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: NITO – Norges ingeniør- og teknologorganisasjon
Kontaktperson: Sine Emborg Tolfsen
E-postadresse: **sine.emborg.tolfsen@nito.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**

   NITO har siden 2016 bedt om at IKT-infrastrukturen i helsevesenet underlegges sikkerhetsloven. Med lagring og drift av samfunnskritiske registre i Norge, herunder helseregistre, får myndighetene bedre kontroll med at selskapene følger lover og regler.

   NITO mener at fokuset på sikkerhetskultur ikke kommer godt nok fram i kapittelet. For å endre og forbedre forståelsen og etterlevelsen av grunnprinsippene for informasjonssikkerhet er opplæring svært viktig for at alle som jobber med sårbare IKT-systemer, slik at de forstår sitt eget ansvar og utøver sikker atferd. Det må settes av tid til opplæring og den må tilpasses de enkelte helsefaggruppenes forutsetninger og arbeidssituasjon. Andre viktige områder er meldekultur for sikkerhetsbrudd og lederansvaret.

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**

Det kommer tydelig frem i kapittelet at utfordringen knyttet til kunnskap beskrives som et «udekket kompetansebehov» innen digital sikkerhet, ikke minst fordi det ligger ganske langt utenfor kjernekompetansen til helsepersonell. Personell i sykehus og andre deler av helsesektoren har hovedfokuset på å gjøre jobben på en best mulig faglig og effektiv måte til pasientens beste, og ikke på digitale sikkerhetstrusler. IKT fagspråk og advarsler blir ofte teoretiske og vanskelig å ta til seg for mange i en travel hverdag. Noe av begrunnelsen for ikke å følge alle prinsippene for informasjonssikkerhet er manglende tilgang på pc-er og tidkrevende inn- og utlogginger på grunn av lite helhetlige løsninger. Dette er fortsatt en stor utfordring.

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**

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**

De nasjonale sikkerhetskravene skal ikke baseres på frivillighet fra helseforetakenes side. En mulighet er å innføre en type obligatoriske minstekrav, med tilhørende kompenserende tiltak og avviksrapportering. Norm for informasjonssikkerhet i helse- og omsorgstjenesten benytter seg i dag ikke av slike standardiserte minstekrav. Normen beskriver en rekke krav som den enkelte virksomhet har ansvar for. At den enkelte virksomhetsleder skal gjøre dette, kan være uheldig. NITO mener nyansatte bør ha obligatorisk opplæring i Norm for informasjonssikkerhet. Kurs i informasjonssikkerhet for nyansatte må imidlertid tilpasses ulike personellgrupper i helsesektoren i forhold til oppgaver og krav i stillingen.

Det er positivt at det settes fokus på kompetanse om digital sikkerhet og sikkerhetskultur og det er viktig å prioritere dette i praksis. NITO mener det er svært viktig å få det inn, både i grunnutdanningen, i etter- og videreutdanninger, og i arbeidsplassrelatert opplæring. Ansatte i topplederstillinger må forstå hvor viktig informasjonssikkerhet er. De som ikke selv besitter tilstrekkelig kompetanse må ha gode rådgivere på toppnivå, som har slik kompetanse og som

kan kommunisere dette på en tydelig og forståelig måte. IKT-kompetanse blir stadig viktigere i alle deler av arbeidslivet.[1] Samtidig utdannes det for få innen IKT i Norge, og ikke minst innen IKT-sikkerhet. NITO mener kunnskap om IKT-sikkerhet må få større plass i alle ingeniør- og teknologutdanningene. Forskning på sikkerhet og sårbarhet må styrkes, og det må utdannes flere spesialister innen IKT-sikkerhet.

Direktoratets forslag om innsatsområder med tilhørende tiltak for arbeidet med digital sikkerhet gir et tydelig signal for de ortopediske verkstedenes prioriteringer. Når mindre virksomheter skal ha større oppmerksomhet på digital sikkerhet, må det prioriteres og anerkjennes som et arbeid som må gjøres. Dette er viktig, siden mer tid til ikke-kliniske oppgaver i hverdagen er vanskelig å prioritere. NITO har også merket seg/er positiv til at kompetanseutfordringene for mindre virksomheter adresseres.

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**
NITO ønsker å trekke frem, at det er viktig med øvelser, og at foretakenes IKT organisasjoner tar del i øvelsene. Øvelser i regi av HelseCert må være scopet, slik at det blir reelle øvelser som også gir utbytte fra et teknisk perspektiv.

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**
Klikk eller trykk her for å skrive inn tekst.

[1] https://www.nito.no/politikk/undersokelser/norges-behov-for-ikt-kompetanse-i-dag-og-framover/

NITO

Direktoratet for e-helse

Pb. 221 Skøyen
0213 Oslo

09.09.09.2022

Vår ref. Sine Emborg Tolfsen Deres ref. 22/448

Oversendelsesbrev – NITOs innspill til kommende stortingsmelding om helseberedskap – tema: Digital sikkerhet

NITO – Norges Ingeniør- og Teknologorganisasjon, er Norges største organisasjon for ingeniører og teknologer med over 97 000 medlemmer. NITOs medlemmer innen helse og helsenæringer arbeider i helseforetakene, statlig, kommunal, ideell og privat sektor. Våre medlemmer har viktige roller i innovativ utvikling av produkter, tjenester og teknologiske løsninger. Mange arbeider systematisk med kvalitetssystemer og internkontroll knyttet til medisinsk behandling av pasientene. Andre ingeniører og teknologer er med på å planlegge, bygge, drifte og vedlikeholde teknologi, bygningsmasse og teknisk utstyr.

Ta gjerne kontakt for utdypende kommentarer og innspill i deres arbeid med innspill til kommende stortingsmelding om helseberedskap – tema: digital sikkerhet.

Med vennlig hilsen

Trond Markussen
President

Egil Thompson
Generalsekretær