Sykehuset Innlandet HF

Vår dato 02.01.2018
Vår referanse 16/01990-17
Deres dato 26.10.2017
Deres referanse 16/01531-54/GRA
Saksbehandler: Håkon Iversøn

Datatilsynet
Postboks 8177 Dep
0034 OSLO

Varsel om vedtak fra Datatilsynet - Overtredelsesgebyr

Det vises til Datatilsynets brev av 24.10.2017 med varsel om mulig vedtak om overtredelsesgebyr. Varselet er begrunnet med påstått overtredelser av pasientjournalloven § 22 om ivaretakelse av informasjonssikkerhet og nærmere angitte bestemmelser i personopplysningsforskriften. Overtredelsene er vurdert i forbindelse med beslutning om å legge drift av helseregionens IKT-infrastruktur til ekstern leverandør.

Etter avtale er frist for å kommentere varselet utsatt til 2.1.2018.
Sykehuset Innlandet HF har gjennomgått grunnlaget for Datatilsynets varsel og har ingen vesentlige innsigelser til at foretaket, som databehandleransvarlig, har et selvstendig ansvar.
Sykehuset Innlandet tar også til etterretning Datatilsynets vurdering om at foretaket burde vært mer aktiv med vurderinger og beslutninger i prosessen med å inngå avtale og etablere underleverandør for Sykehuspartner HF.
Sykehuset Innlandet har enkelte merknader som bes tatt i betraktning i vurdering, utforming og utmåling av Datatilsynets endelige vedtak.

Strukturelle forhold – felles i regionen
Datatilsynet legger i varselet til grunn at sykehuset «*har utvist skyld ved å overlate beslutninger som har betydning for virksomhetens plikter etter personopplysningsforskriften og pasientjournalloven til moderniseringsprosjektet uten å sikre at beslutninger som ble tatt var akseptable i forhold til virksomhetens risikotoleranse og uten å sørge for ledelses-forankring før beslutninger ble tatt*.» Det vises til styresak 069-2016 i Helse Sør-Øst RHF september 2016 der styret i det regionale foretaket vedtok at det skulle inngås kontrakt med en ekstern partner. Styret i Helse Sør-Øst RHF la til grunn at det fortsatt skulle være Sykehuspartner HF som skulle være ansvarlig for de samlede IKT-leveransene mot helseforetakene.
Sykehuset Innlandet merker seg Datatilsynets vurdering om at foretaket, som databehandlingsansvarlig, burde vært mer aktiv og ansvarlig med vurderinger og beslutninger i prosessen med å inngå avtale og etablere underleverandør for Sykehuspartner. Vi vil følge opp dette med nødvendige tiltak og vil innføre forbedringer i system og rutiner på informasjonssikkerhet og personvernområdet som denne saken har synliggjort, slik at Sykehuset Innlandets databehandlingsansvar blir ivaretatt, også ved regionale løsninger og tjenester.

Vår dato	Vår referanse
02.01.2018	16/01990-17

Til orientering er det nå et felles arbeid i helseregionen der foretakenes selvstendighet og ansvar for databehandleransvaret skal sikres formelt og reelt ved endringer eller innføring av nye felles systemer, herunder tydeliggjøre og styrke metoden for gjennomføring av risikovurderinger. Inkludert i dette er vurdering i det enkelte helseforetak om for eksempel restrisiko kan aksepteres eller om det er behov for ytterligere tiltak før endring / innføring av nytt system.

Databehandleravtalen mellom Sykehuset Innlandet HF og Sykehuspartner HF
Databehandleravtalen er bilag i årlig tjenesteavtale (SLA) mellom Sykehuset Innlandet og Sykehuspartner. Kapittel 8 i databehandleravtalen omtaler databehandlerens bruk av underleverandør. I henhold til denne avtalen har Sykehuset Innlandet HF det fulle ansvar som databehandlingsansvarlig. Sykehuspartner HF er hoveddatabehandler og har en rekke underleverandører som refereres til som underleverandørdatabehandlere. Sykehuspartner HF er hovedansvarlig for driften som omfatter ansvar for tilgangsstyring med utøvende kontroll på at tilganger gis i henhold til lov, forskrift, gjeldende retningslinjer og akseptabel risiko. Databehandleren må oppfylle kravene og har det utøvende ansvaret for å ivareta informasjonssikkerheten, mens databehandlingsansvarlig har et kontrollansvar for databehandlerens utførelse av databehandlingen.

Databehandleravtalen beskriver roller, oppgaver og ansvar knyttet til dem. Med bakgrunn i Datatilsynets varsel og erfaring fra den regionale prosessen så langt, må Sykehuset Innlandet følge opp databehandleravtalen på en bedre måte. Det vil være nødvendig å forsterke og forbedre rutiner mellom Sykehuset Innlandet og Sykehuspartner HF, hvor alle endringer knyttet til behandling av personopplysninger, herunder nye eksterne databehandlere, skal forelegges foretaket til godkjenning før endring iverksettes. Sykehuset Innlandet må gjøre egne / selvstendige vurderinger av de gjennomførte ROS-analyser på alle endringene, før eventuell godkjenning. Som tiltak vil Sykehuset Innlandet forsøke å få endret eksisterende databehandleravtale til ny standard databehandleravtale med sjekkliste som Direktoratet for e-helse har utarbeidet. Databehandleravtalen mellom Sykehuset Innlandet og Sykehuspartner skal oppdateres og har som målsetting å være signert innen 1.4.2018.

Drift av dagens infrastruktur
Under punkt 6.3.3 i Datatilsynets brev Opplysninger fremkommet i saken står det at «…*noen av representantene fra de ulike helseforetak var bekymret som følge av risiko knyttet til å legge driften til Bulgaria».*

Sykehuset Innlandet gjør oppmerksom på at etter den planlagte overføring av drift av dagens infrastruktur til underleverandør, var driften i hovedsak planlagt fra Norge i den første fasen og med ressurser virksomhetsoverdratt fra Sykehuspartner HF.

Videre, i brevet til Datatilsynet 16. juni 2017 side 6 kap 2.2 viste Sykehuset Innlandet til at i avtalen med underleverandør, er Sykehuset Innlandet sikret kontroll med risikovurderingene og eventuell aksept av restrisiko ved behandling av personopplysninger utenfor Norge jfr. avtalens Appendix 1-A-6 punkt 2.1. Dette bidrar til å sikre Sykehuset Innlandets kontroll med informasjonssikkerheten.

Tilgangskontroll
Det vises til punkt 6.2.3 Datatilsynets vurdering/Tilgangen som ble gitt til tjenesteleverandør i Bulgaria der det på slutten av første avsnitt er skrevet: Det er derfor uklart om opplysninger har kommet på avveie eller ikke.

Med referanse til PwC rapporten fra ekstern gjennomgang av programmet for modernisering av IKT infrastruktur (iMod) i juni, er det ingen indikasjoner eller bevis på at det har vært misbruk eller forsøk på misbruk av tilgang til helseopplysninger. Dette er også konklusjonen etter Sykehuspartners interne gjennomgang. Uttalelsen er basert på grundig gjennomgang av de logger som finnes. Ytterligere kan vi opplyse at det ikke er oppdaget fravær av tjenester.

Sykehuspartner HF sin analyseplattform har en sentral funksjon for å sikre infrastrukturen og data for helseforetakene i Helse Sør-Øst og oppdage kompromitterende angrep i tidlig fase. Så langt, og i meget stor grad, har Sykehuspartner HF avverget ondsinnede angrep, herunder WannaCry-viruset som i mai 2017 hadde flere suksessfulle angrep mot engelske sykehus.

Henvisning til helseforetakenes vurdering av krav til tidspunkt for risikovurdering
Under punkt 5.4 *Helseforetakenes redegjørelse*, avsnitt 3 i varselet er det gjort et feilsitat fra foretakets brev 16. juni 2017. Her står det at «Helseforetakene legger også til grunn at det ikke er et krav at risikovurdering skal gjennomføres før behandling av personopplysninger iverksettes eller før man iverksetter endring som kan ha betydning for informasjons¬sikkerheten.»

I Sykehuset Innlandet sitt brev av 16. juni 2017 står det på side 3 kap 2.1: "*Risikovurdering må foretas før behandling av personopplysninger iverksettes eller før man iverksetter endring som kan ha betydning for informasjonssikkerheten.*" Dette innebærer at før endringer i tjenester og drift kan gjennomføres, skal Sykehuset Innlandet kunne akseptere restrisiko. Enhver endring som påvirker informasjonssikkerheten kan dermed først gjennomføres av Sykehuspartner HF og dennes underleverandører dersom Sykehuset Innlandet aksepterer restrisiko ved endring.

