SYKEHUSET I VESTFOLD

Informasjonssikkerhet - Anonymisering av helse- og personopplysninger

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	10.09.2019

1. HENSIKT

Formålet med denne instruksen er å etablere et felles sett med forutsetninger for at helse- og personopplysninger skal kunne lagres utenfor risikovurderte og sikrede lagringsområder. Instruksen omfatter:

- Krav som i sin helhet må oppfylles, for at opplysninger kan oppfattes som anonyme
- Krav til utstyr hvor opplysningene skal lagres
- Krav som stilles leder (inklusive opplæring) som gis ansvar for å utlevere anonymiserte opplysninger til andre formål enn kildesystemets formål.

2. ANSVAR

Enhver leder er ansvarlig for å informere om denne instruks og gjøre den tilgjengelig for sine medarbeidere, og spesielt forskningsleder i klinikk, veiledere, stipendiater og andre som er involvert i behandling av helse- og personopplysninger.
Instruksen gir prinsippene for anonymisering. Den enkelte er selv ansvarlig for å gjøre seg kjent med og følge reglene i denne instruks.

3. FREMGANGSMÅTE

Opplysningene skal ikke samlet kunne gi identiteten til den enkelte registrerte. Først når man er sikker på at opplysningene ikke kan knyttes til 5 eller færre personer, kan opplysningene vurderes som anonyme. Sjeldne diagnoser, kombinert med alder, kjønn og bosted vil kunne gi identiteten til enkelte, selv i større byer, og dermed vil sannsynligheten for å ende i en gruppe på 5 eller færre være høyst reell. Det må derfor gjøres en vurdering i hvert enkelt tilfelle.
Data som inneholder koder med koblingsmulighet til en separat kodeliste der identitet på pasienten gjenfinnes, er ikke anonyme. Selv om man fjerner personidentifiserende opplysninger som navn og fødselsnummer fra dataene, eller sletter kodeliste/koblingsnøkkel, så vil dette ofte være utilstrekkelig til at opplysninger kan sies å være anonyme.

Informasjon som alltid må fjernes.

Selv om man fjerner personidentifiserende opplysninger som navn og fødselsnummer fra opplysningene, eller sletter kodelisten, så vil ofte dette ikke være nok.

- Adresse
- Telefonnummer
- Faksnummer
- NPR-ID / DIPS-ID / pasientnummer
- DIPS-ID / pasientnummer
- Kontonummer
- Sertifikatnummer
- Registreringsnummer på bil
- Link til personlige sider på nettet (f.eks. blogg)
- E-postadresser
- Biometriske kjennetegn

Eksempler på informasjon som må vurderes fjernet er:

- Fødselsdato
- initialer
- Postnummer
- Innleggelses- og utskrivningsdato
- Bilder
- Lyd
- Video

Opplysningene skal ikke samlet kunne gi identiteten til den enkelte registrerte. Først når man er sikker på at opplysningene ikke kan knyttes til færre enn 5 personer, kan opplysningene vurderes som anonyme. Hvis man for eksempel har en svært sjelden diagnose, eller bor på et lite sted, vil kanskje opplysningene kunne tilbakeføres til en slik gruppe. Det må derfor gjøres en vurdering i hvert enkelt tilfelle.
Vær oppmerksom på at data som inneholder koder med koblingsmulighet til en separat kodeliste der identitet på pasienten gjenfinnes, ikke er anonyme.

Lyd og bilde
Vær oppmerksom på at stemmer på lyd- og billedopptak aldri regnes som anonyme. Ved anonymisering av bilder og videoer må det også gjøres en egen vurdering av om særtrekk ved den avbildede vil være gjenkjennbar for andre. Ved bruk av bilder av personer som ikke har samtykket til at bildet videreformidles, er det et krav at den avbildede ikke skal kunne gjenkjenne seg selv. Eksempelvis tatoveringer eller andre ytre særtrekk ved den avbildede må ikke vises.

4. GENERELT

5. INTERNE REFERANSER

1.1.11.2.12	Informasjonssikkerhet - Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

6. EKSTERNE REFERANSER

Oslo universitetssykehus (OUS) - Hva er forskjellen på avidentifisert og anonymt?

7. VEDLEGG