Direktoratet for e-helse

TB2023-09

Digital sikkerhet – anbefaling til prioriterte tiltak

Oppfølging av Direktoratets innspill til den kommende helseberedskapsmeldingen

IE-1125

Publikasjonens tittel:
Digital sikkerhet – anbefaling til prioriterte tiltak
Rapportnummer
IE-1125

Utgitt:
14.06.2023

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

Innhold

Sammendrag

Dette dokumentet er svar på oppdrag til Direktoratet for e-helse i tildelingsbrev for 2023. Direktoratet bes om å følge opp mål og innsatsområder fra sitt innspill til den kommende helseberedskapsmeldingen og anbefale hvilke tiltak som skal prioriteres.

Innspillet til stortingsmeldingen ble oversendt HOD 14. oktober 2022. I innspillet beskriver direktoratet en rekke aktiviteter, tiltak og annet arbeid som representerer bredden av det som gjøres i sektoren innen digital sikkerhet i dag. Videre gis en grundig beskrivelse av utfordringsbildet innen digital sikkerhet i helse- og omsorgssektoren. Til sist beskrives seks innsatsområder med 21 tilhørende tiltak som Direktoratet mener er egnet til å løfte den digitale sikkerheten i helse- og omsorgssektoren.

Vurderingene fra innspillet i 2022 er supplert med nye momenter, hovedsakelig en oppdatert omtale av risikotrender.

Direktoratet for e-helse anbefaler at følgende innsatsområder og tiltak prioriteres:

Innsatsområder som alle bør prioriteres høyt, og igangsettes raskt:

- Planverk og øvelser
- Ny teknologi og digitale verdikjeder
- Videreutvikling av eksisterende nasjonale virkemidler

Et nytt, viktig innsatsområde som bør settes høyere på dagsorden i sektoren grunnet utfordringsbildet vi står overfor

- Robust infrastruktur i helse- og omsorgssektoren

Enkelttiltak som direktoratet mener er viktige og som bør prioriteres høyt, men hvor innretningen må vurderes nærmere (se kapittel 3)

- Kartlegging av øvrige innsatsområder (Sikkerhetskultur og kompetanse, etterlevelse og oppfølging, samt støtte til mindre virksomheter)
- Stille forventninger til sektoren
- Utvikle målindikatorer

Realisering av innsatsområder og tiltak vil kreve en kombinasjon av sentrale tiltak og aktiviteter i hver enkelt virksomhet i sektoren.

1 Innledning

Direktoratet for e-helse har fått følgende oppdrag i tildelingsbrevet for 2023 (TB 2023-09): «Direktoratet skal følge opp mål og innsatsområder fra sitt innspill til den kommende helseberedskapsmeldingen og anbefale hvilke tiltak som skal prioriteres, jf. også melding om helseberedskap som kan gi føringer for arbeidet med digital sikkerhet i helse- og omsorgssektoren.»

Dette dokumentet besvarer oppdraget. Dokumentet inneholder våre faglige anbefalinger til tiltak som bør gjennomføres sentralt og i den enkelte virksomhet. Anbefalingene danner grunnlag for fremtidige beslutninger på området digital sikkerhet.

1.1 Om Direktoratets innspill til den kommende helseberedskapsmeldingen med tema digital sikkerhet

Direktoratets innspill til den kommende helseberedskapsmeldingen ble oversendt Helse- og omsorgsdepartementet (HOD) 14. oktober 2022.[1] Innspillet tok utgangspunkt i det påbegynte arbeidet med en strategi for digital sikkerhet i helse- og omsorgssektoren. Utarbeidelse av strategien var et oppdrag i tildelingsbrevet for 2021 til direktoratet, i samarbeid med Helsedirektoratet, Helsetilsynet, Norsk helsenett SF (NHN), de regionale helseforetakene og kommunesektoren/KS. Departementet endret dette oppdraget gjennom tillegg til tildelingsbrev nr. 5 av 16. mai 2022. For å få mest oppmerksomhet og rask utvikling på området, og for å minske antall dokumenter å forholde seg til, vurderte departementet det som hensiktsmessig å innarbeide strategi for digital sikkerhet i helse- og omsorgssektoren i den kommende stortingsmeldingen om helseberedskap.

I innspillet til stortingsmelding beskriver direktoratet en rekke aktiviteter, tiltak og annet arbeid som representerer bredden av det som gjøres i sektoren innen digital sikkerhet i dag. Videre gis en grundig beskrivelse av utfordringsbildet innen digital sikkerhet i helse- og omsorgssektoren (innspillets kapittel 3). Oppsummert mener Direktoratet for e-helse at dette er de viktigste utfordringene for helse- og omsorgssektoren i arbeidet med digital sikkerhet:

- Sektoren står overfor et skjerpet digitalt trusselbilde.
- Et komplekst systemlandskap og mangelfull implementering av grunnleggende sikkerhetstiltak.
- Udekket kompetansebehov.
- Varierende oppfølging av digital sikkerhet i verdikjeder.
- Teknologiskifter og nye samhandlingsformer og leveransemodeller for helsehjelp.
- Uklare roller og ansvar med betydning for digital sikkerhet.

På bakgrunn av utfordringene sektoren står overfor, beskriver innspillet videre forslag til mål, innsatsområder og tiltak for sektoren[2]. Det er disse innsatsområdene og tiltakene Direktoratet

[1] Direktoratet for e-helse sitt innspill til kommende stortingsmelding om helseberedskap. Tema: Digital sikkerhet.
[2] Innspillet besvarer følgende av utredningsinstruksens hovedspørsmål: Hva er problemet, hva skal oppnås, og hvilke tiltak er relevante.

for e-helse prioriterer blant i dette dokumentet. Mål, innsatsområder og tiltak fra innspillet beskrives nærmere i det følgende:

1.1.1 Mål for digital sikkerhet og beredskap i helse- og omsorgssektoren

Alle virksomheter i helse- og omsorgssektoren må øke sin digitale sikkerhet, forebygge digitale hendelser og være forberedt på å håndtere digitale sikkerhetshendelser i tillegg til å sikre fortsatt forsvarlig leveranse av helse- og omsorgstjenester, dersom slike hendelser oppstår. Arbeidet med digital sikkerhet i sektoren må understøtte sektorens kjernevirksomhet. Dette inkluderer forsvarlig helsehjelp, evne til å beskytte befolkningens helse og forebygge sykdom og skade ved å sørge for smittevern, miljørettet helsevern, trygt drikkevann og strålevern, og helseberedskap. Digital sikkerhet er også en forutsetning for å lykkes med andre av sektorens oppgaver, som forskning. Sektoren må være i stand til å tilpasse seg teknologi, trusler og sårbarheter i kontinuerlig endring. Med bakgrunn i utfordringene som sektoren står overfor foreslås følgende mål for arbeidet med digital sikkerhet. Disse adresserer felles og vedvarende utfordringer for sektoren, i tillegg til grunnleggende forutsetninger for å lykkes med sikker digitalisering.

- Virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder.
- Ansvar og roller med betydning for digital sikkerhet i og mellom sektorens virksomheter er avklart, kjent og ivaretatt.
- Sektoren ivaretar sikkerhet i lange og komplekse digitale verdikjeder.
- Det er høy tillit fra innbyggere og pasienter til hvordan sektoren ivaretar digital sikkerhet.
- Virksomhetene evner å effektivt ta i bruk nye teknologier på en sikker måte og er robuste i møte med et risikobilde i endring.
- Virksomhetene i sektoren har høy bevissthet om sårbarheter og trusler, og er forberedt og øvet på å avdekke og effektivt håndtere ekstraordinære IKT-hendelser.

Målene er grundigere beskrevet i Vedlegg B.

1.1.2 Innsatsområder og tiltak

I sitt innspill (kapittel 5) foreslo Direktoratet for e-helse seks satsningsområder innen digital sikkerhet:

- Videreutvikling av eksisterende nasjonale virkemidler
- Kompetanse og sikkerhetskultur
- Planverk og øvelser
- Etterlevelse og oppfølging
- Ny teknologi og digitale verdikjeder
- Støtte til mindre virksomheter

Innsatsområdene gjelder både forebygging og håndtering av uønskede digitale hendelser og adresserer de områdene der sektoren har felles og vedvarende utfordringer og behov. Innsatsområdene fokuserer på at virkemidler og tiltak som fungerer godt i dag må

videreføres og styrkes, samtidig som det trengs nye tiltak på områder der sektoren har et potensial for forbedring og utvikling. Innsatsområdene skal bidra til at sektoren beveger seg mot måloppnåelse.

I tilknytning til innsatsområdene nevnt over det blitt identifisert til sammen 21 tiltak. Tiltakene er av forskjellig art, og omfatter to hovedkategorier av tiltak: Den første er konkrete aktiviteter som f.eks. kartlegging, utredning, etablering av samarbeidsarenaer og utvikling av planverk. Den andre er krav og forventninger som bør stilles til sektoren. Tiltakene er nærmere beskrevet i Vedlegg A og listet opp i vedlegg C.

1.2 Leseveiledning

Dette dokumentet er strukturert på følgende måte: Kapittel 2 beskriver risikotrender som har blitt påpekt av sentrale aktører siden innspillet til helseberedskapsmeldingen ble overlevert departementet, samt foreslåtte endringer i lovverk som er relevante for prioriteringen. Kapittel 3 beskriver resultatet av prioriteringen som er gjort, samt grunnlaget for prioriteringen.

Lesere som ønsker å gå grundigere inn i underlagene for prioriteringene, finner disse i vedleggene. Vedlegg A beskriver tiltakene i mer detalj, inkludert en grov tidsplan for realisering, og en vurdering av kostnad ved tiltakene, risiko ved gjennomføring, og bidrag til risikotrendene som er identifisert knyttet til digital sikkerhet. Vedlegg B gir en vurdering av hvordan innsatsområdene bidrar til å nå målene i innspillet til helseberedskapsmeldingen, samt målene i e-helsestrategien. Vedlegg C lister alle tiltak. Vedlegget gir videre en detaljert oversikt over hvordan tiltakene, slik de omtales i dette dokumentet, er relatert til de konkrete formuleringene i direktoratets innspill til den kommende helseberedskapsmeldingen. I dette dokumentet er tiltakene formulert mer kortfattet for å gjøre tabellariske og grafiske fremstillinger enklere.

I forbindelse med revidert statsbudsjett 11.05.23 ble det kjent at Regjeringen gjennomfører endringer i organisering, roller og ansvar i den sentrale helseforvaltningen. Det tas sikte på at endringene settes i verk 1. januar 2024. Myndighetsoppgavene innen digitaliseringsområdet skal styrkes og kobles tettere til tjenesteutviklingen. Direktoratet for e-helse og Helsedirektoratet slås derfor sammen. I teksten videre refereres det til Direktoratet for e-helse bl.a. som mulig tiltakseier for en del tiltak. I lys av endringen må dette forstås som at rollen vil videreføres i det sammenslåtte Direktoratet for e-helse og Helsedirektoratet. Denne organisasjonen vil ivareta myndighetsoppgavene på digitaliseringsområdet i sektoren, også på området digital sikkerhet.

2 Nye momenter

Kapitlet beskriver viktige risikotrender og foreslåtte endringer i lovverk som er relevant for prioriteringen av tiltak.

2.1 Oppdaterte risikotrender

Risikobildet sektoren møter er i stadig utvikling. Vi har derfor supplert utfordringsbildet omtalt over med oppdatert kunnskap om viktige risikotrender. Vår vurdering av risikotrendene bygger på følgende rapporter:

- ENISAs rapport "*Identifying emerging cyber security threats and challenges for 2030*".[3]
- NSMs rapport "*Risiko 2023*".[4]
- De regionale helseforetakenes rapport "*Trusselvurdering 2022*».[5]
- NSMs rapport «*Sikkerhetsfaglig råd. Et motstandsdyktig Norge*» (2023).[6]

De risikotrendene vi anser som viktigst i prioriteringen er følgende:

- **Sårbarheter i leverandørkjeder:** Både NSM og ENISA fremhever sårbarheten i leverandørkjeder som en fremtredende risiko, eksempelvis at programvarekomponenter som benyttes av mange inneholder bakdører som kan utnyttes av angripere. Leverandørkjeder kan være lange og uoversiktlige, og kan omfatte aktører med mangelfull sikkerhet.
- **Komplekst digitalt økosystem med et stort antall systemer, inkludert gamle systemer:** ENISA peker på at en økning i antall smarte enheter (IoT – Internet of Things) vil gjøre det vanskeligere å ha nødvendig oversikt og håndtere sikkerheten i alle enhetene i økosystemet. Mangfoldet i enheter blir stort, og vil inkludere mobile enheter som eies av private og gamle systemer som er vanskelige å oppdatere. Risikoen dette innebærer forsterkes av at programvaresårbarheter utnyttes raskere enn før, noe som påpekes av NSM.
- **Mer data og bedre verktøy gjør det lettere å lykkes med målrettede angrep:** Både NSM og ENISA peker på at med større tilgang til personlige data fra ulike enheter, og med bedre verktøy (for eksempel basert på kunstig intelligens), blir det lettere for angripere å gjennomføre målrettede angrep rettet mot enkeltpersoner og virksomheter. Dette kan åpne for at det blir lettere å lykkes med for eksempel målrettede utpressingsangrep (eks. kryptovirus).
- **Avanserte sammensatte/hybride trusler:** Både NSM og ENISA forventer at digitale angrep blir mer sofistikerte og i større grad vil kombineres med fysiske eller offline angrep. NSM peker på at krigen i Ukraina har økt bekymringen for sikkerheten i de europeiske landene, og at vi må være forberedt på "et bredt spekter av trusler som i dag er vanskelig å forutse". Dermed blir robuste systemer stadig viktigere.
- **Mangel på kompetanse:** ENISA peker på mangel på kompetanse innen digital sikkerhet, og at dette vil bidra til sikkerhetshendelser. Dette gjelder kunnskap om sikkerhet knyttet til ny teknologi (smarte enheter, kunstig intelligens, rombasert infrastruktur og kvantedatamaskiner), men også om hvordan sikre gamle systemer.

Disse utfordringene og risikotrendene fremhever viktigheten av å jobbe systematisk med digital sikkerhet på alle nivåer – teknisk, organisatorisk og på individnivå. Vi trenger tiltak

[3] "Identifying emerging cyber security threats and challenges for 2030.", ENISA
[4] "Risiko 2023." Nasjonal sikkerhetsmyndighet.
[5] Rapporten er unntatt offentlighet.
[6] "Sikkerhetsfaglig råd - Et motstandsdyktig Norge.", Nasjonal sikkerhetsmyndighet.

som er med på å redusere sårbarheten for angrep. Samtidig vil man i nåværende og fremtidig risikobilde måtte forvente at sektoren vil oppleve digitale angrep med ulik alvorlighetsgrad. Derfor er det også helt nødvendig med tiltak som sikrer at sektor har evne til å håndtere angrep, opprettholde helse- og omsorgstjenester under angrep, og sikre effektiv gjenoppretting.

Helse- og omsorgssektoren er ikke ensartet. Deler av sektoren, spesielt knyttet til de nasjonale tjenestene og spesialisthelsetjenesten, har god kompetanse på digital sikkerhet og evne til å jobbe systematisk både med forebygging og håndtering. Andre deler av sektoren, spesielt de mindre virksomhetene, har mindre kompetanse og evne innen digital sikkerhet. De virksomhetene med størst grad av egen evne og kompetanse, er samtidig ofte i en posisjon der alvorlige digitale hendelser vil kunne gi store konsekvenser for samfunnet. Derfor kan det være viktig med tiltak som støtter disse virksomhetene, selv om de har egenevne til både å beskytte seg og å håndtere hendelser. Merk imidlertid at selv om uønskede digitale hendelser hos mindre virksomheter vil ha lavere konsekvenser for samfunnet, så kan konsekvensene være vesentlige, spesielt om flere mindre virksomheter blir rammet. Med økende grad av sammenkobling og samhandling er det også en betydelig risiko at mindre virksomheter kan bli en angrepsvei inn mot større virksomheter og nasjonale løsninger.

Merk at utfordringene direktoratet beskrev i innspillet til den kommende helseberedskapsmeldingen (se kapittel 1.1) og disse risikotrendene i stor grad er overlappende.

2.2 Forslag til lov om digital sikkerhet

Justis- og beredskapsdepartementet har foreslått i Prop.109 LS (2022-2023) en ny lov om digital sikkerhet (digitalsikkerhetsloven).[7] Proposisjonen foreslår en lov om digital sikkerhet og ber Stortinget om samtykke til godkjenning av to beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av NIS1-direktivet, tilhørende gjennomføringsforordning og cybersikkerhetsforordningen. Loven skal forplikte virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser.

Loven stiller overordnede krav til sikkerhet og varsling, og virkeområdet er kun angitt i form av hvilke sektorer den gjelder i. Dette forutsetter et underliggende regelverk med tydeligere avgrensinger og konkretiseringer. Loven inneholder derfor en vid adgang til å fastsette nærmere bestemmelser i forskrift. Loven etablerer rammeverk for tilsyn med virksomhetene og åpner for ileggelse av pålegg og eventuelt overtredelsesgebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige digitale hendelser.

2.2.1 Særlig om NIS2-direktivet

I november 2022 vedtok EU direktiv (EU) 2022/2555, et nytt direktiv som opphever NIS1 (NIS2-direktivet). Direktivet er foreløpig ikke tatt inn i EØS-avtalen. Direktivet får et utvidet virkeområde sammenlignet med NIS-direktivet. Utvidelsen innebærer at virkeområdet vil omfatte tilbydere av samfunnsviktige tjenester innen 15 definerte sektorer, herunder helse. Videre vil direktivet innføre et størrelsestak slik at alle mellomstore og store bedrifter i

[7] Prop.109 LS (2022-2023)

utvalgte sektorer omfattes av virkeområdet.[8]

NIS2-direktivet styrker sikkerhetskravene til tilbyderne med en minimumsliste over grunntiltak som må anvendes, og gir mer presise bestemmelser for varsling av hendelser. I tillegg adresseres sikkerheten i forsyningskjeder og leverandørforhold. Dersom NIS2 blir tatt inn i EØS-avtalen vil det medføre behov for endringer i lov om digital sikkerhet.

[8] For definisjoner av hvilke virksomheter faller inn under størrelsestaket, se Recommendation 2003/361/EC article 2.

3 Prioritering av innsatsområder og tiltak

Dette kapitlet inneholder direktoratets grunnlag for prioritering og anbefaling av hvilke innsatsområder og tiltak som bør prioriteres. Delkapitlene angir en prioritert rekkefølge på følgende måte:

Kapittel	Forklaring
3.2 Planverk og øvelser 3.3 Ny teknologi og digitale verdikjeder 3.4 Videreutvikling av eksisterende nasjonale virkemidler	Innsatsområder som alle bør prioriteres høyt, og igangsettes raskt. Dette er områder som utfyller hverandre, og som antakeligvis vil involvere ulike kompetansemiljøer i sektoren. De kan derfor gjennomføres i parallell.
3.5 Nytt innsatsområde: Robust infrastruktur i helse- og omsorgssektoren	Et viktig innsatsområde som bør settes høyere på dagsorden i sektoren grunnet utfordringsbildet vi står overfor. Området krever utredning av tiltak.
3.6 Kartlegging av øvrige innsatsområder 3.7 Stille forventninger til sektoren 3.8 Utvikle målindikatorer	Dette er enkelttiltak som direktoratet mener er viktige og som bør prioriteres høyt. Slutteffekten kan være mer usikker da realisering av innsatsområdet vil være avhengig av tiltak basert på kartlegging og utredning. Videre vil det være usikkerhet knyttet til oppfølging av forventninger som stilles til sektoren.

3.1 Grunnlag for prioritering

I vurderingen av hvilke innsatsområder og tiltak som skal prioriteres er det lagt vekt på følgende:

- Hvor godt innsatsområdet bidrar til å møte risikoer knyttet til digital sikkerhet. Her er det tatt utgangspunkt i den oppdaterte oversikten over risikotrender som finnes i kapittel 2. Dette er det viktigste i prioriteringen.
- Innsatsområder vil bli prioritert før enkelttiltak, siden et helt innsatsområde med en helhetlig samling tiltak mest sannsynlig vil ha størst påvirkning på slutteffekt.
- Tiltak som kommer først i en naturlig rekkefølge prioriteres. Tiltakene innenfor de seks innsatsområdene er av ulik art, som f.eks. kartlegging, utredning og kravstilling. I de fleste tilfeller henger tiltakene innen et innsatsområde sammen, og flere av tiltakene følger i en naturlig rekkefølge (f.eks. 'kartlegge' før 'utrede'). Både teknologisk utvikling og trusselbildet utvikler seg raskt, slik at det uansett vil være usikkerhet knyttet til hvilke tiltak som er riktig å velge framover i tid.[9]

For hvert tiltak er det videre gjort en vurdering av:

- Kost,

[9] Siden det er usikkerhet knyttet til hvilke tiltak som er riktig å prioritere på sikt, foreslår direktoratet at det her åpnes opp for en mer dynamisk gjennomføring, basert på risiko og målindikatorer. Det anbefales derfor at det utvikles målindikatorer innenfor hvert prioritert innsatsområde, se mer om dette i kapittel 3.8.

- antatt støtte i sektoren, og
- gjennomføringsrisiko.

Det er tatt hensyn til disse vurderingstemaene i prioriteringen. Se nærmere omtale i vedlegg A.

Videre er det for hver av innsatsområdene vurdert i hvor stor grad de vil ha en positiv effekt for måloppnåelsen for henholdsvis målene i kapittel 1.1.1 og de strategiske målene fra nasjonal e-helsestrategi. Se nærmere omtale i vedlegg B.

3.2 Prioriteres: Planverk og øvelser

Alle sektorens virksomheter må være forberedt på å håndtere digitale sikkerhetshendelser og sikre fortsatt forsvarlig leveranse av helsetjenester. Læring fra øvelser kan lede til forbedringer i sikkerhetstiltakene og en bedre risikoforståelse. Tiltak på området vil også bidra til klarere forståelse av roller og ansvar, bedre og mer sammenhengende planverk, bedre oversikt, og at virksomhetene er bedre forberedt gjennom øvelser – noe som øker håndteringsevnen.

Prioritering av dette området svarer på utfordringer påpekt av NSM knyttet til at Norge har utilstrekkelig håndteringsevne ved store cyberhendelser, og at det er behov for utvikling av krisescenarier, handlingsalternativer og forberedte tiltak så man er klar til å reagere raskt når hendelser og kriser inntreffer. NSM peker også på «en klar sammenheng mellom situasjonsforståelse og responsevne.»[10] Som vist i Vedlegg A så har vi vurdert dette innsatsområdet til å gi et vesentlig og bredt bidrag til å redusere risiko knyttet til digital sikkerhet i sektoren.

Det pågår allerede mye arbeid på dette området, bl.a. gjennom oppdrag om gjennomføring av øvelser gitt til NHN og de regionale helseforetakene. Området er imidlertid så sentralt at det kreves ytterligere innsats.

Nærmere beskrivelse av tiltakene følger nedenfor.

Alle tiltakene innenfor innsatsområdet bør kunne startes opp i løpet av relativt kort tid. Helseberedskapsmeldingen med en påfølgende mulig revidering av nasjonal helseberedskapsplan vil kunne sette føringer for innretning på nasjonalt beredskapsplanverk på IKT-området.

3.2.1 IKT-beredskap i nasjonale styringsdokumenter, støttet av gode og oppdaterte oversikter

- Utarbeide overordnet nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan. Denne vil danne et likt og generisk plangrunnlag regionalt og lokalt med tydelig ansvars- og varslingslinjer i håndtering av IKT-sikkerhetshendelser i sektoren, samt i samvirke med andre sektorer. Tiltaket bør følges opp med en forventning til sektor om at planverk på ulike nivåer i sektoren må være omforent og bygge på overordnet nasjonalt planverk, felles begrepsbruk og forståelse.
- Etablere og vedlikeholde kart over myndighetsroller, systemeierskap og leverandører til bruk i beredskapsarbeidet.

[10] *«Sikkerhetsfaglig råd – Et motstandsdyktig Norge», 2023*. Nasjonal sikkerhetsmyndighet.

- Etablere og vedlikeholde en nasjonal oversikt over all kritisk infrastruktur i helse- og omsorgssektoren.

Kost, antatt støtte i sektoren, samt risiko i gjennomføring er vurdert for tiltakene. Kost for tiltakene vurderes som lav til middels. Basert på bl.a. høringen som ble gjennomført høsten 2022 antas det at tiltakene vil ha høy støtte i sektoren. Tiltakene som gjelder planverk vil ha middels gjennomføringsrisiko, mens tiltakene som gjelder oversikter ha hhv. middels til høy og høy risiko i gjennomføring grunnet kompleksiteten.

Tiltakseier for disse tiltakene bør utpekes av HOD. Tiltakene vil omfatte alle aktører som har roller innen beredskap i helse- og omsorgssektoren.

3.2.2 Øvelser

- Etablere en overordnet strategi eller rammeplan for øvelser som omfatter digital sikkerhet i helse- og omsorgssektoren, med tydelige forventninger til systematisk arbeid med øvelser på nasjonalt og regionalt nivå, samt i hver enkelt virksomhet.

Kost for tiltaket vurderes som middels. Vi antar at tiltaket vil ha middels støtte i sektoren, siden det vil kreve at det prioriteres ressurser til øvelser. Gjennomføringsrisiko vil være middels til høy siden tiltaket vil kreve mye koordinering og involvere mange aktører.

Tiltakseier på nasjonalt nivå bør utpekes av HOD. Tiltaket vil omfatte alle aktører som har roller innen beredskap i helse- og omsorgssektoren, og alle sektorens virksomheter som vil ha nytte av øvelser.

3.2.3 Arenaer og systemer for læring og informasjonsutveksling

- Det bør etableres felles møtearenaer eller samarbeidsfora for systematisk og kontinuerlig arbeid med og fokus på digital beredskap. Slike møtearenaer eller samarbeidsfora kan benyttes til samordning av planverk, kompetansebygging og til å dele erfaringer fra hendelser og øvelser, samt bidra til å koordinere planlegging og deltakelse i øvelser.
- Tilrettelegge for informasjonsdeling i forbindelse med dataangrep, og erfaringsutveksling fra etterfølgende evaluering, i tråd med NSMs grunnprinsipper.

Kost for tiltakene vil være lav til middels. Støtten antas å være høy, basert på høring som ble gjennomført høsten 2022. Det kan være noe mindre støtte til deling av informasjon rundt hendelser.

Gjennomføringsrisiko for etablering av arenaer vil være lav, men kan være noe høyere for informasjonsdeling.

Tiltakseier vil være aktører med roller innen beredskap og digital sikkerhet som Helsedirektoratet, NHN og Direktoratet for e-helse.

3.3 Prioriteres: Ny teknologi og digitale verdikjeder

En bærekraftig helse- og omsorgstjeneste forutsetter at ny teknologi, tjenester og samhandlingsformer tas i bruk, og at det skjer på en sikker måte. Sektoren bør støttes på dette komplekse området. Mange aktører og leverandører er involvert i tjenesteleveransene gjennom lange digitale verdikjeder. Et eksempel på dette er skytjenester. Vurderinger av sikkerhet og personvern ved innføring og bruk av ny teknologi er nødvendig for å sikre trygge og gode tjenester. Slike vurderinger krever sammensatt kompetanse og omfattende oppfølging. På dette området er det et stort potensial for økt samarbeid mellom aktørene, og med relevante fag- og veiledningsmiljøer i og utenfor sektoren.

Som vist i Vedlegg A, så vurderer vi at dette området gir vesentlig bidrag til å møte risikobildet framover, spesielt knyttet til risiko i leverandørkjeden og ny teknologi. ENISA har vurdert kompromittering av programvareavhengigheter i leverandørkjeder som den største cybertrusselen fram mot 2030.[11]

Det pågår allerede mye samarbeid på området. Eksempler er tverretatlig veiledning, veiledning og kurs i regi av Normen, og konkrete prosjekter der f.eks. kommuner samarbeider om anskaffelse og innføring av velferdsteknologi o.l.

Nærmere beskrivelse av tiltakene følger nedenfor.

3.3.1 Mer støtte og samarbeid ved teknologi-innføring

- Legge til rette for bedre støtte til vurdering, innføring og utvikling av ny teknologi i samarbeid med relevante fag- og veiledningsmiljøer i og utenfor sektoren. Dette inkluderer utarbeidelse av veiledningsmateriell, opplæringsaktiviteter, etablering av veiledningstjenester, sandkasser og lignende.
- Legge til rette for samarbeid ved anskaffelser, og ved kravstilling og oppfølging av leverandører. Nettverk og fagforum, interkommunale samarbeid, veiledning og utarbeidelse av felles kravspesifikasjoner kan være måter å gjøre dette på.

Både kost og gjennomføringsrisiko for disse tiltakene vurderes som middels til høy.
Det anbefales at tiltak på dette området sees i sammenheng med bl.a. den foreslåtte Helseteknologiordningen, og at eierskap til tiltakene også vurderes i sammenheng med dette.

3.3.2 Forventninger til sektor innen området

- Sentralt og lokalt beredskapsplanverk må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring. Planverket bør inkludere systemer og rutiner for varsling ved hendelser som berører andre i verdikjeden, særlig de som er avhengig av tjenesteleveranser fra andre aktører.
- DSBs modell for risikostyring i digitale verdikjeder tas inn i veiledere til relevant sektorlovverk og andre relevante veiledere.[12]

[11] "Identifying emerging cyber security threats and challenges for 2030.", ENISA
[12] Rapport *«Risikostyring i digitale verdikjeder».* Direktoratet for samfunnssikkerhet og beredskap (DSB) 2020

Både kost og gjennomføringsrisiko for disse tiltakene vurderes å være lav. Tiltakseier kan være Direktoratet for e-helse som kan ta saken til Normens styringsgruppe.

3.4 Prioriteres: Videreutvikling av eksisterende nasjonale virkemidler

Det er avgjørende at arbeidet med digital sikkerhet i sektoren skjer som en del av en kontinuerlig forbedring. Felles virkemidler som HelseCERT og Normen er helt sentrale bidragsytere til dette forbedringsarbeidet.

For å bidra til at sektorens totale beredskapsevne styrkes, må eksisterende virkemidler som bidrar på tvers av sektoren videreføres og videreutvikles. HelseCERT bidrar til å oppdage eksisterende sårbarheter, samt bistår i å oppdage og å håndtere hendelser. Både Normen og HelseCERT er med på å redusere sårbarheten i sektor ved veiledning og oppdateringer om trusselbildet.

Etter vår vurdering vil en videreutvikling av disse virkemidlene gi et bredt og et vesentlig bidrag til å møte risikobildet framover (se Vedlegg A).

Følgende tiltak foreslås:

- Videreutvikling av HelseCERT - Tiltakseier: NHN/HelseCERT
- Videreutvikling av Normen - Tiltakseier: Styringsgruppen for Normen / Direktoratet for e-helse

Både Normen og HelseCERT er godt etablerte og kjente tiltak i sektoren, og videreutvikling skjer fortløpende. Kost er vurdert til lav til middels, og risiko ved gjennomføring for disse tiltakene er lav.

3.5 Nytt innsatsområde som bør prioriteres: Robust infrastruktur for helse- og omsorgssektoren

I arbeidet med prioritering av tiltak har vi som tidligere nevnt supplert og oppdatert vår vurdering av utfordringsbildet sektoren møter på området digital sikkerhet. Siden sikkerhetsmyndigheter forventer at digitale angrep blir mer sofistikerte og i større grad vil kombineres med for eksempel fysiske angrep, mener vi at betydningen av robust infrastruktur øker. En annen åpenbar driver for mer robust infrastruktur er sektorens økende avhengighet av IKT og digitale tjenester. NSM ser det som en sikkerhetsutfordring at sivile virksomheter og infrastruktur har manglende beskyttelse, og ikke er dimensjonert for hele krisespekteret.[13] Et eksempel på økt robusthet kan være geografisk redundans på tvers av regioner. Videre har NSM utredet opprettelse av en nasjonal sky, som skal redusere avhengigheten til utenlandske skyleverandører og øke graden av nasjonal kontroll.

Direktoratet for e-helse har verken i innspillet til helseberedskapsmeldingen eller i dette dokumentet konkretisert hvilke tiltak som kan være aktuelle for å øke motstandskraft mot angrep og utfall av komponenter og kommunikasjonslinjer. Andre aktører, bl.a. NHN, kommunesektoren og nasjonale myndigheter i andre sektorer, er nærmere til å beskrive

[13] *«Sikkerhetsfaglig råd – Et motstandsdyktig Norge», 2023*. Nasjonal sikkerhetsmyndighet.

konkrete tiltak på området, men Direktoratet ønsker å løfte fram betydningen av robust infrastruktur.

3.6 Prioritere videre kartlegging av øvrige innsatsområder, og se kartleggingsaktiviteter i sammenheng

I vårt innspill til den kommende helseberedskapsmeldingen pekte vi på ytterligere tre innsatsområder:

- Kompetanse og sikkerhetskultur
- Etterlevelse og oppfølging
- Støtte til små virksomheter

Dette er alle viktige innsatsområder som på en god måte treffer risikoområdene som er beskrevet i kapittel 2.1. Felles for disse innsatsområdene er at det bør gjennomføres kartlegging av status og behov i sektoren for å iverksette treffsikre tiltak. Vi trenger mer kunnskap, blant annet om risiko, status og behov i ulike deler av sektoren, og hva som skal til for å støtte sektoren på best mulig måte. Flere av tiltakene som er foreslått kan på sikt ha betydelige kostnader og kompleksitet i gjennomføring. Et eksempel på dette kan være å utvikle og styrke kontroll av digital sikkerhet i sektorens virksomheter.

Kost, antatt støtte i sektoren, samt risiko i gjennomføring er vurdert for kartleggingstiltakene. Gitt det store antallet små virksomheter i sektoren vil antakelig en kartlegging som omfatter disse ha en gjennomføringsrisiko som er middels til høy. De andre områdene som vil omfattes av kartleggingen innebærer antakelig middels kost og risiko. Vi tror det vil være høy støtte i sektor til kartlegging, med unntak av etterlevelse og oppfølging. Dette kan oppleves som et forsøk på å føre tilsyn uten mandat, og god kommunikasjon rundt tiltaket vil være av stor betydning.

Vi vurderer at det er hensiktsmessig å se kartleggingsaktivitetene i sammenheng. Sektoren er kompleks og omfatter tusenvis av virksomheter. En samlet gjennomføring vil derfor være ressursbesparende og effektivt både for kartlegger og respondenter. Samtidig vil resultatene kunne vurderes samlet.

Kartleggingen kan med fordel gjentas jevnlig for å sikre oppdatert kunnskap og for å følge utviklingen innen digital sikkerhet.
Vi foreslår at Direktoratet for e-helse får ansvaret for gjennomføring av kartleggingen som tiltakseier.

3.7 Stille forventninger til sektoren

Våre anbefalinger til prioriterte innsatsområder og tiltak, inneholder både sentrale tiltak og tiltak som gjennomføres i den enkelte virksomhet. Flere av innsatsområdene inneholder tiltak som omfatter å stille forventninger til sektor. I praksis kan dette gjennomføres som:

- Kravstilling gjennom lovgivning og etablerte styringslinjer
- Innarbeidelse av anbefalinger i veiledningsmateriell, evt. som krav i Normen
- Gjennom kommunikasjon og pedagogiske virkemidler

Dette er tiltak som krever få ressurser av dem som kommuniserer forventningene, men hvor gjennomføringen kan innebære kostnader for virksomhetene som skal møte forventningene.

Kommende krav- og lovendringer som vil treffe virksomhetene i helse- og omsorgssektoren må utredes og høres i tråd med utredningsinstruksen og formidles på en hensiktsmessig måte. Særlig vil det være viktig å kommunisere hva virksomhetene må foreta seg for å oppfylle nye krav, og stille forventinger om at dette gjøres. Målet om et felles nivå for digital sikkerhet må støttes og prioriteres fra myndighetssiden, og vil gagne sektoren som helhet dersom man lykkes. Et eksempel på krav som vil treffe virksomhetene fremover er forslag til lov om digital sikkerhet (som gjennomfører NIS-direktivet i norsk rett) og det kommende NIS2-direktivet. Les mer om dette i kapittel 2.2 over.

Innenfor de prioriterte innsatsområdene Planverk og øvelser og Ny teknologi og digitale verdikjeder er det allerede omtalt viktige forventninger som bør stilles til sektoren. I tillegg til disse mener vi følgende forventninger fra innsatsområdet Etterlevelse og oppfølging er viktige å kommunisere til sektoren:

- Nasjonale virkemidler, hjelpemidler og samarbeidsnettverk må sammenstilles og samordnes.

  Et poeng om veiledning og verktøy for digital sikkerhet som påpekes særlig fra kommunal side,[14] er at det kan være vanskelig å navigere i og få oversikt over alle de ulike nasjonale virkemidlene, hjelpemidlene og samarbeidsnettverkene. Dette området er belyst i Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.[15] Direktoratet forventer at det som resultat av denne undersøkelsen vil skje flere sentrale, sektorovergripende tiltak på området. Direktoratet anbefaler at vår sektor bidrar i gjennomføring av tiltakene der det er naturlig, og ellers sørger for at veiledning som utarbeides i sektoren (f.eks. i regi av Normen) er synkronisert med nasjonale virkemidler, hjelpemidler og samarbeidsnettverk.

- Det er viktig å skaffe oversikt over sikkerhetstiltakenes effekt. Ved å måle effekten av sentralt iverksatte tiltak legges det til rette for mer målrettede, konkrete og effektive tiltak i fremtiden.

  Dette er også et område hvor det er samsvar mellom forslag til tiltak og Riksrevisjonens undersøkelse av myndighetenes samordning på området. I helse- og omsorgssektoren blir det derfor viktig at vi får oversikt over effekten av tiltakene som vi iverksetter for å styrke digital sikkerhet gjennom kvalitative og kvantitative evalueringer. I forbindelse med sikkerhetstiltak på nasjonalt eller tverrsektorielt nivå der vår sektor er involvert, bør vi påvirke og understøtte prosessene slik at det legges vekt på vurdering av effekt av tiltak.

3.8 Målindikatorer

Digital sikkerhet er et område der utviklingen skjer raskt. Både trusselbildet og teknologien endres i hurtig tempo. Nasjonal e-helsestrategi legger opp til en dynamisk gjennomføring av tiltak basert på målindikatorer. Vi anbefaler samme tilnærming innen digital sikkerhet, men

[14] Se for eksempel KS sin rapport «Styrking av digital robusthet i kommunal sektor»
[15] Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor. Dokument 3:7 (2022–2023). Riksrevisjonen.

med et viktig tillegg: På vårt område må også endringer i risikobildet være avgjørende for hvilke tiltak som skal iverksettes.

Vi anbefaler derfor at det i første omgang utvikles målindikatorer innenfor de prioriterte innsatsområdene *Planverk og øvelser* og *Ny teknologi og digitale verdikjeder*. Målindikatorene kan ta utgangspunkt i konkretisering og videreutvikling av målene i Direktoratets innspill til helseberedskapsmelding, se Vedlegg B.

Vedlegg A Vurdering av innsatsområder og tiltak

I dette vedlegget er hvert av de seks innsatsområdene med tilhørende tiltak beskrevet og vurdert nærmere. Beskrivelsen danner grunnlaget for prioriteringen i av tiltakene i kapittel 3. Vedlegget starter med en introduksjon til hvordan hvert innsatsområde beskrives i vedlegget.

A.1 Hvordan vurderingen av innsatsområdene beskrives

Hvert innsatsområde starter med en tekstlig beskrivelse av tiltakene.[16] Deretter beskrives vurderingene som er gjort knyttet til tiltakene og innsatsområdene.

A.1.1 Grov tidsplan for realisering

For hvert innsatsområde gis det en tekstlig og grafisk beskrivelse av hvordan tiltakene kan gjennomføres i tid for å realisere innsatsområdet. Beslutningspunkt, f.eks. etter en utredning, er markert som milepæler. I en tabell gis det, for hvert tiltak, en oversikt over foreslått tiltakseier, hvilke aktører som bør involveres, samt målgruppe for tiltaket. Hvis tiltaket har grenseflater eller overlapp med andre tiltak (f.eks. på nasjonalt nivå), eller det er andre forhold som tilsier at tiltakene ses i sammenheng, er dette beskrevet.

A.1.2 Kost og risiko ved gjennomføring av tiltak

Vurderingen av kost og risiko ved gjennomføring av tiltakene, bygger på en vurdering av følgende aspekter:

- Forventet kostnad for tiltaket (lav/middels/høy i samsvar med beskrivelsene i tabell under)
- Antatt grad av støtte i sektoren
- Risiko ved gjennomføring av tiltaket (lav/middels/høy i samsvar med beskrivelsene i tabell under)

Disse aspektene er beskrevet i en tabell, og over tabellen følger begrunnelse for vurderingene. Merk at vurderingen av kostnad er relativ til dagens ressurs/kostnadsnivå. En forutsetning for vurderingene er at arbeid som allerede pågår innenfor dagens ressurser forsetter gjennom den foreslåtte tiltaksperioden. Som eksempel vil tiltak innen pågående initiativer som Normen og HelseCERT (innsatsområde 1) vurderes å ha lav kostnad om de kan realiseres innen rammene av dagens ressursbruk for disse initiativene.

I de tilfellene tiltakene kan tenkes å reise prinsipielle spørsmål er dette også vurdert kort.

[16] Se **Feil! Fant ikke referansekilden.** for tabellarisk oversikt med mapping mellom de opprinnelige t iltaksformuleringene i direktoratets innspill til helseberedskapsmeldingen, og tiltaksformuleringene på overskriftsnivå som er brukt i dette dokumentet.

Begrepsforklaring:

Høy kostnad	Middels høy kostnad	Lav kostnad
• Betydelige investeringsbehov • Høye kostnader knyttet til drift og forvaltning • Krever ressursbruk i svært mange virksomheter • Behov for flere nyansettelser • Investering i verktøy/utvikling	• Noe investeringsbehov / videreutvikling av eksisterende løsninger • Krever ressursbruk i mange virksomheter • Middels høye kostnader knyttet til drift og forvaltning • Behov for noen nye ansettelser	• Lavt eller ingen investeringsbehov • Krever ressursbruk i få virksomheter • Lave eller ingen kostnader knyttet til drift og forvaltning • Omprioritering av eksisterende ressurser.

Høy risiko	Middels risiko	Lav risiko
• Mange aktører fra ulike deler av helse- og omsorgssektoren må involveres, bli enige og/eller bidra med egne ressurser • Tverrsektorielle tiltak • Nyetablering av tiltak hvor det er stor usikkerhet knyttet til innretning og effekt • Det er nødvendig med endringer i mandat for en eller flere aktører.	• Mange aktører fra avgrensede deler av helse- og omsorgssektoren må involveres, bli enige og/eller bidra med egne ressurser • Involvering av aktører fra andre sektorer. • Nye tiltak hvor usikkerheten er begrenset	• Kun et fåtall aktører må være aktivt involverte • Kan bygge på tiltak som allerede er etablerte • Klart avgrenset i tid og omfang • Kan gjennomføres innenfor eksisterende rammer og mandater

Merk at kostnad og risiko ved gjennomføring av tiltak som etterfølger utredninger ikke er vurdert. Dette er fordi disse tiltakene ikke er beskrevet videre i innspillet til helseberedskapsmeldingen, og det er på nåværende tidspunkt er vanskelig å forutsi hvilke tiltak det vil være snakk om. Kostnad og risiko ved gjennomføring av disse tiltakene vil være avhengig av de aktuelle tiltakene, og både kostnad og risiko ved gjennomføring kan være betydelige. Gjennomføring av disse tiltakene vil imidlertid være viktige for å få nytte fra innsatsområdene det gjelder.

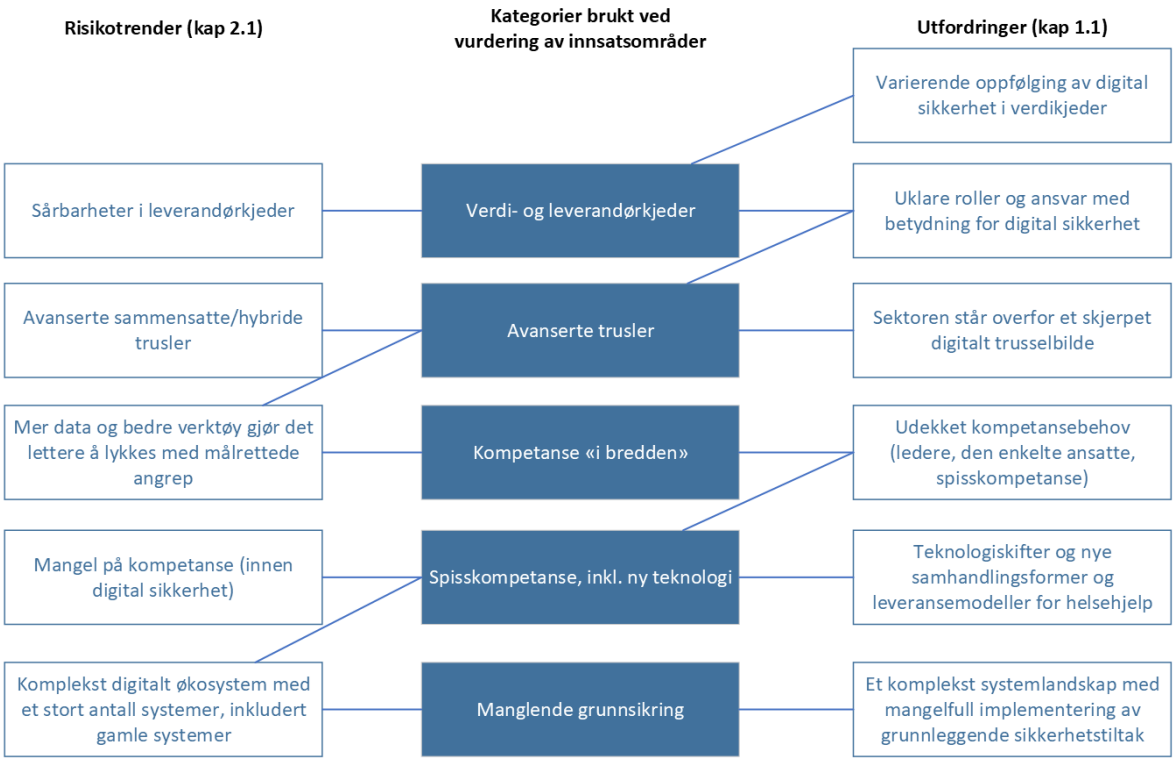
A.1.3 Reduksjon av risiko knyttet til digital sikkerhet

I delkapittel 1.1 gav vi en oversikt over det vi tidligere har identifisert som de viktigste utfordringene for helse- og omsorgssektoren i arbeidet med digital sikkerhet. I kapittel 2 gav vi en oversikt over viktige risikotrender knyttet til digital sikkerhet. Disse utfordringene og risikotrendene benytter vi for å vurdere hvordan hvert innsatsområde bidrar til å redusere risiko knyttet til digital sikkerhet. Vi vurderer innsatsområdenes bidrag til følgende utfordrings- og risikoområder:

- Avanserte trusler
- Kompetanse i «bredden»
- Spisskompetanse, inkl. ny teknologi
- Manglende grunnsikring

- Leverandørkjede-risiko

Figuren under gir en oversikt over hvordan disse områdene relateres til utfordringene og risikotrendene vi har beskrevet.[17]



I tillegg til å vurdere bidraget til å redusere risiko innen disse områdene, gir vi en beskrivelse av:

- Hvordan innsatsområdet bidrar til å redusere sårbarhet
- Hvordan innsatsområdet bidrar til å øke håndteringsevnen
- I hvilken del av sektor innsatsområdet primært vil redusere risiko

[17] For å forklare hvordan figuren er bygget opp, og hva relasjonene som er tegnet opp betyr, så kan vi se på kategorien *Avanserte trusler*. En relasjon til risikotrendene *Avanserte sammensatte/hybride trusler* og *Mer data og bedre verktøy gjør det lettere å lykkes med målrettede angrep* betyr følgende: Når vi vurderer innsatsområdene, og ser på deres bidrag til kategorien *Avanserte* trusler, så dekker dette en vurdering av innsatsområdets bidrag til å håndtere risikotrendene knyttet til avanserte sammensatte/hybride trusler og bedre målrettede angrep som følge av mer data og verktøy, og den relaterte utfordringen at sektoren står overfor et skjerpet digitalt trusselbilde. I figuren kan man også se at vi vurderer en av disse risikotrendene (*Mer data og bedre verktøy gjør det lettere å lykkes med målrettede angrep*) til å passe inn under to kategorier: *Avanserte trusler* og *Kompetanse «i bredden».* I dette tilfellet betyr det at vi anser risikotrenden å høre inn under kategorien *Avanserte trusler*, men at den også er relatert til *Kompetanse «i bredden»* ved at slik kompetanse har innvirkning på evne til å motstå avanserte phishing-angrep, som er et eksempel på et slikt målrettet angrep. Figuren gir ikke en grundig og fullstendig oversikt over alle relasjoner mellom utfordringer og risikotrender, men viser hvordan vi refererer til disse trendene og utfordringene videre i dette dokumentet.

A.2 Innsatsområde 1: Videreutvikling av eksisterende nasjonale virkemidler

Normen og HelseCERT er godt etablerte nasjonale virkemidler i arbeidet med digital sikkerhet i helse- og omsorgssektoren. For å bidra til at sektorens totale beredskapsevne styrkes, må eksisterende virkemidler som bidrar på tvers av hele sektoren videreføres og videreutvikles.

Foreslåtte tiltak:

1.1 Videreutvikle HelseCERT

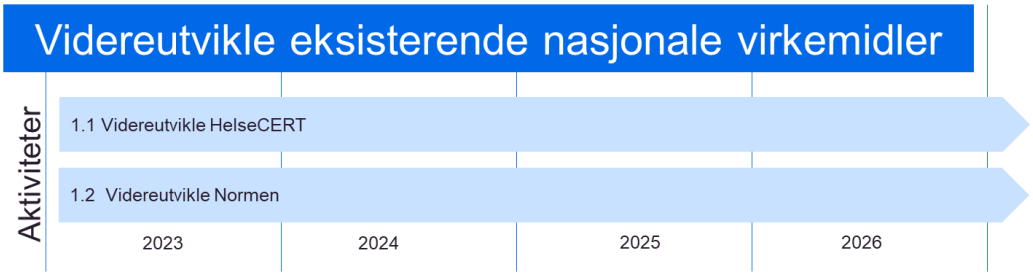
HelseCERT er helsetjenestenes kompetansemiljø for operativ informasjonssikkerhet. HelseCERT jobber kontinuerlig med utviklingen av sitt tjenestetilbud, innenfor rammen av å være et sektorvist responsmiljø, for å sikre at tjenestene på best mulig måte møter behov som følger av et digitalt trusselbilde i endring. Styrking av HelseCERT vil gi økt kapasitet til å gjennomføre sikkerhetstesting av aktørene i sektoren, overvåking av sikkerhetssituasjonen og aktiv kommunikasjon og bistand til aktørene i helse- og omsorgssektoren.