Styringssystem for informasjonssikkerhet og organisering av arbeidet med informasjonssikkerhet og personvern i Sykehuset Innlandet
Sykehuset Innlandet har et omfattende styringssystem for informasjonssikkerhet. Informasjonssikkerhet er et ledelsesansvar og sykehusets styringssystem for informasjonssikkerhet har vært behandlet i foretakets ledermøte, og er besluttet av administrerende direktør. Alle prosedyrer, instrukser, skjema m.m. som gjelder Sykehuset Innlandet, er publisert i foretakets dokumentstyringssystem som er tilgjengelig for alle ansatte.

Sykehuset Innlandet har i databehandleravtalen med Sykehuspartner etablert og dokumentert et sikkerhetsrammeverk for helseforetakets personopplysninger hos databehandler. For eksempel kan ikke databehandler uten avtale med databehandlingsansvarlig overlate personopplysninger til andre, jf. også personopplysningsloven § 15. Databehandler har et selvstendig ansvar for å påse at behandling av personopplysningene skjer i overensstemmelse med kravene til informasjonssikkerhet i pasientjournalloven § 22 med mer. Bare de som har reelt behov for tilgang til systemet og

informasjonen, skal få tilgang. Dersom tredjepart eller underleverandør skal ha tilgang til systemet, skal slik bruk dokumenteres i egen underleverandørdatabehandleravtale. En underleverandør skal utføre oppgaver på samme måte som om databehandler selv stod for utførelsen av disse. Databehandleravtalen med Sykehuspartner inngås hvert år og undertegnes av administrerende direktør.

Sykehuset Innlandet har en sikkerhetsledelse på personvern- og informasjonssikkerhetsområdet, hvor ansvars- og myndighetsforhold er dokumentert og øverste ledelse er involvert. Det vil nå iverksettes tiltak for å sikre og bedre foretakets ansvar for og kontroll på personopplysninger. Dette gjelder også i forbindelse med at Sykehuspartneres databehandleravtaler og deres databehandleravtaler med underleverandører.

Sykehuset Innlandets sikkerhetsfunksjon ligger i organisasjonens stab, Stabsområde Helse, eHelse & teknologi, ledet av en informasjonssikkerhetsansvarlig og er godt forankret i foretakets ledelse og har lang erfaring, god kompetanse og arbeider blant annet med:

- Rådgivning og saksbehandling innen områdene sikkerhetsstrategi, sikkerhetsteknologi, tilsynssaker, informasjonssikkerhet, taushetsplikt, personvern, tilgang til pasientopplysninger, ivaretakelse av personvern ved forskning og kvalitetsregistre
- Planlegge, forberede, iverksette, gjennomføre eller bistå ved planlagte og systematiske tiltak (internkontroll) innen informasjonssikkerhet:
- Sikkerhetsrevisjoner
- Sikkerhetstester
- Risikovurderinger ved innføring av nye eller endring av eksisterende løsninger
- Avvikshåndtering og sikkerhetsbrudd
- Ledelsens gjennomgang av informasjonssikkerhet
- Utarbeide og vedlikeholde styrende dokumentasjon for informasjonssikkerhet etter retningslinjer fra Helse Sør-Øst RHF og Helsedirektoratet
- Følge opp behandling av helse- og personopplysninger til tilsynsmyndigheter

Det er planer om å styrke denne funksjonen samt personvernombudsrollen. Dette er områder vi nå vurderer og evaluerer for å forberede implementering av ny personvernregulering.

Forberedelse til ny personvernregulering

Sykehuset Innlandet finner det naturlig i denne sammenheng å informere om arbeidet med å forberede overgang til ny personvernregulering, herunder arbeid med å sikre:

- Oversikt over hvilke databehandlinger som gjennomføres og hvilket hjemmelsgrunnlag disse har
- Gjennomførte risikovurderinger av løsninger og infrastruktur
- Oversikt over leverandørtilganger, herunder risikovurderinger og databehandleravtaler
- Gjennomgang og oppgradering av rutiner og prosedyrer, herunder tilgang for leverandører
- Prosedyrer og rutiner for gjennomføring av databehandleravtaler og personvernkonsekvensvurderinger. Dette arbeidet er Sykehuspartner sentral i for å sikre felles rutiner og prosedyrer i regionen, samtidig som prosessene skal sikre at den enkelte databehandlingsansvarlig kan ivareta sitt ansvar, herunder å ikke akseptere hva som vurderes som for høy restrisiko.

