DEN NORSKE LEGEFORENING

Deres ref.: Vår ref: HSAK201900462 Dato: 24-10-2019

Høringssvar – utkast til versjon 6.0 av Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

Det vises til ovennevnte høring. Legeforeningen er positiv til revisjonen som skal gjøre at Normen nå er dekkende for nye krav i personvernforordningen, samtidig som den skal være mer tilpasset nåtidens teknologi. Arbeid med forenklinger og leser- og brukervennlighet mener Legeforeningen må være et kontinuerlig prosjekt, men er positive til at dette har fått et særskilt fokus i aktuelle versjon av 6.0. Legeforeningen mener imidlertid at det er tilsvarende viktig å legge ressurser i hvordan Normen eksistens, og nytteverdi, kan formidles ut til målgruppen. Vi vil i det følgende komme med utdypende merknader.

Innledning

Fortrolighet har alltid vært fundamentet for dialogen mellom pasient og lege og dette verdigrunnlaget har fulgt oss opp gjennom vekslende medisinske filosofier, metoder og teknikker. Moderne informasjons- og kommunikasjonsteknologi (IKT) har ikke, og skal ikke, rikke ved verdigrunnlaget. Da tanken om en egen Norm for informasjonssikkerhet ble fremlagt etter årtusenskiftet var det naturlig for Legeforeningen både å støtte forslaget og delta aktivt i arbeidet.

Digitalisering har gitt nye muligheter for organisering og nye verktøy for å støtte opp under klinisk arbeid. Livsviktig informasjon kan gjøres umiddelbart tilgjengelig der pasienten behandles, uavhengig av hvor informasjonen i sin tid ble skrevet ned. For en generasjon siden var man avhengig av å finne en papirjournal, og undersøkelser tydet på at 30% av papirjournalene ikke var tilgjengelige når man trengte dem.

Normen versjon 6.0 – presisering og avgrensning

Store endringer har skjedd i sektoren siden første utgave av Normen kom i 2006, og i forordet til denne versjon 6.0 har man skissert noen av hovedmålene ved denne nye revisjonen; «*sikre at Normens krav er dekkende for nye krav i personvernforordningen og samtidig tilpasset nåtidens teknologi*», «*forenkle fremstillingene og gjøre Normen mer leser- og brukervennlig*», endre virkeområde og tydeliggjøre forholdsmessighet, samt «*gjennomgang og forenkling av teksten*».

Begrepene i tittelen «Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» er imidlertid ikke definert. «Informasjonssikkerhet» og «personvern» er til en viss grad forsøkt forklart i forordet; *«Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Informasjonssikkerhet handler om å beskytte informasjon ut fra prinsipper om konfidensialitet, integritet, tilgjengelighet og robusthet.»* Legeforeningen mener det bør gjøres justeringer i formuleringene her og foreslår at Normen benytter beskrivelser og definisjoner fra andre

autoritative kilder, f.eks. DIFI eller lov- og regelverk. Informasjonssikkerhet handler om å sikre konfidensialitet, integritet og tilgjengelighet og foreslår at dette erstatter «å beskytte". Videre peker vi på at det ikke er vanlig å ha med robusthet som et fjerde punkt. Robusthet er også viktig, men da sikkerhetsbegrepene er knyttet til informasjonen, er robusthet et krav til systemet som forvalter informasjonen, og avgjørende for både konfidensialitet, integritet og tilgjengelighet.

Begrepet helse- og omsorgssektoren er heller ikke definert eller avgrenset (som i helse- og omsorgstjenesteloven). Det står (i kap. 1.3) at «*Normen gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge den*». Imidlertid påpekes det allerede i kap. 1.1 at «*Personvern- og helselovgivningen stiller krav til informasjonssikkerhet og personvern. Disse kravene gjelder uavhengig av Normen*». Det medfører at noen av Normens krav gjelder uten at man har en avtale som forplikter virksomheten til å følge Normen, mens andre kun gjelder ifm. en avtale.

Slik Normen nå fremstår er den en blanding av forskjellige tekster, og det er uklart hvilken status de forskjellige tekstene har og hvilke kilder de er basert på. Så lenge alle deler av teksten er uomtvistelige og har full tilslutning fra alle parter er dette kanskje ikke så viktig. Når vi nå begynner å få erfaringer fra over et ti-år med dette dokumentet i forskjellige versjoner, og begynner å se både tilsiktede og utilsiktede konsekvenser av kravene, er det essensielt for de deltagende parter å vite hvilke endringer som kan vedtas av styringsgruppen, hvilke krav som er sitater fra gjeldende lover og forskrifter, hvilke krav som er tolkninger eller avgrensninger av gjeldende regelverk, og hva som er å betrakte som lærebokmateriale osv. Dette har lenge vært etterspurt fra Legeforeningen, og også blitt lovet i forbindelse med versjon 6.0, men har kun materialisert seg i et vedlegg. Det er ikke tilstrekkelig – det er normdokumentet man tilslutter seg, ikke vedleggene.

Spesielt er det viktig å markere hvilke deler som er gjengivelser og/eller tolkninger av personvernforordningen (GDPR). Dette er fortsatt en relativt ny forordning, og selv om prinsippene i forordningen er godt forenlig med det som er norsk tradisjon vil mange være spesielt opptatt av å sikre at virksomheten drives i samsvar med forordningen (bl.a. grunnet det høye bøtenivået her).

Særlig på et område der lov- og regelverk er under utvikling er det viktig å kunne understøtte fremtidige endringsbehov ved å vite hva som danner grunnlaget for det enkelte avsnitt og krav.

Personvern og pasientvern

Moderne IKT har endret måten helsepersonell jobber på. Muligheten for rask forflytning av informasjon har gjort at man kan fordele oppgaver på en annen måte. Moderne medisin har i stadig større grad utviklet seg til et evidensbasert tverrfaglig teamarbeid.

Når sensitiv informasjon plutselig kan bli tilgjengelig for tusenvis av personer uavhengig av hvor de er lokalisert, i stedet for kun et ti-talls personer på *ett* fysisk sted, er det naturlig at man legger stor vekt på metoder og teknikker for å redusere faren for misbruk. Riktignok er det etiske verdigrunnlaget og taushetsplikten uendret. Teknikkene for å opptre i strid med dette er imidlertid blitt vesentlig mer tilgjengelige. Derfor var også Legeforeningen tilhenger av at man i stor grad la vekt på metoder og teknikker for tilgangsbegrensning i de første versjonene av Normen.

Historien har imidlertid også avslørt andre forhold av vesentlig betydning for informasjonssikkerheten. Informasjonssikkerhet er – som normen jo refererer - mer enn kun avgrensning (konfidensialitet) – det handler også om at informasjon må være korrekt (integritet) og tilgjengelig der det tas beslutninger av betydning for liv og helse (tilgjengelighet). Den eneste måten man kan være absolutt sikker på at informasjon er skjermet for uvedkommende, er å sørge for at den er skjermet for alle. Da bryter man imidlertid med et grunnleggende kriterium for hvorfor informasjonen ble registrert i utgangspunktet, nemlig for å yte god helsehjelp overfor den personen det gjelder. Vi har dessverre fått mange tilbakemeldinger fra våre kollegaer som peker i retning av at metodene for å begrense tilgang har gått

utover tilgjengelighet når man yter helsehjelp – noen ganger med fare for liv og helse. Deler av den kliniske informasjonen kan være livsviktig. Den senere tids debatt i pressen om grensen mellom personvern og pasientvern er et utslag av liknende observasjoner.

Heller enn å sette disse verdiene opp mot hverandre bør man søke å finne løsninger som best mulig ivaretar begge hensyn. Denne problemstillingen, som er avgjørende for god informasjonssikkerhet i helsesektoren, er imidlertid nærmest fraværende i normdokumentet. Man har tatt inn én setning (siste avsnitt kap. 1.3) om at normen skal «søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet». Det er også et par punkter om tilgjengelighet på slutten av kap. 3.2, der man forøvrig har blandet sammen tilgjengelighet og robusthet. Ut over dette er problemstillingen nærmest ikke berørt, mens man for eksempel har en hel side med detaljert angivelse av logging med det formål «å oppdage brudd eller forsøk på brudd» (5.4.5).

