Datatilsynet

SYKEHUSET ØSTFOLD HF
Postboks 300
1714 GRÅLUM

Deres referanse	Vår referanse	Dato
AR300186895	20/02291-1 (19/00219) / SLI	22.06.2020

Varsel om vedtak om overtredelsesgebyr og pålegg

Vi viser til meldingen om brudd på personopplysningssikkerheten (avviksmeldingen) med referanse AR300186895, som dere sendte 14. januar 2019. Bruddet på personopplysnings-sikkerheten (avviket) ble oppdaget 3. januar 2019. Vi beklager lang saksbehandlingstid.

1. Varsel om vedtak om overtredelsesgebyr og pålegg
Datatilsynet varsler med dette følgende overtredelsesgebyr:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 andre ledd og pasientjournalloven § 29, jf. personvernforordningen artikkel 83, pålegges Sykehuset Østfold HF å betale et overtredelsesgebyr på 1 200 000 NOK – en million norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32, jf. personopplysnings-loven § 26 første ledd, jf. personvernforordningen artikkel 24, og pasientjournalloven §§ 22 og 23.*

Vi varsler også følgende pålegg:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav d, pålegges Sykehuset Østfold HF å tilse at styringssystemet for behandling av personopplysninger er egnet til å ivareta kravene i personvernregelverket og pasientjournalloven. Vi viser særlig til rutinene for tilgangskontroll og lagring av personopplysninger. Styringssystemet må innebære oppfølging av at rutinene følges, herunder oppfølging av at kun sikre systemer brukes ved behandling av sensitive personopplysninger. Vi viser til personvernforordningen artikkel 32, jf. artikkel 24, og pasientjournalloven § 23.*

2. Beskrivelse av sakens faktiske forhold
Fra august 2013 og frem til januar 2019 har Sykehuset Østfold HF hatt manglende tilgangsstyring på rapportuttrekk fra elektronisk pasientjournal (EPJ).

Uttrekkene fra EPJ er lister over utskrivningsklare pasienter (USK-lister) og omfatter særlige kategorier av personopplysninger (sensitiv pasientinformasjon). Listene har hjemmel i

pasientjournalloven § 6 annet ledd og har som formål å understøtte administrasjon av pakkeforløp, fristbrudd og løftebrudd, samhandling, operasjon og medisinsk koding.

Avviket omfattet tre ulike lister:

a) En oppdatert USK-liste som omfatter ca. 25-30 pasienter. Denne listen oppdateres hvert 15. minutt.
b) En historisk USK-liste fra 2013 frem til 2019, med 13 800 pasienter og 26 596 utskrivninger.
c) To lister med fødselsnummer og innleggelsesårsak, med ca. 30 pasienter.

Personopplysningene i listene omfatter demografiske opplysninger og navn, fødselsdato, kommune, avdelingstilhørighet og eventuelt informasjon om tilretteleggelse ved overføring av pasient til kommune. To av listene inneholdt som nevnt fødselsnummer og innleggelsesårsak.

Ifølge Sykehuset Østfold HF er det ikke indikasjoner på at personopplysninger er kommet på avveie og at taushetsplikten dermed er brutt. Alle ansatte ved Sykehuset Østfold HF har taushetsplikt og har signert for dette.

2.1 Tilgangskontroll

Sykehuset Østfold HF har etablert en rutine for tilgangskontroll, som ble lagt ved redegjørelsen til Datatilsynet. Vi forstår det slik at avviket er et brudd på interne rutiner for å gi tilgang til ansatte med tjenstlig behov.

Det har ikke vært tilgangskontroll på området/mappene der uttrekkene av særlige kategorier personopplysninger fra EPJ ble lagret og/eller mellomlagret.

Personopplysningene fra rapportuttrekkene har vært tilgjengelig for alle ansatte ved Sykehuset Østfold HF. Sykehuset sier i sitt brev at personopplysningene «lå på et område som det ikke var naturlig for de fleste medarbeidere å gå inn på» og at personopplysningene «var vanskelig tilgjengelig i form av at de var lagret i undermapper blant en større mengde anonymiserte eller sterkt avidentifiserte opplysninger». Videre fremgår det at «[o]pplysningene har ikke vært tilgjengelig for personer som ikke har signert taushetserklæring».