Fremtidig tjenesteutsetting av infrastruktur i Helse Sør – Øst
I dette kapitlet vil vi gjengi deler av det som er førende og gjengitt i utkast til mandat for fremtidig tjenesteutsetting av infrastruktur. Dette synliggjør de nødvendige endringer som vil skje fremover i slike saker.
Det skal gjennomføres en rekke aktiviteter med det formål å avdekke hvorvidt den informasjonssikkerhetsmessige- og personvernmessige risiko ved tjenesteutsetting av infrastruktur i Helse Sør-Øst er innenfor akseptabelt risikonivå.
Sykehuspartner HF skal gjennomføre en overordnet risikovurdering av tjenesteutsetting av infrastrukturen i Helse Sør-Øst, inkl. vurdering mot sikkerhetsloven § 29 a, jf. rapport om tjenesteutsetting til privat sektor fra Direktoratet fra e-helse av desember i år.
Sykehuspartner HF skal også fullføre nødvendig dokumentasjon av eksisterende risikonivå, som skal inngå i vurderingsgrunnlaget ved risikovurdering av alternativene innenfor og utenfor kontrakt.
Sykehuspartner HF skal aktivt og ofte involvere det enkelte behandlingsansvarlige helseforetak.

De behandlingsansvarlige helseforetakene skal i samarbeid med Sykehuspartner HF legge opp til tett dialog med Datatilsynet. Særlig hensynet til gjennomføring av evt. forhåndsdrøfting må diskuteres.
De behandlingsansvarlige helseforetakene skal etter mottak av risikovurderinger og personvernkonsekvensvurderinger aktivt vurdere og godkjenne risikovurderinger, inklusive restrisiko. Dette som et grunnlag for tjenesteutsetting og overdragelse av databehandleroppgaver.

I rapporten «Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten», utgitt av Direktoratet for e-helse i desember 2017 anbefales videre utredning av utfordringer vedrørende databehandlingsansvaret som tilligger helseforetakene når føringer og beslutninger for helseforetakene, som har en direkte konsekvens for databehandlingsansvaret, vil tas av sentrale myndigheter og Helse Sør-Øst RHF som eier.

Vurdering av om gebyr skal ilegges og vurdering av gebyrets størrelse
Sykehuset Innlandet mener opplysningene i dette brevet synliggjør at det er formildende omstendigheter for helseforetaket som Datatilsynet bør legge vekt på i sin vurdering av selve overtredelsesgebyret og gebyrets størrelse.

Sykehuset Innlandet har stor oppmerksomhet på informasjonssikkerhet og personvern og et omfattende styringssystem knyttet til dette. Databehandleravtalen innehar betingelser for å sikre egen kontroll med informasjonssikkerheten. Sykehuset Innlandet mener heller ikke å ha hatt noen interesse eller fordeler som har medvirket til at vi har unnlatt å gjøre en egen risikovurdering når databehandler har inngått avtale med en underleverandør.

Ved vurderingen av alvorligheten av overtredelsen, omtaler ikke varselet skadeomfanget.
Intern gjennomgang hos databehandler og ekstern gransker viser ingen indikasjoner eller bevis på at det har vært misbruk eller forsøk på misbruk av tilgang til helseopplysninger, eller at disse har kommet på avveie.

Vår dato	Vår referanse
02.01.2018	16/01990-17

Ved vurderingen av overtredelsesgebyrets størrelse omtaler varselet verdien av avtalen den regionale databehandleren har inngått med underleverandør. For ordens skyld bemerkes det at avtalen omfatter hele regionen og ikke bare Sykehuset Innlandet.
Sykehuset Innlandet tar saken på største alvor og det er, som nevnt over, allerede iverksatt arbeid med tiltak og forbedringer for å følge opp de forhold som er påpekt av Datatilsynet.

I styremøtet i Sykehuset Innlandet i januar 2018 skal det legges frem en sak som belyser informasjonssikkerhets - og personvernområdet, og hvilke forhold, rutiner, utfordringer og tiltak som gjelder fremover.

Med vennlig hilsen

Alice Beathe Andersgaard
Administrerende direktør

Håkon Iversøn
Informasjonssikkerhetsleder

Dette dokumentet er elektronisk godkjent og sendes ut uten signatur