NORMEN

Logging og innsyn i logg (faktaark 15)

Versjon 4.0

17. mars 2022

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler logging, oppfølging av logg og innsyn i logg. Formålet med faktaarket er å gi veiledning til hvordan virksomheten bør gå frem for å etterleve Normens krav til logging og loggoppfølging. Faktaarket tar også for seg prosessen for innsyn i logg fra behandlingsrettet helseregister. Faktaarket har en teoretisk tilnærming og inneholder punkter en virksomhet må ta stilling til for å etablere tilfredsstillende rutiner for logging, loggoppfølging og logginnsyn.
Dette faktaarket er spesielt relevant for	• Dataansvarlig • Personell som jobber daglig med logging og oppfølging av logger, som for eksempel systemansvarlig • Virksomhetens ledelse og nøkkelressurser innen sikkerhet og personvern. Virksomhetens systemleverandører
Krav i Normen	Faktaarket gjelder for følgende kapitler i Normen - Kapittel 3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengeliget og robusthet - Kapittel 4.2.3 Innsyn - Kapittel 4.2.6 Oppbevaring av helse og personopplysninger - Kapittel 5.4.4 Logging -
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser er spesielt relevante for faktaarket: Personvernforordningen: • Artikkel 5. Prinsipper for behandling av personopplysninger • Artikkel 13. Informasjon som skal gis ved innsamling av personopplysninger fra den registrerte • Artikkel 14. Informasjon som skal gis dersom personopplysninger ikke er blitt samlet inn fra den registrerte • Artikkel 15. Den registrertes rett til innsyn • Artikkel 24. Den behandlingsansvarliges ansvar • Artikkel 32. Sikkerhet ved behandlingen • Artikkel 33. Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten

	Pasientjournalloven • § 18. Informasjon og innsyn • § 22. Informasjonssikkerhet • § 23. Internkontroll • Pasient og brukerrettighetsloven § 5-1. Rett til innsyn i journal • Pasientjournalforskriften § 14. Krav til loggføring • Helseregisterloven § 24. Rett til informasjon og innsyn • Helsepersonelloven § 21 a. Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger • Arbeidsmiljøloven kapittel 9 • NSMs grunnprinsipper for IKT-sikkerhet 2.0- o Grunnprinsipp 3.2 Etabler sikkerhetsovervåkning o Grunnprinsipp 3.3 Analyser data fra sikkerhetsovervåkning - ISO/IEC 27002 – A.12.4 Logging og overvåking - CIS Control 8 – Audit Log Management

Logging og innsyn i logg

I Normen er det flere krav til logging, oppfølging av logg og innsyn i logg. I dette faktaarket sammenstilles og utdypes disse kravene. Som for alle sikkerhetstiltak, skal også tiltak knyttet til logging baseres på en vurdering av risiko og forholdsmessighet.1 Derfor redegjøres det i faktaarket også for en rekke anbefalinger til tiltak virksomheter kan vurdere å implementere innen logging, for å håndtere identifisert risiko.

Faktaarket inkluderer det som tidligere var faktaark 50 om innsyn i hendelsesregistre.

Avgrensning

Faktaarket er avgrenset til logging som gjøres av hensyn til informasjonssikkerhet og personvern knyttet til pasientjournaler og andre behandlingsrettede helseregistre for etterlevelse av pasientjournalloven § 22 og pasientjournalforskriften § 14. Dette gjelder eksempelvis logger av tilgang til informasjonssystem[2], men også sikkerhetslogger fra IKT-infrastruktur[3] for behandlingsrettede helseregistre.

I Normen er det også krav til generell logging i bredere forstand enn hva som behandles i dette faktaarket. For veiledning om hvordan disse kravene kan etterleves vises det til annet veiledningsmateriell.[4] Videre omtales ikke direkte forhold knyttet til bruk av logger for annen beslutningsstøtte eller feilsøking. Disse formålene er imidlertid belyst i Direktoratet for e-helse sine retningslinjer for logging ved data- og dokumentdeling[5].

Kompletterende veiledningsmateriell

For en kompletterende veiledning til dette faktaarket kan det være særlig aktuelt å se på grunnprinsipp 3.2 og 3.3[6] med tilhørende tiltak, i NSMs grunnprinsipper for IKT-sikkerhet 2.0, samt CIS Control 8[7]. Disse rammeverkene gir en generell, men praktisk tilnærming til logging, og vil være nyttige hjelpemidler for å oppnå kravene til logging i Normen.

Oversikt

Faktaarket er bygget opp som følger:

1. Logging og hendelsesregistrering
2. Oppfølging og bruk av logger
3. Innsyn i logg
4. Sikring, oppbevaring og sletting av logger.