Det er viktig at man ikke bare erkjenner behovet for en balansert tilnærming, men at man også gir konkrete råd og stiller krav til hvordan integritet og tilgjengelighet skal sikres – på lik linje med den detaljerte angivelsen av hvordan man sikrer konfidensialitet. Problemene bør erkjennes og beskrives – og løsningene bør angis og omsettes i krav. Ett av de store problemene i sektoren er det som i informatikken kalles «ukontrollert redundans» - det vil si at det finnes kopier av informasjonen som ikke endres når originalen endres.

Tilgangsstyring er viet tre og en halv side med detaljerte angivelser uten å adressere et av hovedproblemene - at det verken finnes algoritmer som er i stand til entydig å definere informasjonsbehovet i enhver tenkelig klinisk situasjon eller teknologi som fullt ut er i stand til å sikre både full tilgjengelighet ved kliniske behov og total avgrensning mot uautorisert tilgang. Løsningen bør derfor være en kombinasjon av holdningsskapende arbeid, organisatoriske tiltak, teknologiske løsninger, mekanismer for å håndtere unntakssituasjoner, samt oppfølging og kontrollrutiner. De fleste produsenter har erkjent dette problemet gjennom å innføre sikkerhetsventiler de kaller «blå-lys» eller «grønn-lys» ordninger – omtalt som «selvautorisering» i Normen. Dette er mekanismer der autentisert personell i visse kategorier kan få tilgang til informasjon de trenger for å yte forsvarlig helsehjelp i situasjoner der utilstrekkelig teknologi hindrer dem tilgang. Det burde stilles klare krav både til at slike mekanismer skal finnes i alle systemer som opererer med tilgangsavgrensning, hvilke minimumskrav som skal stilles, hvordan man dokumenterer årsaken til at mekanismen er benyttet, og – ikke minst – krav om at man dokumenterer den helsehjelp som er gitt der informasjonen er benyttet. Legeforeningen er kjent med at enkelte slike mekanismer ikke tillater dokumentasjon av helsehjelpen man har gitt.

Ett eksempel på krav som adresserer dette er justering av regler for tilgangsavgrensning basert på bruken av selvautorisering. Dersom mekanismene må benyttes ofte kan det være et tegn på for streng tilgangsavgrensning. Det kan da være naturlig å gå inn i enkelttilfeller eller spesielle områder med tanke på å avdekke konkrete problemer og foreta nødvendige justeringer. Hvis derimot mekanismene nesten aldri benyttes kan det være et uttrykk for at tilgangen er for åpen.

Profesjonsnøytralitet

Legeforeningen mener at det er viktig at denne versjonen av Normen nå er skrevet profesjonsnøytralt, dvs. at alle regler gjelder for alle. Kravenes allmenngyldighet har vært tilfellet hele tiden, men i teksten og i eksemplene har Normen tidligere gjerne fokusert på helsepersonell som yter klinisk arbeid og vært bekymret for at helsepersonell tilegner seg informasjon om personer de ikke har behandlingsansvar for, mens det har vært mindre fokus på spesielt IKT-personell.

Betydningen av – og konsekvensene ved – profesjonsnøytraliteten kunne med fordel kommet klarere frem. Det burde for eksempel vært tydelig og skrevet eksplisitt at kravet om logging av tilgang er uavhengig av hvem som har hatt tilgang, hva de har hatt tilgang til og hvilke mekanismer de har

benyttet for denne tilgangen. Således bør det være samme krav til en sykepleier som leser en pleieplan via en standard klient og en konsulent som aksesserer databasen direkte. Vi er klar over at dette siste kan skape noen tekniske utfordringer. Det kan imidlertid ikke være nivået på de tekniske utfordringene som bestemmer om lovverkets krav skal oppfylles.

Snarere har den senere tids erfaring med tydelighet vist at de største truslene mot personvernet og informasjonssikkerheten i helse- og omsorgssektoren ikke kommer fra helsepersonell som ønsker å lese journaler for personer de ikke har behandlingsansvar for, men fra personer med IKT-kompetanse både innfor og utenfor organisasjonen. Innenfor sektoren har vi eksempler på at tilgang er gitt til personer som verken er omfattet av relevant lovgivning eller avtaler. Utenfor ser vi at «hackere» ser verdien helsedata og har klart å skaffe seg tilgang.

