ENDRINGER FRA FORRIGE VERSJON: Oppdatering av lenker, uten endringer av tekst eller innhold.

HENSIKT

Dette policydokumentet beskriver hvordan informasjonssikkerhet og personvern blir ivaretatt ved Sørlandet sykehus HF (SSHF).

MÅLGRUPPE

Dokumentet gjelder for alle ansatte ved SHHF.

DEFINISJONER

Både informasjonssikkerhet og personvern er underlagt Personvernforordningen (GDPR), se oversikt i dokumentet Sikkerhetsregulerende lovverk gjeldende for foretaksgruppen

.

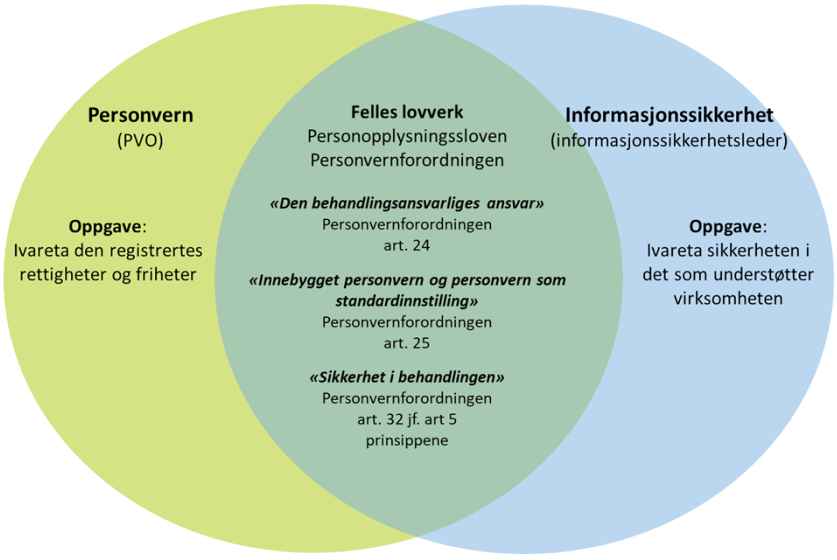
Med *personvern* menes ivaretagelse av den registrertes rettigheter og friheter. Det omfatter ansatte, pasienter og andre som SSHF har registret personopplysninger om. Oppgaven ivaretas av Personvernombudet (PVO) ved SSHF og funksjonen er lovpålagt. Ved brudd på personvernet rapporterer og varsler PVO direkte til Datatilsynet.

- PVO er organisatorisk plassert i Organisasjonsavdelingen

Med *informasjonssikkerhet* menes å sikre all informasjonsbehandling som utføres ved SSHF. Informasjonssikkerhetsleder ved SSHF har det utøvende ansvaret for informasjonssikkerhetsarbeidet i foretaket. Ved brudd på informasjonssikkerhet rapporterer og varsler informasjonssikkerhetsleder til adm. direktør.

- Informasjonssikkerhetsleder er organisatorisk plassert i Avd. for teknologi og innovasjon (ATI), stabsenheten Administrasjon og strategi.

Grensesnittet mellom personvern og informasjonssikkerhet kan illustreres på følgende måte:



Begge fagområdene deler felles fagområde på intranettet: Informasjonssikkerhet og personvern hvor det er opprettet relevante temasider med utdypende informasjon. Se også undersiden Begrepsliste informasjonssikkerhet og personvern.

Oppgaver og ansvar for PVO og informasjonssikkerhetsleder, samt ledere og øvrige ansatte er ytterligere beskrevet i det styrende dokumentet Organisering av informasjonssikkerhets- og personvernarbeidet.

INNHOLD I POLICY

Overordnet målsetning for informasjonssikkerhet og personvern er at all behandling av informasjon er i samsvar med lover, regler og avtaler og er i tråd med prinsippene for behandling av personopplysninger (jf. GDPR art 5). Den registrertes rettigheter og friheter skal ivaretas, og informasjonen som behandles skal

- Være tilgjengelig ved behov (tilgjengelighet)
- Ikke endres utilsiktet eller av uvedkommende (integritet)
- Ikke bli kjent for uvedkommende (konfidensialitet)

Informasjonssikkerhetsarbeidet skal være risikobasert og inngå i virksomhetens helhetlige regime for risiko- og virksomhetsstyring. Ansvar og myndighet følger det ordinære linjeansvaret. Ved målkonflikter skal det legges stor vekt på å ivareta helseberedskap og pasientsikkerhet. Se det styrende dokumentet Mål og strategi for informasjonssikkerhet i Helse Sør-Øst - overordnet styrende dokument, samt SSHF sitt styrende dokument Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet og personvern.

SSHF sitt styringssystem for informasjonssikkerhet og personvern skal være basert på de regionalt vedtatt styrende dokumentene. De styrende dokumentene understøttes av utførende og kontrollerende dokumenter, samt annen nødvendig støttedokumentasjon. Se Ledelsessystem for informasjonssikkerhet - Helse Sør-Øst RHF og SSHF sitt styrende dokument Styringssystem for Informasjonssikkerhet og personvern.

Merk at med behandling av informasjon så menes her alle former for behandling av informasjon; både muntlig, når lagret på papir og når informasjon lagres og behandles elektronisk. Ved bruk av IKT- og fagsystemer vil sikker informasjonsbehandling normalt ivaretas av fagsystemet. Ved behandling av informasjon utenfor fagsystemene lagres disse som filer og dokumenter i mapper. Når slike filer og dokumenter inneholder personopplysninger skal foretakets retningslinjer for Lagring, arkivering og sletting av helse- og personopplysninger følges. Se for øvrig også Arkiv og dokumentasjonsseksjonens temaside på intranett: Dokumentasjonsforvaltning.

PLANLEGGE

Risikovurderinger skal gjennomføres før behandling av helse- og personopplysninger startes, og ved endringer av behandling av informasjon som kan påvirke sikkerheten (jf. Personvernforordningen). Se også SSHF sitt styrende dokument Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet og personvern. Risikovurderingen og aksept av eventuell risiko skal dokumenteres i tråd med foretakets retningslinjer beskrevet i dokumentet Kapittel 11 - Risikostyring - policydokument.

Informasjonsbehandlingen skal dokumenteres i foretakets protokoll over behandlingsaktiviteter (her skal forstås behandling av personopplysninger). Se dokumentet Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet og personvern og ansvarsforhold knyttet til føring av protokollen beskrevet i

dokumentet Organisering av informasjonssikkerhets- og personvernarbeidet. Protokollen føres i modulen «informasjonssystemer» i Kvalitetsportalen.

Dersom det er sannsynlig at en behandling av personopplysninger vil medføre en høy risiko for personers rettigheter og friheter, skal det foretas en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger. Her benyttes begrepet *personvernkonsekvensvurdering* eller DPIA (Data Protection Impact Assessment).

GJENNOMFØRE

Det daglige arbeidet med informasjonssikkerhet og personvern ivaretas av informasjonssikkerhetsleder og PVO gjennom rådgivning og lederstøtte. Videre skal disse også benytte internkontroll som metode for å dokumenter etterlevelse, jf. det styrende dokumentet Internkontroll informasjonssikkerhet og personvern. Det skal arbeides for økt kompetanse og digital sikkerhetskultur blant foretakets medarbeidere og ledere.

Leder på alle nivåer har ansvar for å påse at retningslinjer for informasjonssikkerhet og personvern etterleves innen eget ansvarsområde. Ansvar og oppgaver er ytterligere beskrevet i det styrende dokumentet Organisering av informasjonssikkerhets- og personvernarbeidet.

RAPPORTERE

Rapportering av personvern- og informasjonssikkerhetsarbeidet ivaretas og gjennomføres slik det er beskrevet ovenfor, samt vedtatt i det styrende dokumentet Ledelsens gjennomgang (LGG) - informasjonssikkerhet og personvern. I dette inngår også å dokumentere risiko og etterlevelse av relevante krav og lovverk, både på et overordnet nivå og også pr informasjonssystem og behandling. Det vises for øvrig til Kapittel 11 - Risikostyring - policydokument.

EVALUERE

Evaluering og forbedring ivaretas slik det er beskrevet i det styrende dokumentet Internkontroll informasjonssikkerhet og personvern. I dette inngår risikostyring, overvåkning og hendelseshåndtering, samt måling, evaluering og revisjon som metode for å vurdere om innførte tiltak gir ønsket effekt. Det vises for øvrig til Uønskede hendelser - policydokument.

Kryssreferanser

I.5.2.4-12	Uønskede hendelser - policydokument
I.5.9.1-1	Styringssystem for Informasjonssikkerhet og personvern
I.5.9.1-2	Organisering av informasjonssikkerhets- og personvernarbeidet
I.5.9.1-3	Sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet og personvern
I.5.9.1-5	Internkontroll informasjonssikkerhet og personvern
I.5.9.1-6	Ledelsens gjennomgang (LGG) - informasjonssikkerhet og personvern
I.5.9.1-8	Mål og strategi for informasjonssikkerhet i Helse Sør-Øst - overordnet styrende dokument
I.5.9.1-9	Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet og personvern
I.5.9.1-10	Sikkerhetsregulerende lovverk gjeldende for foretaksgruppen
I.5.9.2-8	Lagring, arkivering og sletting av helse- og personopplysninger
I.5.11-1	Kapittel 11 - Risikostyring - policydokument

Eksterne referanser

1.35 Personopplysningsloven