DEN NORSKE LEGEFORENING

helse-omsorg@stortinget.no

Deres ref.: Dok 8:197 S (2017-2018) Vår ref.: Dato: 24.04.2018

Å håndtere og redusere skadevirkninger av uventede hendelser er en viktig del av hverdagen i helsetjenesten. Helsetjenesten er godt forberedt på å møte kritiske situasjoner som krever samarbeid. Dette synes gjennomgående ivaretatt med god koordinering av helse- og omsorgssektorens innsats og god samhandling med andre sektorer. Det inkluderer også internasjonalt samarbeid. Alt er nedfelt i tredje utgave av Nasjonal helseberedskapsplan (2018).

Innen deler av helsetjenesten trengs det økt risikoerkjennelse. Personvern og konfidensialitet står sentralt i helsetjenesten. Alle må kunne være sikre på at opplysninger ikke misbrukes eller kommer på avveie. De sikkerhetsmessige utfordringene knyttet til IKT i helsetjenesten har økt, både på grunn av økt avhengighet av IKT og økt risiko for lekkasje av sensitiv informasjon. For helsetjenesten er IKT ikke bare infrastruktur, men også IKT-baserte medisinske verktøy som benyttes i utredning og behandling av pasienter. Videre brukes IKT til å forvalte og anvende pasientinformasjon og medisinsk kunnskap, og ikke minst i samhandling om helsehjelp, men også til ledelse, styring og økonomisk forvaltning og kontroll.

Tjenesteutsetting blir stadig mer utbredt i offentlig sektor og private leverandører er nødvendig for å modernisere og digitalisere helsetjenesten, men manglende kontroll og oppfølging kan få svært alvorlige konsekvenser. Avhengigheten av programvare synes å øke raskere enn evnen til å sikre systemene. Ledelse og styring er avgjørende elementer, ansvar og kontroll kan aldri tjenesteutsettes. I helsetjenesten må pasientene vite at deres informasjon ivaretas sikkert og trygt. Et utviklingstrekk er at interessen for personopplysninger øker.

Informasjon om nøkkelpersoner innen forsvar, forvaltning og politikk og deres familier kan utnyttes for å utøve press i konfliktsituasjoner. Helsepersonell, sykehus og kommunenes helse- og omsorgstjenester er potensielle mål for slik informasjonsinnsamling. Det er ikke bare informasjon om sykdom som i slik sammenheng kan bli utnyttet, men også informasjon om hvilken rolle/funksjon en person har i samfunnet, kontaktopplysninger m.v. Flere viktige samfunnsfunksjoner eller stillinger som er kritiske for nasjonens sikkerhet forutsetter jevnlige helsekontroller, og kan genere verdifull informasjon for potensiell ondsinnet angriper.

Helseregistre og store journalsystemer er særlig utsatt siden de inneholder opplysninger om store deler av befolkningen. 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 over hele linjen, altså ikke bare innad i de større helseforetakene. Kommunene har et stort ansvarsområde og må bl.a. ta inn over seg behovet for beredskap mot digitale angrep som skaper sammenbrudd i informasjonstjenester. Lokale ledere og etater kan også risikere å måtte følge opp omfattende helse- og omsorgsoppgaver i forbindelse med alvorlige sykdomsutbrudd og store ulykker lokalt eller ute i verden. Den kommunale beredskapen er avgjørende i flere sammenhenger, og inkluderer både kommuneoverlege med ansvar for miljørettet helsevern/smittevern og fastleger og legevakt.

HelseCERT, helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet, gjorde i 2016 en trusselvurdering for Norsk helsenett og kom med følgende vurderinger: Digitale angrep kan forårsake nedetid/utilgjengelighet 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. Slike, og andre cyberangrep anses som en svært reell trussel. Et slikt angrep vil lamme så å si alt av samfunnets funksjoner. 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 nettverk og systemer er sikre og stabile til enhver tid. Det digitale nødnettet er en god løsning, men mobile løsninger vil tvinge seg frem, ikke bare som beredskap, men som ordinære løsninger, som igjen krever sikkerhetsløsninger.

Norge er som et lite marked med minimal egenproduksjon av legemidler særlig utsatt dersom det oppstår langvarig legemiddelmangel. Forsyningslinjene må derfor være intakte. Det er avhengighet av forsyninger fra utlandet for mange viktige legemidler som f.eks. insulin og antibiotika. For enkelte livsviktige legemidler vil sårbarhet i produksjonsapparatet tilsi at det etableres særskilte beredskapstiltak. Selv kortvarige opphold i forsyningen av legemidler kan gå utover enkeltpasienter.

Etter Legeforeningens syn bør IKT-infrastruktur i helseforetakene omfattes av krav i sikkerhetsloven om skjermingsverdig informasjon/objekt og hensynet til trygge pasientdata og den enkeltes rettssikkerhet bør styrkes gjennom loven. På bakgrunn av dagens risikobilde og de formålsangivelser som oppstilles i sikkerhetsloven er det forhold som taler for at det bør vurderes om loven også bør gjelde for større deler av helsesektorens aktivitet. Også forarbeidene til den nye sikkerhetsloven (Prop. 153 L (2016-2017)) omtaler et endret risiko- og trusselbilde.

Det er foreløpig vanskelig å forutsi hvilke konsekvenser det vil ha for den praktiske hverdagen til blant annet næringsdrivende leger at IKT-infrastrukturen i helseforetakene de samhandler med blir underlagt nærmere angitte krav til skjermingsverdig informasjon/objekt i sikkerhetsloven. Legeforeningen viser her til det pågående arbeidet med sikkerhetsloven. På bakgrunn av dette ser Legeforeningen behov for å presisere at dette er leger som allerede må bruke store deler av sin arbeidshverdag på administrative pålagte oppgaver. Når Legeforeningen anser det som hensiktsmessig at IKT-infrastruktur i helseforetakene omfattes av krav i sikkerhetsloven, er et av de ønskede formål at dette også skal oppleves som en bidragsyter for alle enkeltleger som ønsker å stå for et betryggende og tilfredsstillende sikkerhetsnivå ved behandling av slik verdifull informasjon som de i det daglige håndterer, herunder i samhandling med de store helseforetakene. Legeforeningen mener imidlertid det må vurderes kompensatoriske ordninger i det nærmere arbeidet med gjennomføring av sikkerhetsloven (forskrifter m.v.). I den grad næringsdrivende leger skulle bli mer eller mindre direkte berørt av krav/pålegg i sikkerhetsloven i form av ulike kostander (arbeidsbyrde og økonomi) må dette kompenseres slik at det blir praktisk mulig for slike sårbare virksomheter å etterkomme eventuelle pålagte sikringstiltak. Legeforeningen anser dette som helt vesentlig for å sikre at alle som bør ha et forsvarlig sikkerhetsnivå etter sikkerhetsloven faktisk har forutsetninger for å ha det.