

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 **gjærne 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 Nord RHF

Kontaktperson: Ida Martinussen

E-postadresse: postmottak.@helse-nord.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

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

Klikk eller trykk her for å skrive inn tekst.

Kapittel 3 gir et godt bilde på utfordringer i helse- og omsorgssektoren, men Helse Nord oppfatter at beskrivelsen bør være tydeligere på utfordringer knyttet til drift og forvaltning av medisinteknisk- og bygg-teknisk utstyr. Kapitlet gir et godt generelt bilde av utfordringene knyttet til kompleksitet, verdikjeder og manglende implementering av sikkerhetstiltak, men det kunne med fordel vært presisert at utfordringene er særlig aktuelle for medisinteknisk utstyr. En annen utfordring som kunne vært omtalt er koblingen mellom fysisk og digital sikkerhet. Sykehus skal være tilgjengelig for befolkningen, noe som medfører at fysisk adgangskontroll ikke er hensiktsmessig i mange områder av bygningene. Dette resulterer i risiko for den digitale sikkerheten, ved at uvedkommende har fysisk tilgang til IKT-utstyr og deler av infrastrukturen (f.eks nettverksporter og trådløse nett). Helse Nord oppfatter i tillegg at beskrivelsen bør omtale konsekvensen av de utfordringer som beskrives, der den alvorligste konsekvensen og utfordringen er å miste tilgang til de digitale tjenestene. Helseberedskapen bør gi en tydelig strategi/ retning for hvordan helsetjenesten skal kunne sikre forretningskontinuitet. For spesialisthelsetjenesten vil dette være evnen til å yte forsvarlig helsehjelp, dersom vi skulle bli rammet av de trusler som er beskrevet.

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

Målene som er beskrevet er passende og dekkende, men mål 5, eller mål 6 bør i tillegg beskrive evne og teknologi som sikrer forretningskontinuitet slik at helsetjenesten raskt er i stand til å reetablere plattformer og systemer for å utøve tjenestene som skal understøtte forsvarlig helsehjelp i en beredskapssituasjon. I tillegg savner Helse Nord et mål rundt kompetanse og sikkerhetskultur. Dette er et innsatsområde i kapittel 5, og en kritisk faktor for å håndtere utfordringene skissert i kapittel 3. Økt sikkerhetskompetanse og arbeid med sikkerhetskultur burde således være et uttalt mål i kapittel 4, med fokus på eksisterende ansatte i sektoren, samt som en del av helsefaglige utdanninger.

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

Flere av innsatsområdene, og foreslåtte tiltak er av overordnet karakter. Tiltakene som er foreslått anses som hensiktsmessig, men Helse Nord oppfatter at konkrete tiltak for å sikre forretningskontinuitet for raskt å reetablere infrastruktur og systemløsninger mangler, eks på ett konkret tiltak er en nasjonal sky for bruk i beredskapssituasjoner.

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

Se kommentar under punkt 5

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

Innsatsområdet burde også ha et tiltak for å sikre arbeidet med terminering av tjenester og løsninger. Beskrivelsen av innsatsområdet er god på tiltakene rundt innføring av ny teknologi, nye tjenester og nye verdikjeder. På den andre siden er forsvarlig terminering av eksisterende teknologi og tjenester ikke nevnt, men bør fremheves som et viktig arbeid for å redusere risiko og teknisk gjeld. Et annet konkret tiltak er at DSB sin modell for risikostyring i digitale verdikjeder (Lysene III rapporten) tas inn i veiledere til relevant sektorlovverk. Helse Nord oppfatter at det uklart hva som omfattes av tiltaket. Helse Nord vil fremheve viktigheten av at det i leverandør oppfølgingen skilles mellom virksomhetsansvaret og samfunnsansvaret, en problemstilling som er godt illustrert i Lysne III rapporten. Det følger blant annet av GDPR at virksomheter som benytter leverandør til å levere tjenester (som behandler personopplysninger) er ansvarlig for behandlingen selv om oppgaven er satt ut til tredjepart. Det er virksomheten som er ansvarlig for å gjennomføre dekkende risikovurderinger. Dette omfatter oversikt over verdier, gjennomføring av risikovurdering, risikohåndtering og iverksette risikoreducerende tiltak. Helse Nord oppfatter at virksomhetsansvaret er tydelig regulert, og at det finnes en rekke veiledere eks fra Normen/ NSM/ Digdir som råd gir hvordan denne prosessen kan gjennomføres. En overordnet oversikt og kunnskap om risiko, sårbarheter, og trusler i verdikjeden som bærende samfunnsfunksjoner er avhengig av et samfunnsansvar. Dersom en leverandør leverer tjenester som flere innen spesialisthelsetjenesten, og eller andre samfunnskritiske tjenester benytter seg av bør dette inngå i en slik oversikt. Den enkelte virksomhet er ansvarlig for egen risikovurdering, men hvordan fanger myndighetene opp at flere virksomheter benytter eks samme leverandør/ løsning for samfunnviktige tjenester? I tillegg vil HN fremheve behov for konkrete tiltak innen sektorlovgivningen som gir lovhjemmel for at det kan utføres utvidet bakgrunnssjekk for personell som har særlige rettigheter, og potensiell tilgang til store mengder helse- og personopplysninger. Dette er særlig aktuelt i de tilfeller der sikkerhetsloven ikke kommer til anvendelse.

11) Tilbakemelding på innsatsområde 6: Støtte til mindre virksomheter

Klikk eller trykk her for å skrive inn tekst.

12) Andre innspill og tilbakemeldinger

Ved å gjennomføre egen isolert høring til tema digital sikkerhet, tas dette ut av helheten. Det er utfordrende å kunne gi presise tilbakemeldinger til eks tiltak som bør implementeres for å sikre grunnleggende komponenter i infrastrukturen. Digital sikkerhet bør ses i en helhet, sammen med grunnleggende funksjoner (vann, strøm, internett m.m) som må være operativ for å kunne yte forsvarlig helsehjelp.