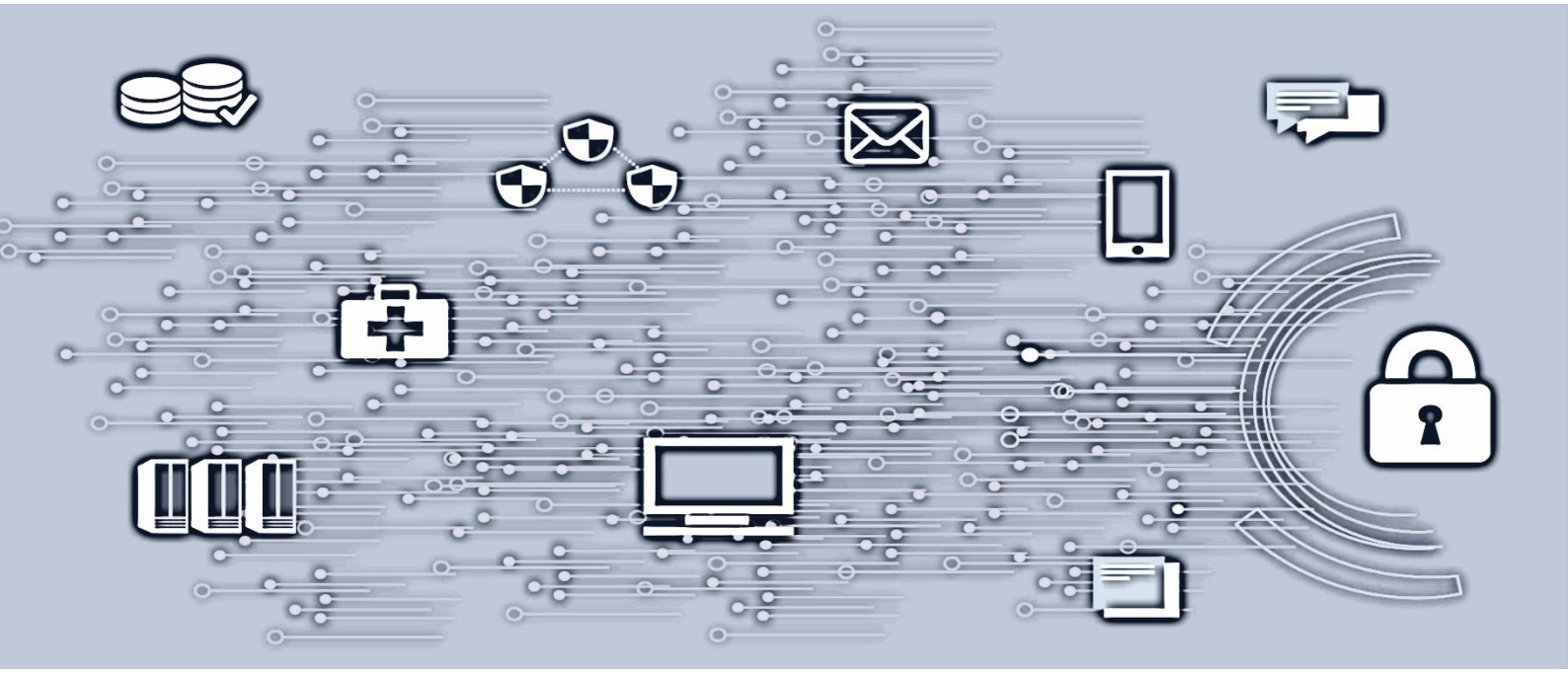
SYKEHUSPARTNER

Formål og krav for drifts- og sikkerhetslogger



Innhold

Versjon	Dato	Godkjent av
1.0	2014-12-09	Christian Jacobsen
1.1	2015-07-02	Christian Jacobsen
1.2	2019-04-11	Christian Jacobsen
1.3	2021-11-22	Christian Jacobsen
1.4	2022-03-06	Christian Jacobsen

1. Formål

Dette dokumentet inneholder Sykehuspartner HFs sikkerhetskrav for sikkerhetslogger og andre typer logger.

2. Definisjon av loggtyper

Sykehuspartner HF definerer tre typer logger:

2.1 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. Skal også inneholde forsøk på uautorisert bruk eller andre hendelser med betydning for informasjonssikkerheten.

2.2 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.

Hvilke logger som skal defineres som sikkerhetslogger, må til en viss grad også vurderes ut fra den konkrete 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 potensielt kunne klassifiseres som en sikkerhetslogg.

Sikkerhetslogger er altså ikke av en fast størrelse, men må vurderes. Det er Avdeling Sikkerhet sammen med CERT som vil være styrende for å tolke hvorvidt en loggkilde kan være av *betydning* for informasjonssikkerheten eller ei.

2.3 Driftslogger

Driftslogger er system- og infrastrukturlogger hvor formålet er å bevare systemstatus, eksempelvis diskfyllingsgrad, last, antall samtidige sesjoner mv.

