SYKEHUSET I VESTFOLD

Uønsket hendelse - brudd på informasjonssikkerhet

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	26.03.2024

Innholdsfortegnelse

1. HENSIKT

Prosedyren skal bidra til at

- hendelse som har medført eller kunne medført brudd på informasjonssikkerhet meldes som uønsket hendelse på skjemaet «HMS/andre uønsket hendelse» i sykehusets kvalitetssystem (EQS), håndteres og følges opp på en systematisk måte slik at
    - normaltilstanden gjenopprettes raskt
    - informasjonssikkerheten vurderes og tiltak iverksettes for å finne rotårsaken og forhindre gjentakelse av samme brudd

- brudd på informasjonssikkerhet som omfatter personopplysninger kan også utløse meldeplikt til
    - Datatilsynet uten opphold og senest innen 72 timer etter å ha fått kjennskap til det. Dette gjelder der bruddet sannsynligvis vil medføre middels eller høy risiko for person(er)s rettigheter og friheter.
    - Statsforvalteren om uønsket hendelse som følge av feil/uønsket hendelse på informasjonssystemer

I tillegg skal det gis informasjon til de registrerte (pasienter, besøkende, studenter, ansatte, forskningsdeltakere) dersom det er sannsynlig at bruddet vil medføre en høy risiko for deres rettigheter og friheter. Informasjonen skal gis så raskt som mulig.

Brudd på personopplysningssikkerhet er alltid brudd på informasjonssikkerhet, men et brudd på informasjonssikkerhet er ikke alltid et brudd på personopplysningssikkerhet.

2. ANSVAR

Ansatte uansett arbeidsforhold
Seksjonsledere
Avdelingssjefer
Klinikksjefer/Servicedirektør
Administrerende direktør (dataansvarlig)
Personvernombudet
Informasjonssikkerhetsleder

3. FREMGANGSMÅTE

3.1 Når skal uønsket hendelse (hendelse) meldes i kvalitetssystemet (EQS)?

Uønsket hendelse skal meldes i EQS av den som oppdager det, når det foreligger:

1. Brudd på konfidensialitet (K) - det har vært en utilsiktet eller ulovlig utlevering av, eller tilgang til, personopplysninger.
2. Brudd på integritet (I) - det har vært en utilsiktet eller ulovlig endring av personopplysninger.
3. Brudd på tilgjengelighet (T) - det har vært et utilsiktet eller ulovlig tap av tilgang til eller tilintetgjøring av, personopplysninger.
4. Brudd på robusthet (R) - manglende evne til å motstå driftsuønsket hendelse og dataangrep og til å gjenopprette normaltilstand på en effektiv måte innen en tidsramme som er i samsvar med virksomhetens behov.

Et brudd kan omfatte én, eller en kombinasjon av disse fire.

3.1.1. Hva skal meldingen i EQS inneholde?

Personopplysninger skal **ikke** noteres i meldingen.

Melder

- Vurder og evt. gjennomfør strakstiltak
- Beskriv den uønskede hendelsen så godt det lar seg gjøre. Trykk «Registrer»

Meldingsansvarlig

- Fyll ut del II av meldingen
- Gjennomfør risikovurdering i ROS MAL - Brudd på personopplysningssikkerhet (informasjonssikkerhet)
  Kontakt personvernombud@siv.no for hjelp til vurdering av meldeplikten(e) når restrisiko R ≥ 5. Se pkt. 3.3 nedenfor.
  Legg utfylt ROS MAL som vedlegg til meldingen.
- Følg opp planlagte tiltak og registrerer dato for «utført» i ROS MAL Tabell 2

3.2 Uønsket hendelse oppstått hos databehandler
Databehandler plikter å informere sykehuset som dataansvarlig så raskt som mulig når en uønsket hendelse oppstår hos databehandler. Meldingen skal registreres og følges opp som beskrevet i pkt. 3.1.1 ovenfor.

3.3 Når skal uønsket hendelse meldes til Datatilsynet?
Uønsket hendelse som omfatter brudd på personopplysningssikkerhet skal meldes til Datatilsynet når det foreligger brudd på en eller en kombinasjon av de fire kategoriene; konfidensialitet - integritet – tilgjengelighet - robusthet. Bruddet må ha medført middels eller høy risiko for pasient/ansatt/publikum (registrerte) sine rettigheter og friheter.

Uønsket hendelse skal meldes til Datatilsynet **innen 72 timer** etter at bruddet er kjent. Dersom det ikke er mulig fordi det mangler informasjon, kan meldingen gis trinnvis.

