Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Logging og oppfølging av logger

Støttedokument
Faktaark nr 15
Versjon: 3.1
Dato: 20.09.2018

Formål	Formålet med logging og oppfølging av logger er å: • gi oversikt over autorisert bruk av helse- og personopplysninger i virksomheten • sette virksomheten i stand til å avdekke uautorisert bruk, eller forsøk på uautorisert bruk av helse- og personopplysninger • forebygge, avdekke og forhindre gjentagelse av sikkerhetsbrudd i informasjonssystemene • legge til rette for pasient/brukers rett til innsyn i logger, slik at vedkommende gis mulighet til å ivareta egne rettigheter • legge til rette for ansattes rett til innsyn i opplysninger som er lagret om vedkommende i loggene
Ansvar	Dataansvarlig har ansvaret for logging, men de daglige oppgavene er normalt delegert til den som er ansvarlig for det enkelte informasjonssystem. Prosjektleder har et særskilt ansvar ifm forskning.
Gjennomføring	Planlegges før et nytt informasjonssystem tas i bruk og gjennomføres under bruk.
Omfang	Alle virksomheter i sektoren som behandler helse- og personopplysninger elektronisk, skal føre og kontrollere loggene.
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☒ Prosjektleder forskning ☒ Sikkerhetsleder ☒ Ansatt / medarbeider ☐ Forsker ☐ Personvernombud ☒ IKT-ansvarlig ☒ Databehandler ☒ Leverandør
Hjemmel	Personvernforordningen artikkel 24, 32
Referanser	• Norm for informasjonssikkerhet, kapittel 5.4.4, 5.5.2, 5.5.4, 5.5.5 (www.normen.no) • Pasientjournalloven § 16 • Helsepersonelloven § 21a. • Forskrift om tilgang til helseopplysninger mellom virksomheter § 11 • EPJ-standard: https://ehelse.no/standarder-kodeverk-og-referansekatalog/standarder-og-referansekatalog/epj-standard-del-1-introduksjon-til-epj-standard-his-805052015 • Veileder for fjernaksess mellom leverandør og virksomhet, (www.normen.no) • Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren, (www.normen.no) • Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger mellom virksomheter, (www.normen.no) • Faktaark 47 - Autorisasjonsregister

Merknad 20.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Nr.	Handling
1.	**Prosedyre for logging** a) Dataansvarlig skal påse at det etableres prosedyrer som sikrer at logging etableres b) Prosedyren skal - Hensyn til at logging kan innebære en ny behandling av personopplysninger som kan være meldepliktig. Meldeplikten gjelder ikke om behandlingen har som formål o å administrere systemet, eller o å avdekke/oppklare brudd på sikkerheten i informasjonssystemet - ivareta kravet om at loggene skal kunne sammenholdes med autorisasjonsregister og tilstedeværelsesregister