Det ene trenger ikke å være til hinder for det andre. Det er imidlertid viktig at både omfanget og detaljeringsgraden i de krav som stilles, og ikke minst fokuset på problemene i de tekstlige deler, gjenspeiler dagens trusselbilde – et trusselbilde som har endret seg betydelig siden Normen kom i første versjon.

Språk, begrepsbruk og organisering av stoff

Som nevnt tidligere gjelder Normen for «*enhver virksomhet som ved avtale har forpliktet seg til å følge den*». Selv om det ikke finnes noen detaljert oversikt, har det grovt vært anslått at Normen kan være aktuell for 17.000 virksomheter. De aller fleste av disse virksomhetene består av én enkeltperson eller et fåtall personer med helsefaglig bakgrunn, uten tilgang til verken juridisk eller teknisk kompetanse. Det er derfor en spesiell utfordring når Normen skrives av personer med nettopp juridisk og teknisk kompetanse å sikre at den er forståelig for de som skal tilslutte seg den. Med forståelig tenker vi både på organisering av stoffet, valg av begreper, presisjonsnivå, valg av eksempler osv.

Dette har lenge vært et viktig poeng for Legeforeningen, og vi er glad for å se at denne nye versjonen er et godt skritt i riktig retning. Utkastet har kommet lagt i å sikre at begreper med flere betydninger enten er skiftet ut eller presisert. Et eksempel er ordet «behandling», som for helsepersonell gjerne vil bety behandling av pasienter, mens IKT-personer tenker på behandling av data. Det er fortsatt noen eksempler, spesielt i kap 5.7, der dette ikke fullt ut er gjennomført, men vi regner med at dette er gjennomført i endelig versjon.

På noen områder kan det være behov for harmonisering av begreper. Vi tenker for eksempel på pasientjournal / fagsystemer / behandlingsrettede helseregistre. Selv om det ikke er noe godt begrep er det likevel å foretrekke at man benytter lovens begrep systematisk – dvs. behandlingsrettet helseregister, og at man heller benytter de andre begrepene i parentes der det er behov for å forklare hva dette begrepet faktisk betyr.

Enkelte ord er dessverre bevisst uklare, som «forholdsmessig», «nødvendig», «egnet» osv. Dette er ord som en så langt mulig bør søkes å unngå, og i stedet invitere bransjen til å være konkret på grenser og omfang. I tilfelle der dette ikke er mulig bør en være eksplisitt på at det er opp til virksomheten selv å tolke disse ordene og avgjøre hvordan de skal forstås.

Man kunne med fordel skilt ut de tekstene som bare gjelder virksomheter over en viss størrelse. Selv om vi i dag ikke har verken retningslinjer eller praksis for å definere grensen entydig, er det grunn til å anta at de aller fleste av de 17.000 virksomhetene vil være under slike grenser.

Mye av det som står om organisering er for eksempel lite relevant for virksomheter på to-tre personer, f.eks. å iverksette ledelsens gjennomgang (kap. 2.5) eller å følge mange av anvisningene om tilgangsstyring (kap. 5.2). I tråd med dette kunne tekstene om Styringssystem og Ledelsens

gjennomgang, som jo er metoder for å ivareta ansvar snarere enn et mål i seg selv, vært flyttet fra kap. 2 om Ledelse og ansvar til kap. 3 om Risikostyring.

Legeforeningen antar at dokumentet skal gjennom en språkvask før endelig versjon vedtas, og legger til grunn at enkelte mindre skrivefeil mv. blir rettet opp da.

Videre prosess

GDPR gir rom for bransjenormer, og det er naturlig å se på Normen som en slik. Det er viktig at versjonshåndteringen av dokumentet samkjøres med prosedyrene for å få det godkjent som bransjenorm, slik at vi ikke risikerer å sitte med én versjon som er vedtatt av Styringsgruppen og en annen som er akseptert etter GDPR.

Med hilsen
Den norske legeforening

Geir Riise
Generalsekretær

Lars Duvaland
Avdelingsdirektør/advokat

Helga Bysting
Rådgiver/advokat

Dokumentet er godkjent elektronisk