SYKEHUSET I VESTFOLD

Policy - Behandling av personopplysninger i sykehuset

Gjelder for:	Hele SiV
Dokumenttype:	Retningslinje
Sist endret:	06.05.2024

Innholdsfortegnelse

1. HENSIKT

Denne retningslinjen

- definerer rammer og føringer for Sykehuset i Vestfold (sykehuset) sin behandling av personopplysninger. Som sykehus behandler vi store mengder personopplysninger. Vi erkjenner viktigheten av å sikre personvernet til våre pasienter, ansatte og besøkende.
- beskriver prinsippene og kravene som vi følger for å sikre at personopplysninger blir behandlet på en trygg og pålitelig måte.
- gjelder for alle informasjonssystemer og prosesser som omfattes av ledelsessystemet for informasjonssikkerhet, og hvor det behandles personopplysninger.

Hensikten med retningslinjen er:
- sikre at alle personopplysninger blir behandlet i samsvar med personvernregelverket[1]
- beskytte personopplysningene til pasienter, ansatte og besøkende.
- redusere risikoen for at personopplysninger kommer på avveie, misbrukes eller feilbehandles.

Det utarbeides prosedyrer som detaljerer arbeidet med behandling av personopplysninger.

Definisjoner – se pkt. 4 nedenfor.

2. ANSVAR

Hvem	Ansvar
Ledere på alle nivåer	- Gjøre retningslinjen kjent for alle sine ansatte - Følge opp at de ansatte etterlever kravene i denne retningslinjen
Alle ansatte uansett arbeidsforhold (ansatte)	- Følge denne retningslinjen

3. FREMGANGSMÅTE

3.1 Prinsipper for behandling av personopplysninger

Alle behandlinger skal følge de grunnleggende behandlingsprinsippene som står i personvernforordningen (pvf) art. 5. Prinsippene er likeverdige.

- Lovlighet, rettferdighet og åpenhet. Sykehuset skal behandle personopplysninger på en lovlig, rettferdig og gjennomsiktig måte. Det innebærer blant annet å sikre at alle behandlinger har et rettslig grunnlag, og at de registrerte informeres om behandlingen av deres personopplysninger.
- Formålsbegrensning. Sykehuset skal bare behandle personopplysninger som er nødvendig for å oppnå spesifikke og legitime formål.
- Dataminimering. Sykehuset skal ikke behandle mer personopplysninger enn det som er nødvendig for å nå formålene.
- Riktighet. Sykehuset skal sørge for at personopplysninger som behandles er nøyaktige og korrekte.

[1] Personvernregelverket: personopplysningsloven, personvernforordningen og relevant særlovgivning

- Lagringsbegrensning. Sykehuset skal bare lagre personopplysninger til formålene er oppnådd. Etter at formålene er oppnådd, så skal opplysningene enten slettes eller anonymiseres.
- Konfidensialitet og integritet. Sykehuset skal sørge for at alle behandlinger har tilstrekkelig informasjonssikkerhet.

Det er sykehuset (dataansvarlig) som er ansvarlig for behandlingen av alle personopplysninger, selv når de utføres av leverandører (databehandlere).

3.2 Oversikt over alle behandlinger (behandlingsprotokoll).

Sykehuset skal ha en oppdatert og komplett oversikt over alle behandlinger. Alle systemer som inneholder personopplysninger, skal føres opp i oversikten. skal danne grunnlag for å prioritere og gjennomføre tiltak, for eksempel risikovurderinger.

3.3 Behandlingens rettslige grunnlag

Alle behandlinger skal ha gyldige rettslige grunnlag (behandlingsgrunnlag).

Det finnes seks behandlingsgrunnlag for behandling av personopplysninger av alminnelig kategori (pvf art. 6):

- Samtykke. Bør unngås, men kan benyttes for eksempel i forbindelse med arrangementer og utsendelse av nyhetsbrev.
- Oppfylle en avtale (eks. arbeidsavtale).
- Nødvendig for å oppfylle en rettslig forpliktelse (eks. forsvarlig helsehjelp)
- Nødvendig for å beskytte vitale interesser.
- Nødvendig for å utføre en oppgave i offentlig interesse eller utøve offentlig myndighet.
- Nødvendig for å ivareta legitime interesser (interesseavveining).