2.2 Logging

Det er ingen funksjonalitet for logging i mappestrukturen som er benyttet. Denne mappestrukturen ble brukt siden det ikke fantes annet IKT-verktøy som kunne ivareta behovene for rapport og uttrekk.

2.3 Internt styringssystem

Sykehuset Østfold HF har besluttet at revidering av personregistre skal inngå i Sykehuset Østfold HFs overordnede, toårige revisjonsplan.

Sykehuset Østfold HF har ikke gjennomført revisjon av, eller på annen måte kontrollert, innhold eller funksjonalitet i den aktuelle mappestrukturen, herunder tilgangskontroll på det

aktuelle området. Datatilsynet legger til grunn at heller ikke lagringssted og lagringstid for uttrekkene fra EPJ er kontrollert.

2.4 Lagringsrutiner
Sykehuset Østfold HF har etablert rutiner for lagring av helseopplysninger og personopplysninger. Vi forstår det slik at avviket er et brudd på interne rutiner for lagringssted og lagringstid.

2.5 Innebygd personvern og personvern som standardinnstilling
Sykehuset Østfold HF gjennomførte et for- og hovedprosjekt i forbindelse med at ny personopplysingslov og personvernforordningen trådte i kraft 20. juli 2018. Prosjektet skulle «avdekke avvik ved at hele organisasjonen var bedre informert om kravene i personopplysningsloven».

Ifølge prosjektplanen identifiserte prosjektet behov for kartlegging av tilganger og automatisert tilgangskontroll (idM) i DIPS, og man skulle vurdere behovet for innføring av en regional standard. Dette punktet har status ferdig, og ansvarlig var systemeier DIPS.

Det fremgår ikke at prosjektet omfattet om journalsystemet DIPS har innebygd personvern og personvern som standardinnstilling eller at prosjektet tok sikte på å avdekke svakheter ved rutinen for lagring av personopplysninger.

2.6 Behandlingsprotokoll
Sykehuset Østfold HF har etablert en komplett og oppdatert protokoll over behandlings-aktivitetene i sykehuset. Slik vi har forstått det, ble USK-listene ført inn i sykehusets protokoller i juni 2018. Sykehuset Østfold HF har oppgitt at de sikrer kontroll over all behandling av personopplysninger ved å risikovurdere all etablering eller endring av personregistre.

2.7 Iverksatte tiltak
Sykehuset Østfold HF viser til at følgende strakstiltak er gjennomført:

- Mapper er gjennomgått, og historiske personopplysninger er slettet.
- Mappene er flyttet, og kun analyseavdelingens medarbeidere har tilgang. Tilgangen styres etter tilhørighet til organisatorisk enhet.
- Rapporter med anonymiserte opplysninger for statistiske behov er flyttet til mapper med tilgangsstyring, der 118 medarbeidere nå har tilgang.
- Personopplysninger knyttet til pasientlogistikk er «kopiert» over til tilgangsstyrte mapper. Tilgangsbehovet for medarbeidere er revidert.

Av langsiktige tiltak viser Sykehuset Østfold HF til følgende:

- Innføring av en analyseplattform som muliggjør mindre grad av manuelle rutiner. Prosjektet er startet opp, og vi forstår det slik at analyseplattformen er etablert.
- Det er etablert et mottaksprosjekt for å beslutte bruk av løsningen.

2.8 Informasjon til de registrerte
Informasjon er ikke gitt til pasientene som er berørt av avviket. Årsaken er at Sykehuset Østfold HF mener at avviket ikke omfatter tap eller spredning av personopplysninger, og det er ikke avdekket at personopplysninger er brukt til andre formål. Sykehuset Østfold HF viser også til at alle ansatte har signert for at de har taushetsplikt.

3. Rettslig grunnlag
Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen artikkel 57.

Vi er også tilsynsmyndighet etter pasientjournalloven, jf. lovens § 26. Pasientjournalloven gjelder for all behandling av helseopplysninger som er nødvendig for blant annet å kvalitetssikre helsehjelp til enkeltpersoner, jf. lovens § 3.

3.1 Om lovvalg
Den nye personopplysningsloven, som inkorporerer EUs personvernforordning i norsk rett, trådte i kraft 20.07.2018. Loven opphevet samtidig personopplysningsloven (2000) og reglene i personopplysningsforskriften (2000).

Denne saken gjelder forhold som oppsto i 2015, altså før ikrafttredelsen av personopplysningsloven (2018), men som har vedvart i tiden etterpå. Vi må derfor ta stilling til om saken skal vurderes etter personopplysningsloven (2018) eller personopplysningsloven (2000).

I personopplysningsloven (2018) § 33 første ledd finnes en særskilt overgangsregel om overtredelsesgebyr, som lyder:

> «Reglene om behandling av personopplysninger som gjaldt på handlingstidspunktet, skal legges til grunn når det treffes vedtak om overtredelsesgebyr. Lovgivningen på tidspunktet for avgjørelsen skal likevel anvendes når dette fører til et gunstigere resultat for den ansvarlige».

Spørsmålet om lovvalg må altså vurderes ut fra hva som regnes som handlingstidspunktet.

Det aktuelle avviket oppsto før ikrafttredelsen av nytt regelverk den 20.07.2018, men vedvarte frem til avviket ble oppdaget i januar 2019. Handlingstidspunktet i denne saken har altså vedvart over tid og i tiden etter at personopplysningsloven (2018) trådte i kraft. Det følger da av personopplysningsloven (2018) § 33 at saken skal vurderes etter denne loven.

Vi viser også til forarbeidene til personopplysningsloven (2018), Prop. 56 LS (2017-2018) side 196, hvor departementet blant annet uttaler følgende om spørsmålet om lovvalg mellom personopplysningsloven (2000) og personopplysningsloven (2018):

> «Utgangspunktet vil være at vedtak hos Datatilsynet og Personvernnemnda vil måtte fattes på grunnlag av de til enhver tid gjeldende materielle regler».

Det samme følger av Personvernnemndas praksis i saker som ble oversendt nemnda før ny lov trådte i kraft, men som ble behandlet etter ikrafttredelsen; se for eksempel PVN-2018-05 og PVN-2018-06.

På denne bakgrunn er det etter vår vurdering klart at saken må vurderes etter personopplysningsloven (2018) og personvernforordningen.

3.2 Om helseopplysninger og taushetsbelagt informasjon

Helseopplysninger om pasienter er en såkalt særlig kategori av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1. Slike opplysninger vil være omfattet av ulike taushetspliktbestemmelser, se for eksempel helsepersonelloven § 21. Vi viser også til forbudet i helsepersonelloven § 21 a mot urettmessig å tilegne seg taushetsbelagt informasjon.

Etter helsepersonelloven § 16 skal virksomheter i helsetjenesten organisere seg slik at helsepersonell blir i stand til å overholde sine lovpålagte plikter etter blant annet helsepersonelloven.

3.3 Grunnprinsippene

De grunnleggende prinsippene for behandling av personopplysninger fremgår av personvernforordningen artikkel 5. Vi viser særlig til artikkel 5 nr. 1 bokstav f, hvor det fremgår:

> «1. Personopplysninger skal (…)
>
> f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling (…), ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».

Det er dataansvarliges ansvar at prinsippene overholdes, og den dataansvarlige skal kunne påvise dette, jf. artikkel 5 nr. 2.

3.4 Kravene til personopplysningssikkerhet og styringssystemer

3.4.1 Personvernforordningen

Personvernforordningen artikkel 32 regulerer kravene til sikkerhet ved behandlingen av personopplysninger. Under følger et utdrag av relevante deler av artikkel 32:

> «1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet, (…)
>
> b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene, (…)
>
> d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

> 2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av (…) ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Plikten til å gjennomføre egnede tekniske og organisatoriske tiltak fremgår tilsvarende av personvernforordningen artikkel 24, som regulerer den dataansvarliges ansvar særskilt.

Innebygd personvern og personvern som standardinnstilling, jf. personvernforordningen artikkel 25, innebærer et krav om at personvernprinsippene er ivaretatt i hele behandlingen. Vi viser igjen til prinsippet om integritet og konfidensialitet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f. Den dataansvarlige har plikt til påse at de elektroniske løsningene som brukes har innebygd personvern.

Etter personvernforordningen artikkel 30 nr. 1 har den dataansvarlige plikt til å føre protokoll over behandlingsaktivitetene som utføres. Protokollen skal blant annet inneholde en beskrivelse av kategoriene av personopplysninger som behandles, jf. artikkel 30 nr. 1 bokstav c, og kategoriene av mottakere som personopplysningene vil bli utlevert til, jf. artikkel 30 nr. 1 bokstav d.

3.4.2 Pasientjournalloven

Kravene til den dataansvarlige ved behandling av journalopplysninger fremgår også av pasientjournalloven.

Pasientjournalloven § 22 første ledd om informasjonssikkerhet lyder:

> «Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll.».

Pasientjournalloven § 23 om internkontroll lyder:

> «Den dataansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, personopplysningsloven og denne loven, jf. forordningen artikkel 24.
>
> Den dataansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den dataansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.
>
> Departementet kan i forskrift gi nærmere bestemmelser om internkontroll».

3.5 Informasjon til berørte personer

Dersom det er sannsynlig at sikkerhetsbruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den dataansvarlige uten ugrunnet opphold underrette de berørte personene om bruddet, jf. personvernforordningen artikkel 34 nr. 1.

Tilsynsmyndigheten kan pålegge den dataansvarlige å informere berørte personer, jf. artikkel 34 nr. 4. De nærmere kravene til innholdet i en slik underretning fremgår av artikkel 34 nr. 2 og 3.

3.6 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 annet ledd og pasientjournalloven § 29, fremgår det at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på bestemmelser i de respektive lovene.

I personvernforordningen artikkel 83 angis vilkårene for ileggelse av gebyr. Bestemmelsen inneholder blant annet en oversikt over hvilke momenter det skal tas hensyn til, både når det vurderes hvorvidt overtredelsesgebyr skal ilegges og i utmålingen av gebyrets størrelse.
De relevante delene av artikkel 83 nr. 1 og nr. 2 gjengis under:

> «1. Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.
>
> 2. (…) Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om overtredelsesgebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til følgende:
>
> a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,
> b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,
> c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,
> d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,
> e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren,
> f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,
> g) kategoriene av personopplysninger som er berørt av overtredelsen,
> h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen,

i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes,
j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42 og
k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen».

Artikkel 83 angir også rammene for overtredelsesgebyrets størrelsesorden. Vi viser i denne forbindelse til artikkel 83 nr. 4. De relevante delene av bestemmelsene lyder:

> «4. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 10 000 000 euro (…):
> a) den behandlingsansvarliges og databehandlerens forpliktelser i henhold til artikkel 8, 11, 25-39 samt 42 og 43 (…)».

I personopplysningsloven § 26 første ledd fremgår det at personvernforordningen artikkel 83 nr. 4 gjelder tilsvarende for overtredelser av forordningen artikkel 24

4. Datatilsynets vurdering

I redegjørelsen for vår vurdering av avviket vil vi følge samme kronologi som under *Beskrivelse av sakens faktiske forhold* over.

4.1 Tilgangskontroll

Sykehuset Østfold HF har etablert en rutine for tilgangskontroll, og avviket representerer et brudd på de interne rutinene for kun å gi tilgang til ansatte med tjenstlig behov. Det har ikke vært tilgangskontroll på området/mappene der uttrekkene av (særlige kategorier av) personopplysninger fra EPJ ble lagret og/eller mellomlagret. Slik vi forstår det, har alle medarbeidere som var ansatt ved sykehuset i perioden 2013-2019 hatt tilgang til mappen.

I vår vurdering av at sensitive personopplysninger har vært tilgjengelige for ansatte uten tjenstlig behov, er det ikke avgjørende at sykehuset mener at opplysningene var lagret på et område der det ikke var naturlig for de fleste medarbeidere å gå inn. Risikoen for brudd på opplysningenes konfidensialitet og integritet har like fullt vært til stede.