1.2 Videreutvikle Normen

Sektorens kjennskap og forpliktelse til Normen som kravsett gjør at en videreutvikling av Normen vil være et sentralt og effektivt virkemiddel for å nå frem med viktige føringer og krav innen digital sikkerhet. Det økte trusselnivået som også treffer helse- og omsorgssektoren, samt tempoet i utviklingen, fordrer at det investeres videre i allerede sterke fagmiljøer. Normen som etablert bransjenorm er et slikt miljø, som i henhold til sitt mandat bidrar med relevant, nødvendig og tilpasset veiledning på fagområdet informasjonssikkerhet og personvern til helse- og omsorgssektoren.

A.2.1 Realisering av innsatsområder og tiltak

Figuren viser en mulig plan for gjennomføring av tiltakene innenfor satsningsområdet:



Både HelseCERT og Normen er godt etablerte løpende tiltak med eksisterende styringsstrukturer som beslutter oppgaveportefølje og prosjekter. Videreutviklingen er derfor illustrert på en generisk måte. For en oversikt over planlagte strategiske fokusområder og initiativer for Normen, se Strategien for Normen 2023-2025[18].

Nærmere om gjennomføring av tiltakene:

Tiltak	Forslag til tiltakseier / involverte aktører / målgruppe	Grenseflater / overlappende tiltak
1.1 Videreutvikle HelseCERT	Tiltakseier: Norsk Helsenett Involverte aktører: Norsk Helsenett Målgruppe: Hele sektoren	

[18] Strategi for Normen (2023-2025).

1.2 Videreutvikle Normen	Tiltakseier: Styringsgruppen for Normen bistått av Direktoratet for e-helse som sekretariat Involverte aktører: Hele sektoren Målgruppe: Hele sektoren	

A.2.2 Vurdering av kost og risiko ved gjennomføring av tiltak

Både HelseCERT (1.1) og Normen (1.2) er etablerte tiltak som allerede har tilordnede ressurser. Begge tiltak vil derfor kunne videreutvikles med et ressursnivå på linje med dagens nivå. Vi anser dermed forventet kostnad for Normen til å være lav. Imidlertid kan en videreutvikling av HelseCERT innebære investeringer i teknisk infrastruktur. Derfor vurderes forventet kostnad for videreutvikling av HelseCERT til å være middels.

Som etablerte tiltak har begge tiltak allerede høy støtte i sektoren. Derfor vurderer vi antatt grad av støtte i sektoren for videreutvikling av disse tiltakene til også å være høy.

Når det gjelder risiko i gjennomføring så er begge tiltak allerede etablerte, og videreføring har lav risiko. Nye investeringer knyttet til HelseCERT kan imidlertid ha middels risiko i gjennomføringen.

Tiltaksområdet bidrar samlet til stor grad av måloppnåelse (se Vedlegg 1), og de utfyller hverandre. Til sammen gir de stor grad av støtte til sektorens virksomheter. Begge tiltak er brede i den forstand at de har mulighet til å bidra inn også i de andre tiltaksområdene. Som eksempel så kan veiledningen i Normen videreutvikles til å i større grad bidra til sikkerhet i ny teknologi, og/eller gi mer støtte til mindre virksomheter.

Tiltak	**Forventet kostnad**	**Antatt grad av støtte i sektoren**	**Risiko i gjennomføring**
1.1 Videreutvikle HelseCERT	Middels	Høy	Lav/middels
1.2 Videreutvikle Normen	Lav	Høy	Lav

A.2.3 Vurdering av reduksjon av risiko knyttet til digital sikkerhet

Bidrag til å redusere sårbarhet	Både Normen og HelseCERT er allerede med på å redusere sårbarheten i sektor ved veiledning og oppdateringer om trusselbilde. HelseCERT kan bidra til å oppdage eksisterende sårbarheter.
Bidrag til å øke håndteringsevne	HelseCERT kan bistå i å oppdage og å håndtere hendelser. Normen kan gi veiledning.
Relasjon til risikobildet Verdi- og leverandørkjederisiko: x Avanserte trusler: X Kompetanse «i bredden»: x Spisskompetanse, inkl. ny teknologi: X Manglende grunnsikring: x	Både Normen og HelseCERT er brede tiltak som kan bidra inn mot hele risikobildet, avhengig av hvilke prioriteringer som gjøres i HelseCERT og styringsgruppa til Normen. Eksempler på hvordan tiltakene allerede bidrar er: • Oppdatert trusselbilde • Sikkerhetsovervåkning • Bistand ved hendelser

Tegnforklaring: X *Vesentlig bidrag* x *Noe bidrag* v *Mulig indirekte bidrag*	• Kompetansebygging i sektor • Veiledning knyttet til ny teknologi • Veiledning knyttet til sikkerhetskrav mot leverandører, samt veiledning til leverandører i sektoren • Veiledning og krav knyttet til basis sikkerhetstiltak Tiltakene er også viktige for å opprettholde nasjonale kompetansemiljø som kan bygge og vedlikeholde spisskompetanse sektoren har behov for.
Del av sektor	Tiltakene kan nå større og mindre virksomheter samt leverandører, avhengig av innretning.

A.3 Innsatsområde 2: Kompetanse og sikkerhetskultur

Digitaliseringen stiller nye krav til kompetanse for å ivareta sikkerheten i sektoren. Økt kompetanse om digital sikkerhet og god sikkerhetskultur, fra virksomhetens øverste ledelse og til den enkelte ansatte, vil redusere risikoen for uønskede digitale hendelser.

Foreslåtte tiltak:

2.1 Kartlegging
Det foreslås at det første steget for å nå målet om økt kompetanse, er å gjennomføre en kartlegging og vurdering av effekten av eksisterende kompetansetiltak. Formålet med kartleggingen er å identifisere virkemidler som fungerer godt, og som kan deles og gjenbrukes i hele sektoren. Eksisterende tiltak innen kunnskapssektoren rettet mot helsefaglige utdanninger bør også inngå. Kartleggingen bør også omfatte kompetansebehov innen digital sikkerhet i sektoren.

2.2 Utredning
Basert på kartleggingen, utrede tiltak med formål å styrke kompetansen om digital sikkerhet hos helsepersonell og roller som støtter helsepersonell, som for eksempel ledere og administrativt ansatte. Kunnskapsgrunnlaget som lå til grunn for etableringen av tiltak i helse- og sosialfaglige utdanninger bør innhentes og inngå i kartleggingen. En utredning bør også vurdere behovet for tverrfaglig kompetanse i sektoren. Tiltakene som identifiseres bør legge vekt på å adressere og gi et løft til satsninger og initiativ som allerede er i drift, og bygge videre på de erfaringene som er gjort av andre satsinger på digital sikkerhet i helse- og omsorgssektoren.

2.3 Digital sikkerhet i helsefaglig utdanning
Bidra til økt oppmerksomhet på digital sikkerhetskompetanse i helsefaglige utdanninger, både i videregående utdanninger og på universitet- og høyskolenivå. Tiltaket kan omfatte både styrking av området i helsefaglige grunnutdanninger, samt gjennom etter – og videreutdanning. Tiltaket bør også legge vekt på å adressere og gi et løft til satsninger og initiativ som allerede eksisterer i de helsefaglige utdanningene, og bygge videre på de erfaringene som er gjort av andre satsinger på digital sikkerhet i de helsefaglige utdanningene.

Tiltak i helseforetakenes regionale handlingsplan for informasjonssikkerhet og personvern understøttes foreslåtte tiltak om karlegging og utredning. Både i Helse Sør-Øst RHF og Helse Midt-Norge RHF planlegges å gjennomføre kultur-undersøkelse innen informasjonssikkerhet og personvern for å kartlegge status og modenhet og foreslå tiltak om opplæringsmateriell

A.3.1 Realisering av innsatsområder og tiltak

Figuren viser en mulig plan for gjennomføring av tiltakene innenfor satsningsområdet:

Realisering av innsatsområdet bør begynne med kartlegging av kompetansebehov innen digital sikkerhet og eksisterende kompetansetiltak i sektoren. Kartleggingen bør også ta for seg helsefaglige utdanninger i kunnskapssektoren, og hvordan kunnskap om digital sikkerhet formidles til kommende utøvere av helseprofesjonene. Kartleggingen danner grunnlag for videre utredning av evt. felles kompetansetiltak i sektoren. I parallell bør det sees på hvordan kunnskap om digital sikkerhet kan styrkes i helsefaglig utdanning.

Kartleggingen kan med fordel gjentas jevnlig for å sikre oppdatert kunnskap.

Nærmere om gjennomføring av tiltakene:

Tiltak	**Forslag til tiltakseier / involverte aktører / målgruppe**	**Grenseflater / overlappende tiltak**
2.1 Kartlegging	Tiltakseier: Direktoratet for e-helse Involverte aktører/målgruppe: hele sektoren, evt. helsefaglige utdanninger i kunnskapssektoren	Hvis kartleggingen skal omfatte helsefaglige utdanninger krever dette koordinering med kunnskapssektoren og tilhørende myndigheter.
2.2 Utredning	Tiltakseier: Direktoratet for e-helse Involverte aktører/målgruppe: hele sektoren, evt. helsefaglige utdanninger i kunnskapssektoren	Hvis utredningen skal omfatte helsefaglige utdanninger krever dette koordinering med kunnskapssektoren og tilhørende myndigheter.
2.3 Styrke digital sikkerhet i helsefaglig utdanning	Tiltakseier: Relevant myndighetsaktør i kunnskapssektoren. Involverte: helsefaglige utdanninger i kunnskapssektoren, fagressurser fra helseforvaltningen og helse- og omsorgssektoren. Målgruppe: helsefaglige utdanninger i kunnskapssektoren	Krever koordinering med kunnskapssektoren og tilhørende myndigheter.

A.3.2 Vurdering av kost og risiko ved gjennomføring av tiltak

Kartlegging og utredning (2.1, 2.2) er avgrensede oppgaver som i stor grad kan gjøres ved omprioritering av eksisterende ressurser. Samtidig vil en kartlegging omfatte store deler av sektor og krever ressurser både fra de som gjennomfører kartlegging/utredning og fra sektor som kartlegges. Forventet kostnad vurderes derfor å være middels. Når det gjelder styrking av digital sikkerhet i helsefaglige utdanninger (2.3) så er det mulig å bygge på allerede eksisterende undervisningsmateriale og erfaringer fra Digsam-prosjektet. Dermed anser vi forventet kostnad for dette tiltaket til å være lav/middels. Merk at eventuelle tiltak som kommer etter utredning kan ha høyere kostnad.

Kompetansetiltak forventes å ha stor grad av støtte i sektoren, men kartleggingstiltak som krever involvering fra sektor kan det være noe mindre støtte til.

Kartlegging og utredning vil kreve sektorinvolvering, og i en omfattende og kompleks sektor vil det innebære en viss risiko for gjennomføringen. Styrking av digital sikkerhet i helsefaglig utdanning vil være et tverrsektorielt tiltak, noe som øker risikoen.

Økt kompetanse og sikkerhetskultur underbygger målene i strategien, og er også i stor grad en forutsetning for å lykkes med andre innsatsområder. Merk at effekten fra innsatsområdet kommer fra alle tiltakene i innsatsområdet samlet: Man starter med kartlegging, går videre til utredning, og etablerer tiltak basert på utredning.

Tiltak	**Forventet kostnad**	**Antatt grad av støtte i sektoren**	**Risiko i gjennomføring**
2.1 Kartlegging	Middels	Middels/Høy	Middels
2.2 Utredning	Middels	Middels/Høy	Lav/Middels
2.3 Styrke digital sikkerhet i helsefaglige utdanning	Lav/Middels	Middels/Høy	Middels/Høy

A.3.3 Vurdering av reduksjon av risiko knyttet til digital sikkerhet

Bidrag til å redusere sårbarhet	Hos ledere: Kan gi bedre beslutninger om sikkerhetsinvesteringer og tiltak. Hos alle ansatte: Kan lede til tryggere bruk av digitale løsninger. Hos IT og informasjonssikkerhets-personell: Kan gi tryggere og mer moderne løsninger, og bedre sikkerhetsstyring.
Bidrag til å øke håndteringsevne	Større sannsynlighet for at ansatte melder fra om hendelser. Bedre kompetanse gir bedre håndtering.

<table>
<tr>
<td>Relasjon til risikobildet
<table>
<tr><td>Verdi- og leverandørkjederisiko</td><td>v</td></tr>
<tr><td>Avanserte trusler</td><td>x</td></tr>
<tr><td>Kompetanse «i bredden»</td><td>X</td></tr>
<tr><td>Spisskompetanse, inkl. ny teknologi</td><td>x</td></tr>
<tr><td>Manglende grunnsikring</td><td>v</td></tr>
</table>
Tegnforklaring:
X Vesentlig bidrag
x Noe bidrag
v Mulig indirekte bidrag</td>
<td>Tiltak 2.3 vil bidra til styrket kompetanse om digital sikkerhet hos nyutdannet helsepersonell, noe som vil øke den generelle kompetansen om digital sikkerhet i sektoren og kunne øke motstandsdyktigheten mot angrep, inkludert avanserte phishing- angrep og digital utpressing. Eventuelle tiltak etter kartlegging og utredning vil kunne bidra til å ytterligere redusere risiko, både når det gjelder bredde- og spisskompetanse. Økt kompetanse vil sette virksomhetene i stand til å gjøre bedre sikkerhetsarbeid generelt.</td>
</tr>
<tr>
<td>Del av sektor</td>
<td>Tiltak 2.3 har nyutdannet helsepersonell som målgruppe, og vil slik kunne gi effekter på lengre sikt både mot større og mindre virksomheter i sektor. Målgruppe for de andre tiltakene vil være avhengig av kartlegging og utredning.</td>
</tr>
</table>

A.4 Innsatsområde 3: Planverk og øvelser

Alle sektorens virksomheter må være forberedt på å håndtere digitale sikkerhetshendelser og sikre fortsatt forsvarlig leveranse av helsetjenester. For å oppnå dette må planverk forbedres, og det må gjennomføres flere øvelser i sektoren, både nasjonalt, regionalt og lokalt. Evaluering og læring gjennom øvelser vil bidra til å identifisere forbedringsområder. Dette er viktige momenter for kontinuerlig forbedring og videreutvikling av planverk.

Foreslåtte tiltak:

3.1 Overordnet nasjonal IKT-beredskapsplan
Tiltaket omfatter å utarbeide en overordnet nasjonal IKT-beredskapsplan. Planen vil ta utgangspunkt i Nasjonal helseberedskapsplan, og vil være utdypende på området IKT-beredskap. Planen vil bidra til å tydeliggjøre roller, ansvar, informasjonsdeling og kommunikasjon ved hendelser som utløser behov for en nasjonalt, samordnet krisehåndtering. Planen bør være overordnet og danne grunnlag for å utforme planer lokalt og regionalt som baserer seg på de samme prinsipper for håndtering av IKT-hendelser og en omforent forståelse for ansvar, roller og begreper.

3.2 Sammenheng mellom planverk
Tiltaket omfatter virkemidler for å sikre sammenheng mellom ulike planverk for IKT-beredskap. Planverk på nasjonalt, regionalt og lokalt nivå må koordineres og sees i sammenheng. Krav om sammenheng i planverk må stilles gjennom vedtatte styringslinjer, og det må gis veiledning til virksomhetene i sektoren.

3.3 Etablere felles arenaer
Tiltaket omfatter etablering av felles møtearenaer eller samarbeidsfora for systematisk og kontinuerlig arbeid med og fokus på digital beredskap. Hovedhensikten med arenaene er å legge til rette for koordinering og kunnskapsdeling. Slike møtearenaer eller samarbeidsfora kan benyttes til samordning av planverk, kompetansebygging og dele erfaringer fra hendelser og øvelser samt bidra til å koordinere planlegging og deltakelse i øvelser. Se også tiltak 3.7 om informasjonsdeling og erfaringsutveksling.

3.4 Kart over roller, systemeierskap og leverandører

Tiltaket omfatter å etablere oversikt over roller, systemeierskap og leverandører i sektoren med betydning for nasjonale e-helseløsninger. Sektorens størrelse, kompleksitet, mangfold av aktører og omfattende bruk av digitale systemer gjør det nødvendig med slik kartlegging for å kunne utarbeide og forbedre planverk og hendelseshåndtering. Kartleggingen vil også ligge til grunn for planlegging, gjennomføring og evaluering av øvelser.

3.5 Nasjonal oversikt kritisk infrastruktur
Tiltaket omfatter å etablere oversikt over kritisk infrastruktur i sektoren. Sektoren har kritisk infrastruktur på både nasjonalt, regionalt og lokalt nivå. Slik oversikt er nødvendig for å kunne prioritere ressurser for forbyggende sikkerhetsarbeid og ved digitale sikkerhetshendelser. De digitale systemene i sektoren er koblet sammen, og det kan derfor være både krevende og nødvendig å skille mellom ulike kategorier kritiske systemer. Det kan være flere former for kritisk infrastruktur, som omfattes av ulike regelverk som for eksempel sikkerhetsloven og NIS-direktivet.

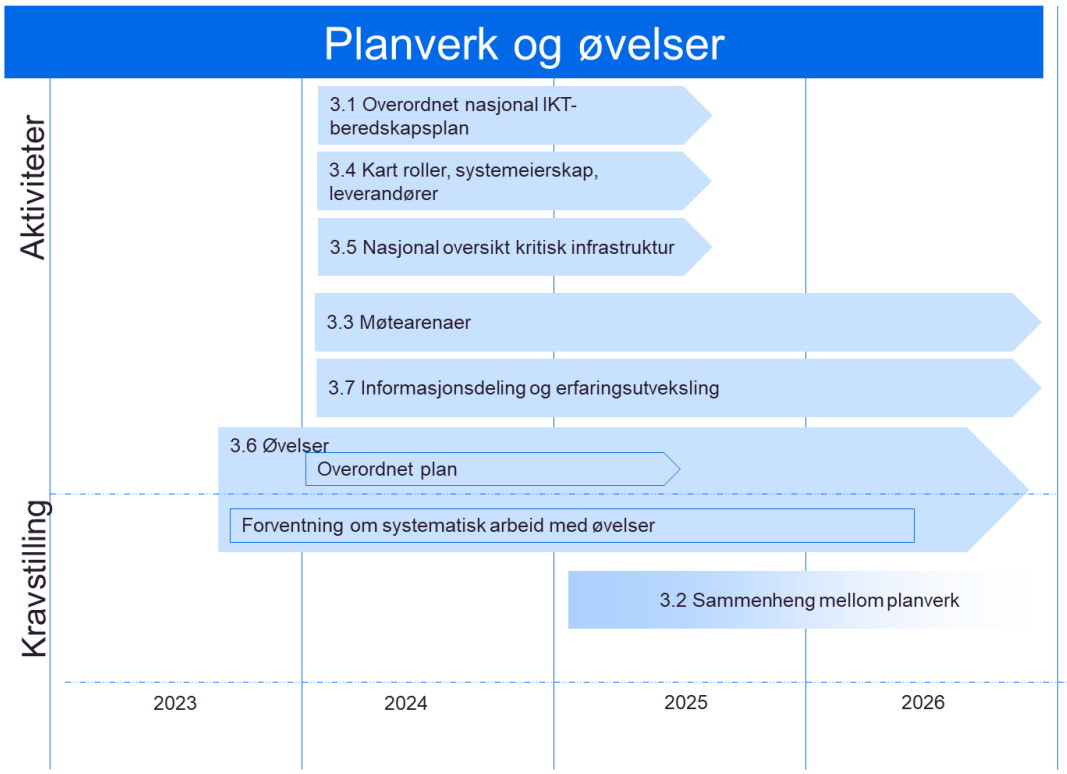
3.6 Overordnet plan for øvelser og forventning om systematisk arbeid med øvelser
Tiltaket omfatter å etablere en flerårig, overordnet plan for øvelser i sektoren på nasjonalt, regionalt og virksomhetsnivå. Målet er å sikre evnen til å levere forsvarlige helsetjenester og ivareta pasientsikkerheten også under krevende forutsetninger. Øvelsene bør bl.a. omfatte scenarier for bortfall av nasjonale e-helseløsninger og brudd i leveranse av kommunikasjon eller elektrisk kraft. Det er viktig at planverk, ROS-analyser, krisescenarioer, trusselvurderinger og tidligere erfaringer ligger til grunn for øvingsplanlegging og gjennomføring. Evaluering, oppfølging og rapportering vil inngå som en del av det systematiske forbedringsarbeidet.

3.7 Informasjonsdeling og erfaringsutveksling
Tiltaket omfatter å styrke og videreutvikle systematisk informasjonsdeling og erfaringsutveksling for sektorens arbeid med planverk, øvelser, sårbarheter og trusler. Slik informasjonsdeling og erfaringsutveksling er viktig i forbindelse med dataangrep, andre sikkerhetshendelser og nesten-hendelser. Tiltaket vil bidra til viktig læring for virksomhetene, og må sees i sammenheng med tiltak 3.3 om å etablere felles arenaer.

Tiltak i helseforetakenes regionale handlingsplan for informasjonssikkerhet og personvern understøttes foreslåtte tiltak. I Helse Sør-Øst RHF planlegges gjennomgang av beredskapsplanverk innen ikt. Tiltaket understøtter foreslått tiltak om å sikre **sammenheng mellom ulike planverk** for IKT-beredskap. Helse Sør-Øst arbeider også systematisk med øvelser og sammen med Norsk helsenett SF skal det gjennomføres øvelser for håndteringen av uønskede kritiske hendels. Tiltaket understøtter foreslått tiltak om **overordnet plan for øvelser i sektoren på nasjonalt, regionalt og virksomhetsnivå**. I tillegg planlegges flere tiltak i Helse Sør-Øst som understøtter foreslått tiltak **om informasjonsdeling og erfaringsutveksling**; Det skal utarbeides en årlig rapport i samarbeid med Norsk helsenett SF om trusler og trender som spesialisthelsetjenesten kan benytte i sitt arbeid med risiko- og sårbarhetsvurderinger, og oversikten over tiltak fra risiko- og sårbarhetsvurderinger skal forbedres.

A.4.1 Realisering av innsatsområder og tiltak

Figuren viser en mulig plan for gjennomføring av tiltakene innenfor satsningsområdet:



Realiseringen av innsatsområdet omfatter både kravstilling og gjennomføring av aktiviteter.

Det bør etableres en overordnet nasjonal IKT-beredskapsplan. Arbeidet med å utvikle en slik plan bør starte i 2024, men den kommende helseberedskapsmeldingen og en eventuelt revidert versjon av Nasjonal helseberedskapsplan vil kunne påvirke arbeidet og gi føringer Parallelt som IKT-beredskapsplanen utarbeides må roller, systemeierskap og leverandører til sektoren kartlegges, og det må etableres en overordnet nasjonal oversikt over kritisk infrastruktur i sektoren.

Sektorens allerede pågående og planlagte øvingsaktivitet fortsetter og utvides. Parallelt bør det stilles større forventning i styringslinjene om systematisk arbeid med øvelser. Slike forventninger bør omfatte omfang, innhold og hyppighet av øvelser, samt evaluering for forbedring. Gjennomføring av øvelser vil være en kontinuerlig aktivitet, som etter hvert i perioden i økende grad vil inngå som del av en overordnet plan.

Det bør også etableres av møtearenaer, informasjonsdeling og erfaringsutveksling for å øke kompetansen på området, og koordinere arbeidet med planverk og øvelser.

Nærmere om gjennomføring av tiltakene:

Tiltak	**Forslag til tiltakseier / involverte aktører**	**Grenseflater / overlappende tiltak**
3.1 Overordnet nasjonal IKT-beredskapsplan	HOD bør utpeke en tiltakseier. Involverte: Helsedirektoratet, Direktoratet for e-helse, Norsk Helsenett, øvrige deler av sektoren.	Helseberedskapsmelding, eventuelt revidert Nasjonal helseberedskapsplan. NIS2 må tas i betraktning (roller/ansvar).
3.2 Sammenheng mellom planverk	Krav stilles gjennom vedtatte styringslinjer, og reflekteres i veiledning ovenfor sektoren.	Nasjonale føringer f.eks. for hendelseshåndtering.

Tiltak	Forslag til tiltakseier / involverte aktører	Grenseflater / overlappende tiltak
3.3 Etablere felles arenaer	Direktoratet for e-helse/ NHN. Store deler av sektoren må dekkes, som over.	
3.4 Kart over roller, systemeierskap og leverandører	HOD bør utpeke en tiltakseier.	
3.5 Nasjonal oversikt over kritisk infrastruktur	HOD bør utpeke en tiltakseier.	Utpeking ift. sikkerhetsloven, St m 9, NIS2
3.6 Overordnet plan for øvelser og forventning om systematisk arbeid med øvelser	HOD bør utpeke en tiltakseier.	Øvelser på nasjonalt nivå; JD og DSB.
3.7 Informasjonsdeling og erfaringsutveksling	E-helse, Norsk Helsenett v/HelseCERT	NIS2

A.4.2 Vurdering av kost og risiko ved gjennomføring av tiltak

Kostnadene for tiltakene forventes å være på et lavt og middels nivå, noe avhengig av ambisjonsnivået. Etablering av overordnet nasjonal IKT-beredskapsplan (3.1) og etablering av sammenheng mellom planverk (3.2) vil i stor grad kunne gjøres ved omprioritering av eksisterende ressurser, men krever samhandling og ressursbruk i flere virksomheter. Her vurderer vi forventet kostnad å være lav eller middels. Etablering av felles arenaer (3.3) kan gjøres ved omprioritering av eksisterende ressurser, både for etablering og deltakelse. Samtidig vil ambisjonsnivået slik det er beskrevet i innspillet (møtearenaer eller samarbeidsfora for systematisk og kontinuerlig arbeid med og fokus på digital beredskap) kunne kreve et høyere kostnadsnivå for å oppnå formålet. De resterende tiltakene (3.4 – 3.7) vil alle kreve at det gjøres et noe større arbeid, og forventet kostnad er derfor vurdert å være middels. Tiltak 3.6 vil i tillegg ha kostnader for virksomhetene i sektor i form av å delta på og gjennomføre øvelser. Her vil kostnad avhenge av omfang og hyppighet av øvelsene som blir gjennomført.

Tiltakene for planverk og øvelser forventes jevnt over å ha høy grad av støtte i sektoren. Klarere ansvarsforhold og bedre planverk og oversikter vil gjøre det lettere for virksomhetene i sektoren å vite hva egen rolle er i en IKT-beredskapssituasjon, og arenaer vil gi mulighet til å lære fra hverandre – noe vi opplever at virksomhetene i sektor er positive til.

Risikoen i gjennomføringen for tiltakene varierer i hele spekteret fra lav til høy. Tiltakene som omfatter nasjonal oversikt over kritisk infrastruktur (3.5), kartlegging av roller, systemeierskap og leverandører (3.4), samt overordnet plan for øvelser og forventning om systematisk arbeid med øvelser (3.6) antas å ha høyest grad av risiko, siden disse involverer mange aktører i sektoren. Etablering av felles arenaer (3.3) vurderes å ha lav risiko i gjennomføringen siden den kan etableres av en enkeltaktør, selv om suksess av tiltaket krever at mange fra sektor deltar i arenaen. Tiltak knyttet til informasjonsdeling og erfaringsutveksling (3.7) vil kreve mer involvering fra ulike aktører enn det å etablere felles arenaer, og vurderes dermed å ha middels risiko. Tiltak knyttet til planverk (3.1, 3.2) vurderes å ha middels risiko siden de krever involvering fra flere aktører.

Tiltak	Forventet kostnad	Antatt grad av støtte i sektoren	Risiko i gjennomføring
3.1 Overordnet nasjonal IKT-beredskapsplan	Lav/Middels	Høy	Middels
3.2 Sammenheng mellom planverk	Lav	Høy	Middels
3.3 Etablere felles arenaer	Lav/Middels	Høy	Lav
3.4 Kart roller, systemeierskap og leverandører	Middels	Høy	Middels/Høy
3.5 Nasjonal oversikt kritisk infrastruktur	Middels	Middels/Høy	Høy
3.6 Overordnet plan for øvelser og forventning om systematisk arbeid med øvelser	Middels	Middels	Middels/Høy
3.7 Informasjonsdeling og erfaringsutveksling	Middels	Middels/Høy	Middels

A.4.3 Vurdering av reduksjon av risiko knyttet til digital sikkerhet

Bidrag til å redusere sårbarhet	Læring fra øvelser kan lede til forbedringer i sikkerhetstiltakene og en bedre risikoforståelse.
Bidrag til å øke håndteringsevne	Klarere rolleforståelse, bedre og mer sammenhengende planverk, bedre oversikt, og bedre forberedelser gjennom øvelser vil øke håndteringsevnen.
Relasjon til risikobildet Verdi- og leverandørkjederisiko: X Avanserte trusler: X Kompetanse «i bredden»: X Spisskompetanse, inkl. ny teknologi: x Manglende grunnsikring: X *Tegnforklaring:* X *Vesentlig bidrag* x *Noe bidrag* v *Mulig indirekte bidrag*	Tiltakene forventes å forbedre evnen til å respondere på uønskede hendelser, inkludert hendelser hvor det er behov for koordinering på tvers av virksomheter. Deltakelse på og læring fra øvelser vil bidra til å øke risikoforståelse, også hos ledere. Kartlegging av sentrale leverandøravhengigheter er en del av innsatsområdet. Erfaringer fra øvelser, samt informasjons- og erfaringsutveksling mellom aktører, vil bidra positivt inn mot det øvrige sikkerhetsarbeidet.
Del av sektor	Avhengig av innretning kan innsatsområdet nå bredt i sektor. Imidlertid, siden de større virksomhetene i sektoren og de nasjonale tjenestene er de mest kritiske for samfunnet som helhet, så vil det være hensiktsmessig å prioritere disse.

A.5 Innsatsområde 4: Etterlevelse og oppfølging

NSM erfarer at de fleste cyberhendelser muliggjøres av manglende implementering av grunnleggende sikkerhetstiltak. Økt etterlevelse av sikkerhetskrav og implementering av

grunnleggende tiltak vil redusere risikoen for uønskede hendelser, og det er viktig at etterlevelsen følges opp. Dette er et sentralt område i den strategiske ledelsen og risikostyring av virksomhetene.

Helseforetakenes regionale handlingsplaner for informasjonssikkerhet og personvern inneholder allerede tiltak på området i form av egenkontroll og selvrapportering. I Helse Midt-Norge RHF planlegges det en gap-analyse som skal gi en oversikt over virksomhetens modenhet i forhold til NSMs grunnprinsipper, og som skal identifisere tiltak som må gjennomføres. I tillegg settes det i handlingsplanen fokus på forbedring av kontrolltiltak og rapportering på informasjonssikkerhet og personvern, for å sikre at ledelsen i foretaket har god kontroll.

Foreslåtte tiltak:

4.1 Tydelig forventning til virksomhetene

Det er viktig at grunnleggende sikkerhetskrav og -anbefalinger etterleves i sektoren, og at etterlevelsen følges opp av hver enkelt virksomhet. Tiltaket gjennomføres ved at det gjennom eksisterende styringslinjer stilles tydeligere krav til sektorens virksomheter om dette. Grunnleggende sikkerhetskrav omfatter bl.a. forventninger om at virksomheten følger kravene i Normen, NSMs grunnprinsipper for IKT-sikkerhet og NSM sine fem effektive tiltak mot dataangrep. Virksomhetene må ha en helhetlig tilnærming til sikkerhetsstyring. Det er derfor viktig at arbeidet med digital sikkerhet inngår som en integrert del av styringen av virksomhetene, der beslutningsansvaret er tydelig plassert hos ledelsen.

4.2 Felles tiltak for støtte og oppfølging

Det er et stort spenn i mulige virkemidler som kan benyttes for å støtte og følge opp etterlevelse. Disse spenner fra enkle verktøy virksomhetene kan velge å ta i bruk, til mer omfattende revisjons- og tilsynsvirksomhet. Dette tiltaket krever derfor nærmere kartlegging, utredning og planlegging, og tiltaket må gjennomføres trinnvis. Vi har derfor valgt å dele tiltaket i tre deltiltak:

- Kartlegging og utredning
- Utvikling av verktøy og veiledning som støtter arbeidet med egenkontroll
- Utvikle og styrke ordninger for ekstern kontroll av digital sikkerhet i virksomhetene.

Delaktivitetene er nærmere beskrevet under:

4.2 a Kartlegge og utrede

Tiltakets første steg er å gjennomføre en kartlegging av hvordan virksomhetene i sektoren i dag fører egenkontroll med og dokumenterer eget sikkerhetsarbeid. Kartleggingen kan omfatte momenter som styringssystem for informasjonssikkerhet, rapportering til ledelsen, sikkerhetsrevisjoner og behov for støtte på området.
I utredningsfasen vil resultatene av kartleggingen benyttes til å foreslå konkrete tiltak for støtte til virksomhetene, samt vurdere nærmere om det er hensiktsmessig å utvikle og styrke ordninger for kontroll av digital sikkerhet i sektoren.

4.2 b Støtte egenkontroll

Videre omfatter tiltaket utvikling av verktøy og veiledning som støtter virksomhetens kontroll av etterlevelse i form av egenkontroll og selvrapportering. Dette kan eksempelvis være dokumentasjon av samsvar med lovkrav (Normen), NSMs grunnprinsipper for IKT-sikkerhet og andre relevante kravsett. Tilgang til felles verktøy, metoder og veiledning vil understøtte virksomhetens egenevne til etterlevelse, men det er fortsatt virksomhetens selv som må definere hva som er forsvarlig praksis og gode tjenester.

