (nye) strategiske virkemidler og tiltak

Figur 3: Visualisering av sammenheng mellom målene i den nasjonale strategien for digital sikkerhet, de særegne behovene i helse- og omsorgssektoren og formålene med en strategi for digital sikkerhet i helse- og omsorgssektoren.

[62] Direktoratet for e-helse. 2020. *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger*.
[63] Direktoratet for e-helse. 2019. *Utredning om bruk av kunstig intelligens i helsesektoren*.
[64] Datatilsynet. 2013. *Personvernutfordringer ved genetiske undersøkelser*.

3.3.1.1 Tydeliggjøre sikkerhetsbehov

En strategi for digital sikkerhet i helse- og omsorgssektoren må sørge for at *sikkerhetsbehovet* blir tydeliggjort i hele sektoren. I en stor og kompleks sektor vil behovet for sikkerhet naturlig nok variere mellom virksomheter. Risikobildet, og ikke minst risikoaksepten, er forskjellig i ulike virksomheter. Samtidig må den grunnleggende sikkerheten være ivaretatt i hele sektoren. Vi ser i tillegg at ny teknologi og nye arbeidsmåter medfører nye og endrede sikkerhetsbehov. Dette fordrer en risikobasert tilnærming til digital sikkerhet der både nåsituasjonen og den fremtidige utviklingen blir ivaretatt.

Tydeliggjøring av sikkerhetsbehov på tvers av variasjonene i sektoren, og hvordan disse bør hensyntas både nå og i fremtiden, bør være en sentral del av formålet med en egen strategi.

3.3.1.2 Tydeliggjøre roller og ansvar

En strategi for digital sikkerhet i helse- og omsorgssektoren må også sørge for at *roller og ansvar* blir tydeliggjort. Mangfoldet av virksomheter, tette koblinger og lange verdikjeder i helse- og omsorgssektoren gjør at dagens aktørbilde og ansvarsforhold er utfordrende å forstå. Ansvar for sikkerhet må være plassert og anerkjent, enten dette gjelder nasjonalt faglig ansvar, RHF-enes ansvar for sikkerheten i store systemer, eller det lokale legekontorets ansvar for pasientsikkerheten og personvernet til den enkelte pasient.

Dataansvar for behandling av helse- og personopplysninger utgjør et svært sentralt ansvar også for digital sikkerhet. På de områdene der det er behov for tydeliggjøring av dataansvar, kan dette bli et moment som tas inn i strategien.

3.3.1.3 Identifisere relevante strategiske virkemidler og tiltak

Videre må en strategi for digital sikkerhet i helse- og omsorgssektoren sørge for at relevante *strategiske virkemidler og tiltak* blir identifisert. En rekke virkemidler og tiltak innenfor sikkerhetsområdet er identifisert, under planlegging eller allerede pågående. Samtidig er det ingen felles retning, eller samlet prioritering av disse tiltakene for sektoren. I *Prop. 65 L (2019–2020) Forslag til lov om e-helse (e-helseloven)* står det at digitalisering i en fragmentert sektor, hvor målet om sammenhengende tjenester står sentralt, utløser behov for tydelige rammebetingelser, felles mål og strategier. Dette er i høyeste grad gjeldende for området digital sikkerhet.

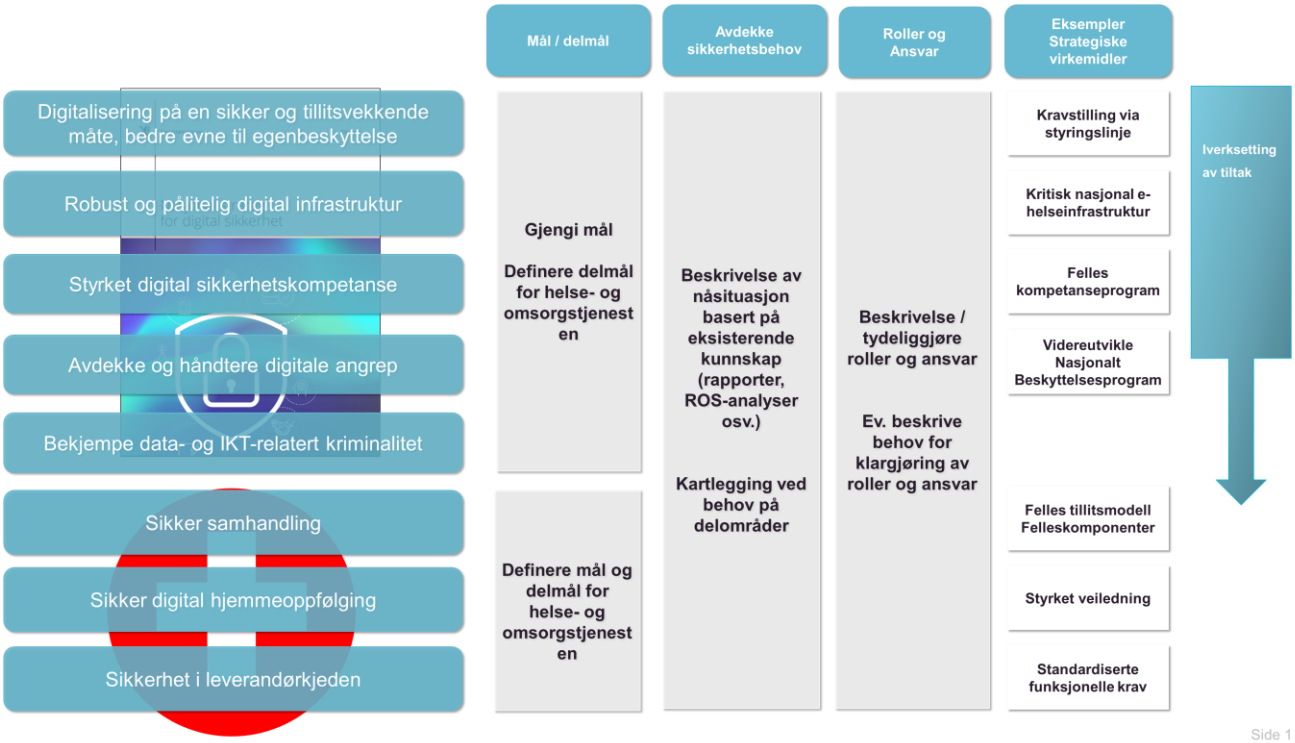
For at den fragmenterte helse- og omsorgssektoren skal kunne oppnå tilstrekkelig sikkerhet, er det med stor sannsynlighet behov for å iverksette større strategiske virkemidler og tiltak. Eksempler på dette er kompetanseløft, øvelser, standardiserte sikkerhetskrav, organisering av tilsyn, revisjon og sikkerhetstesting, leverandørgodkjenning etc. Det vil være nyttig med konkrete veiledere, retningslinjer og andre normerende virkemidler. Det bør også vurderes behov og mulighet for økonomiske virkemidler/insentiver.

3.3.2 Strategiens oppbygning og innhold

Regjeringen ville med den nasjonale strategien for digital sikkerhet oppnå et felles grunnlag for håndtering av digitale sikkerhetsutfordringer. Dette inkluderer store nasjonale tiltak, og strategiske virkemidler, for å angi en felles retning for sikkerhetsarbeidet i hele Norge. Ved å operasjonalisere målene i den nasjonale strategien, samt inkludere sektorens særtrekk og forutsetninger som beskrevet i denne rapporten, vil helsemyndighetene ha et godt verktøy for å kunne oppnå formålene skissert i kapittelet over.

Direktoratet for e-helse skisserer ikke endelige faste rammer for hvordan strategien skal se ut i denne rapporten. Det vurderes som hensiktsmessig at det arbeidet gjøres i forbindelse med utarbeidelsen av selve strategien. Figuren under er en visualisering av hvilke elementer som bør inngå i en ferdig strategi. De strategiske virkemidlene i figuren er kun eksempler.

Det pågår allerede mye viktig arbeid på sikkerhetsområdet i helse- og omsorgssektoren. Dette er blant annet knyttet opp mot målene fra den nasjonale strategien og oppfølging etter hendelser og revisjoner. Det er viktig at strategiarbeidet ikke skaper forsinkelser i implementering av viktige risikoreduserende tiltak. Det foreslås derfor å legge opp til en dynamisk prosess, med enkeltleveranser på områder hvor dette er hensiktsmessig underveis.



Figur 4: Visualisering av elementer i en strategi for digital sikkerhet i helse- og omsorgssektoren.

3.3.3 Strategi eller handlingsplan

Det har i løpet av prosessen blitt løftet spørsmål om det virkelig er behov for en strategi for digital sikkerhet i helse- og omsorgssektoren.[65] I tillegg har noen stilt spørsmål om det ville vært mer nyttig å lage en handlingsplan som operasjonaliserer Nasjonal strategi for digital sikkerhet basert på situasjonen i helse- og omsorgssektoren. En lite konkret strategi kan oppfattes som et unødvendig dokument som ikke brukes. Det kan også være en kompliserende faktor i sikkerhetsarbeidet, for eksempel for virksomheter som må holde seg til flere andre strategier.

Direktoratet for e-helse anbefaler likevel at det utarbeides en egen strategi for digital sikkerhet i helse- og omsorgssektoren, men anerkjenner at denne må være handlingsorientert, kort og poengtert. En strategi vil være bedre egnet til å berede grunnen for nye strategiske virkemidler i sektoren, samt å tydeliggjøre roller og ansvar. Videre er det viktig at digital sikkerhet løftes opp på strategisk nivå i sektoren, og da er det mye som tyder på at en strategi er et bedre egnet virkemiddel enn en handlingsplan. En strategi vil forankre ansvaret, og kommuniserer tydelig nasjonale myndigheters krav og prioriteringer på området. Den legger også i større grad til rette for å få på plass store strategiske virkemidler, enn en handlingsplan vil kunne gjøre alene.

Den nasjonale strategien inneholder en egen tiltaksoversikt. Der strategien er utarbeidet på et overordet nivå, er oversikten mer håndfast og har et kortere tidsperspektiv. Tiltaksoversikten inneholder konkrete tiltak innenfor alle de prioriterte områdene, og har noe «for alle», i tillegg til de store tiltakene enkelte virksomheter har ansvar for. Tiltakene vil også oppdateres etter hvert som situasjonsbildet endrer seg og nye tiltak blir relevante. En strategi for digital sikkerhet i helse- og omsorgssektoren bør også inneholde en egen tiltaksoversikt. Denne kan oppdateres hyppigere enn selve strategien, for å imøtekomme den raske utviklingen på området. Strategiske føringer og generelle tiltak kan gi effekt på tvers av hele sektoren. Samtidig kan mer spissede enkelttiltak, rettet mot visse kritiske virksomheter eller særskilte sårbarheter, være minst like viktige.

Samtidig må det avgjøres hvilke typer tiltak det skal fokuseres på, og hvordan disse skal utformes. De bør bygge på de anbefalte tiltakene i nasjonal strategi, men gjøres tilgjengelige og relevante for sektoren. I tillegg må det suppleres med tiltak innenfor områdene som er spesielt relevante for helse- og omsorgssektoren. Det bør legges til rette for at eksisterende og pågående tiltak som er initiert andre steder i sektoren inkluderes, for å samle trådene og slik skape en helhetlig og felles retning i arbeidet med digital sikkerhet i sektoren.

3.3.4 Målgruppe

En viktig del av utarbeidelsen av en strategi for digital sikkerhet i helse- og omsorgssektoren vil være å lande hvem som skal være målgruppe, og hvem som er sluttbrukerne. De signalene vi har fått inn gjennom de avholdte workshopene og møtene tilsier at strategien bør favne bredt.

Det komplekse aktørbildet i helse- og omsorgssektoren gjør det utfordrende å få til en nasjonal koordinering av digitaliseringen i sektoren. Denne utfordringen er ikke minst gjeldende på området digital sikkerhet. Selv med gode virkemidler som Normen, HelseCERT m.fl., forblir en rekke sikkerhetsutfordringer uløste i sektoren. Det er altså behov for å etablere en felles retning på arbeidet med digital sikkerhet, noe som tilsier at hele sektoren

[65] Dette ble løftet av deltakere i NUIT og i Nasjonalt e-helsestyre.

bør være omfattet av en strategi for digital sikkerhet i helse- og omsorgssektoren, og at sluttbrukerne bør være alt fra virksomhetsledere til den enkelte ansatte. Samtidig vil det være sentralt å få på plass tydelige roller og ansvar for de ulike målgruppene og sluttbrukerne. Dersom noen målgrupper får nye eller endrede roller eller oppgaver basert på dette arbeidet, må det legges ned en ekstra innsats i å nå disse.

Anbefalingen er at hele sektoren skal omfattes av strategien. Den vil nødvendigvis treffe ulike virksomheter ulikt. Mens noen får store nasjonale tiltak de er ansvarlig for å følge opp, gjelder dette på ingen måte alle. Det vil være ulikheter når det kommer til både tiltak og prioritering. Små og store virksomheter, og virksomheter med ulike ansvarsområder og ansvar, har nødvendigvis både ulik risiko og ulik risikoaksept. Sikkerhetsarbeidet i for eksempel RHF-ene vil naturlig nok får langt større betydning for helheten enn sikkerheten på et enkelt legekontor. Samtidig er det nettopp hos de små virksomhetene det ofte skorter på sikkerhetsarbeidet. En kjent utfordring for helsesektoren i flere land, er at små usikre virksomheter kan brukes som en vei inn for trusselaktørene. Sett fra den andre siden, vil sikre løsninger fra kompetente leverandører også i stor grad legge til rette for bedre sikkerhet hos de små virksomhetene.

3.3.5 Effektmål

En god strategi krever at det gjøres et grundig arbeid med å utarbeide konkrete mål for effekt. Det må tas stilling til hva situasjonen er i dag, og hva som er ønsket fremtidig situasjon. Dette er et arbeid som blir en vesentlig del av det videre strategiarbeidet. I arbeidet med å vurdere behovet for, og innretningen på, en strategi for digital sikkerhet i helse- og omsorgssektoren har også visjon og mål blitt diskutert og behandlet på et overordnet nivå.

En strategi for digital sikkerhet i helse- og omsorgssektoren bør danne et felles grunnlag for håndtering av digitale sikkerhetsutfordringer i hele sektoren, og samtidig understøtter de nasjonale og samfunnsmessige sikkerhetsinteressene.

Det er en forutsetning for digitalisering i helse- og omsorgssektoren at informasjonssikkerhet og personvern blir ivaretatt i alle faser av løsningenes livsløp. Innbyggerne skal ha tillit til at den enkeltes helseopplysninger behandles på en trygg og sikker måte. En strategi for digital sikkerhet skal bidra til å realisere de overordnede nasjonale målene for sektoren, for eksempel de som er som er satt i nasjonal e-helsestrategi,[66] og nasjonal helse- og sykehusplan.[67]

Målene fra den nasjonale strategien er gjeldende for hele samfunnet, og bør videreføres i en strategi for digital sikkerhet i helse- og omsorgssektoren. Det er imidlertid behov for å operasjonalisere disse i helse- og omsorgssektorens kontekst, samt potensielt supplere med mål som gjelder særskilt for sektoren.

En viktig del av arbeidet med en strategi er å utlede gode og målbare mål for strategiens effekt. På bakgrunn av målene bør det utledes krav, som ulike innretninger av strategi kan testes mot. Målene bør gjelde effekt for sektoren og befolkningen, mens kravene bør gjelde det løsningene må levere for at målene skal nås.

[66] Direktoratet for e-helse. 2019. *Nasjonal e-helsestrategi og handlingsplan 2017-2022 (oppdatert 2019).*
[67] Helse- og omsorgsdepartementet. 2019. *Nasjonal helse- og sykehusplan 2020 – 2023*. Meld. St. 7 (2019–2020).

3.3.6 Oppfølging av mål/krav/tiltak

En rekke aktører har etterlyst målinger/evalueringer/revisjoner, for dermed å sikre prioritet og etterlevelse i en sektor som fra før av har mange oppgaver som skal utføres med begrensede ressurser. Med økt samhandling øker også behovet for at den enkelte virksomhet kan være trygg på at samhandlende virksomheter etterlever lovkrav og nasjonale føringer.

Eksempler på hvordan krav og mål kan følges opp er alt fra egenevaluering/selvdeklarasjon til måling gjennom Nasjonal e-helsemonitor, eller tilsyn, revisjon og avviksrapportering (Helsetilsynet, Datatilsynet, Riksrevisjonen).

3.3.7 Formidling

Et av punktene som kom frem flere ganger i løpet av de avholde workshopene var behovet for god kommunikasjon av en strategi. For det første må språket være tydelig og enkelt, og ikke minst treffe målgruppen. Her kan det dras lærdom fra den nasjonale strategien der fokuset var på budskap og mål på et overordnet nivå som ikke var for detaljert og komplisert.

For det andre må en strategi for digital sikkerhet i helse- og omsorgssektoren kommuniseres ut til sektoren, slik at budskapet faktisk kommer frem til målgruppen. Det bør legges en kommunikasjonsplan som forteller hva som skal formidles, hvordan det skal formidles og hvilke målgrupper det skal fokuseres på.

For det tredje må det være tydelig at strategien skal forenkle arbeidet med digital sikkerhet og ikke være noe som kun kompliserer arbeidet

3.4 Innretning av arbeidet

For å sikre gjennomslag bør en strategi for digital sikkerhet i helse- og omsorgssektoren være forankret hos HOD.

3.4.1 Organisering av arbeidet

For å kunne gjennomføres effektivt og med høy kvalitet krever arbeidet med en strategi for digital sikkerhet i helse- og omsorgssektoren en formell organisering og tilstrekkelig avsatte ressurser. Arbeidet bør derfor organiseres som et prosjekt. Som det nasjonale fagorganet for e-helse er det naturlig at Direktoratet for e-helse leder prosjektet. Samtidig har NHN, som leverandør av helsenettet, helse- og omsorgssektorens nasjonale kompetansesenter for informasjonssikkerhet og eier av den operative funksjonen HelseCERT, en sentral posisjon innen arbeidet med digital sikkerhet i sektoren. Det er dermed viktig at NHN også har en helt sentral rolle i arbeidet.

Selve utarbeidelsen av en strategi for digital sikkerhet i helse- og omsorgssektoren bør gjennomføres i tett samarbeid med de berørte virksomhetene. Det anbefales derfor at det utpekes en sektorsammensatt styringsgruppe, som, i tillegg til Direktoratet for e-helse og NHN, inkluderer sentrale aktører fra både spesialist- og primærhelsetjenesten.

For å sikre forankring hos aktører som berøres av de ulike temaene bør behovet for referansegrupper også vurderes. Eksempelvis kan RHFene og KS innhente innspill fra henholdsvis HF og utvalgte kommuner, slik at arbeidet kan ha en bred involvering av sektoren, samtidig som det gjennomføres effektivt. Det bør også kartlegges hvorvidt det

eksisterer forskningsmiljøer med innsikt i de ulike temaene i strategien slik at disse eventuelt kan konsulteres.

