DIREKTORATET FOR E-HELSE
Postboks 221 Skøyen
0213 OSLO

Att.Jan Gunnar Broch

Deres ref.:	Vår ref.:	Saksbehandler:	Dato:
22/448	2022/625 - 7787/2022	Lars Erik Baugstø-Hartvigsen	09.09.2022

Høring - Innspill til kommende stortingsmelding om helseberedskap - tema digital sikkerhet

Høringsutkastet gir overordnet et godt bilde av status og utfordringsbilde og samler og fremstiller på en god måte informasjon fra en rekke ulike kilder.

Helse Vest RHF er av det syn at de foreslåtte målene i kapittel 4 er gode og dekkende.

Når det kommer til tiltak er mange av de foreslåtte tiltakene lite konkretiserte og presise. Det er mye pekt på behov for utredninger, vurderinger og «ytterligere bistand». Helse Vest RHF anfører at det vil være ønskelig med mer konkrete, målbare og gjennomførbare tiltak for å oppnå de gode målsetningene på kortere sikt. Vi har et par eksempler for forslag til presiserte tiltak i punktene 6) til 10) i høringssvarskjemaet.

Se for øvrig våre tilbakemeldinger i vedlegget.

Vennlig hilsen

Erik M. Hansen
Direktør for eHelse

Lars Erik Baugstø-Hartvigsen
Informasjonssikkerhetsleder

Dokumentet er elektronisk godkjent

1 Vedlegg: Utfylt høringssvarskjema

Postadresse:
Helse Vest RHF
Postboks 303 Forus
4066 Stavanger

Elektronisk adresse:
post@helse-vest.no
www.helse-vest.no

Besøksadresse:

Generell informasjon:
Sentralbord 51963800
Org.nr: 983658725

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 Vest RHF

Kontaktperson: Lars Erik Baugstø-Hartvigsen

E-postadresse: postmottak@helse-vest.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

Vurder å utdype litt rundt Normen: «Sentrale virkemidler som HelseCERT og Normen har lenge vært viktige for sektoren, og bidrar til at sektorens totale beredskapsevne styrkes, og at grunnleggende krav knyttet til informasjonssikkerhet likerettes og omforenes på tvers av sektoren.». Et eller flere steder kan det gjerne også nevnes at i tillegg til sekretariatet i Normen som ligger hos direktorat for eHelse så har Normen en bredt sammensatt styringsgruppe fra hele sektoren, og at faktaark og veiledere tas frem i bredt samarbeid på tvers i sektoren. Dette kan f.eks. være i kap. 2 eller i omtalen av direktorat for eHelse sist i kapittel 1. Se også tilbakemeldingen på punkt 2) under. Til opplistingen på side 9 om tiltak i de regionale handlingsplanene kan det også nevnes «styring, informasjonssikkerhet i medisinteknisk utstyr, og etterlevelse av NSM sine grunnprinsipper for IKT-sikkerhet». Disse omtales i Vedlegg A, men kan med fordel nevnes også i starten av dokumentet.

Juster tidsangivelsen på vedtak knyttet til sikkerhetsloven (side 10) i tråd med hva som blir realitetene: «Endelig vedtak er planlagt sendt før sommeren 2022.»
Til side 11: «Krav ved overføring til tredjeland er et område i stadig utvikling, og den enkelte virksomhet må gjøre vurderinger av hvorvidt tredjelandet gir like god beskyttelse av personopplysningene som innen EØS, gjerne med støtte i EDPB sin veileder (https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf) for overføring av personopplysninger til tredjeland.»
Videre spør vi oss om alt arbeidet med å sikre etterlevelse av NSM sine grunnprinsipper for IKT-sikkerhet som gjøres i sektoren bør omtales også her? HOD har i styringsdokumenter og oppdragsbrev til en rekke virksomheter kravsatt etterlevelse av disse prinsippene.
GDPR omtales, og artikkel 32 trekkes frem. I tillegg tenker Helse Vest RHF at det er relevant å peke på artikkel 25 om innebygd personvern.

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:

Under omtalen av Normen sin styringsgruppe kan det vurderes å presisere med følgende fra styringsgruppens mandat: «Formålet med styringsgruppen er å sikre at Normen forvaltes og videreutvikles som en bransjenorm og formidles til aktørene i sektoren. Styringsgruppen er et uavhengig organ og kan ikke instrueres av andre.»

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

☒ Ja ☐ Nei ☐ Har ingen kommentar

Helse Vest RHF er enige i fremstillingene i kapittel 3, disse er dekkende. Vi har imidlertid noen kommentarer. Vi foreslår en omformulering av innledningen av kapittelet på side 14: «Helsedata har høy verdi, og er særlig utsatt VED misbruk og uautorisert spredning. Behovet for å sikre konfidensialitet, tilgjengelighet og integritet til både informasjon og systemer er særlig sterkt, fordi det er evnen til å gi forsvarlig helsehjelp og ivareta pasientsikkerheten og taushetsplikt som står på spill.» - alternativt på annet vis trekke frem at opplysningenes sensitive innhold gjør at det er viktig for den enkelte registrerte at informasjonen beskyttes og sikres. I avsnittene om verdikjeder og teknologiskifter kan det gjerne understrekes at leverandørkjedeangrep er en reell og økende sårbarhet (ref. f.eks. SolarWinds), og at bruk av skytjenester gjør slike kjeder enda mer komplekse å overskue og følge opp. Vi er ikke heller nødvendigvis enige i premisset at «Når virksomheter som har roller i nasjonal beredskap og krisehåndtering er avhengige av sårbare leverandørkjeder som strekker seg ut av landet, har det betydning for Norges krisehåndteringsevne.» Det kan

argumenteres for at klok og gjennomtenkte anskaffelser av robuste skytjenester, hvor produksjon kan flyttes til andre geografiske arealer, vil kunne være mer robust enn løsninger som kun kan leveres fra et begrenset territorium eller i en nasjonalstat. Det er et «om» for mye i kapittelet om «Spesialisthelsetjenesten», det bør vel stå: «når det kommer til myndighet, ansvar og arbeidsoppgaver…»

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**

De foreslåtte målene er gode og dekkende. Vi har likevel et forslag til tillegg på side 20: «Gode felles tjenester og ressurser kan gi gevinster både i kvalitet, kostnader og tidsbruk. Det totale potensialet er stort, fordi små forbedringer hos mange virksomheter til sammen vil ha stor effekt. Videre er sektoren sammensatt av mange små virksomheter som i liten grad kan bygge opp IKT-kompetanse og IKT-sikkerhetskompetanse. Felles løsninger vil både være rasjonelt og lettere å sikre og nødvendig leverandørstyring og sikring av leverandørkjeder er lettere å ivareta med færre tjenester med større volum.»

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**

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

Er det mulig å foreslå hvordan HelseCERT og Normen bør videreutvikles? For eksempel er HelseCERT sin fagmiljø for penetrasjonstesting veldig godt, og deres kapasitet kan med fordel styrkes slik at større deler av sektoren kan benytte denne. Og kan det for eksempel tenkes at DBD (Digital beskyttelse i Dybden) breddes og finansieres bedre hos HelseCERT? Videre kan det vurderes at Normen og eventuelt sekretariatet for Normen styrkes i retning av å lage og vedlikeholde kompetansetiltak på sikkerhetskultur og digitalt sikkerhet (ref. også kommentar på punkt 7) under?

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

Teksten på innsatsområdet støttes, men vi foreslår en presisering av tiltakspunkt 1 og 2 i retning av å «Utvikle felles elæringskurs for klinikere, administrativt personell, forskere i sektoren, IKT-personell og leverandører i helsesektoren med fokus på digital sikkerhet. Tiltaket kan gjerne plasseres hos sekretariatet for Normen, da dette har god dialog med sektoren og god kjennskap til hva som finnes av eksisterende kompetansetiltak.» Dette kan også sees i sammenheng med det foreslåtte tiltaket «Videreutvikle Normen» i innsatsområde 1. Kan punktet «bidra til økt oppmerksomhet på digital sikkerhetskompetanse i helsefaglige

utdanninger» knyttes opp mot funn og leveranser fra DigSam-prosjektet, omtalt i Vedlegg A?

8) **Tilbakemelding på innsatsområde 3: Planverk og øvelser**
Innsatsområdet er godt beskrevet. Det kan tenkes at «leverandører» også bør legges til nederst på side 28 under virksomheter som bør delta i planlegging, gjennomføring og læring etter øvelser. På dette området er de foreslåtte tiltakene godt konkretisert.

9) **Tilbakemelding på innsatsområde 4: Etterlevelse og oppfølging**
Helse Vest RHF er helt enige i at det er sentralt at nødvendig sikkerhetsstyring er integrert i ordinær virksomhetsstyring. Tiltak om støtte gjennom veiledning og verktøy er viktig, og gjerne viktigere enn ytterligere kontrolltiltak og krav til dokumentasjon og rapportering. Støtte og veiledning bør i tilfelle komme først, og kontroll etter hvert, for å se om krav og ambisjoner leveres på.

10) **Tilbakemelding på innsatsområde 5: Ny teknologi og digitale verdikjeder**
Innsatsområdet «Ny teknologi og digitale verdikjeder» kan muligens romme dette, men helsesektorens «trygge reise til skyen» i form av ansvarlig og sikker ibruktakelse av skyteknologi er en så stor endringsreise at problemstilling kan løftes tydeligere. For eksempel kan det skrives: «Bruk av ny teknologi gir bedre og mer effektive løsninger, men fører også med seg nye sårbarheter, og behov for ny kunnskap både i anskaffelse, forvaltning, leverandørstyring og utfasing av for eksempel skytjenester». En annen, relatert problemstilling som gjerne faller utenfor denne høringen, er at statens anskaffelsesregelverk og statens standardavtaler ikke nødvendigvis er adekvate og dekkende i forhold til anskaffelser av skytjenester. Et tiltak vil eventuelt kunne være å oppfordre Digitaliseringsdirektoratet til å innhente erfaringer fra skyanskaffelser i ulike deler av forvaltningen, og eventuelt videreutvikle anskaffelsesregelverk og SSA i tråd med funn.

11) **Tilbakemelding på innsatsområde 6: Støtte til mindre virksomheter**
Det er gledelig at det pekes på støtte til mindre virksomheter. Sett fra spesialisthelsetjenestens side vil dette bidra til å styrke sikkerheten i sektoren i stort, samt også kunne tilrettelegge for enklere og raskere digitalisering og bedre samhandling på tvers i sektoren. Data kan også følge pasiententforløp, og det kan tilrettelegges for gode vekslinger når pasient og behandling flyttes mellom virksomheter. Adekvat og sikker datadeling er også et behov for å understøtte dette bildet.

12) **Andre innspill og tilbakemeldinger**
Til innledning: Forslag til ny tekst nederst side 1: «Nødvendig sikkerhetsstyring må være integrert i ordinær virksomhetsstyring. Den som har ansvar for et fagområde eller en tjeneste i en normalsituasjon, har også ansvaret for nødvendige beredskapsforberedelser og håndtering av ekstraordinære hendelser på sitt område (nærhetsprinsippet).»
Videre på side 2 kan gjerne skytjenester og skyleveranser omtales for eksempel slik: «Samtidig introduserer digitalisering avhengigheter og nye sårbarheter gjennom stadig mer komplekse og integrerte systemer, herunder bruk av skytjenester som setter nye

krav til forvaltning, leverandørstyring og ansvarsoppfølging.»
Vi foreslår også at det utdypes litt mer om HelseCERT sitt arbeid på side 4, f.eks. «HelseCERT tilbyr også kostnadsfritt tjenester til helsesektoren gjennom Nasjonalt Beskyttelsesprogram NBP. Tjenester i NBP inkluderer blant annet informasjonsdeling, forebygging, rådgivning, hendelseshåndtering, sårbarhetsskanning og inntrengingstesting»