Nr.	Handling
	- ivareta kravet om at loggene skal analyseres slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke - ivareta kravet om at Datatilsynet skal varsles dersom det har blitt foretatt en uautorisert utlevering av eller tilgang til helse- og personopplysninger
2.	**Logging skal etableres for** a) Tilgang til behandlingsrettede helseregistre og fagsystemer - All tilgang til og autorisert bruk av behandlingsrettede helseregistre og fagsystemer - Alle forsøk på uautorisert bruk av behandlingsrettede helseregistre og fagsystemer - All bruk av nødrettstilgang med begrunnelse b) Infrastruktur - Sikkerhetsrelevante hendelser i sikkerhetsbarrierer (for eksempel brannmur og ruter) slik som: o Alle forsøk på ulovlig tilgang både internt og eksternt o Alle brudd på regler som forbyr trafikk o Alle brudd på regler som slipper inn lovlig trafikk fra eksterne tilknytninger - Alle forsøk på uautorisert bruk av nettverksoperativsystemer
3.	**Logging i forskningsprosjekter skal etableres for** a) All forskningstilgang, registrering, retting og sletting, autorisert og forsøk på uautorisert bruk og kopiering / duplisering av - forskningsdata - forskningsfilen b) All autorisert og forsøk på uautorisert bruk og kopiering / duplisering av - koblingsnøkkelen - fil med koblingsnøkler Både manuell og elektronisk logging kan benyttes.
4.	**Loggen skal som minimum inneholde** a) For autorisert bruk: - Entydig identifikator for den autoriserte brukeren (Se Faktaark 47 - Autorisasjonsregister) - Rollen den autoriserte brukeren har ved tilgangen - Virksomhetstilhørighet for den autoriserte brukeren (vanligvis virksomhet eller databehandler) - Organisatorisk tilhørighet til den som er autorisert (avdelingsnavn eller avdelingskode er normalt tilstrekkelig). Kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur - Hvilken type opplysninger det er gitt tilgang til - Hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer - Grunnlaget for tilgangen (for eksempel helsehjelp, nødrettstilgang, administrativ bruk) - Tidspunkt og varighet for tilgangen (dato og klokkeslett) - Begrunnelse ved bruk av nødrettstilgang - Ved tilgang mellom virksomheter skal i tillegg følgende logges hos virksomhetene: o person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene o hvorfor helseopplysningene er hentet frem o hvilke tidsperioder vedkommende har hentet frem helseopplysningene - Ved fjernaksess fra leverandør: o initiert trafikk mot IP-adresse og portnummer o hva som er utført (kommandoer, transaksjoner, osv). Om mulig skal angivelse av tid for utført kommando også logges o hvilke data/datafiler som er lastet ned til leverandør (datafiler) eller opp til virksomhet (programfiler og patcher) o Navn og entydig identifikator for den/de hos leverandør som har benyttet den aktuelle fjernaksess

Nr.	Handling
	b) For forsøk på uautorisert bruk: - Brukeridentiteten som ble benyttet - Tidspunkt (dato og klokkeslett) - IP-adresse eller annen identifikasjon av PC/arbeidsstasjon/mobiltelefon/nettbrett som ble benyttet (for eksempel MAC-adresse, NAT-adresse eller mobiltelefonnummer)
5.	**Sikring og oppbevaring av logger** a) Logger skal sikres mot innsyn, endring og sletting av uautorisert personell b) Logger skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem
6.	**Logger som bevis** a) Logg som skal benyttes som bevis bør speilkopieres til annet medium før analyser gjennomføres b) Speilkopieringen bør gjennomføres under tilsyn av 2 eller flere personer c) Det bør opprettes en skriftlig protokoll for speilkopieringen som sier hva som er gjort. Protokollen skal signeres av de som var tilstede og oppbevares sammen med det registrerte avviket
7.	**Bruk av logger** a) Elektroniske logger skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd på regelverket (se også pasientjournalloven § 16 og helsepersonelloven § 21 a.) b) For manuelt førte logger skal virksomheten etablere prosedyrer for tilfredsstillende analyse av registrene c) Dersom brudd avdekkes skal personalmessige reaksjoner iverksettes d) Dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, dvs. det er gjentatt tilgang av flere personer som ikke er autorisert, skal nødvendige tekniske tiltak iverksettes e) All bruk av nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som et avvik for å påse at begrunnelse er relevant f) Ved brudd på regler ved tilkobling til nett utenfor virksomheten skal kanalen stenges inntil ny sikker løsning er etablert g) Ved brudd på regler om logisk skille mellom Internett og nettverk der helse- og personopplysninger behandles skal regelbruddet behandles som avvik og personalmessige konsekvenser vurderes h) Ved brudd på regler om at sensitive personopplysninger ikke skal utleveres ved hjelp av e-post skal regelbruddet behandles som avvik og personalmessige konsekvenser vurderes
8.	**Sletting av logger** a) Dersom oppføringer i logger kan knyttes til enkeltpersoner, skal loggene slettes når det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem