SYKEHUSET I VESTFOLD

Informasjonssikkerhet - Loggføring av aktivitet og kontroll av logger

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	13.08.2018

1. HENSIKT

Hensikten med dokumentet er å informere alle ansatte og innleide med tilgang til helseforetakets informasjonssystemer om loggføring av aktivitet og kontroll av logger, og å gi føringer for hvordan kontroll skal utføres og følges opp.

All bruk av sykehusets informasjonssystemer kan bli loggført. Loggene brukes til administrasjon, for å følge opp sykehusets retningslinjer for informasjonssikkerhet og for lovpålagt kontroll av oppslag i behandlingsrettede helseregistre (eks. DIPS). Autorisert personell gjennomgår loggene og iverksetter tiltak om nødvendig.

Dokumentet gjelder for alle medarbeidere, leverandører, konsulenter, vikarer og andre som gis tilgang til sykehusets elektroniske tjenester. Dette omfatter all bruk av virksomhetens informasjonssystemer med loggføring av aktivitet.

2. ANSVAR

Administrerende direktør: Er databehandlingsansvarlig og har ansvaret for at regler og kriterier for bruk av informasjonssystemene er etablert og kjent.

Personvernombudet: Har en rolle i å sikre at den enkeltes personvernrettigheter blir ivaretatt.

Informasjonssikkerhetsleder: Har det utøvende ansvar for virksomhetens informasjonssikkerhetsarbeid, blant annet ved å iverksette og delta i revisjoner, risikovurderinger og kontroll av logger.

Ledere innen ulike enheter og områder har ansvar for å påse at denne instruks implementeres og etterleves innen eget ansvarsområde. Det vil si at dokumentet er kjent, tilgjengelig og blir brukt.

Alle ansatte og innleide ved sykehuset med tilgang til informasjonssystemene, skal forholde seg til denne instruks. Dette gjelder uavhengig av organisatorisk plassering, yrkesgruppe og område.

3. FREMGANGSMÅTE

Type logger

- Hendelseslogger fra behandlingsrettede registre
- Sikkerhetslogger
- Driftslogger

Hendelseslogger fra behandlingsrettede registre

Med hendelseslogg menes eksplisitt logg fra et behandlingsrettet register, hvor formålet er å dokumentere utøvelsen av helsehjelp, pasientens rett til innsyn og dokumentering av helseforetakets forsvarlighet.

En logg som inneholder aktivitetene gjort i et behandlingsrettet register inkluderer, men er ikke begrenset til, innsynslogg, print av sider, henvisninger, sletting, endring eller oppretting av tekst, journalnotater, endring av rettigheter eller tilsvarende. Benyttes til å

gi pasienten innsyn i aktiviteter i dennes journal, til foretakets kontroll for å avdekke uautorisert bruk, eller andre hendelser med betydning for informasjonssikkerheten.

Formålet med hendelseslogger
Helseforetakenes plikt til å loggføre oppslag i behandlingsrettede helseregistre, og jevnlig etterkontrollere logger, følger av pasientjournalloven § 22.
Personopplysningsforskriftens kapittel 2 inneholder nærmere regler om behandlingsansvarliges plikt til å logge tilgang til informasjonssystemet.

Personopplysninger i hendelseslogger
En hendelseslogg skal inneholde det som er nødvendig for å oppfylle formålet med loggen, herunder:

- Pasient som det er gjort oppslag mot
  - Navn
  - Fødselsnummer
  - Henvisningsorganisasjon ved oppslagstidspunktet
- Type oppslag (lest/utskrift/dokumentert/endret)
- Dokumenttype (navn på dokument)
- Pasientadministrativ informasjon det er gjort oppslag på
- Tidspunkt for oppslag (dato, klokkeslett)
- Besluttet tilgang / aktualisering / «grønnlys»
- Ansatt som har utført oppslaget
  - Navn
  - Fødselsnummer
  - Brukeridentitet
  - Rolle
  - Stilling
  - Organisasjonstilhørighet

For systematisk kontroll av oppslaget benyttes i tillegg informasjon om den ansattes stillingshistorikk i helseforetaket og pasientens oppholdshistorikk, samt utdypende opplysninger om oppslaget (besluttet tilgang mm.).

For kontrollformål innhentes kun informasjon som helseforetaket allerede er i besittelse av. Det innhentes ikke informasjon fra andre virksomheter.

Godkjent lagringstid
I praksis oppbevares hendelsesloggen på ubestemt tid. I den systematiske loggkontrollen som foretaket utfører ved hjelp av statistisk metode (mønstergjenkjenning) er det de siste 24 måneder som kontrolleres månedlig.

Krav til tilgangskontroll
Teknisk tilgang til hendelsesloggen er begrenset til helseforetakets loggkontrollør og til ansatte, innleide eller leverandører med en funksjon knyttet til systematisk loggkontroll og innsynskrav fra pasient.

Innsyn i hendelseslogger
Rett til innsyn i hendelsesloggen har:
Pasienten, begrenset til det som angår pasienten
Ansatte, begrenset til det som angår den ansatte
Loggkontrollør som utfører systematisk loggkontroll
Andre ansatte, innleide eller leverandører som på oppdrag fra helseforetaket har en funksjon knyttet til formålet med hendelsesloggen.

Foretakets kontroll av hendelseslogger
Helseforetakets lovpålagte plikt til å utføre systematisk kontroll av hendelsesloggen gjøres på flere måter:

Statistisk loggkontroll / mønstergjenkjenning
Kontrolltiltaket (*hvis dette er besluttet innført ved helseforetaket)* benytter maskinell, statistisk analyse av alle oppslag som er gjort de siste 24 månedene. Metoden baseres på forutsetningen om at de fleste oppslag som gjøres, er tjenstlig begrunnet. Oppslag som avviker fra vanlige oppslagsmønstre gis høyere score og underlegges en grundig manuell kontroll. Dersom den manuelle kontrollen ikke kan forklare oppslaget, rapporteres dette til den ansattes klinikk for videre håndtering.

Rettede loggkontroller
Normalt vil verktøyet for statistisk loggkontroll benyttes med utgangspunkt i en på forhånd identifisert hendelseslogg, enten knyttet til en konkret pasient, en ansatt eller en del av virksomheten. Benyttes f.eks. i forbindelse med rutinekontroll av pasienter som er kjent for allmenheten («kjendis»), henvendelse fra pasient eller fra leder.

Dersom den ansattes nærmeste leder vurderer oppslaget som uvanlig eller mistenkelig, følges dette opp etter egne prosedyrer utarbeidet av HR/personal.

Sikkerhetslogger
Sikkerhetslogger er logger fra informasjonssystemer hvor formålet er å avdekke sikkerhetsbrudd eller avvik. Det skal registreres autorisert bruk og forsøk på uautorisert bruk, samt alle andre typer hendelser med betydning for informasjonssikkerheten, dvs. Konfidensialitet, Integritet, Tilgjengelighet (jf. personopplysningsforskriften kapittel 2).

Formålet med innsamling av sikkerhetslogger
Personopplysningsforskriften § 2-16, sammen med helseregisterloven § 13, definerer at det skal være *hendelser med betydning for informasjonssikkerheten*.

Hvilke logger som har *betydning* for informasjonssikkerheten, må altså vurderes ut fra den *konteksten* informasjonen er i. Driverinformasjon fra et grafikkort vil for eksempel ikke bli definert som sikkerhetslogg på en ordinær PC, men på PC tilknyttet klinisk behandling hvor grafikkortdriverne konfigureres og sertifiseres, vil loggdata som viser endringer i konfigurasjonen kunne være av *betydning* for informasjonssikkerheten, og dermed klassifiseres som sikkerhetslogg. Sikkerhetslogger er altså ikke av en *fast* størrelse, men må vurderes.

Personopplysninger i sikkerhetslogger
Ved innsamling, analysering og lagring av sikkerhetslogger, kan det også inngå personopplysninger.

Personopplysningsforskriften § 7-11 gir anledning til å behandle personopplysninger når disse følger som en konsekvens av registrering av hendelser i et informasjonssystem. Denne behandlingen er unntatt meldeplikt til Datatilsynet. En slik anledning er kun gyldig så lenge formålet er knyttet opp til:

a) Å administrere systemet, eller
b) Å avdekke og/eller oppklare brudd på informasjonssikkerheten i informasjonssystemet

Godkjent lagringstid
Det anføres at sikkerhetslogger skal slettes når det ikke lenger er saklig grunn for oppbevaring. Saklig grunn er i dette tilfellet identifisert å være avdekking og oppklaring av sikkerhetsbrudd og avvik mot informasjonssikkerheten.

Personopplysningsforskriften § 2-16 angir en *minimum* lagringstid på 3 måneder, samtidig som personopplysningsloven § 28 gir et forbud mot lagring av personopplysninger unødvendig.

Erfaring tilsier at det vil være et behov for å oppbevare sikkerhetslogger ut over den lovpålagte minimumsperioden på 3 måneder. Dette skyldes en kompleks infrastruktur

med mange loggkilder og et sammensatt trusselbilde, som medfører at hendelser kan være tidkrevende å undersøke. I tillegg vil enkelte typer sikkerhetsbrudd kunne ta tid å detektere. *Lagring av sikkerhetslogger som inneholder personopplysninger er definert til å være seks – 6 – måneder.*

Krav til tilgangskontroll
Informasjonssystemer som behandler eller samler inn sikkerhetslogger, skal være underlagt tilgangskontroll for å forhindre uautorisert innsyn. Sykehuspartner skal ivareta at kun autorisert og autentisert personell får adgang.

Driftslogger
Driftslogger er system- og infrastrukturlogger hvor formålet er å bevare systemstatus, eksempelvis diskfyllingsgrad, last, antall samtidige sesjoner mv, og dermed understøtte sikker og stabil drift av informasjonssystemene. Inneholder ordinært sett ikke personopplysninger.

Personopplysninger i driftslogger
Ved innsamling, analysering og lagring av driftslogger, kan det i noen tilfeller inngå personopplysninger.

Personopplysningsforskriften § 7-11 gir anledning til å behandle personopplysninger når disse følger som en konsekvens av registrering av hendelser i et informasjonssystem. Denne behandlingen er unntatt meldeplikt til Datatilsynet. En slik anledning er kun gyldig så lenge formålet er knyttet opp til:

a) Å administrere systemet, eller
b) Å avdekke og/eller oppklare brudd på informasjonssikkerheten i informasjonssystemet

Godkjent lagringstid
Det anføres at driftslogger som inneholder personopplysninger skal slettes når det ikke lenger er saklig grunn for oppbevaring. Saklig grunn er i dette tilfellet identifisert å være driftshensyn. Personopplysningsloven § 28 gir et forbud mot lagring av personopplysninger unødvendig.

Erfaring tilsier at det vil være et behov for å oppbevare driftslogger ut over den lovpålagte minimumsperioden på 3 måneder. Dette skyldes den komplekse infrastrukturen, med mange loggkilder. For å understøtte driften, kan det være behov for å se på utvikling over tid. *Lagring av driftslogger som inneholder personopplysninger er definert til å være seks – 6 – måneder.*

Krav til tilgangskontroll
Informasjonssystemer som behandler eller samler inn driftslogger som inneholder personopplysninger, skal være underlagt tilgangskontroll for å forhindre uautorisert innsyn. Helseforetaket og driftsleverandøren (Sykehuspartner IKT) skal ivareta at kun autorisert og autentisert personell får adgang.

Lagringstid for logger uten personopplysninger
Sikkerhets- eller driftslogger som ikke inneholder personopplysninger kan oppbevares uten begrensninger eller krav til tilgangskontroll, utover de hensyn helseforetaket selv etablerer. Dette innebærer at det ikke er gitt noen formalkrav for sletting (varighet) eller for tilgangskontroll (innsyn), ut over de som helseforetaket selv evt. vedtar for det aktuelle systemet.

Utvidet logging
Ved mistanke om, eller etterforskning av, brudd på sikkerhetsbestemmelsene, kan det være aktuelt med utvidet logging eller oppfølging av logger.

Oppfølging av avvik
Ansvar for gjennomgang av loggene tilfaller tjenesteansvarlig. Databehandlingsansvarlige og databehandler er ansvarlig for å rapportere om potensielle straffbare forhold.

Kravliste i tabellform

	Hendelseslogger	**Sikkerhetslogger**	**Driftslogger**
Formål	Ivaretagelse av pasientens personvern og kontroll og oppfølging av oppslag der det er mistanke om uautorisert bruk av tilgang til systemet	Detektere og oppklare sikkerhetsbrudd og avvik	Detektere og oppklare driftsrelaterte problemer
Loggkilder	Behandlingsrettede helseregistre	Infrastrukturtjenester, servere m.v.	Infrastrukturtjenester, servere, klienter m.v.
Lagringssted	I register eller på godkjent lagringsområde	Sentralt loggmottak	Sentralt loggmottak
Klassifisering	Betydelige mengder sensitive personopplysninger	Store mengder personopplysninger, kan oppleves som inngripende	Varierende, men kun ved behov, jf. person-opplysnings-forskriften §7-11
Tilgangskontroll	Egne bestemmelser	Kun godkjent administrator-personell	Kun godkjent administrator-personell.
Lagringstid	Ikke tidfestet	Seks – 6 – måneder	Seks – 6 – måneder

4. GENERELT

5. INTERNE REFERANSER

1.1.11.1.4	Informasjonssikkerhetsinstruks
1.1.11.2.12	Informasjonssikkerhet - Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

6. EKSTERNE REFERANSER

7. VEDLEGG