DEN NORSKE
LEGEFORENING

Akademikerne
Hanne Jordell
Fridtjof Nansens plass 6
0160 Oslo

Deres ref.: Vår ref.: 18/600 Dato: 7.2.2018

**Innspill til IKT-sikkerhetsutvalget**

Legeforeningen viser til e-post fra Akademikerne om innspill til IKT-sikkerhetsutvalget.

Innledningsvis er det verdt å merke seg at begrepet IKT-sikkerhet brukes gjennomgående i Stortingsmeldingen (Meld. St. 38 (2016 –2017)) om IKT-sikkerhet, ikke begrepet informasjonssikkerhet. Fokuset på teknologi og ikke informasjonssikkerhet burde der vært begrunnet. IKT-sikkerhet er evnen til å ha kontroll med risiko med IKT-systemer. Informasjonssikkerhet er å sikre både konfidensialitet, integritet og tilgjengelighet på informasjonen som behandles.

Personvern og konfidensialitet står sentralt i helsetjenesten. Både legene og myndighetene er avhengig av tillit til at vi tar vare på pasientene og informasjonen deres. Derfor er det uhyre viktig at ny teknologi og endrede strukturer ikke skader dette tillitsforholdet. Alle må kunne være sikre på at opplysninger ikke misbrukes eller kommer på avveie. Helsedirektoratet trekker i ny rapport frem at pasientbehandling og pasientsikkerhet i økende grad blir avhengig av IKT[1]. For helsetjenesten er IKT ikke bare infrastruktur, slik en får inntrykk av. Det er IKT-baserte medisinske verktøy som benyttes i utredning og behandling av pasienter, både til å forvalte og anvende pasientinformasjon og medisinsk kunnskap, og ikke minst i samhandling om helsehjelp. Dersom pasienten ikke har tillit til at helsetjenesten ivaretar opplysninger, risikerer man at livsviktig informasjon ikke blir kommunisert, eller at pasienten ikke oppsøker helsetjenesten. Pasienten er fortsatt – og vil alltid være – den viktigste informasjonskilden når helseproblemer krever undersøkelse og behandling.

Et utviklingstrekk er at interessen for personopplysninger øker. Stjålne helseopplysninger kan f.eks. utnyttes til identitetstyveri. Informasjon om politikere, militære og familiene deres kan utnyttes for å utøve press i konfliktsituasjoner. Helsepersonell, sykehus og kommuner er potensielle mål for slik informasjonsinnsamling. Registre og journaler er utsatt siden de inneholder opplysninger om store deler av befolkningen.

[1] Helsedirektoratets rapport «Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren» (06/2017)

Tjenesteutsetting blir stadig mer utbredt i offentlig sektor og private leverandører er nødvendig for å modernisere og digitalisere helsetjenesten, men manglende kontroll og oppfølging av dette kan få svært alvorlige konsekvenser. Ledelse og styring er avgjørende elementer, ansvar og kontroll kan aldri tjenesteutsettes. Det skaper tillitsutfordringer når det blir kjent at potensial for økonomiske innsparinger fører til utflagging av helsedata. Det handler ikke bare om faktisk, men også om opplevd risiko for den enkelte borger. I helsetjenesten må pasientene vite at deres informasjon ivaretas sikkert og trygt. Etter Legeforeningens syn bør det derfor vurderes om sikkerhetsloven[2] bør komme til anvendelse slik at pasientdata og den enkeltes rettsikkerhet beskyttes av den. På bakgrunn av dagens risikobilde og de formålsangivelser som oppstilles i sikkerhetsloven er det forhold som taler for at loven også bør gjelde for større deler av helsesektorens aktivitet.

Kritisk infrastruktur er infrastruktur som ved en alvorlig svikt medfører at samfunnet ikke vil være i stand til å opprettholde de leveranser av varer og tjenester som befolkningen trenger. Helsetjenester vil omfattes av dette.