Videre viser Sykehuset Østfold HF til at de ansatte som har hatt tilgang til mappen og personopplysningene har signert for at de har taushetsplikt. Etter vårt syn er ikke dette relevant for vurderingen av hvilke pasientopplysninger en ansatt skal ha tilgang til. Vi viser til kravet om at ansatte ikke skal ha tilgang til personopplysninger de ikke har tjenstlig behov for, uavhengig av om den ansatte har taushetsplikt eller ikke.

<u>Datatilsynets vurdering:</u>
Personopplysningene i rapportuttrekkene har i prinsippet vært tilgjengelige for alle ansatte ved Sykehuset Østfold HF. Sykehuset har dermed ikke hindret urettmessig tilgang til

personopplysninger. Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24 og artikkel 5 nr. 1 bokstav f, og pasientjournalloven § 22.

4.2 Logging

Sykehuset Østfold HF har ikke logget aktiviteten på området der rapportuttrekkene var lagret. Dersom sykehuset hadde hatt rutine for logging av aktiviteten og fulgt opp loggene på en systematisk måte, kunne sykehuset ha bekreftet og/eller avkreftet om ansatte har benyttet seg av tilgang til og/eller endret personopplysningene/listene. Den manglende loggingen øker risikoen for at man mister oversikt over hvor personopplysninger/ pasientdata befinner seg. Vi er usikre på om Sykehuset Østfold HF nå har etablert et tilstrekkelig system og rutine for logging og oppfølging av logger i sykehuset.

Datatilsynets vurdering:

Sykehuset Østfold HF har ikke logget aktiviteten der uttrekkene fra EPJ var lagret, og sykehuset har dermed ikke kunnet følge opp aktiviteten og avdekke uautorisert tilgang og eventuell kompromittering av personopplysningene. Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24 og 5 nr. 2, og pasientjournalloven § 23.

4.3 Internt styringssystem

Sykehuset Østfold HF har ikke utført jevnlig kontroll av ansattes tilgang til mapper, lagring og sletting på serveren.

I prosedyren «*Helseopplysninger – lagring, arkivering og sletting*» er alle nivåer i sykehuset gitt et ansvar for å påse at rutinene etterleves. I forbindelse med lagring av rapportuttrekkene fra EPJ har ikke sykehuset ved administrerende direktør fulgt opp det overordnede ansvaret for at tilgangskontrollen ved sykehuset fungerer. Vi kan heller ikke se at øvrige ledere har påsett at tilgangskontrollen fungerte som forutsatt.

Dette kunne for eksempel vært gjort ved å etterspørre internrapportering om etterlevelse av den nevnte prosedyren. Internrevisjon av tilgangsstyring samt oppfølging av logger og lagring bør jevnlig utføres, slik at man til enhver tid har oversikt over risikobildet. Sikkerhetsleder, som har det utøvende ansvaret for informasjonssikkerhet, kan være et sentralt ledd i en slik aktivitet. Sykehuset kan også rådføre seg med personvernombudet i prosessen med å sikre at bare ansatte med tjenstlig behov har tilgang til pasientopplysninger som rapportuttrekkene fra EPJ.

Datatilsynets vurdering:

Sykehuset Østfold HF har ikke hatt styring med de ansattes tilgang til rapportuttrekk med sensitive personopplysninger i årene 2013-2019. Ledelsen, som har overordnet ansvar for lagring, tilgangskontroll og sletting, har ikke sørget for at tilgangskontrollen fungerte som forutsatt i forbindelse med rapportuttrekkene fra EPJ. Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24 og 5 nr. 2, og pasientjournalloven § 23.

På grunn av den mangelfulle styringen har ikke Sykehuset Østfold HF fått korrigert løsningen med hensyn til konfidensialitet, integritet og tilgjengelighet. Dette er et brudd på

personvernforordningen artikkel 32, jf. artikkel 24 og 5 nr. 1 bokstav f og nr. 2, og pasientjournalloven §§ 22 og 23.

4.4 Lagringsrutiner

Personopplysningene i rapportuttrekkene fra EPJ har ikke blitt slettet etter hvert som formålet med behandlingen av opplysningene har blitt oppfylt. Sykehuset Østfold HF har dermed ikke overholdt prinsippet om lagringsbegrensning.

Datatilsynets vurdering:
Sykehuset Østfold HF har lagret rapportuttrekk fra EPJ fra 2013-2019 lenge etter at formålet med behandlingen av opplysningene var oppnådd og behovet for lagring av opplysningene opphørte. Dette er et brudd på personvernforordningen artikkel 32, jf. artikkel 24 og 5 nr. 1 bokstav e, og pasientjournalloven § 23.

4.5 Innebygd personvern og personvern som standardinnstilling

Sykehuset Østfold HF plikter som behandlingsansvarlig å ha programmer, systemer og/eller løsninger som har innebygd personvern og personvern som standardinnstilling. Vi kan ikke se at det har vært fokus på innebygd personvern i sykehusets prosjekt for å ivareta personvernregelverket eller i andre beskrevne tiltak.

Datatilsynets vurdering:
Løsningen for rapportuttrekk fra EPJ var ikke i samsvar med kravene til innebygd personvern/personvern som standardinnstilling i personvernforordningen artikkel 25, jf. artikkel 32 og 24.

4.6 Behandlingsprotokoll

Rapportuttrekkene fra EPJ ble ikke integrert i protokollene ved Sykehuset Østfold HF før i 2018. Sykehuset Østfold HF angir at det alltid gjøres sikkerhetsvurderinger av nye eller endrede behandlinger. Datatilsynet stiller seg tvilende til om protokollføringen gjort i juni 2018 var komplett. Etter vår vurdering skulle dette ha medført at det ble avdekket et behov for sikkerhetstiltak for løsningen – som for eksempel tilgangskontroll, logging og sletting av personopplysningene i uttrekkene.

Datatilsynets vurdering:
Kravet til protokoll i personvernforordningen artikkel 30 er ikke overholdt i forbindelse med rapportuttrekkene fra EPJ.

4.7 Iverksatte tiltak

Sykehuset Østfold HF iverksatte strakstiltak etter at avviket ble oppdaget. Det er også iverksatt langsiktige tiltak som tyder på at sykehuset har forstått alvorligheten i avviket.

Sykehuset Østfold HF må forsikre seg om at tiltakene har ønsket effekt og at sykehuset har tilfredsstillende sikkerhetsnivå. Vi viser til punkt 4.3 *Internt styringssystem* over.

Datatilsynets vurdering:
Datatilsynet har ingen merknader til de iverksatte strakstiltakene.

Vi mener likevel at Sykehuset Østfold HF ikke har etablert tilstrekkelig styring når det gjelder behandling av personopplysninger, herunder for tilgangskontroll og lagringsrutiner, jf. personvernforordningen artikkel 32, jf. artikkel 24, og pasientjournalloven § 23.

4.8 Informasjon til de registrerte

De berørte pasientene har ikke blitt informert om lagringen av og tilgangskontrollen til rapportuttrekkene med til dels svært sensitive opplysninger om dem.

Sykehuset Østfold HF mener at avviket ikke omfatter tap eller spredning av personopplysninger, og det er ikke avdekket at personopplysningene er brukt til andre formål.

Pasienter har en berettiget forventning om konfidensialitet når de behandles ved et sykehus. De forventer at kun helsepersonell med tjenstlig behov skal ha tilgang til opplysninger om seg og sin helsetilstand.

At de ansatte har taushetsplikt, er ikke relevant for vurderingen av hvilke opplysninger en ansatt skal ha tilgang til. Taushetsplikten kan likevel begrense skadevirkningene av urettmessig tilgang til personopplysninger. I taushetsplikten ligger det en forutsetning om at helsepersonell ikke skal spre taushetsbelagt pasientinformasjon.

Etter personvernforordningen artikkel 34 utløses plikten til å underrette de berørte personene dersom sikkerhetsbruddet medfører «høy risiko» for fysiske personers rettigheter og friheter.

I denne saken har opplysningene vært tilgjengelige for samtlige ansatte. Det er umulig å ettergå om ansatte faktisk har gjort innsyn eller på annen måte har behandlet opplysningene, og i tilfelle hvor mange. Risikoen for de registrerte kan sies å være høy dersom opplysninger ligger åpent tilgjengelige for alle ansatte ved et sykehus, der flesteparten av de ansatte ikke vil ha tjenstlig behov for opplysningene.

