SYKEHUSET I VESTFOLD

Informasjonssikkerhet - Lagring, arkivering og sletting av helse- og personopplysninger

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	30.09.2020

1. HENSIKT

Hensikten med prosedyren er at lagring, arkivering og sletting av helse- og personopplysninger ved helseforetaket, gjøres i samsvar med gjeldende krav til informasjonssikkerhet og med gyldig behandlingsgrunnlag.

2. ANSVAR

Administrerende direktør: Er databehandlingsansvarlig og har ansvaret for at lagring og forvaltning av person- og helseopplysninger gjøres med nødvendig sikkerhet og kun i samsvar med gyldig behandlingsgrunnlag.
Informasjonssikkerhetsleder: Har det utøvende ansvar for virksomhetens informasjonssikkerhetsarbeid, blant annet ved å godkjenne risikovurderinger og utføre internkontroll med informasjonssikkerheten i virksomheten.
Personvernombudet: Har en rolle i å sikre at den enkeltes personvernrettigheter blir ivaretatt, at all bruk av personopplysninger skjer i samsvar med gyldig behandlingsgrunnlag og følger virksomhetens retningslinjer for informasjonssikkerhet.
Ledere innen ulike enheter og områder har ansvar for å påse at denne prosedyre implementeres og etterleves innen eget ansvarsområde. Det vil si at dokumentet er kjent, tilgjengelig og blir brukt.
Alle ansatte ved sykehuset som skal lagre og behandle helse- og personopplysninger, skal forholde seg til denne prosedyre. Dette gjelder uavhengig av organisatorisk plassering og yrkesgruppe.

3. FREMGANGSMÅTE

Lagring av helse- og personopplysninger vil kunne kreve ressurser, både direkte økonomiske og med hensyn til lagring. Dette fordi det er krav til sikring av disse opplysninger. Kravet til sikring gjelder også om navn og andre direkte kjennetegn er erstattet med en kode, eller dataene på andre måter er indirekte identifiserbare, da disse opplysninger er regulert av samme lovverket som om opplysningene skulle være identifiserbare.

Det er videre viktig at måte og sted for lagring, oppgis i melding til personvernombud. Ved senere behov for annen lagringsplass, må dette først meldes personvernombudet før slik lagring kan gjøres.
Eventuelle kopier av datasett skal også oppgis i meldingen til personvernombudet.

Håndtering av lagring deles i det videre opp i elektronisk lagring og papirmessig lagring.

Elektronisk lagring og forvaltning

Elektronisk lagring og forvaltning omfatter følgende hovedfokus:

- Elektronisk lagring av helse- og personopplysninger
- Lagring av innsamlede helse- og personopplysninger hos eksterne
- Arkivering av innsamlede helse- og personopplysninger
- Sletting av innsamlede helse- og personopplysninger

Elektronisk lagring av person- og helseopplysninger
For å kunne lagre helse- og personopplysninger, må det være både gyldig behandlingsgrunnlag, som er registrert i sykehuset, og sikkerhetsmessig godkjent lagringsområde eller fagapplikasjon.

Lagring av helse- og personopplysninger i alle typer forskningsstudier, kvalitetsregistre, tematiske registre og interne kvalitetsregistre kan først gjøres etter at databehandlingen er godkjent. Godkjenningen omfatter formell godkjenning fra enten REK, Personvernombudet (evt. Datatilsynet, personvernombudet sender melding), Statens legemiddelverk med flere, som gir formelt behandlingsgrunnlag for databehandlingen, samt intern forankring i klinikk. Videre må lagring av opplysningene være i samsvar med det som er meldt på meldeskjema og som godkjenningen baseres på.

For lagring av helse- og personopplysninger i fagsystemer (tilsvarende DIPS, Sak/Arkiv, medisinsk tekniske systemer mfl.) skal dette risikovurderes etter egen prosedyre Informasjonssikkerhet - Risikovurdering ved nye og endrede IKT-behov og databehandlinger

Godkjente lagringsområder vil være etablerte risikovurderte fagsystemer, foretaksspesifikke filområder og godkjente eksterne tilbydere som listet under.

Det er etablert standardiserte lagringsområder i helseforetaket. Disse områder er sikkerhetsmessig risikovurdert, og kan bestilles av prosjektleder i samsvar med det som er meldt i meldeskjemaet.

I sykehusets nettverk

- O:\Sensitivt\Forskning01 - 02
  - her skal alle prosjektregistre for forskningsstudier lagres, uavhengig av hvem som formelt godkjenner studien
- O:\Sensitivt\Kvalitetsregistre01
  - her skal alle interne kvalitetsregistre lagres, helsepersonelloven §26, jf pasientjournalloven § 6, lagres
- O:\Sensitivt\Klinikk01
  - her skal eventuelle kliniske spesialistmoduler/registre lagres
- Medinsight
  - registerstøtteløsning tilgjengelig i hele SiVHF
  - søknad om bruk av løsningen sendes direkte til systemforvalter

Bestilling av lagringsområde på O:\Sensitivt:

- Håndteres i forbindelse med melding til personvernombudet, Forskning og Innovasjon og intern forankring av studie ved sykehuset.
- For andre formål enn de som fremgår av interne melderutiner, benytt skjemaet i Min Sykehuspartner -> Bestille -> Tilganger -> +Forskningsprogram og «Sensitive mapper»

Eksternt
- Sikker lagring etablert av Usit (Tjenester for Sensitive Data (TSD 2.0) - hovedside med intro: http://www.uio.no/tjenester/it/forskning/sensitiv/)
  - Krever utfylling av databehandleravtale som USIT sørger for. Kopi av signert avtale sendes til pvo@siv.no.

Dersom standard lagringsområder ikke kan brukes, eller andre lagringsområder ønskes i tillegg, må det gjennomføres en egen risikovurdering av informasjonssikkerheten ved annet lagringsområde/metode. Informasjonssikkerhetsleder vurderer og eventuelt godkjenner annet lagringsområde, se egen prosedyre Informasjonssikkerhet - Risikovurdering ved nye og endrede IKT-behov og databehandlinger. Dette omfatter alle

andre lagringsområder enn de som er angitt som standard, inkludert ved behov for lagring hos annen juridisk enhet.

Kodenøkler for avidentifiserte data, for små serier kan lagres på papir som sikres mot uvedkommende tilgang ved nedlåsing, men for store serier anbefales det å oppbevare kodenøkler elektronisk på en type kryptert minnepenn som er godkjent av informasjonssikkerhetsleder. Andre måter må eventuelt avtales med informasjonssikkerhetsleder.

Alle lagringsområder, inkludert for kodenøkler, skal være i samsvar med det som er meldt til personvernombudet. Nye behov for lagring, skal først meldes personvernombudet før de tas i bruk.

Følgende lagringsområder kan *ikke* benyttes for lagring av helse- og personopplysninger (listen er ikke uttømmende):

- ordinære avdelingsvis fellesområder i sykehusnettet
- ordinære personlige områder i sykehusnettet
- privat eid utstyr
- ordinært universitets/høyskolenett eller andre tilsvarende nettverk i utdanningsvirksomheter

Lagring hos eksterne
All lagring av personopplysninger utenfor foretakets nettverk/utstyr krever gjennomført risikovurdering, som må godkjennes av foretakets informasjonssikkerhetsleder, før lagring kan gjøres. All lagring utenfor foretakets nettverk/utstyr krever også inngått databehandleravtale før slik lagring kan gjøres. Databehandleravtale signeres etter avklaring med informasjonssikkerhetsleder.

Arkivering av personopplysninger
Dersom personopplysninger skal lagres etter avslutning av prosjekt, må følgende være oppfylt:

- Godkjenning av prosjektet må omfatte tiden for arkivering, eller slik forlengelse for arkivering må søkes og godkjennes.
- Prosjektleder, medarbeidere, ledere m.fl. skal ikke ha tilgang til dataen i arkiveringsperioden.

Sletting av person- og helseopplysninger
Ved prosjektavslutning eller etter endt arkivering, dersom aktuelt, slettes alle person- og helseopplysninger.

For spørsmål rundt sletting og/eller anonymisering, kan man ta kontakt med personvernombudet for rådgivning.

Papirmessig lagring og forvaltning
Lagring av helse- og personopplysninger i papirform, skal som hovedregel også lagres indirekte identifisert, så sant ikke annet er avtalt med personvernombudet. Dette fordi samtidig tilgang til kodenøkkel og kodede opplysninger skal være vanskeliggjort. Kodenøkkel og kliniske opplysninger må derfor lagres fysisk adskilt, enten i ulike avlåste rom eller arkivskap med begrenset tilgang. Signerte samtykker skal lagres sammen med kodenøkkel.

Når opplysningene er i bruk, og det er behov for samtidig tilgang til kodenøkkel og registreringsskjema (CRF), kan kravet til indirekte identifisering fravikes. Dette gjelder typisk under registrering eller monitorering, når hensynet til opplysningenes kvalitet og integritet er avgjørende.

Når opplysningene ikke lenger brukes på denne måten, og arkiveres, gjelder krav til indirekte identifisering ved å adskille kodeliste og kliniske opplysninger.

Makulering av helse- og personopplysninger skal skje ved å kaste papirene i avlåste beholdere for makulering av sensitive opplysninger eller ved bruk av makulatorer.

Avvik eller dissens
Lagring og behandling av helse- og personopplysninger uten tilstrekkelig informasjonssikkerhet og gyldig behandlingsgrunnlag, er avvik og skal meldes i foretakets avvikssystem samt til nærmeste overordnende.

4. GENERELT

5. INTERNE REFERANSER

1.1.11.2.9	Informasjonssikkerhet - Risikovurdering ved nye og endrede IKT-behov og databehandlinger
1.1.11.2.12	Informasjonssikkerhet - Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

6. EKSTERNE REFERANSER

- Lov 2014-06-20 nr. 43: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) (https://lovdata.no/dokument/NL/lov/2014-06-20-43)
- Lov 2014-06-20 nr. 42: Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) (https://lovdata.no/dokument/NL/lov/2014-06-20-42)
- Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) med tilhørende forskrift (http://www.lovdata.no/all/nl-20000414-031.html)
- Lov 1999-07-02 nr. 64: Lov om helsepersonell m.v. (helsepersonelloven) (http://www.lovdata.no/all/hl-19990702-064.html)
- Lov 1999-07-02 nr. 63: Lov om pasientrettigheter (pasientrettighetsloven) (http://www.lovdata.no/all/hl-19990702-063.html

7. VEDLEGG