Direktoratet for e-helse

Innspill til kommende stortingsmelding om helseberedskap – tema: Digital sikkerhet

Høringsseminar
29.06.2022

Agenda

1. Om høringen og høringsprosessen

2. Bakgrunn for innspillets innhold
   - Strategi for digital sikkerhet i helse- og omsorgssektoren
   - Endret oppdrag

3. Innhold i innspillet
   - Utfordringsbilde
   - Mål
   - Innsatsområder og forslag til tiltak

4. Spørsmål

Innspill til stortingsmelding om helseberedskap ble sendt på en bred høringsrunde 9. juni

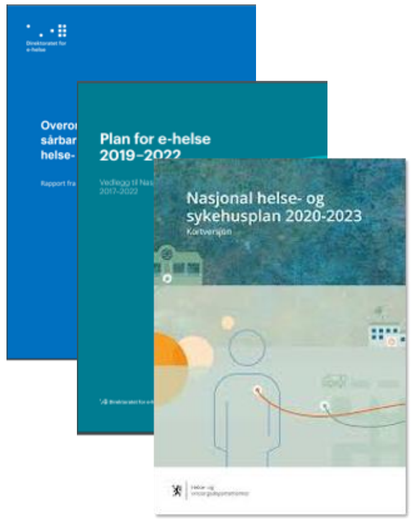
- Innspillet bygger i stor grad på tidligere arbeid med *Strategi for digital sikkerhet i helse- og omsorgssektoren*

- Høringsfristen er satt til 9. september, 3 måneder etter utsending.
- Ikke mulig å søke om utsatt svarfrist, sene svar ettersendes til HOD.

- Det er opprettet en egen høringsside på ehelse.no, og høringen er åpen for alle.

Stortingsmelding om helseberedskap våren 2023

Innspillet bygger på arbeidet med Strategi for digital sikkerhet i helse- og omsorgssektoren



Sektorspesifikke behov

- ✓ Trusselbilde
- ✓ Sikkerhetsbehov som følger av teknologisk utvikling og digitalisering i sektoren
- ✓ Forutsetninger og særtrekk ved sektoren

Strategien ble drøftet bredt med samarbeidspartnere og aktører fra sektoren, dokumentgjennomgang og arbeidsmøter

1-1 møter med aktører i og utenfor sektoren

- ✓ NTNU (CCIS)
- ✓ Datatilsynet
- ✓ NSM
- ✓ Digdir
- ✓ HDIR
- ✓ NSM
- ✓ JD
- ✓ Legemiddelverket
- ✓ Riksrevisjonen
- ✓ Apotekforeningen
- ✓ NorSis
- ✓ Profesjonsorganisasjoner
- ✓ Nasjonalt senter for e-helseforskning
- ✓ KS Fagråd for informasjonssikkerhet
- ✓ KS Fag- og prioriteringsutvalg
- ✓ KS SNIP-nettverket
- ✓ IKT Norge
- ✓ Melanor

Jevnlige møter med samarbeidspartnere og presentasjoner i Nasjonal styringsmodell

- ✓ Utvidet kjerneteam
- ✓ Styringsgruppemøter
- ✓ Nasjonal styringsmodell
  - ✓ NUIT
  - ✓ NUFA
  - ✓ Nasjonal e-helsestyre

Workshops

- ✓ Temabaserte workshops med deltagere fra sektoren: 6 gjennomførte WS høsten 2021
  - Påmeldingsbasert med 30 – 50 deltagere per WS
  - Fokus på utfordringsbildet og forslag til tiltak innenfor hvert av temaområdene i strategien
- ✓ Oppfølgingsworkshop januar
  - Invitasjonsbasert med 32 deltagere
  - Fokus på innsatsområder

Forstudie og øvrige dokumenter

- ✓ Forstudie
- ✓ Overordnet risiko- og sårbarhetsvurdering for IKT i helse og omsorgssektoren
- ✓ Riksrevisjonens vurdering av helseforetakenes forebygging av angrep mot sine IKT-systemer
- ✓ Digital sårbarhet – sikkert samfunn (Lysne-utvalget)
- ✓ Nasjonal e-helsestrategi
- ✓ Nasjonal strategi for digital sikkerhet m/tiltaksoversikt

Endret oppdrag fra helse- og omsorgsdepartementet

Direktoratet for e-helse mottok 16. mai endring av oppdrag om strategi og tiltaksoversikt digital sikkerhet i helse- og omsorgssektoren:

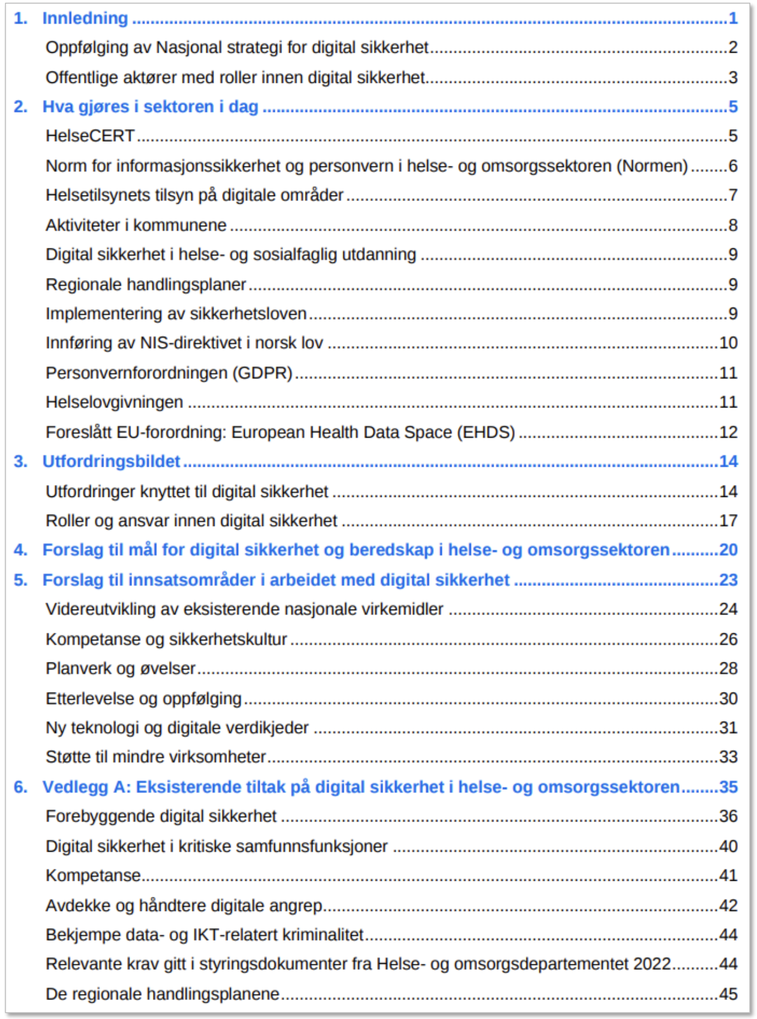
«Direktoratet skal, som erstatning for Strategi for digital sikkerhet i helse- og omsorgssektoren, utarbeide et innspill om digital sikkerhet i helse- og omsorgssektoren til stortingsmeldingen om helseberedskap. Direktoratet sender innspillet på bred høringsrunde og innarbeider høringsinnspill. Frist: Innen 15. oktober 2022.»

Departementets begrunnelse for endringen:

«Basert på en vurdering av hvordan vi kan få mest oppmerksomhet og raskest utvikling på området, i tillegg til det økte trusselnivået etter Russlands invasjon av Ukraina, har departementet besluttet å endre gjennomføring hvor HOD overtar eierskapet til strategien.

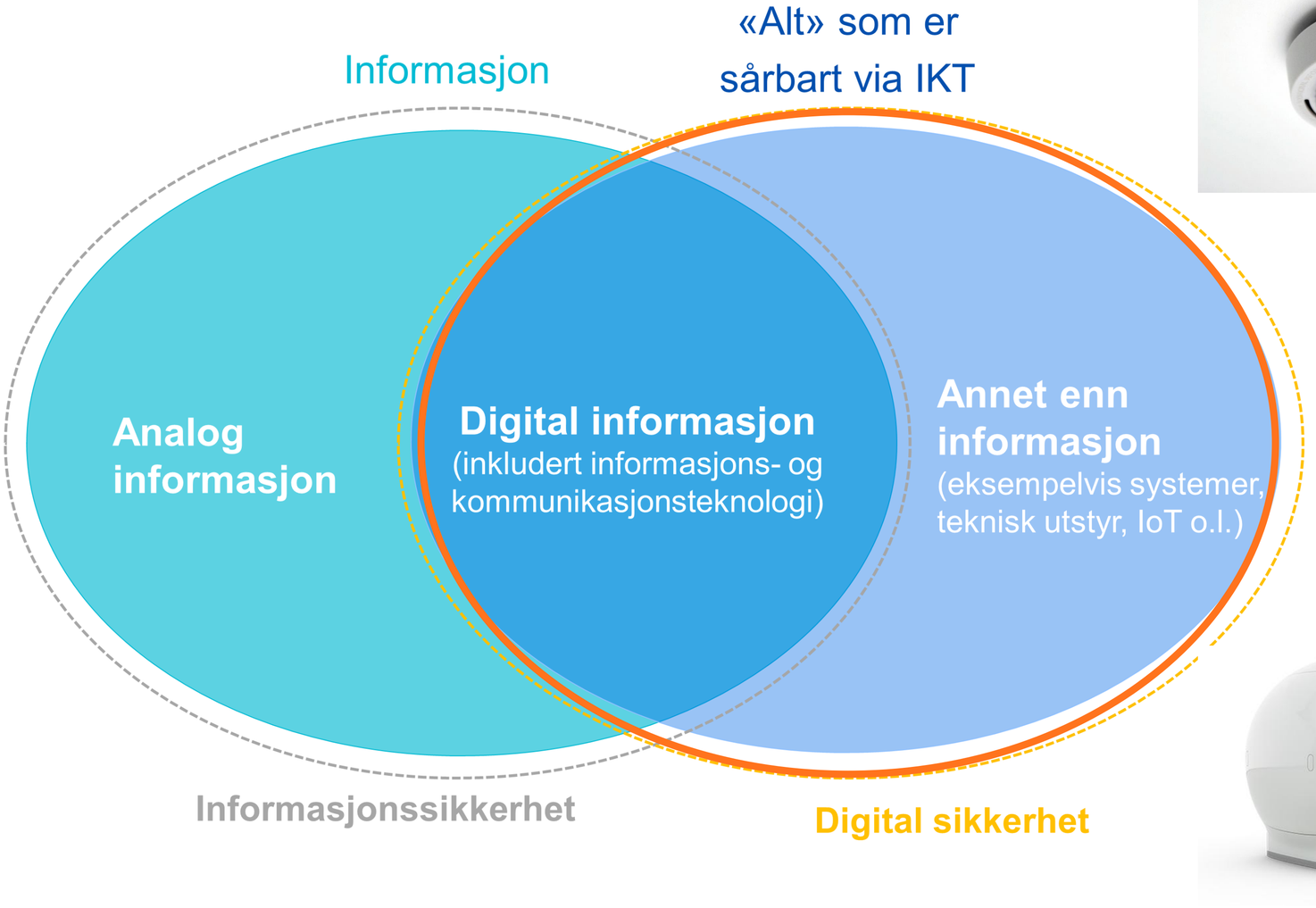
Parallelt med dette er det vedtatt at det skal legges frem en stortingsmelding om helseberedskap våren 2023. Stortingsmeldingen skal ta for seg fem scenarier hvor digitale trusler er ett av dem. For å unngå duplisering og minske antall dokumenter å forholde seg til, ser departementet det som hensiktsmessig å innarbeide strategi for digital sikkerhet i helse og omsorgssektoren inn i helseberedskapsmeldingen.»

Innhold i innspillet til stortingsmeldingen



- Hele teksten er gjennomgått og redigert for å øke relevansen opp mot beredskap
- Nytt forord
- Beskrivelse av hva som gjøres på området digital sikkerhet i sektoren i dag
  - Som vedlegg: en oversikt over eksisterende tiltak på digital sikkerhet i sektoren i dag
- Beskrivelse av utfordringsbildet
- Forslag til mål for arbeidet med digital sikkerhet i nasjonal helseberedskapsplan
- Forslag til seks innsatsområder i det videre arbeidet med digital sikkerhet i helseberedskapen

Begrepet **digital sikkerhet**



Skjerpet trusselbilde

DAN GOODIN, ARS TECHNICA SECURITY 09.19.2020 08:00 AM

A Patient Dies After a Ransomware Attack Hits a Hospital

The outage resulted in a significant delay in treatment. German authorities are investigating the perpetrators on suspicion of negligent manslaughter.

PHOTOGRAPH: LUKAS SCHULZE/GETTY IMAGES

NRK Logg inn

Urix Presidentvalget Nyhetsbrev Urix forklarer Korrespondentbrevet Podcast: Krig og fred Urix på NR

Hacking-skandale ryster Finland - pasienter presset for penger

enter er på avveie etter penger.

Bjørnar Hjellen
@bjornarhjellen
Journalist

Kilde: NTB-NRK

Publisert 25. okt. 2020 kl. 12:58

Ohisalo

NRK Nyheter Sport Kultur Humor Distrikt Mer Logg inn Søk

Troms og Finnmark Tips oss Se Nordnytt Hør P1 Finnmark Hør P1 Troms Hør Ettermiddagssending i Troms og Finnmark Om oss

Datainnbrudd mot ambulanser på flere sykehus i Nord-Norge: – Et alvorlig datainnbrudd

Det er kommunikasjonssystemet mellom AMK-sentralen og luftambulanser og ambulansene som er rammet.

Skadevaren er oppdaget i et IKT-program som benyttes i ambulanser og luftambulansehelikoptre i Helgelandssykehuset, Nordlandssykehuset, Universitetssykehuset Nord-Norge og Finnmarkssykehuset.
FOTO: ESKIL MEHREN / NRK

Ida Louise Rostad
Journalist

Torgeir Skeie
Journalist

Rune N. Andreassen
Journalist

Gisle Forland
Journalist

Linda Pedersen
Journalist

Vi rapporterer fra **Tromsø**

Publisert 8. apr. kl. 14:06
Oppdatert 8. apr. kl. 18:58

oa.no

Digital +Alt
Kun 5 kr for 5 uker
BESTILL HER

POLITIKK OG SAMFUNN ØSTRE TOTEN HELSE DATAANGREP SKOLE

Slik er konsekvensene for innbyggerne etter dataangrepet: Forsinkelser i hjemmetjenesten og endringer i ungdomsskolen

Sektor for helse, omsorg og velferd

Labo

Alarmsystemet er nede. Alle beboere er utstyrt med bjeller for å kunne varsle. Bemanningen er styrket.

Kura er i normal drift

Konsekvenser for de ansatte:

Datasystemer er utilgjengelige

Sensorikken i pasientrommene fungerer ikke

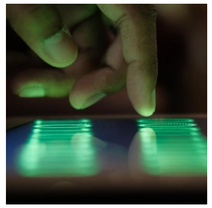
Redusert funksjonalitet på medisinkabinetter og medisintraller

Manuelle registreringer og manuell dokumentasjon i pasientjournal

Kura i normal drift.

Manuelle bestillinger på medisiner, mat og utstyr

Utfordringsbildet som legges til grunn



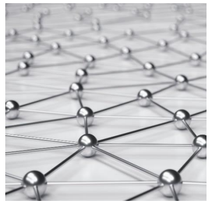
Sektoren står overfor et skjerpet digitalt trusselbilde

Udekket kompetansebehov

Komplekst systemlandskap og mangelfull implementering av grunnleggende sikkerhetstiltak

Teknologiskifter og nye samhandlingsformer og leveransemodeller for helsehjelp

Varierende oppfølging av digital sikkerhet i verdikjeder



Uklare roller og ansvar

Direktoratet for e-helse foreslår seks mål for arbeidet med digital sikkerhet i den nasjonale helseberedskapen

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.

Direktoratet for e-helse foreslår seks innsatsområder

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

Videreutvikling av eksisterende nasjonale virkemidler

Overordnet beskrivelse

- Det er sentralt at arbeidet med digital sikkerhet i sektoren skjer som en del av en kontinuerlig forbedring, og felles virkemidler som HelseCERT og Normen er helt sentrale bidragsytere til dette forbedringsarbeidet.
- For å bidra til at sektorens totale beredskapsevne styrkes, må eksisterende virkemidler som bidrar på tvers av hele sektoren videreføres og videreutvikles.
- 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.
- HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet, og er også sektorvis responsmiljø. De har tjenester som er sentrale i både forebyggende sikkerhetsarbeid og i hendelseshåndtering. Kontinuerlig utvikling av tjenestetilbudet, innenfor rammen av å være et sektorvist responsmiljø, sikrer at tjenestene på best mulig måte møter behov som følger av et digitalt trusselbilde i endring.