Behandling av særlig kategori personopplysninger (sensitive) er i utgangspunktet forbudt (pvf. art. 9). Det finnes mange unntak fra forbudet Det kreves da et særskilt grunnlag i tillegg til behandlingsgrunnlag etter art. 6. Særskilt grunnlag kan være:

- Den registrerte har gitt uttrykkelig samtykke.
- Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle og utøve sine arbeidsrettslige, trygderettslige og sosialrettslige plikter og rettigheter i den grad behandlingen er tillatt etter lov eller tariffavtale.
- Behandlingen er nødvendig for å verne den registrertes eller en annen persons vitale interesser hvis den registrerte ikke er i stand til å gi samtykke.
- Behandlingen utføres av en stiftelse, sammenslutning eller ideelt organ som har mål av politisk, religiøs eller fagforeningsmessig art, så lenge det er snakk om personopplysninger om medlemmer og liknende, det foreligger nødvendige garantier og opplysningene ikke utleveres uten samtykke.
- Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort.
- Behandlingen er nødvendig i forbindelse med rettskrav eller domstolene handler innenfor rammen av sin domsmyndighet.
- Behandlingen er nødvendig av hensyn til viktige allmenne interesser og har hjemmel i lov.
- Behandlingen er nødvendig i forbindelse med forebyggende medisin, medisin i arbeidslivet, vurdering av en arbeidstakers arbeidskapasitet, medisinsk diagnostikk, ytelse av helse- eller sosialtjenester, sosialfaglig eller medisinsk behandling eller forvaltning av helse- eller sosialtjenester og -systemer. Dette gjelder imidlertid bare dersom opplysningene behandles av en fagperson underlagt taushetsplikt, og behandlingen av personopplysninger må ha hjemmel i lov eller følge av avtale med helsepersonell.
- Behandlingen er nødvendig av allmenne folkehelsehensyn.

- Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål, på visse betingelser og under forutsetning av at behandlingen har hjemmel i lov.

Der forordningen sier at en behandling av personopplysninger krever hjemmel i lov, stiller den også visse krav til loven eller ting loven skal inneholde. Det vil si at en hvilken som helst lovhjemmel i seg selv ikke nødvendigvis er tilstrekkelig.

I tillegg sier personopplysningsloven §§ 6, 7 og 9 at særlige kategorier av personopplysninger kan behandles:

- når det er nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter
- dersom Datatilsynet har gitt tillatelse til det og har fastsatt vilkår for å verne den registrertes grunnleggende rettigheter og interesser
- dersom behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål. Dette gjelder så lenge samfunnets interesse i at behandlingen finner sted klart overstiger ulempene for den enkelte. Det må også foreligge visse tiltak og man må ha rådført seg med personvernombudet.

Sykehuset må vurdere hvilket rettslig grunnlag som er rett å bruke for de enkelte behandlingene, da de registrertes rettigheter er avhengig av de rettslige grunnlagene. Merk også at flere rettslige grunnlag krever supplerende rettslige grunnlag.

3.4 Personopplysningssikkerhet

De generelle kravene til informasjonssikkerhet omfatter konfidensialitet, integritet og tilgjengelighet og robusthet. Dette gjelder også for personopplysninger. Sykehuset skal derfor sørge for å gjennomføre tekniske og organisatoriske egnede tiltak for å oppnå et akseptabelt sikkerhetsnivå.

Så langt det er mulig og hensiktsmessig skal personopplysninger:

- Pseudonymiseres eller krypteres.
- Sikres vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet.
- Sikres slik at tilgjengelighet kan bli gjenopprettet etter en fysisk eller teknisk hendelse.

Det skal gjennomføres regelmessige tester, analyser og vurderinger av sikkerhet ved behandling av personopplysninger. Risikovurderinger skal gjøres med utgangspunkt i de registrertes perspektiv.

3.5 Brudd på personopplysningssikkerheten

Brudd på personopplysningssikkerheten skal meldes i læringssystemet (EQS).

Ved brudd på personopplysningssikkerheten, skal sykehuset uten ugrunnet opphold, og senest innen 72 timer, melde bruddet til Datatilsynet. Tidsfristen gjelder også selv om det ikke foreligger full oversikt over hendelsen. Forutsetningen er at bruddet medfører risiko for de registrertes rettigheter og friheter.

Dersom det er sannsynlig at bruddet medfører høy risiko for de registrertes rettigheter og friheter, så skal de registrerte også informeres uten ugrunnet opphold.

Brudd som følge av feil / uønsket hendelse på informasjonssystemer skal varsles til Statens helsetilsyn:

- ved dødsfall eller svært alvorlig skade på pasient eller bruker
- som følge av ytelse av helse- og omsorgstjenester
- når utfallet er uventet ut fra påregnelig risiko

3.6 Innebygd personvern
Sykehuset skal sikre at alle systemer og tjenester har innebygd personvern og personvern som standardinnstilling. Det innebærer at det skal stilles krav til innbygd personvern i forbindelse med anskaffelse eller utvikling av systemer som skal behandle personopplysninger, og at systemene blir satt opp på en personvernvennlig måte.

3.7 Bruk av databehandlere
Alle databehandlere skal reguleres med databehandleravtale. Databehandleravtalene skal inneholde relevante sikkerhetskrav. Databehandlere skal kontrolleres og revideres etter behov.

3.8 De registrertes rettigheter
Sykehuset skal legge til rette for at de registrerte kan utøve sine rettigheter:

- Rett til å bli informert. Kommunen skal gi tilstrekkelig informasjon som er kortfattet, åpen, forståelig og lett tilgjengelighet. Kommunen skal også sikre at informasjonen er tilpasset målgruppene.
- Rett til innsyn. Kommunen skal etablere en sikker løsning for innsyn og utlevering. Innsyn bør skje enten gjennom at de får tilgang til fagsystemer, eller gjennom et digitalt skjema. Utlevering bør skje til den registrertes digitale postkasse.
- Rett til korrigering. Krav om korrigering bør skje gjennom et digitalt skjema.
- Rett til sletting. Krav om sletting bør skje gjennom et digitalt skjema.
- Rett til begrensning. Krav om begrensning bør skje gjennom et digitalt skjema.
- Rett til å protestere. Krav om protestering bør skje gjennom et digitalt skjema.
- Rettigheter ved automatiserte avgjørelser.
- Rett til dataportabilitet. Den registrerte har rett til å få utlevert sine personopplysninger i et maskinlesbart og vanlig brukt filformat. Fagsystemene bør ha funksjonalitet for å laste ned personopplysninger, enten via brukergrensesnittet eller via et API.

Merk at enkelte rettigheter er avhengig av hvilket rettslig grunnlag som ligger til grunn for behandlingen.

4. GENERELT

Definisjoner

- En **personopplysning** er enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»). Det kan være opplysninger som navn, adresse, fødselsnummer, IP-adresse, e-postadresse, biometriske opplysninger, helseopplysninger eller andre identifikatorer.
- **Behandling** er enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke.
- **Behandlingsansvarlig** er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Kommunen er i all hovedsak behandlingsansvarlig.
- **Databehandler** er en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige. Leverandørene er i all hovedsak databehandlere.
- **Personopplysningssikkerhet** er informasjonssikkerhet på personopplysninger.
- **Brudd på personopplysningssikkerhet** er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
- **Pseudonymisering** handler om å behandle personopplysninger på en slik måte at opplysningene ikke lengre kan knyttes til en fysisk person uten bruk av tilleggsopplysninger. Tilleggsopplysningene må sikres og lagres atskilt fra de pseudonymiserte opplysningene.

5. INTERNE REFERANSER

1.1.11.1.4	Sikkerhetsinstruks
1.1.11.2.23	Uønsket hendelse - brudd på informasjonssikkerhet

6. EKSTERNE REFERANSER

Normen (Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren)
Personopplysningsloven
Personvernforordningen
Ledelsessystemer for informasjonssikkerhet

- NS-ISO/IEC 27002:2022 5.1 «Policyer for informasjonssikkerhet»
- NS-ISO/IEC 27002:2022 5.34 «Personvern og beskyttelse av PII»

7. VEDLEGG