ENDRINGER FRA FORRIGE VERSJON: Nytt dokument, basert på tilsvarende regionalt dokument NO-22

KILDE

Dette dokumentet er basert på HSØ Regionalt ledelsessystem for informasjonssikkerhet, dokument NO-22 v1.1: «*Loggføring av aktivitet og kontroll av logger*». Oppdatert etter personopplysningslov av 20. juli 2018. Tilpasninger er tatt inn ifm loggføring ved bruk av Kjernejournal, samt innføring av statistisk logganalyse.

HENSIKT

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

MÅLGRUPPE

Alle medarbeidere, leverandører, konsulenter, vikarer og andre som gis tilgang til Sørlandet sykehus HF (SSHF) sine elektroniske tjenester. Dette omfatter all bruk av virksomhetens informasjonssystemer med loggføring av aktivitet.

ANSVAR

- **Administrerende direktør** er behandlingsansvarlig og har ansvaret for at regler og kriterier for bruk av informasjonssystemene er etablert og kjent.
- **Systemeier (og systemforvalter)** er ansvarlig for gjennomgang av logger iht SSHF sine rutiner
- **Personvernombudet** har en rolle i å medvirke til 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** har ansvar for å påse at denne instruks implementeres og etterleves innen eget ansvarsområde. Det vil si at dokumentet er kjent, tilgjengelig og etterleves.
- **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.

FREMGANGSMÅTE

Generelt

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.

Type logger

- Logger fra personregistre og behandlingsrettede helseregistre
- Sikkerhetslogger
- Driftslogger

Disse er beskrevet under.

Utvidet logging

Ved mistanke om brudd på sikkerhetsbestemmelsene eller begjæring fra domstol eller påtalemyndigheten kan det være aktuelt å iverksette utvidet logging og oppfølging av logger.

Avvik

Når kontroll av logger avdekker brudd på SSHF sine sikkerhetsbestemmelser registreres dette som uønsket hendelse og følges opp iht SSHF sine rutiner for dette.

Logger fra personregistre og behandlingsrettede helseregistre
En logg inneholder aktivitetene gjort i et personregister og inkluderer, men er ikke begrenset til, innsynslogg, print av sider, henvisninger, sletting, endring eller oppretting av tekst, journalnotater, endring av rettigheter eller tilsvarende.

Loggene kan gi de registrerte informasjon om:

1) Virksomhetens bruk av opplysningene om dem,
2) Hvem som har hatt innsyn i opplysningene,
3) Virksomhetens kontroll for å avdekke eventuell uautorisert bruk av opplysningene, og
4) andre hendelser med betydning for informasjonssikkerheten.

Logger fra behandlingsrettede helseregistre

Loggen inneholder aktiviteter som en identifiserbar bruker står ansvarlig i et behandlingsrettet helseregister (pasientjournalen).

Innholdet i loggen skal gis i et format og med et innhold som gjør det mulig å gjenskape de handlinger brukeren har foretatt i systemet.

Loggen benyttes også til å gi pasienten innsyn i aktiviteter i journalen, til sykehusets kontroll for å avdekke urettmessig bruk av tilgangen, eller andre hendelser med betydning for informasjonssikkerheten.

Formålet med loggen

Helseforetakenes plikt til å loggføre oppslag i behandlingsrettede helseregistre, og jevnlig etterkontrollere logger, følger av pasientjournalloven § 22. Formålet med analyse av logger er således helseforetakets lovpålagte plikt til å beskytte helseopplysninger mot uberettiget innsyn.

Pasienter har rett til vern mot spredning av legems- og sykdomsforhold, samt andre personlige opplysninger om dem. Formålet med loggen er å sikre pasienten innsyn i hvem som har benyttet tilgangen til pasientjournalen.

Opplysninger i logger fra oppslag i personregistre og behandlingsrettede helseregistre

En logg skal inneholde det som er nødvendig for å oppfylle formålet med loggen, herunder:

- Den registrerte som det er gjort oppslag mot
  - Navn
  - Fødselsnummer
  - Henvisningsorganisasjon ved oppslagstidspunktet
- Type oppslag (lest/utskrift/dokumentert/endret)
- Dokumenttype (navn på dokument)
- Administrativ informasjon det er gjort oppslag på
- Tidspunkt for oppslag (dato, klokkeslett)
- Besluttet tilgang / aktualisering / «grønnlys»
- Medarbeider 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 oppslag utført av andre virksomheter, dvs. dokumentdeling via Kjernejournal (tilgang mellom virksomheter) skal det i tillegg minimum loggføres:

- Virksomheten oppslaget er utført fra
  - Navn
  - Org.nr. / RESHID
- Underliggende enhet
  - Eks. etat/avdeling/seksjon
- Identitet på den som har gjort oppslaget hos virksomheten
- Begrunnelse for oppslaget
- Pasientens tilknytning til virksomheten på oppslagstidspunktet
  - Dvs. er pasienten til behandling i virksomheten?

Lagringstid

Loggen oppbevares i minimum 24 måneder og ellers så lenge det er nødvendig for å oppfylle formålet.

Dataansvarlig setter rammene for lagringstid og avgjør nødvendig lagringstid iht. formålet.

Krav til tilgangskontroll til logger

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

Pasienten har også tilgang til et aggregat av loggen via helsenorge.no, men har ikke teknisk tilgang til hele loggen slik den fremkommer over.

Personer som kan be om innsyn i logg fra personregistre og behandlingsrettede helseregistre

Retten til innsyn i loggen gjelder følgende:

- Pasienten, begrenset til det som angår den registrerte
- Ansatte, begrenset til det som angår ansatte
- Loggkontrollør som utfører systematisk loggkontroll
- Andre ansatte, innleide eller leverandører som på oppdrag fra helseforetaket har en funksjon knyttet til formålet med loggkontroll.
- Tilsynsmyndighet

Kontroll av logger med aktivitet i behandlingsrettede helseregistre

Kontroll med logg av oppslag og annen aktivitet i behandlingsrettede helseregistre forutsettes å gjennomføres systematisk, og er et ansvar som påhviler sykehuset og er en lovpålagt plikt.

Kontrolltiltaket benytter maskinell, statistisk logganalyse 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 konkluderer med at oppslaget er uvanlig, formidles dette i henhold til sykehusets prosedyrer til den ansattes klinikk for avklaring av om oppslaget er lovlig.

Verktøyet for statistisk loggkontroll kan også benyttes med utgangspunkt i en på forhånd identifisert logg, enten knyttet til en konkret pasient, ansatt eller del av sykehuset. Benyttes f.eks. i forbindelse med henvendelse fra pasient eller fra leder. Se også Kontroll av oppslag i elektronisk pasientjournal (EPJ) og andre fagsystemer

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.

Logger fra adgangskontrollsystem som avdekker bruk av adgangskort anses ikke som en sikkerhetslogg, men som hendelseslogg.

Formålet med sikkerhetslogger

Pasientjournalloven § 22, sammen med helseregisterloven § 21, jf. personvernforordningen artikkel 32, definerer at formålet 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.

Personvernforordningen artikkel 32 gir anledning til å behandle personopplysninger når disse følger som en konsekvens av registrering av hendelser i et informasjonssystem. En slik anledning er kun gyldig så lenge formålet er knyttet opp til;

- å administrere systemet,
- å gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder tilgangsstyring, logging og etterfølgende kontroll
- å avdekke og/eller oppklare brudd på personvern og informasjonssikkerheten i informasjonssystemet, herunder
    - utilsiktet eller ulovlig tilintetgjøring
    - tap
    - endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

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 og/eller den registrertes personvern.

Personopplysningene i sikkerhetsloggene skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for, jf. personvernforordningen artikkel 5 nr. 1 c). Godkjent lagringstid skal fastsettes etter vurdering av nødvendig og egnet sikkerhetsnivå, jf. personvernforordningen artikkel 32.

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 24 måneder.

Krav til tilgangskontroll

Informasjonssystemer som behandler eller samler inn sikkerhetslogger, skal være underlagt tilgangskontroll for å forhindre uautorisert innsyn, tap, ødeleggelse eller skade. Sykehuspartner HF 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.

Personvernforordningen artikkel 32 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;

- å administrere systemet,
- å gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder tilgangsstyring, logging og etterfølgende kontroll
- å avdekke og/eller oppklare brudd på personvern og informasjonssikkerheten i informasjonssystemet, herunder
    - utilsiktet eller ulovlig tilintetgjøring
    - tap
    - endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

Lagringstid for driftslogger med personopplysninger

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. Personopplysningene i driftsloggene skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for, jf. personvernforordningen artikkel 5 nr. 1 c). Godkjent lagringstid skal fastsettes etter vurdering av nødvendig og egnet sikkerhetsnivå, jf. personvernforordningen artikkel 32.

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 i Helse Sør-Øst til å være 24 måneder.

Lagringstid for driftslogger 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.

Krav til tilgangskontroll

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

KRAVLISTE I TABELLFORM

	Logg fra personregister og behandlingsrettet helseregister	**Sikkerhetslogg**	**Driftslogg**
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	Personregistre og behandlingsrettede helseregistre	Infrastrukturtjenester, servere m.v.	Infrastrukturtjenester, servere m.v.
Lagringssted	I register eller på godkjent lagringsområde	Sentralt loggmottak	Sentralt loggmottak
Klassifisering	Betydelige mengder sensitive personopplysninger	Store mengder personopplysninger	Varierende, men kun ved behov, jf. personvernforordningen artikkel 32
Tilgangskontroll	Egne bestemmelser	Kun godkjent administratorpersonell	Kun godkjent administratorpersonell
Lagringstid	Ikke tidfestet, normalt som for det aktuelle registeret loggen er hentet fra	24 måneder	24 måneder

Kryssreferanser

I.5.9.8-2	Kontroll av oppslag i elektronisk pasientjournal (EPJ) og andre fagsystemer
I.5.10.3-1	Prosedyre for utlevering av innsynslogg, Dips Arena. Dokumentsenteret SSHF

Eksterne referanser

178 Regionalt ledelsessystem for informasjonssikkerhet