DEN NORSKE LEGEFORENING

Høring i Stortingets Justiskomité 16. januar 2018 – Meld. St. 38 (2016-17). IKT-sikkerhet

Fra Legeforeningen: Marit Hermansen, president, og Kjartan Olafsson, leder i IT-utvalget.

Legeforeningen ønsker å fremheve to sårbare felter: Personvern/konfidensialitet og tilgang til IKT-systemer.

Innledningsvis er det verdt å merke seg at meldingen heter IKT-sikkerhet, ikke informasjonssikkerhet. Fokuset på teknologi og ikke informasjonssikkerhet burde 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. Betydningen av GDPR[1] for norske forhold er ikke drøftet i meldingen, dette er en alvorlig svakhet. GDPRs krav om "privacy by design" og "privacy by default" understreker betydningen av å vurdere IKT-sikkerhet og informasjonssikkerhet samt personvern under ett. "Privacy by design" og "privacy by default" innebærer blant annet at personvern skal være en vesentlig del av kjernefunksjonaliteten og skal hensynstas gjennomgående ved både utvikling av produkter og ved valg av løsninger og standardinnstillinger. Personvern må være innebygd i IT-systemenes design og arkitektur, og må derfor bygges inn allerede under utviklingen av et IKT-produkt, ikke som en tilleggsfunksjon lagt til i etterkant. Dermed kan ikke informasjonssikkerhet og personvern utelates når IKT-sikkerhet drøftes.

Forslaget om forenkling av Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) imøteser Legeforeningen positivt, som en tilpasning til GDPR.

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[2]. For helsetjenesten er IKT ikke bare infrastruktur, slik en får inntrykk av i meldingen *("Direktoratet for e-helse har myndighets- og premissgiverrollen i det nasjonale arbeidet med IKT-infrastruktur.")*. 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.

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 om ikke bare faktisk, men opplevd risiko for den enkelte borger. I helsetjenesten må pasientene vite at deres informasjon ivaretas sikkert og

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

trygt. Etter Legeforeningens syn bør det derfor vurderes om sikkerhetsloven[3] bør komme til anvendelse slik at pasientdata og den enkeltes rettsikkerhet beskyttes av sikkerhetsloven.

Samtidig er det slik at tilgang til offentlige digitale tjenester i praksis er blokkert for alle pasienter som ikke er i stand til å håndtere autentisering på sikkerhetsnivå 4, det høyeste sikkerhetsnivået for pålogging (BankID, osv.). Det er problematisk, fordi det forhindrer dem fra for eksempel å kunne få hjelp fra pårørende. Rent konkret kan pasienter ha tillit til at pårørende plasserer piller i riktig skuff i dosetten uten noen form for autentisering, de kan gi pårørende fullmakt til å hente legemidler på apoteket ved bare å skrive under på et skjema, men de kan ikke gi pårørende tillatelse til å lese reseptene som denne medisineringen er basert på dersom de ikke selv er i stand til å logge seg på helsenorge.no. Det er et tankekors. Det bør derfor være mekanismer der fastlegen, i samråd med pasienten, kan utstede en autentisering for pårørende eller andre hjelpere. Dette vil også være i tråd med GDPR føring om å styrke individets kontroll med egne opplysninger.

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.

I følge Helsedirektoratets rapport kan digitale angrep forårsake at kritiske systemer blir utilgjengelige [2]. 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. 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.

Det er positivt med øvelser der kritiske systemer er ute av funksjon, men man burde også gjennomføre øvelser der de faktisk fungerer - for å observere hvilke restriksjoner mange teknologiske løsninger legger på helsepersonell med henvisning til IKT-sikkerhet. 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 svært lite omtalt i meldingen, trass i stort ansvarsområde og at mange aktører har et selvstendig IKT-ansvar.

I statsbudsjett 2018 står det slik om personvern og informasjonssikkerhet[4]:
"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 pasientbehandling og i verste fall feil behandling eller skade. Godt personvern krever at alle hensynene ivaretas." Det er essensielt å finne løsninger som **både** ivaretar informasjonssikkerheten **og** pasientsikkerheten.

[3] Lov om forebyggende sikkerhetstjeneste
[4] https://www.statsbudsjettet.no/Statsbudsjettet-2018/Dokumenter/Fagdepartementenes-proposisjoner/Helse--og-omsorgsdepartementet-HOD/Prop-1-S-/Del-3-Omtale-av-sarlige-tema/10-IKT-og-digitalisering-/