Samlet sett har vi derfor kommet til at Sykehuset Østfold HF plikter å informere de berørte pasientene.

Ettersom det er tale om flere tusen pasienter, der enkelte kanskje er avdøde, mener vi likevel at informasjonen til pasientene kan være felles og ikke individuell. Informasjonen kan for eksempel gjøres tilgjengelig via sykehusets internettside (eller i en annen egnet og offentlig tilgjengelig kanal). Vi gjør oppmerksom på at informasjonen må være utformet på en måte som gjør det mulig for pasienter å forstå omfanget av og innholdet i sikkerhetsbruddet. Vi mener også at det bør informeres om Datatilsynets vedtak i saken.

<u>Datatilsynets vurdering:</u>
Sykehuset Østfold HF plikter å underrette de registrerte som er berørt av avviket, jf. personvernforordningen artikkel 34.

4.9 Oppsummering

Pasientopplysninger skal ikke lagres slik at ansatte uten tjenstlig behov har tilgang til dem. Ved Sykehuset Østfold HF har pasientopplysninger i form av rapportuttrekk fra EPJ vært lagret på en server og i en mappestruktur uten tilgangskontroll.

Ettersom helsepersonells primærformål er helsehjelp, må sykehuset ha etablert et teknisk støttesystem som ivaretar kravene personvern og informasjonssikkerhet. Sykehuset må også legge til rette for at kun sikre systemer brukes i håndteringen av sensitive opplysninger. Slik kan helsepersonells taushetsplikt og informasjonssikkerheten rundt pasientopplysninger ivaretas i hele behandlingskjeden. Det er et ledelsesansvar at slike tekniske løsninger er etablerte og fungerer som forutsatt.

Vi mener det har vært grunnleggende mangler ved det interne styringssystemet og informasjonssikkerheten ved behandlingen av rapportuttrekkene ved Sykehuset Østfold HF.

4.10 Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har kommet til at Sykehuset Østfold HF har brutt personvernforordningen artikkel 32, jf. 24 og pasientjournalloven §§ 22 og 23.

Lovbruddet har for en stor del skjedd før personopplysningsloven (2018) og personvernforordningen trådte i kraft. Datatilsynet kunne også tidligere ilegge overtredelsesgebyr, jf. personopplysningsloven (2000) § 46, men beløpet var da begrenset til inntil 10 ganger folketrygdens grunnbeløp (p.t. ca. 1 000 000 NOK).

Vi viser imidlertid til drøftelsen under punkt 3.1 og legger til grunn at gebyret skal utmåles etter nytt regelverk. I utgangspunktet er det dermed grunnlag for å ilegge Sykehuset Østfold HF et overtredelsesgebyr på inntil 10 000 000 euro (p.t. ca. 107 000 000 NOK), jf. forordningen artikkel 83 nr. 4. Vi vil likevel se hen til at lovbruddene har skjedd også i perioden da tidligere personvernregelverk gjaldt.

Under gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges.

a) *karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd*

Avviket knyttet til rapportuttrekkene har pågått gjennom ca. seks år, og helseopplysninger om tusenvis av pasienter har ligget tilgjengelig for alle ansatte. Selv om det ikke finnes dokumentasjon på at ansatte har gjort urettmessig innsyn i rapportuttrekkene, er det ikke mulig å ettergå om slikt innsyn har skjedd og om pasientopplysninger har kommet på avveie.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Sykehuset Østfold HF har gjennomført risikovurderinger knyttet til informasjonssikkerhet og har rutiner for tilgangsstyring. Lagringen av rapportuttrekk med helseopplysninger uten tilgangsstyring har likevel ikke kommet frem gjennom ledelsens oppfølging i årene 2013 – 2019. Lovbruddet må betegnes som uaktsomt.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd
Sykehuset Østfold HF har nå sørget for skjerming eller sletting av rapportuttrekkene.

d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32
Sykehuset Østfold HF har hatt et styringssystem som blant annet omfatter tilgangsstyring til taushetsbelagte opplysninger. Styringssystemet har likevel ikke vært egnet til å fange opp lagringen av rapportuttrekkene i mapper uten tilgangsstyring. Datatilsynet mener at dette gir uttrykk for mangler ved det interne styringssystemet.

g) kategoriene av personopplysninger som er berørt av overtredelsen
I denne saken har helseopplysninger vært tilgjengelige for et stort antall ansatte. Etter personvernforordningen artikkel 9 nr. 1 er helseopplysninger betegnet som en særlig kategori personopplysninger, det vil si svært sensitive opplysninger. Dette øker alvorlighetsgraden av lovbruddet.

h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen
Sykehuset Østfold HF meldte selv fra om avviket til Datatilsynet.

4.11 Utmåling av gebyret
I vurderingen av gebyrets størrelse, har vi sett hen til at Sykehuset Østfold HF raskt sørget for sletting eller skjerming av rapportuttrekkene og at sykehuset selv meldte avviket til Datatilsynet. Det er heller ikke kjent at praksisen har fått konkrete konsekvenser for enkeltpasienter, selv om dette tillegges mindre vekt.

Vi har vektlagt at lovbruddet dels har funnet sted før personopplysningsloven (2018) og personvernforordningen trådte i kraft. Etter tidligere gjeldende personopplysningslov (2000) var gebyret avgrenset til maksimalt ca. 1 000 000 NOK.

I denne saken har en større mengde helseopplysninger har ligget tilgjengelig for alle sykehusets ansatte gjennom flere år.

I tillegg mener vi at avviket illustrerer mangler ved Sykehuset Østfold HFs styringssystem når det gjelder intern tilgangsstyring.

Datatilsynet har kommet til at et overtredelsesgebyr på 1 000 000 NOK er rimelig i denne saken.

4.12 Vurdering av om pålegg skal gis
Sykehuset Østfold HF har ikke hatt tilstrekkelig god styring med de ansattes tilgang til rapportuttrekk med sensitive personopplysninger i årene 2013 – 2019. Mappene der

rapportuttrekkene var lagret var ikke tilgangsstyrte, og aktiviteten i mappene ble ikke logget. Rapportuttrekkene har også blitt lagret lenge etter at det ikke lenger var behov for listene.

At en slik utstrakt lagring av uskjermede helseopplysninger kunne skje over lang tid, mener vi tyder på mangler ved det interne styringssystemet.

Vi har derfor funnet grunnlag for å pålegge Sykehuset Østfold HF å tilse at styringssystemet for behandling av personopplysninger er egnet til å ivareta kravene i personvernregelverket og pasientjournalloven.

Pålegg:
Datatilsynet mener at Sykehuset Østfold HF ikke har etablert et system for tilgangsstyring som er tilstrekkelig for å forhindre at lignende avvik vil skje i fremtiden. Vi finner det derfor nødvendig å ilegge Sykehuset Østfold HF pålegg om å tilse at styringssystemet for behandling av personopplysninger er egnet til å ivareta kravene i personvernregelverket og pasientjournalloven. Vi viser særlig til rutinene for tilgangskontroll og lagring av personopplysninger. Styringssystemet må innebære oppfølging av at rutinene følges, herunder oppfølging av at kun sikre systemer brukes ved behandling av sensitive personopplysninger. Vi viser til personvernforordningen artikkel 32, jf. artikkel 24, og pasientjournalloven § 23.

5. Videre fremdrift
Dette brevet er å anse som et forhåndsvarsel om vedtak om pålegg og overtredelsesgebyr, jf. forvaltningsloven § 16.

Dersom dere har kommentarer til dette varselet, ber vi om at dere sender oss en tilbakemelding om dette så snart som mulig og senest **innen 05.08.2020**.

6. Innsyn og offentlighet
Alle dokumentene i saken er i utgangspunktet offentlige, jf. offentlighetsloven § 3. Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentene fra offentlig innsyn, ber vi dere om å begrunne dette.

Hvis dere har spørsmål, kan dere ta kontakt med Veronica Jarnskjold Buer på telefon 22 39 69 53 eller Susanne Lie på telefon 22 39 69 57.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør

Susanne Lie
seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: SYKEHUSET ØSTFOLD HF, Kirsten Wøien Fredriksen, Postboks 300, 1714 GRÅLUM