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

Høringsutkastet består av fem hoveddeler som Direktoratet for e-helse ønsker tilbakemelding på:

- En oversikt over hva som gjøres i sektoren i dag knyttet til digital sikkerhet, med hovedfokus på beredskap, herunder forebyggende arbeid
    - Hva gjøres i sektoren i dag – kapittel 2
    - Oversikt over eksisterende tiltak knyttet til digital sikkerhet i sektoren – vedlegg A
- En beskrivelse av de største utfordringene sektoren står overfor på området – kapittel 3
- Et forslag til mål for digital sikkerhet og beredskap i helse- og omsorgssektoren – kapittel 4
- Et forslag til innsatsområder i arbeidet med digital sikkerhet, med forslag til tiltak for hvert innsatsområde – kapittel 5

Der høringsinstansen har innspill, er det ønskelig med **en kort begrunnelse** og **gjerne konkrete forslag til endringer**.

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

Frist: 09.09.2022

Kontaktinformasjon

Navn på virksomhet: Helse Midt-Norge RHF

Kontaktperson: Bjørn-Einar Kolstad

E-postadresse: bjorn.einar.kolstad@helse-midt.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

Digitaliseringsrundskrivet fra Kommunal- og distriktsdepartementet bør være med. Det framgår tydelige krav i rundskrivet knyttet til både informasjonssikkerhet og personvern. Videre omfatter rundskrivet krav, anbefalinger og veiledning innen andre tema som indirekte bidrar til å styrke den digitale sikkerheten på tvers i offentlig sektor.

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:

Det kan nevnes i teksten at det finnes regionale og foretaksvise tiltak, i tillegg til de nasjonale som allerede er nevnt.

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

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

Utfordringsbildet setter blant annet fokus på et *udekket kompetansebehov*, herunder utfordringen med å rekruttere og beholde spesialistkompetanse. Dette forsterker det totale utfordringsbildet knyttet til digital sikkerhet, da dette forholdet kan gjøre det krevende å kunne gjennomføre alle lovpålagte og andre nødvendige tiltak. Denne utfordringen bør komme tydeligere frem i dokumentet.

Det er en stadig større grad av mobilitet i alle typer løsninger (fra kontorstøtte til medisinsk utstyr) som også kan benyttes i det private hjem. Selv om det står indirekte en del rundt dette i teksten i dokumentet, kan sikkerhetsutfordringen rundt manglede sikring også «innenfor brannmuren» fremheves bedre.

Det oppleves at det er mangelfull helhetlig kunnskap om avhengigheter mellom ulike IKT-system og hvordan bortfall av et system påvirker evnen til å yte helsehjelp. Dette kan delvis henge sammen med mangelfull kommunikasjon og uklare ansvar mellom leverandører og brukere av IKT-tjenester. Denne utfordringen bør i større grad omtales. Jf. også Helsetilsynets rapport *Forsvarlig pasientbehandling uten IKT?* av april 2021.

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**

Klikk eller trykk her for å skrive inn tekst.

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 krevende å velge *enten* Ja eller Nei ovenfor, da spørsmålet er stilt samlet for alle områdene)

De innsatsområdene som er foreslått støttes. Innspillene nedenfor (svarpunkt 5 – 11) gir likevel innspill til hva innsatsområdene/tiltakene bør suppleres eller forsterkes med.

Ettersom realismen med å gjennomføre tiltak under innsatsområdene også avhenger av muligheten til å rekruttere og beholde spesialistkompetanse, bør dette forholdet også nevnes innledningsvis i kapittel 5 (*Forslag til innsatsområder i arbeidet med digital sikkerhet*). Tilstrekkelig tilgang på spesialistkompetanse vurderes til å være en forutsetning for å oppnå målene gjennom de foreslåtte innsatsområdene.

I punktlisten som oppsummerer innsatsområdene (første side av kapittel 5) kan det vurderes om betydningen av å kunne styre risiko ved bruk av skytjenester eksplisitt bør nevnes under kulepunktet *Ny teknologi og digitale verdikjeder*.

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

Tiltak rundt videreutvikling av HelseCERT og Normen støttes.

I tillegg til administrative verktøy levert av bl.a. Microsoft, benytter også MTA og annet utstyr seg i stadig større grad av skytjenester. Helsesektoren ville hatt stor nytte av en felles nasjonal tilnærming rundt risiko ved bruk av skytjenester, da dette kan vurderes ulikt i ulike organisasjoner, noe som kan oppleves som krevende mht. samhandling, nasjonale anskaffelser mv. Dette anbefales vurdert som et nasjonalt virkemiddel.

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

Spesialistkompetanse:

Innsatsområdet slik det er beskrevet dekker i hovedsak innsatsfaktorer for å øke kompetanse- og sikkerhetskultur hos helsepersonell og andre ansatte («den enkelte»), men mangler innsatsfaktorer for utfordringen med spesialistkompetanse. Jf. kommentaren under kapittelet «Utfordringsbildet» mht. utfordringen og med å rekruttere og beholde spesialistkompetanse, og hvor kritisk dette er for virksomhetenes evne til å håndtere digital sikkerhet på en tilfredsstillende måte. Tiltak for denne utfordringen bør adresseres i dette dokumentet (i dette kapittelet eller i andre deler av dokumentet).

Kommentarer for øvrig for de foreslåtte tiltakene:

Det pågår mange initiativ hos de ulike aktørene i sektøren rundt kompetanse og sikkerhetskultur. Eventuelle *felles* aktiviteter og tiltak må være godt forankret i sektoren og må være målrettede og relevante.

Første foreslåtte tiltak i dokumentet er: *Gjennomføre en kartlegging og vurdering av eksisterende kompetansetiltak, med formål om at virkemidler som fungerer godt kan deles og gjenbrukes i hele sektoren*.

Andre foreslåtte tiltak i dokumentet er: *Basert på kartleggingen, vurdere behovet for en utredning av tiltak med formål å styrke kompetansen om digital sikkerhet hos helsepersonell.*

Disse to tiltakene foreslås spisset og slått sammen til ett tiltak, for eksempel:

Tilby relevante, konkrete og lett tilgjengelige kurs som styrker kompetansen om digital sikkerhet

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**

En styrking av tilsyn og andre kontrollfunksjoner er positivt og nødvendig, men viktigheten av at ledelsen legger til rette for etterlevelse gjennom å sikre tilstrekkelig kompetanse og ressurser, tydelige forventninger, hensiktsmessige styringssystemer mv. bør fremheves.

10) **Tilbakemelding på innsatsområde 5: Ny teknologi og digitale verdikjeder**
Klikk eller trykk her for å skrive inn tekst.

Jf. kommentarer under punkt 3 *Utfordringsbildet*:

- Det bør foreslås tiltak knyttet til kartlegging av IKT-systemenes kritikalitet og avhengigheter, og at dette skal være kjent i hele verdikjeden

- Det er en stadig større grad av mobilitet i alle typer løsninger (fra kontorstøtte til medisinsk utstyr) som også kan benyttes i det private hjem. Selv om det står indirekte en del rundt dette i teksten i dokumentet, bør sikkerhetsutfordringen rundt manglede sikring også «innenfor brannmuren» fremheves bedre.

Jf. kommentar i punkt 6 i svarskjemaet *Videreutvikling av nasjonale virkemidler*:
I tillegg til administrative verktøy levert av bla. Microsoft, benytter også MTA og annet utstyr seg i stadig større grad av skytjenester. Helsesektoren ville hatt stor nytte av en felles nasjonal tilnærming rundt risiko ved bruk av skytjenester, da dette kan vurderes ulikt i ulike organisasjoner, noe som kan oppleves som krevende mht. samhandling, nasjonale anskaffelser mv. Tiltak anbefales.

11) **Tilbakemelding på innsatsområde 6: Støtte til mindre virksomheter**
(Direktoratet for e-helse kan vurdere om kommentaren nedenfor også hører hjemme i andre deler av dokumentet, f.eks. under *Ny teknologi og digitale verdikjeder*).

En del mindre virksomheter har ikke nødvendigvis tilstrekkelige sikkerhetsløsninger, inklusive rutiner, som understøtter mobile enheter mv. på en god måte sikkerhetsmessig. Dette blir særlig gjeldende når disse virksomhetene skal koble seg på fellesløsninger/felleskomponenter/felles infrastruktur sammen med større virksomheter, da de større virksomhetene da kan bli eksponert for utilsiktede sikkerhetshull. Tiltakene bør være å gi støtte til mindre virksomheter rundt dette, supplert med krav og tilsyn som sikrer at disse følges.

12) **Andre innspill og tilbakemeldinger**
En del av tiltakene i høringsdokumentet har form som «kartlegge» og «utrede». Det anbefales å søke å gjøre tiltakene mer konkrete og direkte, der dette er mulig.

For en del av tiltakene som er foreslått i høringsdokumentet (jf. kapittel 5) går det implisitt frem hvem som er ansvarlig for tiltaket, for andre ikke. Det kan vurderes om forslag til ansvar bør tydeliggjøres.

Klikk eller trykk her for å skrive inn tekst.