Også forarbeidene til sikkerhetsloven omtaler et endret risiko- og trusselbilde. Det vises til utdrag fra Innst. 352 L (2015-2016) (Innstilling fra utenriks- og forsvarskomiteen om Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)):

"*Komiteen viser til at vi i dag står overfor et sammensatt risiko- og trusselbilde. Den sikkerhetspolitiske situasjonen er i stadig endring. Samfunnet blir mer og mer sårbart, og teknologien utvikler seg i raskt tempo. Det er viktig at sikkerhetsloven holder tritt med utviklingen. Lovforslaget er et viktig tiltak for å styrke vår forebyggende sikkerhet.*

*Komiteen merker seg at sikkerhetsloven ikke har vært under særskilt revidering siden den trådte i kraft i 2001. Komiteen deler derfor Forsvarsdepartements vurdering av behov for en mer gjennomgående gjennomgang av gjeldende lov sett opp mot dagens og morgendagens nasjonale og globale utfordringer innenfor forebyggende sikkerhet.*

*Komiteen merker seg at det gjøres endringer i lovens generelle virkeområde og støtter at dette utvides til å gjelde alle anskaffelser til kritisk infrastruktur....*"

I IKT-sikkerhetsutvalgets mandat er det blant annet angitt følgende:

*"Behovet for forsvarlig IKT-sikkerhet i samfunnet har økt i takt med digitaliseringen. Et viktig aspekt er befolkningens trygghet, som inkluderer både kriminalitetsbekjempelse og beskyttelse av personvernet. Et annet aspekt er det teknologiske, der spesielt funksjonaliteten til samfunnskritiske infrastrukturer og tjenester står i fokus. Et tredje aspekt er at forsvarlig IKT-sikkerhet generelt i samfunnet vil bidra til et mer robust samfunn og dermed ha positive virkninger for nasjonal sikkerhet. Et fjerde aspekt er digitaliseringens betydning for økonomisk vekst og utvikling. For å høste gevinster av digitaliseringen er det viktig at virksomheter, offentlig forvaltning, og samfunnet som helhet har tillit til at de digitale tjenestene fungerer som forutsatt, er tilgjengelig når de trengs der de trengs og har et forsvarlig sikkerhetsnivå."*

Det er viktig at det rettes tilstrekkelig oppmerksomhet mot IKT-sikkerhet i helsesektoren, noe man også har sett av flere hendelser den siste tiden, og vi oppfordrer IKT-sikkerhetsutvalget til å gi helsesektoren en vesentlig plass i sitt arbeid. Det er av kritisk betydning for helsevesen og samfunn at systemene (eksempelvis på sykehus eller prehospitale tjenester som ambulansetjeneste, legevakt, eller annen beredskap) til enhver tid fungerer. Teknisk utstyr og informasjonssystemer må være tilgjengelig for dem som har behov for det, og derfor være sikret mot inntrengning, overstyring og andre former for angrep. Lammes helsevesenet, lammes også samfunnet.

---

[2] Lov om forebyggende sikkerhetstjeneste

HelseCERT, helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet, har gjort en trusselvurdering for Norsk helsenett og kommet til følgende: Digitale angrep kan forårsake nedetid på kritiske systemer, og dermed påvirke pasientsikkerheten. Svake ledd i verdikjeden øker risikoen og digital kriminalitet er i dag den mest synlige trusselen i helse- og omsorgssektoren. De største eksterne truslene er tjenestenektangrep fra internett og løsepengevirus som krypterer store filområder. Ifølge Helsedirektoratets rapport[1] kan digitale angrep forårsake at kritiske systemer blir utilgjengelige. Dette kan få svært alvorlige konsekvenser. Hacking ved et barnesykehus i Boston for noen år siden pågikk et par uker, der en innlagt pasient med komplisert sykdom var målet for oppmerksomheten. Et sykehus i Kentucky ble rammet da en ansatt åpnet en e-post som infiserte nettverket. Det tok fem dager før sykehuset var i full drift igjen. I England ble minst 81 av de 236 offentlige sykehusene/foretakene i det britiske helsevesenet rammet og bl.a. fikk nesten 20 000 pasienter avlyst sine timeavtaler og over 1200 diagnostiske verktøy ble satt ut av drift etter angrep av det såkalte Wannacry-viruset. Nå senest er Helse Sør-Øst rammet, konsekvensene er p.t. uvisse.

Risikoen for målrettede angrep mot helsetjenesten fra utenlandske grupper/stater har blitt lite vurdert og/eller omtalt i en rekke offentlige utredninger/rapporter, og trolig blitt undervurdert. Når man nå ser stadig nye eksempler på saker der ting går galt, der risikovurderinger ikke er gjort tilstrekkelig, eller der IKT-systemer svikter, og eksempler på saker der det skjer målrettede angrep mot IKT-systemer i helsetjenesten, er det på tide at man tar innover seg det endrede risikobildet også i Norge Med den samhandling og utveksling av helseopplysninger på tvers av virksomheter man allerede har, og man i større grad legger opp til (både i spesialisthelsetjenesten og mellom spesialisthelsetjenesten og primærhelsetjenesten, eksempelvis også Én innbygger - én journal), må det tas høyde for et endret risikobilde på på alle plan i helsetjenesten.

Pasientsikkerheten blir i økende grad avhengig av IKT-sikkerhet. Nettopp derfor kan ikke IKT-sikkerhet sees uavhengig av den virksomhet den tjener. Legeforeningen mener at det er behov for et bedre samspill mellom medisinske fagmiljøer og teknologiske/sikkerhetsmiljøer gjennom utvikling av klinisk informatikk som akademisk disiplin.

Infrastruktur i helsesektoren vil inngå i kritisk infrastruktur og Legeforeningen mener det må gjøres en grundig vurdering av hvordan IKT-systemene innen helse skal sikres, og at det må vurderes hvorvidt IKT-systemer i helsesektoren underlegges sikkerhetsloven. I den forbindelse må et eventuelt utvidet anvendelsesområde for sikkerhetsloven også ta i betraktning eventuelle konsekvenser for næringsdrivende leger.

At IKT i helsetjenesten også er samfunnskritisk infrastruktur betyr at nasjonen må ha kompetanse til å håndtere hendelser og ondsinnede angrep. Ved både tilsiktede (kriminalitet, terror, spionasje) og ikke-tilsiktede hendelser (ulykker, naturhendelser) er det behov for å beskytte informasjonen og sørge for at våre nettverk og systemer er sikre og stabile til enhver tid. Nødnett er en god løsning, men mobile løsninger vil tvinge seg frem, ikke bare som beredskap, men som ordinære løsninger knyttet til den prehospitale kjede, legevakt og kommunehelsetjenesten ellers. Gjennomgående er kommunalt nivå lite inkludert, trass i stort ansvarsområde og at mange aktører har et selvstendig IKT-ansvar.

Helsevesenet er sammensatt av mange enheter fra store helseforetak til små fastlegekontor. Drift og informasjonssikkerhet ivaretas av organisasjoner med helt forskjellige muligheter og forutsetninger for det. Små legekontor har samme ansvar som store helseforetak. Enkeltleger er ansvarlig for å vurdere om deres elektroniske journalleverandør har en lovlig løsning, og når legen skal opprette elektronisk kommunikasjon med et helseforetak er legen ansvarlig for å vurdere helseforetakets informasjonssikkerhet. I praksis kan dette vise seg å være svært vanskelig og det bør vurderes om myndighetene bør ta et større ansvar for også slike deler av helsesektoren. Eksempelvis kan dette være mer sentraliserte løsninger for drift med innebygd informasjonssikkerhet, godkjenning av dialogpartnere eksempelvis ved tilknytningen til Helsenett, godkjenning/sertifiseringer av IKT-leverandørers løsninger.

I statsbudsjettet 2018 står det slik om personvern og informasjonssikkerhet: *"Personvern er imidlertid mer enn hensynet til konfidensialitet. Et formål med personvernlovgivningen er også å sikre at personopplysninger blir brukt på rett måte. Viktige personvernhensyn er at opplysninger skal være korrekte og oppdaterte, og tilgjengelige for rett person til rett tid. Rett bruk av informasjon er avgjørende for god pasientsikkerhet og forsvarlig og effektiv helsehjelp. Manglende tilgang til oppdaterte og korrekte opplysninger om pasienten kan føre til dårligere pasient–behandling og i verste fall feil behandling eller skade. Godt personvern krever at alle hensynene ivaretas."*[3]

Det er essensielt med løsninger som **både** ivaretar informasjonssikkerheten **og** pasientsikkerheten.

Med hilsen

Den norske legeforening

Geir Riise, generalsekretær

Anne Ringnes, saksbehandler

[3] Prop. 1S 2017-2018 HOD Kap. 10 IKT og digitalisering: Personvern og informasjonssikkerhet