Helsedirektoratet

Returadresse: Helsedirektoratet, Postboks 220 Skøyen, 0213 Oslo, Norge

Direktoratet for e-helse
Jan Gunnar Broch

Deres ref.:	
Vår ref.:	21/21383-3
Saksbehandler:	Ulrik Pettersen
Dato:	12.09.2022

Direktoratet for e-helse - Høring - Innspill til kommende stortingsmelding om helseberedskap - tema digital sikkerhet

Helsedirektoratet viser til høringsbrev og -notat med invitasjon til å gi innspill på temaet digital sikkerhet i helse- og omsorgssektoren til kommende stortingsmelding om helseberedskap. Dokumentet har vært på intern høring i Helsedirektoratet, og de innspill som er mottatt fremkommer i vedlagt høringsskjema.

Helsedirektoratet opplever at Innspill til kommende stortingsmelding om helseberedskap på en fin måte reflekterer og viderefører tidligere arbeidet med en strategi for digital sikkerhet i helse- og \ Omsorgssektoren. Utarbeidelse av strategien var et oppdrag i fjorårets tildelingsbrev til direktoratet, i samarbeid med Helsedirektoratet, Helsetilsynet, Norsk helsenett SF, de regionale helseforetakene og kommunesektoren/KS.

Vennlig hilsen

Nina Aulie e.f.
direktør

Ulrik Pettersen
ekstern konsulent

Dokumentet er godkjent elektronisk

Vedlegg: 1

Helsedirektoratet
Avdeling sikkerhet
Ulrik Pettersen
Postboks , • Besøksadresse: • Tlf.: (+47) 47 47 20 20
Org.nr.: 983 544 622 • postmottak@helsedir.no • www.helsedirektoratet.no

Høringssvarskjema: Innspill til kommende stortingsmelding om helseberedskap – tema: Digital sikkerhet

Skjemaet sendes til postmottak@ehelse.no og merkes med saksnummer 22/448.

Frist: 09.09.2022

*****

Kontaktinformasjon

Navn på virksomhet:
Helsedirektoratet

Kontaktperson: Ulrik Pettersen
E-postadresse: ulrik.pettersen@helsedir.no

1) **Er det mangler i beskrivelsen av pågående initiativer knyttet til digital sikkerhet i nasjonal helseberedskap (kapittel 2), i form av initiativer som ikke er beskrevet, eller mangler i eksisterende beskrivelser? Utdyp gjerne i fritekstfeltet.**

☐ **Ja** ☐ **Nei** ☒ **Har ingen kommentar**

Klikk eller trykk her for å skrive inn tekst.

2) **Er det mangler i vedlegget med oversikt over eksisterende tiltak knyttet til digital sikkerhet i sektoren (vedlegg A) i form av tiltak som ikke er beskrevet, eller mangler i eksisterende beskrivelser? Utdyp gjerne i fritekstfeltet.**

☐ **Ja** ☐ **Nei** ☒ **Har ingen kommentar**

Ved utdypning, angi tiltak, ansvarlig, relevant for, beskrivelse:

Klikk eller trykk her for å skrive inn tekst.

3) **Er beskrivelsen av utfordringsbildet (kapittel 3) i tilstrekkelig grad dekkende for den reelle situasjonen? Utdyp gjerne i fritekstfeltet.**

☐ **Ja** ☒ **Nei** ☐ **Har ingen kommentar**

Som nevnt i innspillet er det internasjonale utviklingen med f.eks. EHDS et tydelig utviklingstrekk, dette må også ses i lys av den økte betydningen EU samarbeidet har fått for nasjonalt helseberedskapsarbeid. Norsk tilknytting til EUs infrastrukturer for primær og sekundærbruk av data vil både kunne styrke vår evne til å ta i bruk digitale løsninger for å håndtere kriser, og øker digital sårbarhet (ref. dualiteten over).

I listen av offentlige aktører med en rolle for digital sikkerhet listes ikke FHI. FHI har en viktig rolle ift å overvåke smittespredning i og utenfor landets grenser der IKT systemer og løsninger understøtter arbeidet, eks. Smittestopp under Corona pandemien. FHI er også kompetent myndighet for EU samarbeidsprosjektet HERA IT Platform, og skal utvikle nasjonal tilpasning til EUs sentrale system for overvåkning og analyse av grensekryssende helsetrusler. Grensekryssende helsetrusler er i dette prosjektet definert bredt, virus, atomangrep, cyber angrep, mm. FHI bør defineres inn i listen, og arbeidet FHI deltar i på europeisk nivå kan inngå i situasjonsbeskrivelsen.

Både under flyktningkrisen i 2015 og under covid-19 pandemien erfarte Norge store utfordringer knyttet til utlevering av digital ID og digitale innloggingsløsninger for personer uten fødselsnummer eller d-nummer. Det gjorde det utfordrende å registrere og overvåke smittetilfeller, samt gi tilgang

til egne helseopplysninger digitalt. I beredskapsøyemed bør denne utfordringen løses, slik at vi er bedre forberedt ved neste krise.

4) **Beskriver de foreslåtte målene for digital sikkerhet og beredskap i helse- og omsorgssektoren (kapittel 4) et passende og dekkende målbilde? Utdyp gjerne i fritekstfeltet.**

☒ **Ja** ☐ **Nei** ☐ **Har ingen kommentar**

Mål og beskrivelse av innsatsområder på dette området, er utarbeidet i et tett og konstruktivt samarbeid mellom Direktoratet for e-helse og Helsedirektoratet. Det er naturlig at Helsedirektoratet også fremover har en rolle på dette området. Dette gjelder bl.a. deling av erfaringer og råd om krisehåndtering, operasjonalisering av et nasjonalt rammeverk for helsesektorens håndtering av konsekvenser av alvorlige digitale trusler og hendelser, samt strategiske beredskapsøvelser og kompetansebygging. Tydeliggjøring av roller og ansvar innen beredskap og krisehåndtering, bl.a. gjennom aktørkart og et mer operasjonalisert nasjonalt beredskapsplanverk anses som gode og viktige tiltak.

5) **Er de foreslåtte innsatsområdene og de foreslåtte tiltakene (kapittel 5) hensiktsmessige, og er de realistiske å gjennomføre? Utdyp gjerne i fritekstfeltet.**

☒ **Ja** ☐ **Nei** ☐ **Har ingen kommentar**

Det er tvil om de forslåtte innsatsområde og tiltak er nok til å oppnå målet "Ansvar og roller med betydning for digital sikkerhet …." beskrevet i kap. fire. Tiltaket "Etablere kart over myndighetsrolle ..." under "Planverk og Øvelser" sikter i noen grad målet om klar ansvarsfordeling. Dette oppleves likevel som ikke tilstrekkelig. Begrunnelsen for dette er at Riksrevisjonen og Helsedirektoratet har blant andre påpekt at det er behov for klarere roller på alle nivå.

En kan også vurdere om en bør å belyse hvorvidt tilsynet med etterlevelse av forventninger og krav til risikovurderinger, beredskap og krisehåndtering ved ekstraordinære IKT-hendelser bør forsterkes med referanse til mål: "Sektoren ivaretar sikkerhet i lange og komplekse digitale verdikjeder" Begrunnelsen for dette er at verdien av digital informasjon og infrastruktur er meget høy (og økende), sårbarhetene er viktige å gjøre noe med og trusselbildet er særdeles krevende. Alle disse faktorene tilsier at også bruken av et virkemiddel som tilsyn bør trappes opp. Plasseringen av tilsynsvirksomheten bør også drøftes, herunder også koblingen til sektortilsyn og kompetansemiljø.

Forslag: Definere et eget innsatsområde for klargjøring og bevishetsgjøring av ansvars- og rollefordelingen knyttet til digital sikkerhet på alle nivå herunder myndigheter, virksomensledere og den enkelte medarbeidere. Et annet tiltak under dette innsatsområde kan være å sikre at ansvar for digital sikkerhet omtales og tydeliggjøres i alt relevante regelverk. Normen kan vurdere om det er behov for å supplere eksisterende veiledere og faktaark som beskriver krav til beredskapsplaner

6) **Tilbakemelding på innsatsområde 1: Videreutvikling av eksisterende nasjonale virkemidler**

Klikk eller trykk her for å skrive inn tekst.

7) **Tilbakemelding på innsatsområde 2: Kompetanse og sikkerhetskultur**

Klikk eller trykk her for å skrive inn tekst.

8) **Tilbakemelding på innsatsområde 3: Planverk og øvelser**

Klikk eller trykk her for å skrive inn tekst.

9) **Tilbakemelding på innsatsområde 4: Etterlevelse og oppfølging**

Klikk eller trykk her for å skrive inn tekst.

10) **Tilbakemelding på innsatsområde 5: Ny teknologi og digitale verdikjeder**

Klikk eller trykk her for å skrive inn tekst.

11) **Tilbakemelding på innsatsområde 6: Støtte til mindre virksomheter**

Klikk eller trykk her for å skrive inn tekst.

12) **Andre innspill og tilbakemeldinger**

Det anbefales å nummerere utfordringer, mål, innsatsområder og tiltak.