HELSE SØR-ØST

Anonymisering av helse- og personopplysninger

Versjonsnummer	**Dato**	**Godkjent av**
1.0	22.12.2016	
1.1	23.10.2018	

1 Hensikt og omfang

Angi kort hensikten med å styre aktiviteten som beskrives i dokumentet. Beskrivelsen kan ikke være et mål i seg selv. Evt. med beskrivelse av målgruppe, omfang og avgrensning. Normalt vil 1-2 setninger være tilstrekkelig.

Anonymisering er å gjøre personopplysninger anonyme. For at opplysning skal kunne anses anonymisert må identifiserende faktorer må fjernes eller bearbeides slik at det i praksis skal være umulig å gjøre en tilknytning mellom informasjon og individ. Flere teknikker kan brukes for å nå målet om å gjøre opplysninger anonyme.

Formålet med denne instruksen er å etablere et felles sett med forutsetninger for å anonymisere helse- og personopplysninger, slik at de 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.

Instruksen er en del av virksomhetens internkontrollsystem, slik som beskrevet i helseregisterloven (hlsregl) og personopplysningsloven (popplyl).

2 Ansvar

Kort om ansvar (ikke oppgaver) som vesentlige stillinger/roller har for de aktivitetene som beskrives. En setning pr. rolle. Ikke beskriv ansvar for dokumentet.

- 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

Klar og konsis beskrivelse av ramme, aktivitet eller prosess. Ansvar for aktivitet kan angis samtidig (2 kolonner). Kan være nødvendig med flere avsnitt med egen overskrifter.

Opplysningene skal samlet ikke 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.

For mer inngående veiledning om hva anonymisering innebærer og fremgangsmåte ved anonymisering vises det til Datatilsynets veileder for anonymisering, se lenke/referanse nederst i dokumentet.

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.

3.1 Informasjon som alltid må fjernes

- 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

3.2 Informasjon som må vurderes fjernet

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

3.3 Lyd og bilde

Stemmer på lyd- og billedopptak regnes aldri 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 Definisjoner

Ordinært gis forklaring på fag- og fremmedord i teksten. Dette feltet benyttes når det er helt nødvendig med egen definisjonsliste for ord som ikke er allment kjent.

Se dokumentet Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

- Personopplysninger er i artikkel 4 i EUs personvernforordning definert som « enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator, eller et eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske genetiske, psykiske, økonomiske, kulturelle eller sosial identitet» Indirekte identifiserbare personopplysninger (også kalt avidentifiserte opplysninger) er lovregulerte opplysninger med krav til sikring og kontroll. Behandling av slike opplysninger er omfattet av de samme kravene til samtykke eller annet lovlig grunnlag som gjelder for opplysninger med navn og fødselsnummer.

- Anonymisering innebærer at enhver mulighet til å identifisere enkeltindivider i dataene er fjernet. Det skal være umulig å knytte opplysningene tilbake til individet for å kunne si at noe er anonymt. Opplysninger som kan klassifiseres som anonyme, har ingen lovregulering og ingen juridiske krav til samtykke eller formålsavgrensning.

- Anonymisering gir mulighet for å dele data med andre som ellers ikke lovlig ville kunne mottatt dem. Det gir også muligheten for å oppbevare data videre selv om godkjent varighet er utløpt.

5 Avvik eller dissens

Dette feltet benyttes kun hvis det er helt spesielle forhold knyttet til avvik eller dissens. Melding av avvik bør være en selvfølge som det er ikke er nødvendige å skrive noe om.

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

6 Referanser

Sikkerhetsregulerende lovverk gjeldende for helseforetaksgruppen

Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet