NOTAT

Til: Styret i Sykehuset Innlandet HF

Fra: Administrerende direktør Alice Beathe Andersgaard

Dato: 13. november 2017

Sak: **Orientering til styret om varsel om vedtak fra Datatilsynet – overtredelsesgebyr – Sykehuset Innlandet**

Innledning

Datatilsynet sendte 26. mai 2017 brev til alle helseforetakene i Helse Sør-Øst RHF.
I brevet ba de om en redegjørelse blant annet for hvilke risikovurderinger og aksept av restrisiko som lå til grunn for beslutningen om å tjenesteutsette ansvaret for IKT-drift i regionen, infrastruktur moderniseringsprosjektet(Imod). De viser til likelydende brev fra helseforetakene datert 14. juni 2017 der det er gjort rede for hvilke vurderinger som er gjort i forbindelse med at det er inngått avtale med ekstern leverandør om strategisk samarbeid og IKT-drift.

Sykehuset Innlandet svarte på brevet fra Datatilsynet 15.06.17.
Generelt bemerkes det i dette svaret at det foreligger et felles styringssystem for informasjonssikkerhet i regionen, som forutsetter gjennomføring av risikovurdering i forkant for beslutninger om endringer som kan påvirke risiko og trusselnivå. For å avgjøre om gjenværende risiko er akseptabel, vil tekniske løsninger og håndtering av restrisiko måtte vurderes. Gjennomføring av risikovurdering vil dermed måtte gjennomføres stegvis ettersom faktisk informasjon om en løsning avklares.
Bakgrunnen for beslutningen om å benytte ekstern leverandør i Helse Sør-Øst, var en kombinasjon av regionens klare behov for oppgradering og fornying av infrastrukturen, og det at fremtidige fellesregionale løsninger vil kreve meget store investeringer i IKT infrastruktur. Eksisterende infrastruktur i regionen er fragmentert og til dels utdatert og vurderingen var at en modernisering i egen regi ville ta lengre tid enn ved bruk av ekstern leverandør. Kombinasjonen av de store investeringene som kreves fremover for å opprettholde et forsvarlig nivå på infrastruktur, samt de store investeringene som kreves for å gjennomføre de funksjonelle programmene ledet frem til beslutningen om å benytte en ekstern leverandør i dette arbeidet.

Den 26.10.17 kom svarbrevet fra Datatilsynet: «Varsel om vedtak – overtredelsesgebyr - Sykehuset Innlandet HF».
Dette er et varsel om at Datatilsynet, i medhold av pasientjournalloven §§ 29 jf. 22 og 5 vil fatte følgende vedtak:
Sykehuset Innlandet HF pålegges å betale et overtredelsesgebyr til statskassen, pålydende
Kr. 800 000,- -kroner åttehundretusen-, for

1. *overtredelse av bestemmelsen i personopplysningsforskriften om sikkerhetsledelse og organisering av sikkerhetsarbeidet i virksomheten jf. §§ 2-3, 2-7 og 2-15,*
2. *brudd på krav om å gjennomføre risikovurdering ved endringer som har betydning for informasjonssikkerheten i samsvar med kravene i § 2-4 jf.2-1 pasientjournalloven § 22 samt*

3. *overtredelse av bestemmelsene om tilgangskontroll i personopplysningsforskriften §§ 2-11 og 2-13 til 2-15.*

Sentralt i svaret fra Datatilsynet er hvilket ansvar helseforetakene har for databehandler-ansvar og hvor viktig det er med gode og omfattende risikovurderinger som legges til grunn for endringer.

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral. Dette er et forhåndsvarsel (jf. forvaltningsloven § 16). Dersom foretaket har merknader til dette varselet, må Sykehuset Innlandet sende Datatilsynet en tilbakemelding om dette så snart som mulig og senest innen 24. november 2017.

Likelydig brev fra Datatilsynet med varsel om vedtak i forbindelse med overtredelsesgebyr er sendt alle helseforetakene i Helse Sør-Øst.

Plan og status

De lovovertredelser og kritikkverdige forhold som er omtalt i Datatilsynets forhåndsvarsel, er i all hovedsak knyttet til manglende risikovurderinger, manglende ledelsesforankring og mangelfullt system for å sikre at helseforetakene blir satt i stand til å ta sitt lovpålagte ansvar som databehandlingsansvarlig.

Helse Sør-Øst RHF engasjerte i perioden 4.-23. mai 2017 et eksternt revisjonsfirma, PwC Norge, for gjennomgang av programmet for infrastrukturmodernisering (iMod). Konklusjon i denne rapporten er at det var mangelfull kontroll på tilgangsstyringen til helseopplysninger i dette prosjektet, at systemet for gjennomføring av risikovurderinger ikke har fungert som en effektiv kontrollmekanisme og at det var manglende styrings-dokument for gjennomføring av infrastrukturmoderniseringen.

De forhold som fremkommer av datatilsynets brev er i tråd med de funn PwC tidligere har gjort i sine gjennomganger av program for infrastruktur moderniseringen (iMod) i Helse Sør-Øst. Helse Sør-Øst RHF har som følge av den eksterne gjennomgangen til PwC allerede gjort tiltak med hensyn til forsterkning av risiko- og sårbarhetsanalyser.

Følgende tiltak er igangsatt i foretaksgruppen:

- Helse Sør-Øst RHF har satt Infrastrukturmoderniseringen (iMod-prosjektet) i bero inntil videre.
- Det er iverksatt arbeid med klargjøring av rutiner, roller og ansvar på området informasjonssikkerhet. Arbeidet utføres i hvert helseforetak og gjennomgås med administrerende direktører i foretakene og informasjonssikkerhetslederne i foretakene.

Sykehuset Innlandet vil se på hvordan databehandleransvaret, risikovurderinger og ledelsesforankring generelt kan settes bedre i system i foretaket.

Det arbeides også med en plan for å håndtere de funn og tiltak som fremkommer av dette varselet fra Datatilsynet.

Det er planlagt en sak til styret i Sykehuset Innlandet i desember om informasjonssikkerhet og personvern.

Sykehuset Innlandet vil be om utsettelse på svarfristen til Datatilsynet som er satt til 24.november

Vedlegg: Varsel om Overtredelsesgebyr fra Datatilsynet.