3.3.1 Uønsket hendelse som SKAL meldes til Datatilsynet

- **Forsendelsesfeil**
  - Beskyttelsesverdige personopplysninger er sendt til feil mottaker pr. post eller e-post.
  - Digitale forsendelser som avslører andres e-postadresse i en kontekst hvor mottakerne skal beskyttes.
  - Forsendelser til riktig mottaker, men som ved en feil også inneholder beskyttelsesverdige personopplysninger om andre.
  - Postforsendelser til riktig mottaker, men hvor det er informasjon om mottakeren som skal skjermes for andre er synlig utenpå forsendelsen. Eksempel på dette er innkalling til medlemsmøte i en religiøs menighet.
  - Postforsendelser hvor innholdet mangler eller innholdet er der, men konvolutten er revet opp.
- **Hacking eller datainnbrudd**, hvor personopplysninger har blitt hentet ut, er endret på eller er utilgjengelig, eller at det er sannsynlig at dette har skjedd.
- **Tilgangsstyring feilet, er mangelfull eller manglende**, slik at uvedkommende har fått tilgang til beskyttelsesverdige personopplysninger.
- **Nettpublisering av personopplysninger** som ikke skulle ha vært publisert, eller at personopplysningene ikke har blitt anonymisert.
- **Fysisk innbrudd** hvor ukrypterte digitale data eller papirdokumenter med personopplysninger er forsvunnet.
- **Kastet/kvittet seg med opplysninger uten sletting eller makulering**
  Mistet/gjenglemt/forlagt eksempelvis:
  - Papirdokumenter
  - Laptop, nettbrett eller telefoner der innholdet ikke er kryptert
  - Minnepinner eller andre små lagringsmedier der innholdet ikke er kryptert

3.3.2 Hva skal meldingen til Datatilsynet inneholde?
Beskriv den uønskede hendelsen så godt det lar seg gjøre, mulige konsekvenser og utførte/planlagte tiltak for å hindre gjentakelse. Bruk ROS MAL - Brudd på personopplysningssikkerhet (informasjonssikkerhet)

3.3.3. Saksgang SIV - melding til Datatilsynet
Meldingsansvarlig sender meldingen og utfylt ROS MAL til personvernombud@siv.no når restrisiko R ≥ 5. E-posten og vedleggene må ikke inneholde personopplysninger.

Personvernombudet vurderer om det foreligger meldeplikt og utarbeider tilråding som sendes til dataansvarlig (adm. direktør). Saksdokumentene vedlegges.
Kopi til meldingsansvarlig.

Dataansvarlig tar endelig stilling til om hendelsen skal meldes til Datatilsynet og underretter meldingsansvarlig og personvernombudet om beslutningen.

Personvernombudet sørger for melding til Datatilsynet der det er besluttet (via Altinn).
Kopi til dataansvarlig og meldingsansvarlig.

3.4 Når skal berørte informeres?

- Dersom det er ingen/lav/middels risiko, er det ikke nødvendig å informere den/de berørte
- Dersom det er høy risiko, skal berørte informeres
  Eksempler (ikke uttømmende): Bruddet har ført til/kan føre til diskriminering eller forskjellsbehandling, ID-tyveri, bedrageri eller svindel, økonomisk tap, tap av omdømme og eller tap av liv eller helse.

Unntak fra informasjonsplikten:

- Det er gjennomført tekniske og organisatoriske sikkerhetstiltak for personopplysningene som er berørt av hendelsen, f.eks. tiltak som gjør opplysningene uleselige.
- Det er truffet tiltaket i etterkant som gjør at det er lite trolig at hendelsen har ført til utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert tilgjengeliggjøring av eller tilgang til personopplysninger.
- Om varslingen innebærer en uforholdsmessig stor innsats (f.eks. ved at hendelsen berører et stort antall individer) skal allmennheten underrettes slik at den registrerte likevel underrettes på en effektiv måte.

3.4.1 Hva skal det informeres om?

Informasjonen skal som minimum inneholde:

- Beskrivelse av bruddet og om hendelsen har medført sletting, endring eller uautorisert tilgjengeliggjøring/tilgang helse- og personopplysningene
- Navn og kontaktinformasjon til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes.
- Beskrivelse av de sannsynlige konsekvensene av bruddet.
- Beskrivelse av de tiltakene som den behandlingsansvarlige har truffet eller foreslår å sette i gang for å håndtere bruddet, inkludert (dersom det er relevant) tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

3.4.2. Hvordan skal informasjonen gis?

Meldingsansvarlig eller den meldingsansvarlig utpeker, skal så langt som mulig ta direkte kontakt med den/de som er berørt. Informasjonen skal gis eksplisitt og ikke sammen med annen informasjon.

Informasjonen skal gis skriftlig i brevs form. E-post skal ikke brukes. Informasjon til en større gruppe kan alternativt eller samtidig med individuell informasjon, legges ut på SiV.no og eller annonseres i ulike medier (eks. aviser).

3.5. Varsel til Statsforvalteren ved IKT-bortfall

Helsepersonell har plikt til å varsle om forhold som kan medføre/har medført fare for pasienters sikkerhet, herunder teknisk utstyr og IKT jf. helsepersonelloven § 17.

Kontakt ikt@siv.no for hjelp til å vurdere om hendelsen er/kan være forårsaket av IKT-bortfall.

4. GENERELT

Krav til internkontroll for informasjonssikkerhet

Den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll).

5. INTERNE REFERANSER

1.1.8.3.1.1	Uønsket hendelse - styringsdokument.
1.1.8.3.1.2	EQS - registrere melding
1.1.8.3.1.5	EQS - Kategorisering av uønskede hendelser
1.1.11.1.2	Mål og strategi for informasjonssikkerhet
1.1.11.4.15	ROS MAL - Brudd på personopplysningssikkerhet (informasjonssikkerhet)

6. EKSTERNE REFERANSER

Personopplysningsloven
Personvernforordningen

Normen - ehelse
Veileder om internkontroll for informasjonssikkerhet og personvern - ehelse
Nye retningslinjer for uønsket hendelsesmeldinger | Datatilsynet
Informasjon til de berørte | Datatilsynet

7. VEDLEGG