Forslag til tiltak

- ✓ Videreutvikling av HelseCERT
- ✓ Videreutvikling av Normen
- ✓ (Eventuelle øvrige tiltak vil bli lagt til etter hvert)

Kompetanse og sikkerhetskultur

Overordnet beskrivelse

- Kompetanse om digital sikkerhet er en forutsetning for å kunne beskytte verdier mot uønskede digitale hendelser.
- I følge NSM er det nødvendig med et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra virksomhetenes øverste ledelse til den enkelte ansatte .
- Manglende kompetanse om på området kan føre til svakheter i prosesser der digital sikkerhet inngår som en del av vurderingen, for eksempel ved anskaffelse, introduksjon og bruk av ny teknologi og etterlevelse av sikkerhetskrav.
- Det finnes gode virkemidler knyttet til kompetanseheving i sektoren i dag. Deling og gjenbruk av slike ressurser er en effektiv måte å heve kompetansenivået på.

Forslag til tiltak

- ✓ Gjennomføre en kartlegging og vurdering av eksisterende kompetansetiltak, med formål om at virkemidler som fungerer godt kan deles og gjenbrukes i hele sektoren.
- ✓ Utrede behovet for, og mulige modeller for utvikling og utbredelse av, felles kompetanseressurser.
- ✓ Legge til rette for økt fokus på digital sikkerhetskompetanse i helsefaglig utdanning, og at etter- og videreutdanning styrkes.

Planverk og øvelser

Overordnet beskrivelse

- Alle sektorens virksomheter må være forberedt på å håndtere digitale sikkerhetshendelser og sikre fortsatt forsvarlig leveranse av helsetjenester.
- Manglende planverk fører til uklarheter rundt roller og tilhørende ansvar ved IKT-beredskap og nasjonal kriseledelse.
- Et viktig grep for å styrke IKT-beredskapen er å sørge for at IKT-beredskap inngår i nasjonale styringsdokumenter
- Gjennomføring av øvelser er sentralt for at planverk og rollebeskrivelser omsettes til praktiske ferdigheter.
- I dag gjennomføres det få øvelser i sektoren der digital sikkerhet inngår som tema. Regelmessig gjennomføring av øvelser vil styrke virksomhetenes bevissthet, organisering og ferdigheter innen digital sikkerhet.

Forslag til tiltak

- ✓ Utarbeide en egen nasjonal IKT-beredskapsplan for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan.
- ✓ Etablere en nasjonal oversikt over kritisk infrastruktur i helse- og omsorgssektoren.
- ✓ Etablere kart over myndighetsroller, systemeierskap og leverandører som skal være til bruk i beredskapsarbeidet.
- ✓ Stille forventning om hyppigere og mer regelmessig gjennomføring av øvelser som omfatter digital sikkerhet, både på nasjonalt nivå og i hver enkelt virksomhet. Dette inkluderer samvirkeøvelser med andre relevante virksomheter, både innad i sektoren og med virksomheter i andre sektorer lokalt, i egen region og nasjonalt.
- ✓ Stille forventning om at virksomheter i sektoren oftere planlegger, gjennomfører og evaluerer øvelser, og aktivt benytter erfaringene som del av sitt kontinuerlige forbedringsarbeid.
- ✓ Tilrettelegge for informasjonsdeling i forbindelse med dataangrep, og erfaringsutveksling fra etterfølgende evaluering, i tråd med NSMs grunnprinsipper.

Etterlevelse og oppfølging

Overordnet beskrivelse

- Økt kontroll med digital risiko vil styrke den forebyggende sikkerheten og øke virksomhetenes evne til å motstå uønskede digitale hendelser.
- En forutsetning for å oppnå dette er etterlevelse av grunnleggende sikkerhetskrav og anbefalinger.
- NSM erfarer at de fleste cyberhendelser hadde vært avverget eller fått begrenset skadeomfang om NSMs grunnprinsipper hadde vært fulgt.
- Det digitale landskapet i helse- og omsorgssektoren er fragmentert, og det er stor variasjon innen modenhet og utfordringer på området digital sikkerhet.
- Det er viktig at grunnleggende sikkerhetskrav og -anbefalinger etterleves i sektoren, og at etterlevelsen følges opp.

Forslag til tiltak

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

Ny teknologi og digitale verdikjeder

Overordnet beskrivelse

- Ny teknologi, tjenester og samhandlingsformer som tas i bruk sektoren innebærer ofte at flere aktører og leverandører er involvert. Dette danner lange digitale verdikjeder.
- Å ivareta god beredskap i slike verdikjeder stiller nye krav til sektorens virksomheter, og beredskapsarbeidet må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring.
- Risikovurdering av digitale verdikjeder som går på tvers av virksomheter og landegrenser er kompetansekrevende og virksomhetene i sektoren vil kunne ha nytte av støtte i dette arbeidet
- Det ligger et stort potensial i samarbeid med relevante fag- og veiledningsmiljøer i og utenfor sektoren.
- Også mellom virksomheter med like behov vil det være hensiktsmessig med økt samarbeid ved anskaffelser, kravstilling og oppfølging av leverandører.

Forslag til tiltak

- ✓ Stille forventning om at sentralt og lokalt beredskapsplanverk må tilpasses nye leveransemodeller og et teknologi- og risikobilde i endring. Dette bør inkludere rutiner/systemer for varsling ved hendelser som berører andre i verdikjeden (særlig de som er avhengig av andres tjenesteleveranse)
- ✓ Ta DSBs modell for risikostyring i digitale verdikjeder inn i veiledere til relevant sektorlovverk .
- ✓ 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.
- ✓ Legge til rette for samarbeid ved anskaffelser, og ved kravstilling og oppfølging av leverandører.

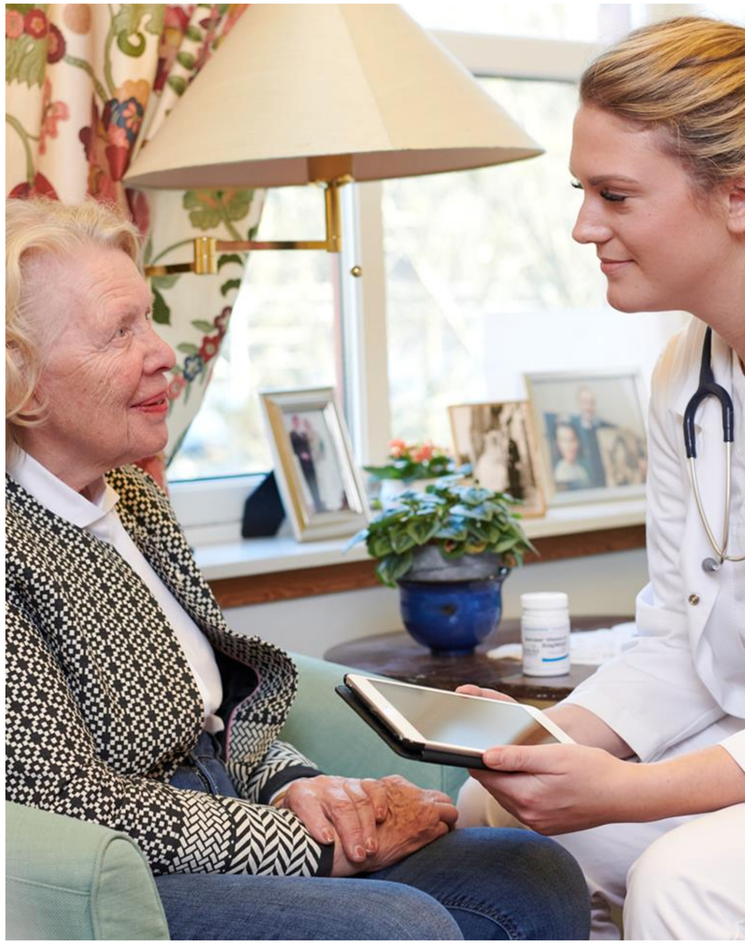
Støtte til mindre virksomheter

Overordnet beskrivelse

- For å øke sektorens totale beredskapsevne i et skjerpet trusselbilde må den digitale sikkerheten styrkes også i de mindre virksomhetene
- 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.
- I en situasjon med økt samhandling og tettere knyttede digitale verdikjeder kan sikkerhets-tilstanden i de mindre virksomhetene utgjøre en sårbarhet også for øvrige deler av sektoren.
- Det er nødvendig med tiltak for å styrke beredskapsevnen i de små virksomhetene, og disse tiltakene må ta utgangspunkt i forutsetningene og rammebetingelsene i disse virksomhetene.
- Dette vil kunne redusere sannsynligheten for vellykkede angrep og legge til rette for bedre håndtering av hendelser.
- Antallet mindre virksomheter i sektoren er høyt, og tiltak som gir effekt i den enkelte virksomhet kan ha stor samlet effekt for sektoren.

Forslag til tiltak

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



Direktoratet for e-helse ønsker særlig tilbakemeldinger på

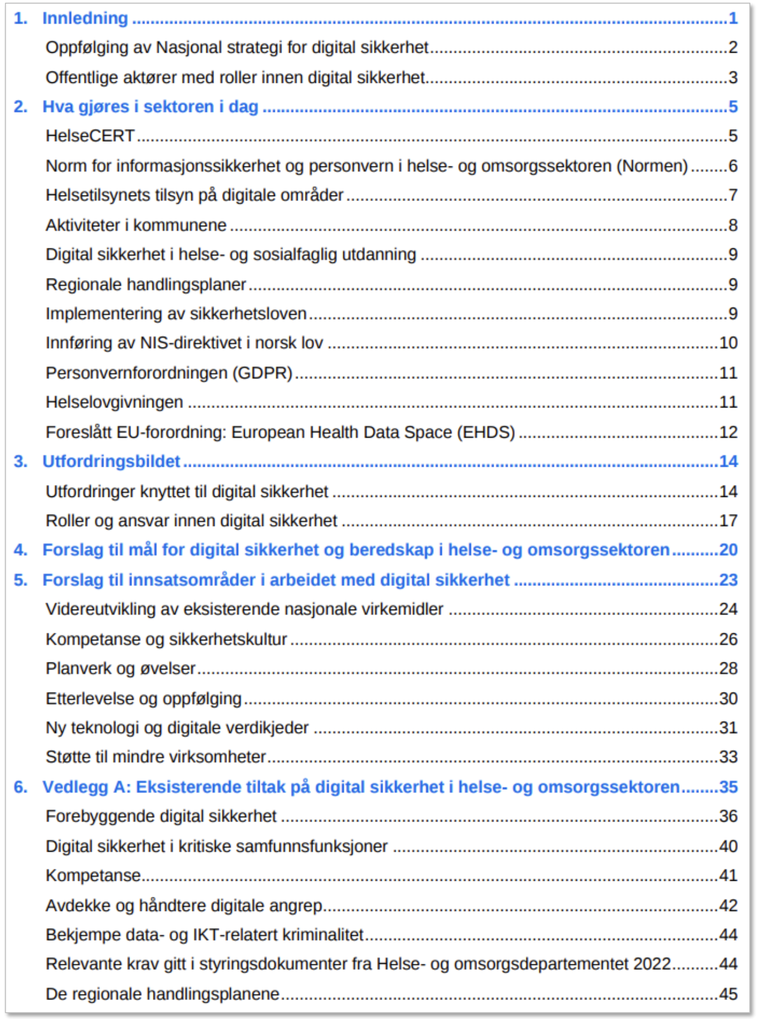
1. Er det mangler i beskrivelsen av pågående initiativer knyttet til digital sikkerhet i nasjonal helseberedskap (kapittel 2 og vedlegg A)? Vi ønsker beskrivelse av initiativer som ikke er med og innspill der eksisterende beskrivelser er upresise eller mangelfulle.

2. Er beskrivelsen av utfordringsbildet (kapittel 3) i tilstrekkelig grad dekkende for den reelle situasjonen?

3. Beskriver de foreslåtte målene for arbeidet med digital sikkerhet i nasjonal helseberedskap (kapittel 4) et passende og dekkende målbilde?

4. Er de foreslåtte innsatsområdene og de foreslåtte tiltakene (kapittel 5) hensiktsmessige, og er de realistiske å gjennomføre?

Huskeliste og eventuelle spørsmål



- Vennligst benytt høringssvarskjemaet for å sende høringssvar
- Det bes om ett innspill per organisasjon
- Spørsmål?

Kontakt:
Seksjonssjef Jan Gunnar Broch,
jan.gunnar.broch@ehelse.no