Datatilsynet

UNIVERSITETSSYKEHUSET NORD-NORGE HF
Postboks 100
9038 TROMSØ

Deres referanse	Vår referanse	Dato
AR374040813	20/01798-1	08.07.2020

Krav om redegjørelse - melding om avvik - Universitetssykehuset Nord-Norge HF

Datatilsynets oppgave er å føre kontroll etter personopplysningsregelverket slik at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Sakens bakgrunn
Vi viser til avviksmeldingen dere sendte inn 14. mai 2020. I meldingen har dere varslet om at det som følge av menneskelig svikt ble publisert feil liste da offentlig postjournal skulle legges ut på sykehusets nettsider. Listen som ble lagt ut var usladdet og inneholdt navn og personnummer i tillegg til sakstittel. Listen ble raskt fjernet da avviket ble oppdaget, men hadde på det tidspunktet vært tilgjengelig på nettsiden i 1,5 døgn.

Dere har opplyst at avviket skyldes en svikt i kontrollrutinene som i hovedsak består i at to personer skal kontrollere at publisering av offentlig journal skjer på riktig måte.

Rettslig bakgrunn
Dere har plikt til å hindre uautorisert tilgang til personopplysninger hvor det er behov for konfidensialitet. Opplysninger om at en person er pasient ved sykehuset vil i mange tilfeller ikke bare være en opplysning om personlige forhold, men også en helseopplysning. Sykehusets plikt til konfidensialitet følger av helsepersonellovens §§ 21 flg. Det er også fastsatt i forskrift om offentlig journal § 10 at «opplysningar som er omfatta av teieplikt i lov eller i medhald av lov skal ikkje gå fram av den offentlege journalen».

Pasientjournalloven §§ 22 og 23 inneholder krav til informasjonssikkerhet og internkontroll som skal sikre at sykehusets behandling av pasientopplysninger skjer i samsvar med personvernforordningen artikkel 32 og 24.

Pasientjournalloven § 23 pålegger sykehuset å gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, personopplysningsloven og pasientjournalloven, jf. forordningen artikkel 24.

I andre ledd stilles det krav til dokumentasjon: «Den dataansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den dataansvarlige

og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.»

Kravet om tekniske og organisatoriske tiltak gjelder også for informasjonssikkerhet i § 22.

For å vurdere om dere har et system som i tilstrekkelig grad oppfyller kravene i pasientjournalloven §§ 22 og 23 jf. personvernforordningen artikkel 32 og 24 trenger vi en nærmere redegjørelse for tiltakene som er iverksatt for å unngå at slike avvik oppstår.

Vi ber om svar på følgende:

1. Hvordan ble det varslede avviket oppdaget?
2. Gi en oversikt over hvilke typer personopplysninger som er offentliggjort og konsekvenser det kan ha hatt overfor de berørte.
3. Hvordan er de berørte ivaretatt etter at avviket fant sted?
4. Er det gjennomført risikovurdering for å kartlegge sårbarheter ved sykehusets system for publisering av postjournal? Hvis ja, legg ved risikovurderingen. Hvis nei, forklar hvorfor det ikke er gjennomført slik vurdering.
5. Hvilke tekniske tiltak hadde dere iverksatt, i tillegg til manuell kontroll, for å sikre at taushetsbelagte opplysninger ikke offentliggjøres i forbindelse med publisering av postjournal da avviket fant sted?
6. Hvilke tekniske og /eller organisatoriske tiltak var iverksatt for å sikre etterkontroll når offentlig postjournal er publisert da avviket ble oppdaget?
7. Hva er deres vurdering av informasjonssikkerhet og internkontroll ved publisering av postjournal sett i forhold til gjeldene taushetsplikt og kravene i personvernforordningen artikkel 32 og 24?
8. Hvordan sikrer sykehuset tilstrekkelig opplæring, herunder tilstrekkelig kjennskap til aktuelt regelverk, av ansatte som har arbeidsoppgaver knyttet til publisering av offentlig postjournal?

Legg ved dokumentasjon på rutiner og tekniske tiltak som var iverksatt for å forebygge og eventuelt avdekke feil ved publisering av postjournal da avviket fant sted.

Videre fremdrift
Dere må svare på spørsmålene våre innen **3. august 2020**.

Hjemmelsgrunnlag
Etter personvernforordningen artikkel 58 nr. 1 har vi myndighet til å kreve de opplysningene som trengs for at vi skal kunne gjennomføre oppgavene våre.

Klageadgang
Dere kan klage på pålegget om å gi oss informasjon. En eventuell klage må sendes til oss **innen tre dager** etter at dette brevet er mottatt (jf. forvaltningsloven § 14). Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernnemnda for klagebehandling.

Innsyn og offentlighet
Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3.) Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn ber vi dere om å begrunne dette.

Mer informasjon om personvern, internkontroll og informasjonssikkerhet kan dere finne på våre nettsider, www.datatilsynet.no.

Hvis dere har spørsmål, kan dere ta kontakt med Grete Alhaug på telefon 90781530.

Med vennlig hilsen

Grete Alhaug
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer