DEN NORSKE LEGEFORENING

DIREKTORATET FOR E-HELSE
PB 6737, St. Olavs plass
0107
Oslo

Deres ref.: 22/448 Vår ref: HSAK202200252 Dato: 26-08-2022

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

Legeforeningen 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 Legeforeningens organisasjonsledd. Disse uttalelsene ligger til grunn for foreliggende høringsuttalelse, som er behandlet av Legeforeningens sentralstyre.

Innledning

Legeforeningen vil gi ros for at helseberedskap ses på samlet. Det er mange likhetstrekk mellom ulike samfunnssektorer, og dermed også viktig å identifisere områder der både utfordringene og løsningen kan være felles. Det er imidlertid også viktig å benytte perspektivet til den enkelte sektor, både for å prioritere, men også for å se på utfordringsbildet i sin helhet. Dette er ikke bare avgrenset til digital sikkerhet. Legeforeningen mener at dette perspektivet ikke er synliggjort i tilstrekkelig grad i det tilsendte notatet. Digital sikkerhet er tema, men det burde i mye større grad sett på hvordan digital sikkerhet forholder seg til de andre faktorene i helseberedskapen, med utgangspunkt i det som er helsesektorens overordnede mål; å yte gode, sikre og likeverdige helsetjenester.

Pasient- og pårørendeperspektivet er i praksis fraværende. Det står en del om hvilke tiltak som er pågående i sektoren, men ikke hvordan dette tilpasses for å støtte opp om virksomhetens egenart. Overordnet fokus burde således vært på helseberedskap, ikke teknologiberedskap.

Selv om det er samlet betydelig med kunnskap og erfaring med bruk av informasjonsteknologi under pandemien har man ikke trukket konsekvensene av dette i notatet.

Direktoratet for e-helses rolle som både faglig premissleverandør og forvaltningsorgan og konsekvensene av denne rollen for helseberedskapen er ikke redegjort for.

DEN NORSKE LEGEFORENING

Pasientsikkerhet, pårørende og private aktører

Til tross for at notatet skal handle om helseberedskap er pasientsikkerhet knapt nevnt, og synes ikke å ha noen innflytelse på innholdet. Således skal figur 1 være en illustrasjon av digital sikkerhet og vise overlapp med informasjonssikkerhet. «Pasientsikkerhet» burde imidlertid inngå i figuren, og burde egentlig vært på topp. Gjennomgangen av *Nasjonal strategi for digital sikkerhet* er relevant. En oppfølging av strategien burde imidlertid dreie seg om hvordan dette forholder seg til pasientsikkerhet.

Pårørende er en viktig ressurs i helseberedskapen. Det har vært anslått at pårørende utfører nesten like mange årsverk til pleie og omsorg som hele sektoren. I et beredskapsperspektiv burde det i mye større grad legge grunnlag for å kunne utnytte denne ressursen så riktig som mulig, og gode IKT-verktøy kunne være viktig virkemidler for å understøtte denne viktige ressursen. Dette omtales ikke i det hele tatt.

I kapittel 1 listes det opp offentlige aktører med rolle innen digital sikkerhet. Det er selvsagt viktig. Samtidig unnlater man å nevne den betydelige rolle private aktører spiller. Under pandemien leverte HelseNorge viktige verktøy, men var ikke i stand til dekke andre viktige behov som sektoren trengte. Private aktører leverte løsninger som flittig ble brukt. I et beredskapsperspektiv er vi avhengige av å ha en kompetent og levedyktig industri som kan bidra på en slik måte. Monopolløsninger er konkurransehemmende, og dermed en trussel mot helseberedskapen. Man burde i stedet se på hvordan IKT-næringen kan få bærekraftige rammebetingelser. Således burde samarbeid med private IKT-aktører og tilrettelegging av stabile rammebetingelser for dem inngå i notatet.

Spørsmål som man ønsker tilbakemelding på

1. Er det mangler i beskrivelsen av pågående initiativer knyttet til digital sikkerhet i nasjonal helseberedskap (kapittel 2 og vedlegg A)? Vi ønsker beskrivelse av initiativer som ikke er med og innspill der eksisterende beskrivelser er upresise eller mangelfulle.

Legeforeningen anser det som naturlig å omtale arbeidet med informasjonssikkerhet i tråd med NSM sine grunnprinsipper for sikkerhetsstyring. Mange virksomheter fokuserer sitt sikkerhetsarbeid rundt identifisering av verdier, ROS-analyser, ledelsens gjennomgang, tiltaksplaner, hendelseshåndtering og øvelser. Dette er et omfattende arbeid, viktig for bevisstgjøring og med muligheter for tilpasning til virksomhetens spesifikke aktivitet og risikobilde.

Mye av den digitale sikkerheten ligger utenfor legekontorenes rekkevidde for kontroll: Fastlegekontorene og privatpraktiserende leger er pålagt medlemskap i NHN og er helt avhengig av tilgjengelighet og oppetid i NHN for tilgang til sentrale databaser og tjenester som kjernejournal, reseptformidler, mm. Mange har NHN som eneste tilknytning til internett og er avhengig av denne kanalen for kommunikasjon med alle andre aktører. Både fastlegekontorene, private legekontor og kommunene trenger støtte til vurderinger knyttet til risiko ved nedetid. Dette er spesielt aktuelt for kontorene som har varianter av fjernserver/skylagring. Det er ikke nevnt noe i kapittel 2 om samhandling mellom primær- og spesialisthelsetjenesten når det gjelder bortfall av tjenester/brudd i helsenett/tap av data/etc. Brudd i kommunikasjon mellom nivåene er ikke nevnt.

Det er positivt at man har et fokus på å støtte mindre virksomheter, men dersom det blir aktuelt å pålegge slike virksomheter ytterligere forpliktelser, er det viktig at man hensyntar forutsetningene man har for å ivareta forpliktelsene i aktuelle virksomhet, og at forpliktelser eventuelt uansett kombineres med støtte, veiledning, mv. Behovet for veiledning til mindre virksomheter er uansett viktig. Det kan f.eks. være nyttig om mindre legekontor gis mulighet til å ta imot noen på kontoret som kan veilede mht. å beskytte seg mot, avdekke og håndtere digitale angrep. Kan det utredes om Normen i større grad skal tilby veiledningsfunksjoner til mindre virksomheter? Kan et samarbeid med virksomheter som for eksempel Trinnvis være et egnet virkemiddel?

Normen (Norm for informasjonssikkerhet i helsesektoren) har vært et viktig og riktig bidrag til å bedre informasjonssikkerhet og personvern i sektoren. Dette omtales også. Legeforeningen er som kjent både aktiv støttespiller og deltager i arbeidet, og Legeforeningens representant er i dag nestleder. Det som imidlertid ikke nevnes, er at en viktig grunn til at Normen har vært vellykket, er at det er en uavhengig bransjenorm som forvaltes av et selvstendig organ med representanter fra sektoren.

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

Notatet er veldig generelt og overordnet, og kan virke fjernt fra utfordringene som oppleves ute i helsetjenesten. Notatet omtaler nesten ikke pasientsikkerhet eller helsepersonellperspektivet og kravene til tilgjengelighet, integritet og konfidensialitet. Sikring av tekniske IKT-løsninger vil i stor grad måtte gjøres av sentrale statlige organer utenfor den operative helsetjenesten. Dersom sikkerhetsløsningene som utvikles skal være forenlige med helsetjenestens formål og løpende krav til pasientbehandling, må sektorspesifikke behov synliggjøres. Effektive og sikre tilgangs- og kommunikasjonsløsninger er i dag nødvendige for å kunne yte forsvarlig helsehjelp, også under høyt tidspress, og dette stiller særskilte krav til løsningene.

Det er komplisert og omfattende å sette seg inn i lovgivningen rundt IKT-systemene og mange har valgt å sette bort drift av server for EPJ i forskjellige former både ved server fysisk i hus og ved fjernserver. I praksis er de fleste legekontorene gjennom sine avtaler med NHN, kommune og EPJ-leverandør helt prisgitt at disse aktørene gjør sin jobb er i tråd med normen. Mange av landets fastleger og øvrige leger i primærhelsetjenesten har med andre ord i liten grad mulighet og kompetanse til å kontrollere og ettergå dette, selv om de sitter på dataansvaret. Det bør tydeliggjøres at kommunene må ta dette i betraktning ved gjennomgang av risikobildet lokalt gjennom sitt ansvar for tilrettelegging for tjenestene. Her er det helt klart behov for en nasjonal strategi på hvordan en skaffer oversikt og hvordan risiko kartlegges.

Når man i utfordringsbildet viser til et «stort og komplekst landskap av systemer», ser man bort fra at dette landskapet faktisk er nødvendig for at sektoren skal kunne fokusere på sin hovedmålsetting. Myndighetenes rolle burde snarere være å definere, utvikle og kontrollere standarder som systemene skal følge enn å forsøke å drive overordnet styring. Det står at «NSM erfarer at det ofte er de samme feilene som gjøres, både i offentlige og private bedrifter». Dette illustrerer behovet for standarder, og gir vel også en indikasjon på at det

ikke er IKT-industrien eller helsevirksomhetene som er problemet, men snarere mangelfull nasjonal koordinering, mangelfullt utgangspunkt i tjenestens behov og fasilitering av den daglige driften i helsetjenesten.

Det bør omtales hvor sektoren står nå og hvilke hovedutfordringer som må gripes fatt i. Et eksempel er det kritiske behovet for innsyn på tvers av virksomheter. Den akuttmedisinske kjeden er tidskritisk, og består av forskjellige virksomheter: fastlegen, kommunal legevakt, sykehusenes AMK-sentral og akuttavdelinger. Vi ser mange eksempler på at informasjonsmangel hindrer pasientbehandling og skader pasientene. Et annet eksempel er at røntgen- og laboratoriesvar ikke er tilgjengelig der pasienten befinner seg til enhver tid. Slike utfordringer bør legges til grunn for en digital sikkerhetsstrategi, slik at aktørene kan finne felles mål for arbeidet.

Store geografiske og tjenestemessige avstander mellom de som opplever utfordringene og de som kan løse dem er en viktig erfaring å ta med seg, og er i seg selv er en trussel mot den digitale sikkerhet.

I høringsutkastet trekker man frem som en utfordring avhengighet av tekniske løsninger, komplekse systemlandskaper og lange kommunikasjonskjeder. Det er derimot i liten grad omtalt hvilken beredskap man har dersom det skulle oppstå svikt. Behovet for å utarbeide beredskapsplaner er nevnt. Det er lite konkretisert hva disse planene skal omfatte. Hva slags beredskap skal man nå legge planer for? Skal man f.eks. legge planer for beredskap ved nedetid på NHN eller andre kritiske kommunikasjonskanaler? Dette bør spesifiseres.

Det finnes mange gode sikkerhetsløsninger i helsetjenestens egne fagsystemer og infrastrukturen i helsenettet, men behovene for å åpne kommunikasjonen mellom fagsystemer og ut mot eksterne systemer gir nye risikoelementer. Spørsmålet om hvilke elementer i IKT-strukturen som det er særlig viktig å sikre, bør besvares. Helsetjenesten er avhengig av nasjonal, digital utveksling av data mellom elektronisk pasientjournal, slik som elektroniske meldinger for henvisning, epikrise, rekvisisjoner og svar, e-resept, m.m. Disse løsningene må alle være sikret slik at de kan fungere under alle scenarier. Fremtiden vil bringe flere slike systemer, med enda større avhengigheter – noe som gjør helsetjenesten enda mer sårbar. Enkle og robuste mekanismer ved bortfall av elektronisk pasientjournal og elektronisk samhandling er kritiske tiltak. Det må være en plan for håndtering av bortfall av teknologiske hjelpemidler i krisesituasjoner.

Det ville vært naturlig å omtale hvilken lærdom vi har fra pandemien når det gjelder helseberedskapssituasjoner. F.eks. så vi under pandemien behov for nye applikasjoner, nye integrasjoner, sammenkopling av datakilder, tilgjengeliggjøring av data på tvers av virksomheter, etablering av muligheter for befolkningen selv til både å skrive og lese data som helsepersonell ikke hadde kapasitet til (som prøveresultater og vaksinasjonsbevis). Hvilke konsekvenser har disse erfaringene for sikkerhetstenkningen?

3. Beskriver de foreslåtte målene for arbeidet med digital sikkerhet i nasjonal helseberedskap (kapittel 4) et passende og dekkende målbilde?

I notatet plasseres ansvaret hos helsevirksomhetene, og vektlegger å bygge opp deres IT-kompetanse, men er i liten grad tilpasset sektorens særskilte behov og forutsetninger:

tjenestens formål, oppbygging, struktur og utfordringsbilde. Forståelse av dette er nødvendig for å kunne avgjøre hva som må sikres, og hvem som er best egnet til å gjennomføre forskjellige tiltak. Vi savner en beskrivelse av statens rolle og hvordan disse skal tydeliggjøres og ivaretas.

4. Er de foreslåtte innsatsområdene og de foreslåtte tiltakene (kapittel 5) hensiktsmessige, og er de realistiske å gjennomføre?

Støtte til mindre virksomheter

Det er glimrende at man ser på dette som et særskilt område. Vi savner et avsnitt som beskriver statens ansvar for å sikre sentral infrastruktur på vegne av hele sektoren, og tiltak for å øke kvaliteten på denne. Det er særlig viktig for de små aktørene, som verken har økonomi eller kompetanse til å utvikle løsningene. Også de store helseforetakene trenger å kunne stole på nasjonal sikring av infrastruktur og kritiske elementer.

Vi trenger:

- sentraliserte løsninger for drift med innebygget informasjonssikkerhet
- godkjenning av dialogpartnere, f.eks. ved tilknytningen til Helsenettet
- godkjenning av IKT-leverandørers løsninger

Får vi denne hjelpen, vil det gi helsearbeiderne i klinikken muligheten til å fokusere på trygg pasientbehandling og sikker informasjonshåndtering lokalt.

Det er særlig viktig at staten tar ansvar for å utvikle hensiktsmessige og sikre løsninger i overgangen mellom internett og Norsk helsenett, slik at virksomhetene kan basere sitt eget sikkerhetsarbeid på interne fremfor eksterne systemer og prosesser. Staten må ta ansvar for konkrete tiltak som f.eks. disse:

- Sikre kommunikasjon med pasienter gjennom HelseNorge (og andre mekanismer), herunder sikre elektroniske meldinger, timebestilling, e-konsultasjon, videokonsultasjon, prøvesvartjeneste med videre. Gode universelle identifiserings- og autentiseringsmekanismer for pasientene og virksomhetene.
- Sikre kommunikasjon med velferdsteknologi utenfor institusjonene, herunder hjemmeoppfølging og informasjonsflyt fra/til teknisk utstyr og helseapper.
- Sikre kommunikasjon mellom helsetjenesten og virksomheter utenfor helsenett. Det sendes store mengder sensitive data til legekontor/helseforetak fra NAV, forsikringsselskaper, statsforvaltere og kommunale tjenester (bl.a. barneverntjenesten). Mye av meldingsflyten går i SvarUt og ankommer i Altinn, som har sikkerhetsoppsett med svakere sikkerhet enn pasientjournalsystemene har. Altinn er mange steder ikke bygget opp for sikre forsvarlig mottak av sensitive opplysninger og pasientopplysninger skal ikke sendes til helsepersonellets private Altinn-innboks. Det er behov for løsninger som sikrer at informasjonen kommuniseres til pasientjournalsystemene og kan behandles sikkert der.

- Sikre en enhetlig praksis fra statlige myndigheters side når det gjelder rekvirering, skjema, melderutiner, osv. Løsningen må integreres med fagsystemene og sikre lagring/tilgjengelighet både sentralt og i lokalt fagsystem. Mange parallelle løsninger med særegen pålogging, manuelle prosesser og dobbeltarbeid for helsepersonellet utfordrer både dataintegritet, konfidensialitet, kvalitet og effektivitet i tjenesten. Mangel på gode, effektive løsninger fører også til at helsearbeidere benytter usikre metoder for å løse kliniske problemer i hverdagen.
- Staten bør understøtte systemer for internkontroll og kvalitetsforbedring som er rettet mot helsepersonell og helsevirksomheter, slik at IKT-sikkerhetstiltak kan innarbeides.

Legeforeningen støtter sterkt at små virksomheter ikke må overlates til seg selv. Ansvar for retningslinjer og ikke minst utarbeidelse og testing av praktiske verktøy for sikker implementering må ligge på store aktører regionalt og nasjonalt, slik høringsnotatet anfører. Leverandører av hard- og software må involveres tungt, ikke minst EPJ-leverandører til foretak, kommuner og fastlegepraksiser slik at verktøyene integreres med helsepersonells daglige arbeidsflater på en forståelig måte, også for dem uten spesiell IT-kunnskap.

Kompetansetiltak

De foreslåtte generelle opplæringstiltak støttes. Det er risiko for at slike blir for omfattende og generelle til at de når målgruppen i klinikken. Det er nødvendig at man jobber med tiltak helt ut til den enkelte medarbeider. Slike tiltak må være enkle å ta i bruk og innrettet mot klinikknære utfordringer. Legeforeningen støtter punktet om at digital sikkerhet og kompetanse må inn i helseutdanningene og det må gjelde alle involverte profesjoner.

I hverdagen kan man oppleve at sikkerhetstiltak hindrer effektivitet. Eksempler fra sykehus er betydelig tidsbruk for gjentatte ganger i løpet av en dag å måtte logge inn i systemer og programmer i forbindelse med tilsyn på ulike avdelinger, og begrenset tilgjengelighet til pasientinformasjon på tvers av avdelinger. Her må det finnes en rimelig balanse mellom nødvendig personvern (ivaretakelse av taushetsplikten) på den ene siden og effektivitet i arbeidshverdagen på den andre siden.

I notatet er manglende kompetanse begrenset til å gjelde helsepersonell både når det gjelder informasjonssikkerhet og de tekniske løsninger de benytter. Det er selvsagt et viktig perspektiv. Imidlertid er det like viktig at de som utvikler, innfører og vedlikeholder disse tekniske løsningene har en grunnleggende forståelse for sektorens oppgaver, prioriteringer og virksomhet. Hvis denne kompetansen mangler, er det lett å innføre helt feil løsninger – som kan sette både pasientsikkerheten og informasjonssikkerheten i fare. Dermed burde en også diskutere hvordan man skal gi teknologene grunnleggende helsefaglig innsikt, tilsvarende den teknologiske innsikt man forventer at helsepersonell skal utvikle. Manglende forståelse for egen kunnskapsmangel kan i seg selv være en trussel.

DEN NORSKE LEGEFORENING

Planverk og øvelser

Øvelser på området støttes, gjerne felles øvelser på tvers av profesjonsgrenser og involverte aktører/bransjer. Det er viktig for å nå ut i tjenesteapparatet at slike innarbeides i det generelle beredskapssystemet i helsevirksomhetene, og uheldig dersom IKT-området løsrives helt.

Etterlevelse og oppfølging

Det er viktig at malverk og dokumentasjonskrav ikke er for omfattende. Dersom kompleksitet og tidsbruk på kartlegging og rapportering blir for stor, vil det ikke gjenstå tid til å gjennomføre de tiltakene som kan forbedre situasjonen i helsevirksomhetene. Det beste kan bli det godes fiende. Som alltid må viktighet og nytte veies mot ressursbruk. Ressursene, både arbeidskraft og materiell, må fordeles ut fra truslers alvorlighetsgrad og ev. konsekvenser, og antatt risiko for at det det som fryktes, skjer.

Nytt innsatsområde: Forskning og fagutvikling

Forskning og fagutvikling burde vært et eget innsatsområde, og kan synes uteglemt. Trusselbildet er ikke statisk. For å følge med trengs det ikke bare en fortløpende overvåkning, men også å utvikle ny kunnskap, ny innsikt og nye metoder. Dette er oppgaver som naturlig hører hjemme i uavhengige forskningsmiljøer, og i dokumentet bør det diskuteres hvordan man skal kunne utvikle og vedlikeholde forskning på helsesektorens spesifikke utfordringer, ikke bare generelle metoder.

Legeforeningen ønsker lykke til med det videre arbeidet med stortingsmeldingen og ser frem til å bidra på egnet tidspunkt.

Med hilsen
Den norske legeforening

Siri Skumlien
generalsekretær

Kari-Jussie Lønning
Fagdirektør/lege

Anne Ringnes
Spesialrådgiver

Dokumentet er godkjent elektronisk