3.4.2 Finansiering på kort og lengre sikt

Utarbeidelsen av en strategi for digital sikkerhet i helse- og omsorgssektoren vil kreve ressurser fra Direktoratet for e-helse og NHN. Det vil være aktuelt å hente inn ekstern bistand. Implementering og oppfølging av strategien vil også medføre ressursbehov. Dette er en langsiktig prosess, og tiltakene må derfor sees i både et kort- og et langsiktig perspektiv. For å sikre oppfølging av tiltakene må arbeidet knyttes opp mot prosesser for budsjettrammer og måloppnåelse i helse- og omsorgssektoren.

3.4.3 Forankring

HOD, Direktoratet for e-helse og NHN må ha et omforent budskap og en tydelig ambisjon for arbeidet med strategien. Det blir viktig å sørge for forankring underveis i de nasjonale utvalgene i Nasjonal styringsmodell for e-helse slik at dette blir en strategi for hele sektoren. Strategiprosessen bør også involvere andre relevante aktører på departementsnivå, særlig for å sørge for god koordinering opp mot Nasjonal strategi for digital sikkerhet og andre relevante strategier.

Innspillene vi har fått inn i arbeidet så langt viser at det er et stort behov for å forenkle og skape en tydelig retning på det digitale sikkerhetsarbeidet i sektoren. En strategi for digital sikkerhet i helse- og omsorgssektoren, og det bildet den tegner av utfordringene i sektoren, må være gjenkjennbar for målgruppene slik at løsningene på disse utfordringene oppleves som relevante og gjennomførbare. Dette stiller store krav til en oppdatert situasjonsforståelse, noe som betyr at selve utarbeidelsen bør innrettes slik at både sektoren og andre interessenter (eksempelvis relevante forskningsmiljøer og sentrale leverandører) blir involvert underveis i arbeidet. Bred involvering i strategiarbeidet vil i tillegg gi sluttbrukerne eierskap til strategien, som igjen vil bidra til implementering i sektoren.

Det er gjort et omfattende arbeid med å informere og involvere sektoren i arbeidet med å vurdere behovet for en strategi. Dette har vært viktig for å kunne gi en velbegrunnet anbefaling. Samtidig har det skapt forventninger om en arena for å gi innspill til selve strategien. Forankringen i sektor må derfor være mer formell enn den har vært i dette forarbeidet. Det kan for eksempel gjøres ved en jevn involvering av sektoren, sammen med innspillsrunder, eller formelle høringsrunder. Dette er tidkrevende, men kan gjøres per tema og parallelt med produksjon for å sikre kontinuerlig og effektiv fremdrift. Det kan også være nyttig å ha en sektorsammensatt styringsgruppe for arbeidet. Erfaringer som er delt fra arbeidet med Nasjonal strategi for digital sikkerhet understøtter viktigheten av at dette ivaretas i både planleggingen og gjennomføringen av arbeidet.

3.4.4 Kartlegging av status

Et godt situasjonsbilde, er også sentralt for å kunne lage en treffsikker strategi som faktisk bidrar til å løse utfordringene i sektoren, i stedet for å komplisere bildet ytterligere.

Vi har spurt deltakerne som har gitt innspill om de anser at det er nødvendig å gjennomføre et omfattende arbeid for å kartlegge nåsituasjon på sikkerhetsområdet i sektoren. Selv om mange har spilt inn at man vet for lite om sikkerhetstilstanden i egen virksomhet, så oppfatter vi at dette er knyttet til det ansvaret hver enkelt virksomhet har for å følge opp digital sikkerhet i egen virksomhet. Vi oppfatter det slik at man gjennom f.eks. Lysne-utvalgets

rapport, Meld. St. 38 (2016–2017) om IKT-sikkerhet — Et felles ansvar, Situasjonsbildet utgitt av NHN og andre rapporter som beskriver risiko og sårbarheter i sektoren, har en tilfredsstillende oversikt over situasjonen som utgangspunkt for et strategiarbeid.

Det kan være behov for noe videre kartlegging på enkeltområder. Et eksempel kan være kartlegging av kompetansebehov. Et annet eksempel er kommunesektoren, som selv har trukket frem behovet for en kartlegging i våre workshoper. Vi har imidlertid fått innspill om at Digitaliseringsdirektoratet allerede har fått i oppdrag å kartlegge sikkerhetstilstanden i kommunal sektor. Det vil være viktig å inkorporere funnen fra denne kartleggingen i arbeidet.

4 Anbefaling

Direktoratet for e-helse anbefaler at det utarbeides en egen strategi for digital sikkerhet i helse- og omsorgssektoren.

