

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
POSTBOKS 8005 DEP
0030 OSLO

Deres ref:

Vår ref:

2024/1088-7/008

Saksbehandler

Ida-Kristin Martinussen/

Dato:

Bodø, 09.12.2024

Høringsinnspill Helse Nord RHF – forslag til forskrift til digitalsikkerhetsloven - digitalsikkerhetsforskriften

Helse Nord RHF viser til høringsbrev - forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften).

Helse Nord RHF støtter formålet til digitalsikkerhetsloven, og vil påpeke viktigheten av å implementere et robust og effektivt regelverk for digital sikkerhet. Norge er et av de mest digitaliserte landene i verden, og digitalisering er et viktig verktøy for å løse utfordringene vi står overfor. For å kunne levere best mulig helsetjenester er vi avhengig av teknologi og digitalisering, men en forutsetning for den teknologiske utviklingen er at vi klarer å levere tjenester med tilfredsstillende digital sikkerhet.

Helse Nord RHF har noen konkrete innspill til digital sikkerhetsforskriften:

1. Virkeområde for tilbydere av samfunnsviktige tjenester - Helse

I forslag til forskrift til digital sikkerhetsloven (digitalsikkerhetsforskriften) § 1 reguleres tilbydere av samfunnsviktige tjenester. Etter § 1, første ledd nr. 19 og 20 omfattes Helse- og omsorgsdepartementet med underliggende etater og foretak, som er den nasjonale helseberedskapen, og tjenester som tilbys av de regionale helseforetakene. Etter samme bestemmelses nummer 21 omfattes sentrale systemer for rekvirering og utlevering av legemidler og andre medisinske produkter.

Helse Nord RHF stiller spørsmål ved om det kommer tydelig nok frem at dette også omfatter regionenes IKT leverandører, og de IKT-tjenester som tilbys for å understøtte sykehusdriften.

2. Sikker plattform

I høringsnotatet brukes begrepet «sikker plattform» ved noen anledninger, uten at dette er definert. Et konkret eksempel er § 8, andre ledd: «Sikkerhetstiltakene skal som et minimum ha som formål å bidra til *sikker plattform*, sikker drift og vedlikehold, samt sikker hendelseshåndtering og gjenoppretting.» (min utheving).

Det er uklart om det med begrepet «sikker plattform» menes virksomhetens nettverk og informasjonssystemer, eller om det er noe ytterligere? Dette kan med fordel tydeliggjøres i høringsnotatet.

3. Teknologiske sikkerhetstiltak

I forslag til forskrift § 10 angis teknologiske sikkerhetstiltak, og det foreslås noen konkrete kategorier av sikkerhetstiltak som minst skal implementeres. Den teknologiske utviklingen skjer hurtig, og teknologien som brukes må gjenspeile det aktuelle trusselbildet som gjelder på tidspunktet teknologien tas i bruk. Helse Nord RHF oppfatter derfor at forskriften med fordel kan ha en noe mer teknologinøytral, og i større grad basere seg på en risikobasert tilnærming. Dette gjelder for eksempel to- eller flerfaktorautentisering (MFA).

Helse Nord RHF er enig i at det som hovedregel bør innføres MFA, og at dette er et viktig tiltak for å redusere sårbarhet for at uvedkommende får tilgang til virksomhetens nettverk og informasjonssystemer. I et sykehus er det en rekke frittstående systemer, som ikke nødvendigvis er koblet til sykehusnettet. Vi tolker dette til å ikke gjelde frittstående systemer, for eksempel medisinsk utstyr som ikke er koblet til virksomhetens infrastruktur. Eksempelvis en blodtryksmåler med batteridrevet skjerm til bruk ved bortfall av ekom. Dette kunne med fordel vært tydeligere beskrevet i høringsnotatet.

4. Varslingsplikt til tilsynsmyndighet

Ifølge forslag til forskrift §17 skal varsel om betydelig hendelse gis til tilsynsmyndighet. Myndigheter med sektoransvar fører tilsyn etter digitalsikkerhetsloven i den enkelte sektor. Helse Nord RHF er positiv til at tilsyn gjennomføres av tilsynsmyndigheter i egen sektor. Egne tilsynsmyndighet har god kjennskap til sin sektor og kan enklere foreta forholdsmessige vurderinger ses helhetlig samt sammen med andre fagområder som eksempelvis pasientsikkerhet.

En utfordring ved at myndighet med sektoransvar fører tilsyn er at mange ulike tilsyn kan føre til fragmentert tilsynsregime innen digital sikkerhet. Etablering av en standardisert tilsynsmetodikk på tvers av tilsynsorganer kan bidra til en mer enhetlig tolkning av kravene for varsling av hendelser og vurdering av konsekvensene og risikoene ved en hendelse.

5. Økonomiske og administrative konsekvenser

Spesialisthelsetjenesten behandler og forvalter store mengder sensitive personopplysninger. Spesialisthelsetjenestens behandling av personopplysninger er allerede regulert av personvernforordning (GDPR), og igjennom særlover som pasientjournalloven, helseregisterlov m.fl. Videre er de juridiske enhetene som inngår i Helse Nord regulert av sikkerhetsloven.

Lov om digital sikkerhet, og forslag til digitalsikkerhetsforskriften, styrker sikkerhetskravene til tilbyderne med en minimumsliste over grunntiltak som anvendes, og gir mer presise bestemmelser for varsling av hendelser. Basert på innholdet i digitalsikkerhetsloven, og forslag til digitalsikkerhetsforskriften vurderes det prinsipielt å være begrenset grad av nye krav som vil tilføres. Beste praksis for sikkerhetsstyring, etablere prosesser for en proaktiv, iterativ og helhetlig tilnærming til forsvarlig sikkerhetsnivå, samt beredskap og hendelseshåndtering er gjelder allerede. Helse Nord RHF legger derfor til grunn at denne forskriften i begrenset grad innebærer nye økonomiske og administrative konsekvenser, forutsatt at de ulike føringene og kontrollene sikres god harmonisering.

Vennlig hilsen

Ida-Kristin Martinussen
Informasjonssikkerhetsleder