HELSE VEST

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Att.Odin Tveiten

Deres ref.:	Vår ref.:	Saksbehandler:	Dato:
24/3567	2024/861 - 12874/2024	Lars Erik Baugstø-Hartvigsen	11.12.2024

Høring - forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

Helse Vest RHF viser til høringsnotatet og sender med dette over våre innspill til forslag til ny digitalsikkerhetsforskrift. I forbindelse med høringen har Helse Vest RHF bedt om høringsinnspill fra sine helseforetak og Helse Vest IKT AS. Vi har mottatt innspill fra Helse Bergen HF og Sjukehusapoteka Vest HF. Relevante moment er innarbeidet i dette høringssvaret, som er skrevet i samråd med regionens IKT-selskap Helse Vest IKT AS.

God informasjonssikkerhet og digital sikkerhet er avgjørende viktig for å understøtte den samfunnsviktige tjenesten som helsehjelp i spesialisthelsetjenesten utgjør. Samtidig er vår sektor underlagt en rekke krav allerede som til dels er overlappende med utkastet til ny forskrift for hva digital sikkerhet angår.

Helse Vest RHF er av den oppfatning av forskriften gir en del absolutte krav på områder hvor det gjerne kan være mer hensiktsmessig å legge en risikobasert tilnærming til grunn, og vi har noen forslag til endringer som kan understøtte dette.

Kommentarer knyttet til de økonomiske og administrative konsekvensene

Justisdepartementet ber høringsinstansene om innspill på de konsekvensene forslagene i høringsforslaget vil få for dem. I høringsnotatet står det:
«For virksomheter som allerede er underlagt sikkerhets- og varslingskrav i eksisterende sektorregelverk, antar departementet at forskriftsforslaget ikke medfører vesentlige økonomiske eller administrative konsekvenser.»

Helse Vest RHF deler Justisdepartementets syn på at disse konsekvensene blir ganske små, jamfør at vår sektor har et omfattende sektorregelverk som også inkluderer digital sikkerhet. Et område vi imidlertid legger til grunn at vil kunne få økte økonomiske og administrative konsekvenser, er knyttet til oppfølgingsplikten omtalt i §14 vedrørende *«hvordan tilbydere av samfunnskritiske tjenester skal **påse** at leverandører og andre utfører arbeid slik at krav til forsvarlig sikkerhet kan overholdes»*. Vi har ikke kvantifisert dette, men legger til grunn at

Postadresse:
Helse Vest RHF
Postboks 303 Forus
4066 Stavanger

Elektronisk adresse:
post@helse-vest.no
www.helse-vest.no

Besøksadresse:

Generell informasjon:
Sentralbord 51963800
Org.nr: 983658725

egnede tiltak etter en risikobasert tilnærming vil kunne gjennomføres uten vesentlig merkostnad.

Helse Vest RHF oppsummerer her tilbakemeldinger til de ulike foreslåtte bestemmelsene i forskriften:

§ 1. Tilbydere av samfunnsviktige tjenester

Foretakene i Helse Vest er avhengige av leveranser fra den regionale IKT-leverandør Helse Vest IKT AS for å kunne levere samfunnsviktig tjenester. Det er derfor viktig at regelverket også gjelder for Helse Vest IKT AS. Slik punktene 19 og 20 er utformet fremstår dette noe uklart.

Vi foreslår derfor at punkt 19 tydeliggjøres slik at det klart fremkommer hvilke virksomheter som er underlagt forskriften, for eksempel de regionale helseforetakene med underliggende etater og virksomheter (både helseforetak og aksjeselskap).

«19. Helse- og omsorgsdepartementet med underliggende etater, foretak **og andre offentlig eide virksomheter**, som utgjør den nasjonale helseberedskapen.»

Punkt 20 foreslår vi å stryke, da vi mener ny formulering i punkt 19 over er dekkende for de tjenester som leveres av de regionale helseforetakene.

§ 6. Styringssystem for sikkerhet

Helse Vest RHF støtter at tilbydere av samfunnsviktige tjenester skal etablere og vedlikeholde et styringssystem for sikkerhet som omfatter digital sikkerhet. Det er viktig å kunne bygge videre på de styringssystemer virksomhetene allerede har. Innenfor spesialisthelsetjenesten er det allerede styringssystemer som omfatter krav i henhold til sikkerhetsloven, krav til informasjonssikkerhet i henhold til personopplysningsloven og helselovgivningen.
Det bør i forskriften utvises varsomhet med å bruke ord som «skal». For eksempel kan en virksomhet ha et godt og dekkende styringssystem uten at det nødvendigvis er basert på anerkjente standarder, men som i sum understøtter intensjonen i bokstavene a til e. Vi foreslår en endring til *«Sikkerhetsstyringssystemet **bør** baseres på anerkjente standarder og bidra til…».*

§ 7. Risikovurdering

I ledd 3 peker forskriften på en rekke minimumskrav knyttet til innholdet i slike risikovurderinger. Vi anbefaler at dette punktet enten fjernes (at bokstavene g til l utgår) i sin helhet, eller at det står at risikovurderingene «*kan*» eller «*bør*» inneholde.

§ 8. Risikohåndtering

Det gjøres et omfattende arbeid i virksomhetene med informasjonssikkerhet for å finne egnede risikoreduserende tiltak. Det finnes også andre kilder til veiledninger for risikovurderinger enn de som er og blir utarbeidet av Nasjonal sikkerhetsmyndighet. Det bør fremkomme at virksomhetene også kan benytte annen anerkjent ROS-metodikk for å ivareta gode risikovurderinger og håndtering av risiko.

§ 10. Teknologiske sikkerhetstiltak

Helse Vest mener for strenge «skal»-krav (a til h) på teknologisk sikring er uheldig da de i mange tilfeller vil være problematiske å etterleve, samtidig som helseforetakene skal levere sine tjenester og drive pasientbehandling. Vi mener at det må kunne legges en risikobasert tilnærming til grunn for etterlevelse av disse kravene, slik at det også hensyntas konteksten informasjonssystemet skal brukes i.

Fra Helse Bergen HF (HBE) sitt høringssvar til oss fremkommer det for eksempel følgende knyttet til §10 punkt a:

«Samtidig har HBE et komplekst IKT-landskap med omtrent 1000 ulike informasjonssystemer. Det er store ulikheter mellom systemene og mange støtter ikke to- eller flerfaktorautentisering, særlig innenfor medisinsk og teknisk utstyr samt mindre fagsystemer. Det er ikke realistisk for HBE å erstatte alle slike systemer med systemer som støtter to- eller flerfaktorautentisering. Selv om HBE kan stille krav til slik autentisering er det lite trolig at det i alle tilfeller finnes tilgjengelige løsninger i markedet som støtter to- eller flerfaktor autentisering samtidig løsningene tilfredsstiller andre krav som stilles, feks til funksjonalitet, pasientsikkerhet og pris. Det er derfor ikke realistisk at HBE vil være i stand til å etterleve kravet om to- eller flerfaktor autentisering slik kravet er formulert.

HBE mener at kravet må omformuleres slik at to- eller flerfaktor autentisering stilles som krav basert på bestemte kriterier, eller at det åpnes for unntak. Kriteriene kan være at to- eller flerfaktor autentisering kreves basert på risikovurdering, basert på mulighet for slik autentisering eller basert på noen scenarioer med økt risiko (feks. fjerntilgang). Selv med mulighet for unntak vil det i HBE trolig være et så stort behov for unntak at det i praksis vil være krevende å overholde krav til unntaksprosess for hvert enkelt tilfelle.»

Helse Vest støtter Helse Bergen HF sin tilnærming, og at det må kunne legges en risikobasert tilnærming til grunn for disse kravene (a til h), slik at det også hensyntas konteksten informasjonssystemet skal brukes i.

§ 17. Varslingsplikt

Gitt viktigheten av evne til å forstå omfanget av hendelser anbefaler vi at varslingsplikten tydeliggjøres til å stå: «Varsel skal gis **så snart som mulig**, og senest innen 24 timer etter at tilbyder fikk kjennskap til hendelsen.

Avsluttende merknader

Oppsummert støtter Helse Vest RHF NIS-direktivenes intensjoner om å sikre og ivareta et høyt digitalt sikkerhetsnivå. Samtidig er det viktig at regelverk, tiltak og metode kan tilpasses de ulike sektorenes egenart. Spesialisthelsetjenesten er allerede underlagt krav informasjonssikkerhet i henhold til personopplysningsloven, jamfør personvernforordningen. Videre er det stilt eksplisitte krav i helselovgivningen i forhold til behandling av informasjon. I tillegg er vi underlagt sikkerhetsloven med forskrifter, hvor det også stilles krav til sikker håndtering av informasjon.

Samtidig vil det nye regelverket kunne bidra til å at vi også bør kunne forvente større krav til digital sikkerhet lenger ute i leverandørkjedene. Dette vil også bli mer forutsigbart i den viktige leverandøroppfølgingen, og de samfunnsviktige virksomhetenes oppfølgingsplikt. Det er viktig å sikre de samfunnsviktige virksomhetenes evne til å kunne påse at leverandører, og andre som ufører oppgaver på deres vegne, gjør dette på en slik måte at virksomhetenes krav til forsvarlig sikkerhet kan overholdes.

Vennlig hilsen

Erik M. Hansen
Direktør e-helse

Lars Erik Baugstø-Hartvigsen
Informasjonssikkerhetsleder

Dokumentet er elektronisk godkjent av:Erik Magne Hansen direktør e-helse

Digital kommunikasjon

Vi har elektronisk saksbehandling og er opptatt av at informasjon, også taushetsbelagt, skal kunne sendes på en rask og sikker måte. Vi ber derfor om at et eventuelt svar på denne henvendelsen sendes gjennom en av disse kanalene:

- Privatpersoner og private virksomheter: eDialog
- Offentlige virksomheter: eFormidling (via eget sak-/arkivsystem)