4.2 c Utvikle og styrke kontroll
Tiltaket omfatter ordninger for eksternt tilsyn, kontroll og dokumentasjon av sikkerhetsarbeid i virksomhetene i helse- og omsorgssektoren. Dette inkluderer både styrking av eksisterende tilsynsordninger og utredning og videreutvikling av nye virkemidler. Også her vil det være et stort spenn i mulige tiltak: Gjensidige revisjoner av samhandlingsparter, styrket rapportering i eksisterende styringslinjer, ekstern revisjon opp mot standarder, monitoreringsorgan for Normen[19] og tilsyn er noen eksempler.
Tilsyn er et sterkt virkemiddel for å bedre etterlevelse. I dag er det lite kontroll av hvordan krav til digital sikkerhet i helse- og omsorgssektoren etterleves utover det som skjer i regi av Datatilsynet og Helsetilsynet. Det vil åpnes for etablering av sektortilsyn innen digital sikkerhet når lov om digital sikkerhet vedtas og NIS-direktivet innføres i norsk rett. En forutsetning for gode tilsynsordninger er at det eksisterer nødvendige lovhjemler, tilsynsgrunnlag og tilsynskompetanse.

Området er komplekst og videre utredning er nødvendig.

4.3 Sammenstille og samordne
Et poeng om veiledning og verktøy for digital sikkerhet som påpekes særlig fra kommunal side, er at det kan være vanskelig å navigere i og få oversikt over alle de ulike nasjonale virkemidlene, hjelpemidlene og samarbeidsnettverkene. Dersom disse i større grad sammenstilles, vil det lette arbeidet med digital sikkerhet betydelig og gjøre arbeidet mer effektivt.

Dette området er belyst i Riksrevisjonens undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.[20] Der pekes det på at det er mange ulike regelverk som stiller krav til digital sikkerhet i den enkelte virksomhet. Regelverkene overlapper og er lite harmonisert. Myndighetenes veiledning er heller ikke koordinert og de som gjør tilsyn er lite samordnet.

Det forventes at det som resultat av Riksrevisjonens undersøkelse vil skje flere sentrale, sektorovergripende tiltak på området. Vår anbefaling er at vår sektor bidrar i gjennomføring av tiltakene der det er naturlig, og ellers sørger for at veiledning som utarbeides i sektoren (f.eks. i regi av Normen) er synkronisert med nasjonale virkemidler, hjelpemidler og samarbeidsnettverk». Dette har vært en rettesnor for arbeidet med Normen i lengre tid. Direktoratet for e-helse deltar også aktivt i Nettverk for veiledningsaktører innen informasjonssikkerhet i regi av Digitaliseringsdirektoratet.

4.4 Krav om oversikt over effekt av tiltak
Ved å måle effekten av iverksatte tiltak legges det til rette for mer målrettede, konkrete og effektive tiltak i fremtiden. Tiltakseier bør derfor ha oversikt over effekten av tiltakene de er ansvarlige for.

Riksrevisjonens undersøkelse av myndighetenes samordning på området understøtter behovet for å måle effekt av tiltak. Riksrevisjonen peker bl.a. på at man ikke har hatt grunnlag for å løpende vurdere effekt av tiltakene i den Nasjonale strategien for digital sikkerhet.

[19] I styringsgruppen for Normen har det vært diskutert å etablere Normen som en atferdsnorm etter personvernforordningens artikkel 40. Dette vil kreve at det utpekes et monitoreringsorgan som følger opp etterlevelse av adferdsnormen, jf. artikkel 41.
[20] Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor. Dokument 3:7 (2022–2023). Riksrevisjonen.

Det er derfor viktig at sektorens tiltakseiere sørger for å få oversikt over effekt av tiltakene som iverksettes for å styrke digital sikkerhet gjennom kvalitative og kvantitative evalueringer. Dette vil legge grunnlaget for kontinuerlig forbedring gjennom mest mulig effektive tiltak.

Det bør utvikles målindikatorer for målene som er beskrevet i kapittel 1.1.1.

I forbindelse med sikkerhetstiltak på nasjonalt eller tverrsektorielt nivå der vår sektor er involvert, bør prosessene påvirkes og understøttes slik at det legges vekt på vurdering av effekt av tiltak.

A.5.1 Realisering av innsatsområder og tiltak

Figuren viser en mulig plan for gjennomføring av tiltakene innenfor satsningsområdet:

Realisering av innsatsområdet bør begynne med å stille tydelige forventinger til oppfølging og etterlevelse. I parallell med tydelige krav gjøres en aktivitet som omfatter kartlegging og utredning. Et neste steg er at det utarbeides et sett med verktøy som støtter selvrapportering av etterlevelse innen digital sikkerhet og ordninger for kontroll og dokumentasjon av sikkerhetsarbeidet. Andre tiltak som er relevante for å realisere innsatsområdet er tiltak som å sammenstille og samordne nasjonale virkemidler, hjelpemidler og samarbeidsnettverk og å stille krav om at tiltakseiere på nasjonalt nivå skaffer oversikt over tiltakenes effekt. Disse kan iverksettes umiddelbart.

Kartleggingen kan med fordel gjentas jevnlig for å sikre oppdatert kunnskap.

Nærmere om gjennomføring av tiltakene:

Tiltak	**Forslag til tiltakseier / involverte aktører**	**Grenseflater / overlappende tiltak**
4.1 Tydelig forventning til virksomhetene	Tiltakseier: Krav stilles av relevante myndighetsaktører gjennom vedtatte styringslinjer og reflekteres i veiledning overfor sektoren.	

	Involverte aktører: Hele sektoren, med fokus på virksomhetenes ledelse	
4.2 a Kartlegge og utrede	Tiltakseier: Direktoratet for e-helse Involverte aktører: Store deler av sektoren	Oppfølging av mindre virksomheter
4.2 b Støtte egenkontroll	Tiltakseier: Direktoratet for e-helse Involverte aktører: Store deler av sektoren	Oppfølging av mindre virksomheter, Normen
4.2 c Utvikle og styrke kontroll	Tiltakseier: Helsetilsynet, Norsk Helsenett, Datatilsynet, Normens styringsgruppe m.fl. Involverte aktører: Store deler av sektoren	
4.3 Sammenstille og samordne	Tiltakseier: Beslutning gjøres sentralt og implementeres gjennom vedtatte styringslinjer. Involverte aktører: Hele sektoren, med fokus på virksomhetenes ledelse	
4.4 Krav om oversikt effekt tiltak	Tiltakseier: Rapportering gjennom vedtatte styringslinjer. Involverte aktører: Hele sektoren, med fokus på virksomhetenes ledelse	

A.5.2 Vurdering av kost og risiko ved gjennomføring av tiltak

Tiltakene som omfatter å stille forventinger til sektoren (4.1) og kartlegge sektoren (4.2 a) vil kreve relativt lite ressurser på myndighetssiden, og vil kunne gjennomføres innenfor eksisterende ressurser, eller ved en omprioritering av ressurser. Imidlertid vil det å stille forventninger kunne lede til kostnader for sektor. Vi har satt forventet kostnad til middels. Utvikling og forvaltning av nye verktøy og ordninger for kontroll og tilsyn (4.2 b, c) vil kreve bredt sammensatt kompetanse og vil sannsynligvis innebære middels (4.2 b) til høyt (4.2 c) kostnadsnivå, avhengig av innretning. Sammenstilling og samordning av nasjonale virkemidler (4.3) vurderes å ha lav kostnad, siden det er et arbeid som allerede pågår innenfor dagens ressurser. Krav om oversikt over effekt av tiltak (4.4) forventes å ha et middels kostnadsnivå siden det vil kreve ressurser å utvikle og benytte måleindikatorer.

Sammenstilling og samordning (4.3) er et uttalt ønske fra sektor, og antas å ha høy støtte. De andre tiltakene vurderes til å ha lav til middels støtte. Det kan oppleves som ressurskrevende å etterleve krav til rapportering og dokumentasjon av etterlevelse.

Det å etablere tilsyn/kontroll på området (4.2 c) vurderes å ha høy risiko. Dette er et nytt og relativt inngripende tiltak som vil involvere flere aktører fra sektoren, inkludert mulige endringer i krav og mandat. Det å utvikle støtte for egenkontroll (4.2 b) vurderes imidlertid å

ha lav risiko siden dette kan gjøres ut fra dagens regelverk og veiledning. Når det gjelder sammenstilling og samordning av nasjonale virkemidler (4.3) så er dette i utgangspunktet et tverrsektorielt tiltak, noe som øker risikoen. Imidlertid anser vi det som liten risiko å bidra til mer samordning som del av det pågående veiledningsarbeidet. De resterende tiltakene vurderes å ha middels risiko, siden de krever involvering fra virksomheter i sektor.

Tiltak	Forventet kostnad	Antatt grad av støtte i sektoren	Risiko i gjennomføring
4.1 Tydelig forventning til virksomhetene	Middels	Lav/middels	Middels
4.2 a Kartlegge og utrede	Middels	Middels	Middels
4.2 b Støtte egenkontroll	Middels	Middels	Lav
4.2 c Utvikle og styrke kontroll	Høyt	Lav/middels	Høy
4.3 Sammenstille og samordne	Lavt	Høyt	Lav
4.4 Krav om oversikt effekt tiltak	Middels	Middels	Middels

A.5.3 Vurdering av reduksjon av risiko knyttet til digital sikkerhet

Bidrag til å redusere sårbarhet	Det er manglende etterlevelse (i deler av sektor) i dag, og styrket etterlevelse vil gi redusert sårbarhet.
Bidrag til å øke håndteringsevne	Etterlevelse av tiltak knyttet til deteksjon, håndtering og gjenoppbygging vil øke håndteringsevnen.
Relasjon til risikobildet Verdi- og leverandørkjederisiko: x Avanserte trusler: x Kompetanse «i bredden»: x Spisskompetanse, inkl. ny teknologi: v Manglende grunnsikring: X X *Vesentlig bidrag* x *Noe bidrag* v *Mulig indirekte bidrag*	Dette innsatsområdet er rettet mot å redusere risiko knyttet til manglende implementering av grunnleggende sikkerhetstiltak. Bedre oppfølging og etterlevelse vil igjen gjøre virksomhetene mer motstandsdyktige mot digitale angrep. Etterlevelse av grunnleggende sikkerhetskrav som Normen og NSMs grunnprinsipper for IKT-sikkerhet vil gi redusert risiko på områdene som tematisk dekkes av krav og anbefalinger.
Del av sektor	Kan rettes mot både større og mindre virksomheter, basert på resultat fra kartlegging og utredning. Antar at behovet er størst i virksomheter som har få egne sikkerhetsressurser. Kommunene vil spesielt tjene på sammenstilling og samordning av veiledning.

A.6 Innsatsområde 5: Ny teknologi og digitale verdikjeder

Ny teknologi vil ha stor betydning for den fremtidige helsetjenesten, men kan også skape større avhengighet til leverandører og gir lange og komplekse digitale verdikjeder. Å ivareta

god beredskap i slike verdikjeder stiller nye krav til sektorens virksomheter, og arbeidet må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring.

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

5.2 DSBs modell for risikostyring i digitale verdikjeder inn i relevante veiledere
Styring av risiko ved utvikling og bruk av ny teknologi, tjenester og samhandlingsformer krever gode rutiner for vurdering, innføring og oppfølging. Risikovurdering av digitale verdikjeder som går på tvers av virksomheter og landegrenser er kompetansekrevende, og virksomhetene i sektoren vil kunne ha nytte av støtte i dette arbeidet.

5.3 Bedre innføringsstøtte ved ny teknologi
Tiltaket vil legge til rette for bedre støtte til vurdering, innføring og utvikling av ny teknologi i samarbeid med relevante fag- og veiledningsmiljøer i og utenfor sektoren. Dette inkluderer utarbeidelse av veiledningsmateriell, opplæringsaktiviteter, etablering av sandkasser og lignende.

5.4 Samarbeid ved anskaffelser, kravstilling og oppfølging av leverandører
Tiltaket vil legge til rette for samarbeid ved anskaffelser, og ved kravstilling og oppfølging av leverandører. Nettverk og fagforum, interkommunale samarbeid, veiledning og utarbeidelse av felles kravspesifikasjoner kan være måter å gjøre dette på. Økt samarbeid og støtte til virksomheter i anskaffelsesprosesser kan medføre mer effektiv tidsbruk og høyere kvalitet i anskaffelser og oppfølging av leverandører.

A.6.1 Realisering av innsatsområder og tiltak

Figuren viser en mulig plan for gjennomføring av tiltakene innenfor satsningsområdet:

Tiltakene som gjelder å kommunisere forventninger om tilpasning av beredskapsplanverk samt innfasing av DSB-modellen for risikostyring i relevant veiledningsmateriale kan gjøres umiddelbart, f.eks. ved at Direktoriet for e-helse fremmer en sak til styringsgruppen for Normen.

Tiltakene 5.3 og 5.4 er mer omfattende, og vil antakelig måtte gjennomføres i flere faser. Mulige synergieffekter mot helseteknologiordningen bør utforskes.

Nærmere om gjennomføring av tiltakene:

Tiltak	**Forslag til tiltakseier / involverte aktører**	**Grenseflater / overlappende tiltak**
5.1 Forventning om tilpasning beredskapsplanverk nye leveransemodeller	Kravstilling gjennom Normen: Direktoratet for e-helse fremmer forslag. Involverte/målgruppe: Hele sektoren	
5.2 DSBs modell for risikostyring i digitale verdikjeder inn i relevante veiledere	Kravstilling gjennom Normen: Direktoratet for e-helse fremmer forslag Involverte/målgruppe: Hele sektoren	
5.3 Bedre innføringsstøtte ved ny teknologi	Flere aktuelle tiltakseiere. Involverte/målgruppe: Hele sektoren	Helseteknologiordningen, tverretatlig veiledningstjeneste for kunstig intelligens.[21]
5.4 Samarbeid ved anskaffelser, kravstilling og oppfølging av leverandører	Flere aktuelle tiltakseiere. Involverte/målgruppe: Hele sektoren	Helseteknologiordningen

A.6.2 Vurdering av kost og risiko ved gjennomføring av tiltak

Tiltak knyttet til å stille forventninger til sektor (5.1) og å innarbeide DSBs modell i relevante veiledere (5.2) vil kreve relativt lite ressurser på myndighetssiden, og vil kunne gjennomføres innenfor eksisterende ressurser, eller ved en omprioritering av ressurser. Det å stille forventninger vil kunne lede til kostnader for sektor. Disse har likevel lav forventet kostnad. Det er forventet middels/høy kostnad for tiltakene som ikke kun innebærer å stille forventninger til sektor (5.3, 5.4), avhengig av ambisjonsnivå. Spesielt vil det kreve ressurser å etablere sandkasser og/eller økt støtte til virksomheter ved anskaffelser. Det er forventet et middels investeringsbehov tilknyttet å utvikle et standardisert kravsett for anskaffelser og et selvdeklareringsskjema for leverandører, samt middels årlige kostnader for å forvalte kravsettene. En eventuell videreutvikling av selvdeklareringsordningen til en sertifiseringsordning vil kreve bredt sammensatt kompetanse (juss (særlig innen EU-rettslige problemstillinger), sikkerhet, samfunnsøkonomisk analyse, standardisering osv.) og vil sannsynligvis innebære en middels til høy kostnad. Merk at for virksomhetene i sektor kan disse tiltakene føre til reduserte kostnader.

Det antas at tiltak som forenkler anskaffelser og innføring av ny teknologi (5.3, 5.4) vil bli godt tatt imot i sektoren, mens støtten knyttet til forventningsstilling og veiledning (5.1, 5.2) vurderes til å være noe lavere.

Tiltak knyttet til bedre innføringsstøtte og økt samarbeid (5.3, 5.4) vil måtte involvere mange aktører fra sektoren. Dette øker risikoen. Det er imidlertid lav risiko knyttet til å stille forventninger og å oppdatere veiledning (5.1, 5.2)

[21] Tverretatlig veiledningstjeneste, Helsedirektoratet

Tiltak	Forventet kostnad	Antatt grad av støtte i sektoren	Risiko i gjennomføring
5.1 Forventning om tilpasning beredskapsplanverk nye leveransemodeller	Lav	Middels	Lav
5.2 DSBs modell for risikostyring i digitale verdikjeder inn i relevante veiledere	Lav	Middels	Lav
5.3 Bedre innføringsstøtte ved ny teknologi	Middels/høyt	Høy	Middels/høyt
5.4 Samarbeid ved anskaffelser, kravstilling og oppfølging av leverandører	Middels/høyt	Høy	Middels/høyt

A.6.3 Vurdering av reduksjon av risiko knyttet til digital sikkerhet

Bidrag til å redusere sårbarhet	Redusert sårbarhet ved innføring av ny teknologi. Bedre oppfølging av digital sikkerhet i verdikjeder.
Bidrag til å øke håndteringsevne	Bedre i stand til å håndtere hendelser i digitale verdikjeder, og som er knyttet til ny teknologi.
Relasjon til risikobildet Verdi- og leverandørkjederisiko: X Avanserte trusler: x Kompetanse «i bredden»: v Spisskompetanse, inkl. ny teknologi: X Manglende grunnsikring: x *Tegnforklaring:* X *Vesentlig bidrag* x *Noe bidrag* v *Mulig indirekte bidrag*	Dette innsatsområdet er spesielt innrettet mot å møte risiko knyttet til ny teknologi og leverandørkjeder. Bedre støtte knyttet til ny teknologi kan også bidra til at sektoren tar i bruk nyere systemer, og disse har ofte også bedre sikkerhet. En del av de avanserte truslene er knyttet til ny teknologi som kunstig intelligens, og tiltak innen dette innsatsområdet kan bidra til tryggere digitalisering som gjør sektorens virksomheter bedre rustet også mot avanserte trusler knyttet til slik teknologi. Veiledning på området vil også bidra til viktige avklaringer rundt roller og ansvar i et komplekst landskap.
Del av sektor	Tiltak kan rettes mot ulike deler av sektoren.

A.7 Innsatsområde 6: Støtte til mindre virksomheter

For å øke sektorens totale beredskapsevne i et skjerpet trusselbilde må den digitale sikkerheten styrkes også i de mindre virksomhetene. I sektoren er det mange små og mellomstore virksomheter som legekontor, psykologpraksiser og tannlegekontor. Alle virksomheter har et ansvar for å ivareta sin egen digitale sikkerhet, og ofte har mindre virksomheter begrenset tilgang på kompetanse og kapasitet innen digital sikkerhet, og få muligheter til å bruke mer tid på ikke-kliniske oppgaver.

De mindre virksomhetene må hver for seg bruke tid og ressurser på å utføre sammenliknbare oppgaver innen digital sikkerhet. Dette inkluderer sikkerhetsstyring i egen virksomhet, gjennomføring av risikovurderinger og oppgaver knyttet til teknisk IKT-sikkerhet.

6.1 Kartlegge sikkerhetstilstanden og -behov i de mindre virksomhetene i sektoren.
Direktoratet for e-helse anbefaler at det gjennomføres en undersøkelse blant mindre helsevirksomheter (fastleger, tannlegekontorer o.l.) for å avdekke sikkerhetstilstand og -behov hos disse. Formålet med undersøkelsen vil være å skaffe kunnskapsgrunnlag om hvilke behov mindre helsevirksomheter har for veiledning, tjenester for å oppnå et forsvarlig sikkerhetsnivå og løsninger som kan understøtte de mindre virksomhetenes driftssikkerhet. Undersøkelsen kan omfatte momenter som styringssystem for informasjonssikkerhet, hvem som utfører sikkerhets- og driftsoppgaver for mindre helsevirksomheter, kompetansebehov og vurdering av risiko. De mindre virksomhetenes kapasitet til å avdekke og håndtere sikkerhetshendelser bør inngå som en del av kartleggingen.

6.2 Utrede mulige felles ordninger og tjenester som vil gi verdi for bredden av mindre virksomheter
Basert på avdekkede behov bør det i etterkant av undersøkelsen utredes og iverksettes effektive tiltak for å bedre virksomhetenes egenevne til å levere tjenester på en sikker og trygg måte.

A.7.1 Realisering av innsatsområder og tiltak

Figuren viser en mulig plan for gjennomføring av tiltakene innenfor satsningsområdet:

Realisering av innsatsrådet bør begynne med en kartlegging av sikkerhetstilstanden og sikkerhetsbehovene hos de mindre virksomhetene i sektoren (fastleger, tannlegekontorer o.l.). Basert på denne kartleggingen bør man deretter utrede mulige felles ordninger som vil gi verdi for bredden av mindre virksomheter. Deretter kan man, med utgangspunkt i utredningen, iverksette identifiserte tiltak for å bedre virksomhetenes egenevne til å levere tjenester på en sikker og trygg måte.

Kartleggingen kan med fordel gjentas jevnlig for å sikre oppdatert kunnskap.

Nærmere om gjennomføring av tiltakene:

Tiltak	**Forslag til tiltakseier/involverte aktører / målgruppe**	**Grenseflater/ overlappende tiltak**
6.1 Kartlegging	Tiltakseier: Direktoratet for e-helse	En eventuell kartlegging og videre utredning vil kunne ses i sammenheng med de foreslåtte tiltakene under innsatsområde 2: kompetanse og sikkerhetskultur. Det vil kunne være hensiktsmessig å gjennomføre disse tiltakene i parallell. Det vil for eksempel være unaturlig å gjennomføre

		kartlegging av sikkerhetstilstanden i de mindre virksomhetene uten å også kartlegge sikkerhetskompetanse og sikkerhetskultur. Motsatt vil det være lite effektivt å gjennomføre tiltakene under innsatsområde 2 uten å legge egen vekt på tilstanden i de mindre virksomhetene.
6.2 Utredning	Tiltakseier: Direktoratet for e-helse	

A.7.2 Vurdering av kost og risiko ved gjennomføring av tiltak

Kartlegging og utredning (6.1, 6.2) er avgrensede oppgaver som i stor grad kan gjøres ved omprioritering av eksisterende ressurser. Samtidig krever det ressurser både fra de som gjennomfører kartlegging/utredning og fra sektor som kartlegges. Området som skal kartlegges/utredes er preget av mange små aktører og å få involvert disse i tilstrekkelig grad kan være krevende. Derfor vurderes forventet kostnad å være middels. Merk at eventuelle tiltak som kommer etter utredning kan ha høyere kostnad.

Vi opplever at det er høy støtte i sektor til å støtte små virksomheter bedre, men det kan være mindre grad av støtte når det kommer til å delta i kartlegging/utredning.

Kartlegging og utredning vil kreve involvering i sektor, og det kan bli krevende å få tilstrekkelig med innspill fra de små virksomhetene. Dette innebærer en middels til høy risiko for gjennomføringen.

Tiltak	**Forventet kostnad**	**Antatt grad av støtte i sektoren**	**Risiko i gjennomføring**
6.1 Kartlegging	Middels	Høy	Middels/høy
6.2 Utredning	Middels	Høy	Middels

A.7.3 Vurdering av reduksjon av risiko knyttet til digital sikkerhet

Bidrag til å redusere sårbarhet	Redusert sårbarhet hos en stor mengde mindre virksomheter.
Bidrag til å øke håndteringsevne	Bedre evne hos de små virksomhetene til å oppdage og håndtere hendelser.
Relasjon til risikobildet Verdi- og leverandørkjederisiko: x Avanserte trusler: x Kompetanse «i bredden»: X Spisskompetanse, inkl. ny teknologi: v Manglende grunnsikring: X	Effekt vil avhenge av hvilke behov og tiltak som iverksettes etter kartlegging og utredning. Det forventes at tiltak vil bidra til bedre grunnsikring i de mindre virksomhetene, samt bedre kompetanse om digital sikkerhet i disse virksomhetene. Leverandører er spesielt viktige for de mindre virksomhetene, siden disse ofte har bedre sikkerhetskompetanse enn de mindre virksomhetene har selv. Tiltakene vil kunne bidra til å

Tegnforklaring: X *Vesentlig bidrag* x *Noe bidrag* v *Mulig indirekte bidrag*	styrke de mindre virksomhetene i sine relasjoner til leverandører. Samlet sett vil bedre sikkerhet i de mindre virksomhetene redusere risiko i sektoren, inkludert risiko for at mindre virksomheter blir en angrepsvei inn til større virksomheter og nasjonale tjenester.
Del av sektor	Tiltak er rettet mot de mindre virksomhetene i sektor.

Vedlegg B Vurdering av måloppnåelse

Som del av å vurdere nytte av innsatsområdene, har Direktoratet gjort en vurdering av i hvilken grad hvert enkelt innsatsområde bidrar til henholdsvis mål for digital sikkerhet og beredskap i helse- og omsorgssektoren, samt målene i den nasjonale e-helsestrategien for helse- og omsorgssektoren. I dette vedlegget gir vi en nærmere beskrivelse av disse målene, og presenterer Direktoratets vurdering av hvordan de ulike innsatsområdene bidrar til å nå disse målene.

B.1 Vurdering av måloppnåelse knyttet til Mål for digital sikkerhet og beredskap i helse- og omsorgssektoren

Følgende mål er beskrevet i Direktoratets innspill til den kommende helseberedskapsmeldingen:

Virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder.
Alle virksomheter har et ansvar for egen digital sikkerhet og helseberedskap. Gjennom en risikobasert tilnærming må det sørges for nødvendig egenevne til å overvåke, oppdage, håndtere og beskytte seg mot digitale hendelser. Det er mange likheter mellom virksomhetene i deres oppgaver og utfordringer knyttet til digital sikkerhet, uavhengig av virksomhetens størrelse. Sektoren består av mange små virksomheter som i liten grad kan bygge opp egen IKT-sikkerhetskompetanse. Felles tjenester og ressurser kan gi gevinster både i kvalitet, kostnader og tidsbruk.

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

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

Det er høy tillit fra innbyggere og pasienter til hvordan sektoren ivaretar digital sikkerhet. Godt og systematisk sikkerhetsarbeid i sektoren bidrar til å bygge tillit hos innbyggere og pasienter. Noen områder kan være av særlig betydning. Dette omfatter bl.a. håndtering av sikkerhetshendelser, hvordan sikkerheten i digitale innbyggerløsninger framstår, og at det er tilstrekkelig åpenhet om sektorens arbeid med digital sikkerhet. Det er nødvendig at innbyggerne både har tillit til at helseopplysninger er sikret mot tilgang fra

uvedkommende og at helseopplysningene er tilgjengelig for helsepersonell som trenger tilgang.

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

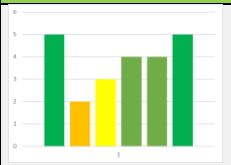
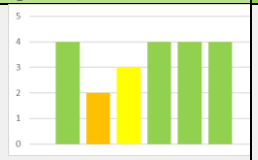
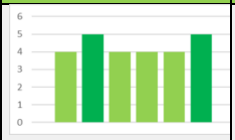
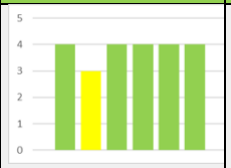
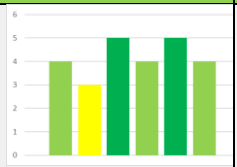
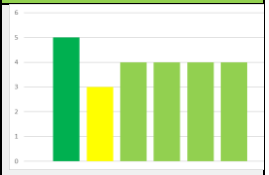
Trusler, teknologi og relasjoner som sektorens virksomheter opererer i, endrer seg raskt. Trygg og effektiv innovasjon oppnås ved å sørge for god digital sikkerhet samtidig som en utnytter mulighetene teknologien gir for å utvikle bedre tjenester. Virksomheter må være i stand til å vurdere sikkerhet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

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

Virksomhetene i sektoren må være i stand til å forebygge, avdekke, varsle og håndtere enhver form for IKT-hendelse som truer evnen til å levere helse- og omsorgstjenester, pasientsikkerheten og skjerming av sensitiv helseinformasjon. Det er nødvendig med gode risikovurderinger, tiltak for å avdekke, begrense og stanse alvorlige IKT-sikkerhetshendelser, samt evne til å gjenopprette sikker tilstand for berørte systemer etter hendelser.

Etterfølgende tabell viser hvordan Direktoratet vurderer at innsatsområdene vil bidra til å oppnå disse målene.

Mål fra direktoratets innspill til helseberedskapsmelding:	Videreutvikling av eksisterende nasjonale virkemidler (Normen, HelseCERT)	Kompetanse og sikkerhetskultur	Planverk og øvelser	Etterlevelse og oppfølging	Ny teknologi og digitale verdikjeder	Støtte til mindre virksomheter
Virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder	Fulltreffer (5) Normen og HelseCERT er svært sentrale virkemidler for å støtte sektorens virksomheter	I stor grad (4) God sikkerhetskultur understøtter robusthet	I stor grad (4) Planverk og øvelser er viktig for virksomhetens egenevne	I stor grad (4) Vil kunne bidra til å avdekke mangler	I stor grad (4) Vil kunne være et viktig bidrag til virksomhetene innenfor området	Fulltreffer (5) Normen og HelseCERT er svært sentrale virkemidler for å støte sektorens virksomheter
Ansvar og roller med betydning for digital sikkerhet i og mellom sektorens virksomheter er avklart, kjent og ivaretatt	Litt (2) Normen kan bidra til å bevisstgjøre om ansvar, men i liten grad avklare ansvar	Litt (2) Kompetansetiltak kan bidra til å bevisstgjøre om ansvar, men i liten grad avklare ansvar	Fulltreffer (5) Gjennom planverk og øvelser kan ansvar både plasseres og mangler avdekkes	Middels (3) Det kan kontrolleres at roller er på plass, og at ansvar er forstått	Middels (3) Tiltaket kan bidra til ansvars-avklaringer mot leverandører	Middels (3) Tiltaket kan bidra til å bevisstgjøre små virksomheter om sitt ansvar
Sektoren ivaretar sikkerhet i lange og komplekse digitale verdikjeder.	Middels (3) Normen kan veilede på området	Middels (3) Kompetansetiltak kan veilede på området	I stor grad (4) Tilpasning av planverk opp mot lange leveransekjeder	I stor grad (4) Vil kunne bidra til å avdekke mangler	Fulltreffer (5) 'Skreddersydde' tiltak til målet	I stor grad (4) Tiltaket kan gi god støtte innenfor et vanskelig område
Det er høy tillit fra innbyggere og pasienter til hvordan sektoren ivaretar digital sikkerhet	I stor grad (4) Bidrar positivt til digital sikkerhet -> tillitsbyggende	I stor grad (4) Bidrar positivt til digital sikkerhet -> tillitsbyggende	I stor grad (4) Bidrar positivt til digital sikkerhet -> tillitsbyggende	I stor grad (4) Bidrar positivt til digital sikkerhet -> tillitsbyggende	I stor grad (4) Bidrar positivt til digital sikkerhet -> tillitsbyggende	I stor grad (4) Bidrar positivt til digital sikkerhet -> tillitsbyggende
Virksomhetene evner å effektivt ta i bruk nye teknologier på en sikker måte og er robuste i møte med et risikobilde i endring	I stor grad (4) Veiledning er et viktig virkemiddel på området	I stor grad (4) Kompetansetiltak er et viktig virkemiddel på området	I stor grad (4) Planverk og øvelser er viktige for robusthet	I stor grad (4) Vil kunne bidra til å avdekke mangler	Fulltreffer (5) 'Skreddersydde' tiltak til målet	I stor grad (4) Tiltaket kan gi god støtte innenfor et vanskelig område

Mål fra direktoratets innspill til helseberedskapsmelding:	**Videreutvikling av eksisterende nasjonale virkemidler (Normen, HelseCERT)**	**Kompetanse og sikkerhetskultur**	**Planverk og øvelser**	**Etterlevelse og oppfølging**	**Ny teknologi og digitale verdikjeder**	**Støtte til mindre virksomheter**
Virksomhetene i sektoren har høy bevissthet om sårbarheter og trusler, og er forberedt og øvet på å avdekke og effektivt håndtere ekstraordinære IKT-hendelser	Fulltreffer (5) Normen og HelseCERT er svært sentrale virkemidler for å støte sektorens virksomheter	I stor grad (4) God sikkerhetskultur understøtter robusthet	Fulltreffer (5) 'Skreddersydde' tiltak til målet	I stor grad (4) Vil kunne bidra til å avdekke mangler	I stor grad (4) Vil kunne bidra til å avdekke mangler	I stor grad (4) Tiltaket kan gi god støtte innenfor et vanskelig område
Gjennomsnitt:	I stor grad (3,8)	Middels / I stor grad (3,5)	I stor grad (4.3)	I stor grad (3,8)	I stor grad (4,1)	I stor grad (3,6)
Oppsummering i søylediagram:						

B.2 Vurdering av måloppnåelse knyttet til Nasjonal e-helsestrategi for helse- og omsorgssektoren, Strategiske mål for digitalisering.

Nasjonal e-helsestrategi fra januar 2023 er helse- og omsorgssektorens felles strategi for digitalisering, og skal bidra til felles overordnede prioriteringer og økt gjennomføringsevne på e-helseområdet i Norge. Strategien beskriver at digital sikkerhet er en forutsetning for målene i denne strategien. Det bør derfor være mulig å identifisere sammenhenger mellom innsatsområdene innen digital sikkerhet og hvordan de kan påvirke de strategiske målene i nasjonale e-helsestrategi positivt. En slik vurdering er gjengitt i kapittel tre. De strategiske målene er:

Aktiv medvirkning i egen og næres helse
Digitale helse- og omsorgstjenester skal tilrettelegge for at innbyggere og pårørende, uavhengig av sosial bakgrunn, enkelt kan involvere seg i forebygging, behandling og oppfølging av egen og næres helse og mestring. Når, hvor og hvordan helse- og omsorgstjenester utføres skal i større grad tilpasses innbyggers behov. Dette vil bidra til bedre utnyttelse av kompetanse og kapasitet

Enklere arbeidshverdag
Helsepersonell skal ha tilgang til nødvendig informasjon og brukervennlige digitale arbeidsverktøy som gir god beslutningsstøtte og støtter og videreutvikler deres arbeidsprosesser. Dette vil bidra til styrket pasientsikkerhet, reduksjon i uønsket variasjon og en mer attraktiv arbeidssituasjon for helsepersonell.

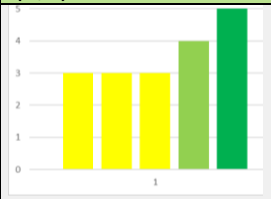
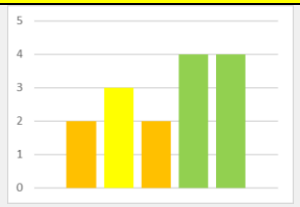
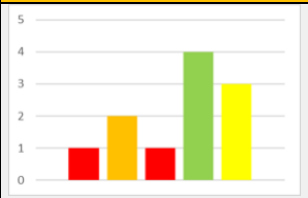
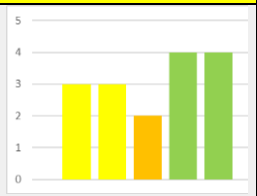
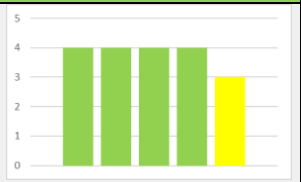
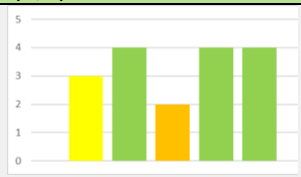
Helsedata til fornying og forbedring
Helse- og omsorgstjenestene, helsepersonell og helseforvaltningen skal i økende grad ta beslutninger basert på data. Mer datadrevne beslutninger vil bidra til bedre ressursutnyttelse, økt kvalitet og innovasjon i tjenesten, samt bedre forskning, helseovervåkning og folkehelse. Det vil også gjøre sektoren bedre forberedt i møte med kriser.

Tilgjengelig informasjon og styrket samhandling
Digital samhandling, styrket informasjonsforvaltning og økt standardisering skal sørge for at oppdaterte helseopplysninger er sikre, av god kvalitet og lett tilgjengelig ved behov. Dette vil legge til rette for en mer aktiv innbygger, bedre og mer effektiv helsehjelp samt bedre datanalyser til kvalitetsforbedring, helseovervåkning og styring.

Samarbeid og virkemidler som styrker gjennomføringskraften
Gjennomføringskraften på e-helseområdet skal styrkes gjennom økt samarbeid og bedre bruk av virkemidler som regelverk og finansieringsmodeller. Dette vil gi en samordnet og helhetlig e-helseutvikling som gir gode og bærekraftige helse- og omsorgstjenester.

Etterfølgende tabell viser hvordan Direktoratet vurderer at innsatsområdene vil bidra til å oppnå disse målene.

Strategiske mål fra nasjonal e-helsestrategi	Videreutvikling av eksisterende nasjonale virkemidler (Normen, HelseCERT)	Kompetanse og sikkerhetskultur	Planverk og øvelser	Etterlevelse og oppfølging	Ny teknologi og digitale verdikjeder	Støtte til mindre virksomheter
Aktiv medvirkning i egen eller næres helse	Middels (3) Normen vil kunne gi veiledning innen områder med noe betydning for målet	Litt (2) Enkelte relevante kompetansetiltak	Ubetydelig (1) Vil ha liten betydning	Middels (3) Oppfølging av sikring av f.eks. DHO	I stor grad (4) Målrettet tiltak inn mot f.eks sikring av DHP	Middels (3) Tiltaket kan gi noe støtte innen området
Enklere arbeidshverdag	Middels (3) Normen gir veiledning innen områder med noe betydning for målet	Middels (3) Relevante kompetansetiltak	Litt (2) Tilgjengelighet til EPJ	Middels (3) Oppfølging av relevante sikkerhetstiltak	I stor grad (4) Målrettet tiltak	I stor grad (4) Tiltaket kan gi god støtte innen området til små virksomheter
Helsedata til fornying og forbedring	Middels (3) Flere relevante veiledningstiltak i Normen Generelt vil også god digital sikkerhet som følge av etterlevelse av Normen og tjenestene fra HelseCERT bidra til at helsedata av god kvalitet er tilgjengelig fra virksomhetene.	Litt (2) Enkelte relevante kompetansetiltak	Ubetydelig (1) Vil ha liten betydning	Litt (2) Generelt vil også god digital sikkerhet som følge av etterlevelse av grunnleggende sikkerhetstiltak bidra til at helsedata av god kvalitet er tilgjengelig fra virksomhetene.	I stor grad (4) Sikker innføring og bruk av ny teknologi gir gode kilder til helsedata, for eksempel sensorteknologi. Kunstig intelligens tar i bruk helsedata til fornying og forbedring.	Litt (2) En god grunnsikring medvirker til tilgjengelige helsedata av god kvalitet fra små virksomheter
Tilgjengelig informasjon og styrket samhandling	I stor grad (4) HelseCERT bidrar sterkt til en tilgjengelig samhandlingsinfrastruktur. Normen som felles sikkerhetskrav er viktig for samhandling	I stor grad (4) God sikkerhetskultur understøtter robusthet	I stor grad (4) Robusthet og tilgjengelig informasjon	I stor grad (4) Robusthet og tilgjengelig informasjon	I stor grad (4) Sikring av ny teknologi viktig for tilgjengelig informasjon	I stor grad (4) Styrking av sikkerhet hos små vikromheter styrker tillitten til disse som samhandlingsparter
Samarbeid og virkemidler som	Fulltreffer (5)	I stor grad (4)	Middels (3)	I stor grad (4)	Middels (3)	I stor grad (4)

Strategiske mål fra nasjonal e-helsestrategi	**Videreutvikling av eksisterende nasjonale virkemidler (Normen, HelseCERT)**	**Kompetanse og sikkerhetskultur**	**Planverk og øvelser**	**Etterlevelse og oppfølging**	**Ny teknologi og digitale verdikjeder**	**Støtte til mindre virksomheter**
styrker gjennomføringskraft						
	Nasjonale virkemidler sektoren står sammen om	Felles kompetansetiltak egner seg godt for samarbeid	Øvelser vil kunne fokusere på samarbeid mellom aktører i sektor	Oppfølging av relevante tiltak	Enklere og sikrere ibruktakelse av ny teknologi	Felles tiltak = økt gjennomføringskraft
Gjennomsnitt:	Middels / I stor grad (3,6)	Middels (3)	Litt (2,2)	Middels (3,2)	I stor grad (3,8)	Middels / I stor grad (3,4)
Oppsummering i søylediagram						

B.3 Oppsummering av Direktoratets vurdering av måloppnåelse for hvert innsatsområde

Følgende oppsummerer Direktoratets vurdering av hvordan de ulike innsatsområdene bidrar til å nå målene.

- **Innsatsområde 1: Videreutvikling av eksisterende nasjonale virkemidler.** Innsatsområdet bidrar samlet til stor grad av måloppnåelse, og tiltakene innen innsatsområdet utfyller hverandre. Til sammen gir de stor grad av støtte til sektorens virksomheter. Begge tiltak er brede i den forstand at de har mulighet til å også bidra inn i de andre innsatsområdene. Som eksempel så kan veiledningen i Normen videreutvikles til å i større grad bidra til sikkerhet i ny teknologi, og/eller gi mer støtte til mindre virksomheter.
- **Innsatsområde 2: Kompetanse og sikkerhetskultur.** Økt kompetanse og sikkerhetskultur underbygger målene i strategien, og er også i stor grad en forutsetning for å lykkes med andre innsatsområder. Merk at effekten fra innsatsområdet kommer fra alle tiltakene i innsatsområdet samlet: Man starter med kartlegging, går videre til utredning, og etablerer tiltak basert på utredning.
- **Innsatsområde 3: Planverk og øvelser.** Samlet sett har innsatsområdet godt bidrag knyttet til måloppnåelse for målene i innspillet til helseberedskapsmeldingen. Spesielt er innsatsområdet svært godt egnet til å bidra til oppfyllelse av målene å avklare ansvar og roller i sektoren og bidra til at sektoren har bevissthet om sårbarhet og trusler og er øvet i å håndtere hendelser. Merk at selv om tiltakene utfyller hverandre, så kan flere av tiltakene gjennomføres uavhengig av hverandre. Tiltakene gir effekt alene, men kan også forsterke hverandre. Eksempelvis så vil det å stille en forventning om systematisk arbeid med øvelser kunne ha en effekt i seg selv, men denne effekten kan forsterkes ved å også etablere felles arenaer (tiltak 3.3) hvor man kan bedrive koordinering og kunnskapsdeling om blant annet øvelser. Selv om tiltakene er relativt uavhengige av hverandre, så anser vi at tiltak innen innsatsområdet har størst effekt om de inkluderer arbeid knyttet felles oversikt og planverk (tiltak 3.1-3.2, 3.3-3.6) i kombinasjon med tiltak knyttet til arenaer og informasjons-/erfaringsutveksling (tiltak 3.3, 3.7) som setter virksomhetene i bedre stand til å koordinere med og lære fra andre i sektoren.
- **Innsatsområde 4: Etterlevelse og oppfølging. I**nnsatsområdet bidrar godt til målbildet. Tiltakene bygger i noen grad på hverandre, og hvor sterk effekten av innsatsområdet blir vil avhenge av hvilken styrke man velger på tiltakene. Eksempelvis, så vil det forventes en viss grad av effekt fra å stille tydelige forventninger til virksomhetene (tiltak 4.1), noe sterkere effekt fra å støtte egenkontroll (tiltak 4.2 b), og enda sterkere effekt fra å etablere ekstern kontroll/tilsyn (tilta 4.2 c). Tiltak knyttet til sammenstilling (tiltak 4.3) og måling av effekt (tiltak 4.4) kan gjennomføres relativt uavhengig av de andre tiltakene i innsatsområdet.
- **Innsatsområde 5: Ny teknologi og digitale verdikjeder.** Dette innsatsområdet bidrar spesielt til mål knyttet til ivaretakelse av sikkerhet i lange og komplekse digitale verdikjeder, og evne til å ta i bruk ny teknologi og møte et risikobilde i endring. Tiltakene er relativt uavhengige av hverandre. Imidlertid er det slik at de tiltakene som har lav kostnad og risiko (tiltak 5.1, 5.2) også har relativt lavere nytte enn de med høyere kostnad og risiko (tiltak 5.3, 5.4).
- **Innsatsområde 6: Støtte til mindre virksomheter.** Dette innsatsområdet bidrar bredt til målbildet. Merk at effekten fra innsatsområdet kommer fra alle tiltakene i innsatsområdet samlet: Man starter med kartlegging, går videre til utredning, og etablerer tiltak basert på utredning.

For alle innsatsområder antas effekten av de samlede tiltakene innen innsatsområdet å ha lang varighet, forutsatt at tiltakene forvaltes.

Vurderingen av måloppnåelse peker mot innsatsområde 5, *Ny teknologi og digitale verdikjeder,* som det området som samlet sett har det bredeste bidraget til målbildet. Merk imidlertid at etter Direktoratets vurdering bidrar alle innsatsområdene hver for seg godt til det samlede målbildet, og det er vanskelig å prioritere blant innsatsområdene kun basert på bidrag til å oppnå disse strategiske målene.

Vedlegg C Liste over tiltak

Dette vedlegget gir en detaljert oversikt over hvordan tiltakene, slik de omtales i dette dokumentet, er relatert til de konkrete formuleringene i direktoratets innspill til den kommende helseberedskapsmeldingen.

Foreslåtte tiltak fra Direktoratets innspill (IE-1108) til kommende helseberedskapsmelding

Innsatsområde	Tiltaket slik det ble formulert i IE-1108	Tiltaket slik det formuleres på overskriftsnivå i dette dokumentet
Videreutvikling av eksisterende nasjonale virkemidler	Videreutvikle HelseCERT	1.1 Videreutvikle HelseCERT
	Videreutvikle Normen	1.2 Videreutvikle Normen
Kompetanse og sikkerhetskultur	Gjennomføre en kartlegging og vurdering av eksisterende kompetansetiltak, med formål om at virkemidler som fungerer godt kan deles og gjenbrukes i hele sektoren	2.1 Kartlegging
	Basert på kartleggingen, vurdere behovet for en utredning av tiltak med formål å styrke kompetansen om digital sikkerhet hos helsepersonell	2.2 Utredning
	Bidra til økt oppmerksomhet på digital sikkerhetskompetanse i helsefaglige utdanninger	2.3 Digital sikkerhet i helsefaglig utdanning
Planverk og øvelser	Utarbeide overordnet nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan. Denne vil danne et likt og generisk plangrunnlag regionalt og lokalt der tydelig ansvars- og varslingslinjer i håndtering av IKT-sikkerhetshendelse i sektoren fremkommer samt i samvirke med andre sektorer.	3.1 Overordnet nasjonal IKT-beredskapsplan
	Planverk på ulike nivåer må være omforent og bygge på overordnet planverk, felles begrepsbruk og forståelse.	3.2 Sammenheng mellom planverk
	Det bør etableres felles møtearenaer eller samarbeidsfora for systematisk og kontinuerlig arbeid med og fokus på digital sikkerhet. Slike møtearenaer eller samarbeidsfora kan benyttes til samordning av	3.3 Etablere felles arenaer

	planverk, kompetansebygging og dele erfaringer fra hendelser og øvelser samt bidra til å koordinere planlegging og deltakelse i øvelser.	
	Etablere kart over myndighetsroller, systemeierskap og leverandører til bruk i beredskapsarbeidet.	3.4 Kart over roller, systemeierskap og leverandører
	Etablere en nasjonal oversikt over kritisk infrastruktur i helse- og omsorgssektoren.	3.5 Nasjonal oversikt over kritisk infrastruktur
	Etablere en overordnet strategi eller rammeplan for øvelser som omfatter digital sikkerhet i helsesektoren med tydelige forventninger til systematisk arbeid med øvelser på nasjonalt nivå og i hver enkelt virksomhet. Dette vil kunne sikre regelmessige øvelser og bidra til helhetlig tilnærming, samsvar mellom mål og virkemiddel, samt koordinering i egen sektor og med andre virksomheter i andre sektorer og på flere nivå.	3.6 Overordnet plan for øvelser og forventning om systematisk arbeid med øvelser
	Tilrettelegge for informasjonsdeling i forbindelse med dataangrep, og erfaringsutveksling fra etterfølgende evaluering, i tråd med NSMs grunnprinsipper.	3.7 Informasjonsdeling og erfaringsutveksling
Etterlevelse og oppfølging	Tydeligere forventing om at etterlevelse følges opp internt i den enkelte virksomhet, og at sikkerhetsstyring integreres i den ordinære virksomhetsstyringen.	4.1 Tydelig forventning til virksomhetene
	Virksomhetene støttes gjennom veiledning og verktøy, og det forberedes ordninger for kontroll og dokumentasjon av sikkerhetsarbeid.	4.2 Felles tiltak for støtte og oppfølging a. Kartlegge og utrede b. Støtte egenkontroll c. Utvikle og styrke kontroll
	Det er behov for å sammenstille og samordne nasjonale virkemidler, hjelpemidler og samarbeidsnettverk	4.3 Sammenstille og samordne
	Stille krav om at tiltakseiere på nasjonalt nivå skaffer oversikt over tiltakenes effekt.	4.4 Krav om oversikt over effekt av tiltak

Ny teknologi og digitale verdikjeder	Stille forventning om at sentralt og lokalt beredskapsplanverk må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring. Dette bør inkludere rutiner/systemer for varsling ved hendelser som berører andre i verdikjeden (særlig de som er avhengig av andres tjenesteleveranse).	5.1 Forventning om tilpasning beredskapsplanverk nye leveransemodeller
	Ta DSBs modell for risikostyring i digitale verdikjeder inn i veiledere til relevant sektorlovverk.	5.2 DSBs modell for risikostyring i digitale verdikjeder inn i relevante veiledere
	Legge til rette for bedre støtte til vurdering, innføring og utvikling av ny teknologi i samarbeid med relevante fag- og veiledningsmiljøer i og utenfor sektoren. Dette inkluderer utarbeidelse av veiledningsmateriell, opplæringsaktiviteter, etablering av sandkasser og lignende.	5.3 Bedre innføringsstøtte ved ny teknologi
	Legge til rette for samarbeid ved anskaffelser, og ved kravstilling og oppfølging av leverandører. Nettverk og fagforum, interkommunale samarbeid, veiledning og utarbeidelse av felles kravspesifikasjoner kan være måter å gjøre dette på.	5.4 Samarbeid ved anskaffelser, kravstilling og oppfølging av leverandører
Støtte til mindre virksomheter	Kartlegge sikkerhetstilstanden og -behov i de mindre virksomhetene i sektoren.	6.1 Kartlegging
	Utrede mulige felles ordninger og tjenester som vil gi verdi for bredden av mindre virksomheter.	6.2 Utredning

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no