2.4 Eksempler på loggkilder som avgir sikkerhetslogger

Eksempler på loggkilder (ikke uttømmende) som defineres som sikkerhetslogger:

Infrastruktur	Sikkerhetskilder	Klient/server	Applikasjoner
Routere og switcher	Proxy-logger	WSUS/patchestatus	Inn- og utlogginger
Domenekontrollere	IDS-verktøy	Antivirus	Aktualisering (eks i EPJ)
DNS og DHCP	EDR-verktøy	Innlogging/utlogging	Utskrift
Brannmurslogger	E-postsikkerhet	Stopp/start av prosesser	Slettinger (eks i EPJ)

3. Avgrensninger

Følgende avgrensninger er gitt i dette dokumentet:

3.1 Hendelseslogger fra behandlingsrettede registre

Dette dokumentet tar ikke mål av seg å kunne besvare alle de krav og forutsetningene, samt forskjellige aktivitetene som må gjennomføres for å etablere en hendelseslogg fra et behandlingsrettet register. For øvrige spørsmål om hendelseslogger fra et behandlingsrettet register (for eksempel et PAS/EPJ), kontakt dataansvarlig helseforetak, eller Avdeling Sikkerhet.

3.2 Sikkerhets- eller driftslogger som ikke inneholder personopplysninger

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

Hovedregelen for denne typen logger er likevel som for andre sikkerhetslogger satt til 24 måneder.

4. Drifts- og sikkerhetslogger som inneholder personopplysninger

4.1 Formålet

Sykehuspartner har definert at formålet med drifts- og sikkerhetslogger er å **understøtte sikker og stabil drift**. Drifts- og sikkerhetslogger skal kunne brukes til proaktivt eller reaktivt feilretting, så fremt denne behandlingen ikke er i strid med opprinnelig formål om sikker og stabil drift.

Drifts- og sikkerhetslogger også skal kunne brukes til å forhindre, avdekke og oppklare sikkerhetsbrudd og avvik mot informasjonssikkerheten. Det vil si hendelser som har negativ konsekvens for systemets-, brukerens-, eller informasjonens konfidensialitet, integritet, tilgjengelighet og kvalitet.

4.2 Personopplysninger i drifts- og sikkerhetslogger

Ved innsamling, analysering og lagring av drifts- og sikkerhetslogger, kan det også inngå personopplysninger.

Sykehuspartner kan ikke gjøre nytte av informasjon som kommer frem under slike formål, til å overvåke eller kontrollere den enkelte, eller på annen måte bruke disse personopplysninger på en måte som er i strid med det opprinnelige formålet.

4.3 Godkjent lagringstid

Det anføres at drifts- og sikkerhetslogger skal slettes når det ikke lenger er saklig grunn for oppbevaring. Saklig grunn er i dette tilfellet identifisert å være å forhindre, avdekke eller korrigere forhold som påvirker sikker og stabil drift.

Sykehuspartner HF forvalter en svært kompleks infrastruktur for regionens helseforetak med mange loggkilder og et sammensatt drifts- og trusselbilde som medfører at hendelser kan være tidkrevende å undersøke, og enkelte typer brudd kan ta tid å detektere.

Ved å etablere gode sikkerhetskontroller i det sentrale loggmottaket, er det besluttet at lagringstid for drifts- og sikkerhetslogger skal være tjuefire – 24 – måneder.

4.4 Krav til tilgangsstyring

Informasjonssystemer som behandler eller samler inn drifts- og sikkerhetslogger, skal være underlagt tilgangskontroll for å forhindre uautorisert innsyn. Sykehuspartner HF skal ivareta at kun autorisert og autentisert personell får tilgang.

5. Kravliste i tabellform

	Hendelseslogger	Sikkerhetslogger	Driftslogger
Formål	Bestemmes av dataansvarlig	**Sikker og stabil drift** gjennom å forhindre, detektere og korrigere sikkerhetsbrudd og avvik	**Sikker og stabil drift** gjennom proaktivt eller reaktivt feilretting.
Loggkilder	Helseregistre, kliniske applikasjoner, MTU ++	Infrastrukturtjenester, servere, klienter, brannmurer, sikkerhetsprogramvare mv.	Infrastrukturtjenester, servere, klienter, brannmurer, driftsprogramvare mv.
Lagringssted	I register eller på godkjent lagringsområde	Sentralt loggmottak	Sentralt loggmottak
Klassifisering	Betydelige mengder særlige kategorier av personopplysninger, også svært inngripende og detaljerte opplysninger om den enkelte.	Inneholder ofte ulike personopplysninger, unntaksvis også særlige kategorier, også om ansatte.	Varierende, kan inneholde personopplysninger, men som hovedregel ikke særlige kategorier.
Tilgangs-kontroll	Egne bestemmelser.	Kun godkjent administratorpersonell	Kun godkjent administratorpersonell.
Lagringstid	Som hovedregel minst ti – 10 – år, hjemlet i egen lov. Avklares med dataansvarlig.	24 måneder	24 måneder