Det er behov for en egen strategi for digital sikkerhet for helse- og omsorgssektoren som er konkret og handlingsrettet. En slik strategi bør bygge videre på Nasjonal strategi for digital sikkerhet, og målene i denne, men tilpasses og utdypes i tråd med sektorens særtrekk og behov. En strategi for digital sikkerhet i helse- og omsorgssektoren må også være fremtidsrettet, og ikke fokusere kun på dagens behov. Det er viktig med bred involvering av sektoren og andre interessenter i utformingen av en strategi, slik at sektoren oppnår et felles og styrket grunnlag for håndtering av sikkerhetsutfordringer.

En strategi for digital sikkerhet i helse- og omsorgssektoren bør dekke hele sektoren, og sette en tydelig retning fra nasjonale myndigheter, samtidig som den forenkler sikkerhetsarbeidet for den enkelte virksomhet. For å oppnå en ønsket effekt bør den også inneholde konkrete mål og reelle strategiske virkemidler. En vesentlig del av strategien må være beskrivelse av nye virkemidler på nasjonalt nivå. Selv om hver enkelt virksomhet har ansvaret for digital sikkerhet i egen virksomhet, er det viktig at virksomhetene får støtte gjennom nasjonale tiltak.

I workshopene og møtene som har blitt gjennomført som en del av dette arbeidet, har interessenter i sektoren løftet en rekke relevante sikkerhetsutfordringer og innspill til hva som bør være formålet med en strategi for digital sikkerhet i helse- og omsorgssektoren. Tilbakemeldingene tyder på at disse formålene er viktige for hva som skal oppnås med en strategi, uavhengig av tema:

- Tydeliggjøre sikkerhetsbehov
- Tydeliggjøre roller og ansvar
- Identifisere relevante strategiske virkemidler og tiltak.

Arbeidet med en strategi for digital sikkerhet i helse- og omsorgssektoren bør ha en formell organisering og tilstrekkelig avsatte ressurser. Som det nasjonale fagorganet for e-helse er det naturlig at Direktoratet for e-helse leder prosjektet. Samtidig må NHN, som leverandør av Helsenettet, og funksjon som helse- og omsorgssektorens nasjonale kompetansesenter for informasjonssikkerhet også ha en helt sentral rolle i arbeidet. Selve utarbeidelsen bør gjennomføres i tett samarbeid med aktørene som blir berørt av strategien.

VEDLEGG

Vedlegg 1 Gjennomførte møter

Arbeidsgruppen har innhentet innspill og informert om arbeidet løpende med bred deltakelse i arrangerte workshoper og møter. Under vises en oversikt over involveringsaktivitetene.

Åpne workshoper:

- Workshop 1: Innledende innspill og involvering av sektor (10.06.20)
- Workshop 2: Nåsituasjonen og ønsket fremtidig situasjon (23.06.20)
- Workshop 3: Webinar med kommuner. Utfordringsbildet, temaområder og innretning (25.08.20)
- Workshop 4: Temaområder og innretning (10.09.20)

Representasjon i workshoper:

- Direktoratet for e-helse
- Helsedirektoratet
- Norsk Helsenett SF (NHN)
- Leverandører innen IT, EPJ og medisinsk utstyr
- Fagforeninger/interesseorganisasjoner
- Kommuner, KS, KiNS og KommuneCSIRT
- RHF og regionale IT-driftsselskaper

Orientering til og innspill fra interessenter:

- KS – Fagrådet for informasjonssikkerhet og personvern (09.06.20)
- NUFA (26.08.20)
- Justis- og beredskapsdepartementet (JD) (31.08.20)
- NUIT (09.09.20)
- Helsetilsynet (10.09.20)
- Nasjonal sikkerhetsmyndighet (NSM) (11.09.20)
- Datatilsynet (16.09.20)
- Nasjonalt e-helsestyre (17.09.20)

Vedlegg 2 Relevante regulatoriske føringer

Behovet for å beskytte helseopplysninger og pasientsikkerheten er hjemlet i nasjonal lovgivning. For sektoren spesifikt henvises det til både Helsepersonelloven,[68] Helse- og omsorgstjenesteloven,[69] Pasient- og brukerrettighetsloven,[70] Spesialisthelsetjenesteloven, [71] Helseregisterloven[72] samt en rekke andre reguleringer med krav til sikkerhet. Under har vi kort beskrevet noen av de relevante regulatoriske føringene på nasjonalt nivå.

Personvernforordningen (GDPR)

EUs personvernforordning (EU) 2016/679 av 27. april 2016 (Personvernforordningen),[73] ble implementert i Norge som lov ved ny personopplysningslov i 2018. Forordning handler om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger. Datatilsynet fører tilsyn med virksomheter etter personopplysningsloven. Dette gjelder også virksomheter i helse- og omsorgssektoren, som er en sektor hvor det oppbevares og behandles svært mye personopplysninger.

Ny personopplysningslov førte i 2018 også til enkelte endringer og tilpasninger i helselovgivningen. Personvernforordningen ga noen nye føringer for den registrertes rettigheter og virksomhetenes plikter ved behandling av helse- og personopplysninger. Disse endringene ble tatt med inn i Normen 5.3 i 2018 og senere i Normen 6.0, som er gjeldende fra 5. februar 2020.

Sikkerhetsloven

Ny sikkerhetslov[74] trådte i kraft 01.01.2019. Loven erstatter tidligere lov om forebyggende sikkerhetstjeneste. Bakgrunnen for ny sikkerhetslov er at samfunnet og virkelighetsbildet innen sikkerhet har gjennomgått store endringer de siste to tiårene. Den raske teknologiske utviklingen medførte et behov for å revidere og modernisere loven for å gjøre den mer dynamisk gjennom en risikobasert tilnærming og utforming av funksjonelle krav.

Ny sikkerhetslov er innrettet med sikte på å beskytte viktige samfunnsfunksjoner som skal ivareta og understøtte de nasjonale sikkerhetsinteressene. Disse funksjonene er i kalt grunnleggende nasjonale funksjoner (GNF). Gjennom den legaldefinisjonen som begrepet nasjonale sikkerhetsinteresser er gitt i ny lov, samt at begrepet vitale er utelatt foran nasjonale sikkerhetsinteresser, er ny lov gitt et utvidet virkeområde sammenlignet med den tidligere loven. Den omfatter nå også informasjon og informasjonssystemer som er skjermingsverdige pga. integritet eller tilgjengelighet, samt infrastruktur (som er en helt ny verdi) og aktivitet som understøtter GNFer. Dette skal bidra til en mer helhetlig tilnærming til sikkerhetsarbeidet på tvers av sektorer, men det fører også til at flere virksomheter kan bli omfattet av loven enn tidligere.

Loven gjelder for alle statlige, fylkeskommunale og kommunale organer. For private virksomheter og statsforetak som ikke er forvaltningsorganer, er det nå det enkelte fagdepartement som vedtar om loven skal gjelde helt eller delvis for virksomheten. Vilkår for at en slik virksomhet underlegges loven er at den enten behandler sikkerhetsgradert

[68] Lov om helsepersonell mv. (helsepersonelloven)
[69] Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven)
[70] Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven)
[71] Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven)
[72] Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
[73] Lov om behandling av personopplysninger (personopplysningsloven)
[74] Lov om nasjonal sikkerhet (sikkerhetsloven)

informasjon eller driver aktivitet, eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur, som har avgjørende betydning for grunnleggende nasjonale funksjoner.

Det er per dags dato vanskelig å si noe definitivt om hvordan ny sikkerhetslov vil påvirke helse- og omsorgssektoren. Basert på hva som har kommet frem i tidligere arbeid på dette området, blant annet DSBs arbeid med å kartlegge kritiske samfunnsfunksjoner, er det imidlertid naturlig å anta at i hvert fall deler av helse- og omsorgssektoren vil bli omfattet av ny sikkerhetslov. Dette gjelder særlig i lys av utvidelsen i loven til å omfatte informasjon og informasjonssystemer som er skjermingsverdige pga. integritet eller tilgjengelighet, samt at det allerede er identifisert GNFer i sektoren som kan føre til at mange virksomheter blir underlagt loven.

NIS-direktivet

NIS-direktivet er Europaparlamentets og Rådets direktiv (EU) 2016/1148 av 6. juli 2016 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU[75] Direktivet ble vedtatt i EU 6. juli 2016. Det skal sikre et høyt felles sikkerhetsnivå i viktige nettverks- og informasjonssystemer.[76] Det pålegger medlemsstatene å sørge for at visse virksomheter iverksetter flere sikkerhetstiltak. Disse omtales som «operatører av essensielle tjenester», hvilket innebærer at bortfall av disse kan få alvorlige negative konsekvenser for samfunnssikkerheten, samt økonomiske og samfunnsmessige aktiviteter[77].

JD foreslår å implementere kravene i direktivets punkt 2 i form av en ny lov om nettverk- og informasjonssystemsikkerhet. Loven skal forplikte virksomheter som har en særlig viktig rolle i opprettholdelsen av et funksjonelt indre marked til å gjennomføre IKT-sikkerhetstiltak og varsle om alvorlige hendelser. Den nye loven vil gjelde for virksomheter som er:

- tilbydere av samfunnsviktige tjenester innenfor sektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur
- tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.

75 Justis- og beredskapsdepartementet. 2016. *NIS-direktivet – Posisjonsnotat*.

76 Justis- og beredskapsdepartementet. 2018. *Høring – NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*.

77 Justis- og beredskapsdepartementet. 2016. *NIS-direktivet – Posisjonsnotat*.

Vedlegg 3 Referanseliste

Collier, Kevin (CNN). 2019. *"Hundreds of dental offices crippled by ransomware attack"*. Link til innhold.

Datatilsynet. 2013. *Personvernutfordringer ved genetiske undersøkelser*. Link til innhold.

Digi. 2020. «*Kvinne døde etter løsepengevirus-angrep*». Link til innhold.

Digitaliseringsdirektoratet. *Oversikt over nasjonale fellesløsninger*. Link til innhold.

Direktoratet for e-helse. 2020. *Nasjonal e-helsemonitor*. Link til innhold.

Direktoratet for e-helse. 2020. *Normen*. Link til innhold.

Direktoratet for e-helse. 2020. *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger*. Link til innhold.

Direktoratet for e-helse. 2019. *Anbefaling av tillitsmodell for data- og dokumentdeling*. Link til innhold.

Direktoratet for e-helse. 2019. *Nasjonal e-helsestrategi og handlingsplan 2017-2022 (oppdatert 2019)*. Link til innhold.

Direktoratet for e-helse. 2019. *Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren*. Link til innhold.

Direktoratet for e-helse. 2019. *Plan for utvikling av felles grunnmur for digitale tjenester i helse- og omsorgstjenesten*. Link til innhold.

Direktoratet for e-helse. 2019. *Utredning om bruk av kunstig intelligens i helsesektoren*. Link til innhold.

Direktoratet for samfunnssikkerhet og beredskap. 2020. *Risikostyring i digitale verdikjeder*. Link til innhold.

Direktoratet for samfunnssikkerhet og beredskap. 2016. *Samfunnets kritiske funksjoner*. Link til innhold.

Direktoratet for samfunnssikkerhet og beredskap. 2014. *Risikoanalyse av cyberangrep mot ekom-infrastruktur*. Link til innhold.

Helse- og omsorgsdepartementet. 2020. *Forslag til lov om e-helse (e-helseloven)*. Prop. 65 L (2019–2020). Link til innhold.

Helse- og omsorgsdepartementet. 2019. *Nasjonal helse- og sykehusplan 2020 – 2023*. Meld. St. 7 (2019–2020). Link til innhold.

Helse- og omsorgsdepartementet. 2012. *Én innbygger – én journal*. Meld. St. 9 (2012–2013). Link til innhold.

HelseCERT. 2018. *Situasjonsbilde 2018*. Link til innhold.

Helsedirektoratet. 2019. *Overordnede risiko- og sårbarhetsvurderinger for nasjonal beredskap i helse- og omsorgssektoren 2019*. Link til innhold.

Independent Security Evaluators. 2016. *Securing Hospitals - A research study and blueprint*. Link til innhold.

Justis- og beredskapsdepartementet og Forsvarsdepartementet. 2020. *Nasjonal strategi for digital sikkerhet*. Link til innhold.

Justis- og beredskapsdepartementet. 2018. *IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet*. NOU 2018: 14. Link til innhold.

Justis- og beredskapsdepartementet. 2018. *Høring – NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*. Link til innhold.

Justis- og beredskapsdepartementet. 2017. *IKT-sikkerhet — Et felles ansvar*. Meld. St. 38 (2016–2017). Link til innhold.

Justis- og beredskapsdepartementet. 2016. *NIS-direktivet – Posisjonsnotat*. Link til innhold.

Justis- og beredskapsdepartementet. 2015. *Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden*. NOU 2015: 13. Link til innhold.

KS. 2020. *KOMP-iS-filmene*. Link til innhold.

Nasjonal Sikkerhetsmyndighet. 2020. *Grunnprinsipper for IKT-sikkerhet 2.0*. Link til innhold.

Nasjonal Sikkerhetsmyndighet. 2020. *Helhetlig digitalt risikobilde 2020*. Link til innhold.

Nasjonal Sikkerhetsmyndighet. 2020. *Risiko 2020*. Link til innhold.

Nasjonal Sikkerhetsmyndighet. 2017. *Rammeverk for håndtering av IKT-hendelser*. Link til innhold.

Newman, Lily Hay (Wired). 2020. “*A Ransomware Attack Has Struck a Major US Hospital Chain”*. Link til innhold.

Norges vassdrags- og energidirektorat. 2020. *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen*. Link til innhold.

Norsk Helsenett. 2019. *Årsrapport 2019*. Link til innhold.

Norsk Helsenett. *Elektronisk meldingsutveksling (EDI)*. Link til innhold.

Politiets sikkerhetstjeneste. 2020. *Nasjonal trusselvurdering 2020*. Link til innhold.

Sundhedsdatastyrelsen. 2018. *Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022*. Link til innhold.

Trumpy, Jens Hugo. 2002. «Bør pasientene automatisk få kopi av sin epikrise?» *Tidsskrift for Den norske legeforening*, 122: 394-6. Link til innhold.