---

[1] Normen 6.0 kapittel 3.1 Forholdsmessighet
[2] Se Normens definisjon på informasjonssystem i vedlegg 6.2 i Normen
[3] Se Normens definisjon på infrastruktur i vedlegg 6.2 i Normen
[4] Se NSMs grunnprinsipper for IKT-sikkerhet
[5] Direktoratet for e-helse: Retningslinjer for logging ved data- og dokumentdeling
[6] NSM Grunnprinsipper for IKT-sikkerhet 2.0 – 3.2 Etabler sikkerhetsovervåking og 3.3 Analyser data fra sikkerhetsovervåking
[7] CIS Controls: https://www.cisecurity.org/controls/ - Tilgang til kontrollene er gratis, men krever registrering.

1. Logging og hendelsesregistrering
Formålet med logging og hendelsesregistrering 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 medarbeideres rett til innsyn i opplysninger som er lagret om vedkommende i loggene.

Nr	Handling
1.	**Rutine for logging** a) Det skal utarbeides rutiner som sikrer at logging etableres, følges opp og håndteres i tråd med Normen og regulative krav. Rutinen skal[8] - ivareta kravet om at loggene enkelt skal kunne analyseres ved hjelp av analyseverktøy, samt at loggene skal analyseres slik at hendelser oppdages og håndteres før de får utilsiktede konsekvenser - ivareta kravet om at logger skal kunne sammenholdes med autorisasjonsregister - ivareta kravet til korrekt tidsstempel på loggene for å sikre loggintegritet (se punkt 7) - ivareta kravet til oppbevaring og lagring av logger (se punkt 12 og 13) - ivareta kravet om at Datatilsynet skal varsles ved brudd på personopplysningssikkerheten.[9] b) Rutinen bør gjennomgås minimum årlig og ved behov, eksempelvis ved endringer i Normen eller regulative krav, for å vurdere forbedringer og sikre at rutinen er i tråd med gjeldende krav. For ytterligere veiledning om å utarbeide en rutine og en strategi for logging vises det til NSMs grunnprinsipper 3.2 og tiltak 3.2.1.[10]
2.	**Når logging skal etableres** Logging skal etableres for tilgang til[11]: a) Behandlingsrettede helseregistre: - Tilgang til og autorisert bruk av behandlingsrettede helseregistre, inkludert bruk av selvautorisering med begrunnelse - Forsøk på uautorisert bruk av behandlingsrettede helseregistre.

[8] Normen 6.0 kapittel 5.4.4 Logging
[9] Personopplysningsloven artikkel 33
[10] NSM Grunnprinsipper for IKT-sikkerhet 2.0 – 3.2 Etabler sikkerhetsovervåking
[11] Normen 6.0 kapittel 5.4.4 Logging

Nr	Handling

	b) Informasjonssystem og infrastruktur for behandlingsrettet helseregister:
	- Autorisert bruk av informasjonssystemene
	- Bruk av administratortilgang
	- Sikkerhetsrelevante hendelser i sikkerhetsbarrierer (for eksempel brannmur og ruter), slik som
	  ○ forsøk på ulovlig tilgang både internt og eksternt
	  ○ brudd på regler som forbyr trafikk
	  ○ brudd på regler for å slippe inn lovlig trafikk fra eksterne tilknytninger
	- Forsøk på uautorisert bruk av nettverksoperativsystemer
	- Endring av konfigurasjon og programvare
	- Ved bruk av ukrypterte kanaler (som for eksempel e-post og SMS) skal logging etableres for å kontrollere at regler ikke brytes[12]
	- Autorisert og uautorisert tilgang til logger (se også punkt 12).
	
	For ytterligere veiledning om hvilke deler av IKT-systemene som bør overvåkes vises det til grunnprinsipp 3.2 og tiltak 3.2.3.[13]

3.	**Hva som skal logges** a) Ved autorisert bruk av behandlingsrettet helseregister skal følgende logges[14]: - Identiteten til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger (det skal være en entydig identifikator for den autoriserte brukeren) - Organisatorisk tilhørighet til den som er autorisert (avdelingsnavn eller avdelingskode er normalt tilstrekkelig). Organisatorisk tilhørighet kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur. - Grunnlaget for tilgjengeliggjøringen (for eksempel helsehjelp, selvautorisering med begrunnelse, administrativ bruk) - Tidspunkt og varighet for tilgjengeliggjøringen (dato og klokkeslett). Det skal i tillegg registreres hvilken pasients opplysninger og hvilken type opplysninger om pasienten, som personellet har hatt tilgang til.[15] b) I tillegg til punktene over bør det vurderes å logge følgende opplysninger: - Rollen den autoriserte brukeren har ved tilgangen - Hvem som har fått utlevert helseopplysninger som er knyttet til pasientens navn eller fødselsnummer. Dette kan eksempelvis gjelde utlevering til helsepersonell som ikke er gitt tilgang til systemet, men likevel har tjenstlig behov (f.eks. helsepersonell som får utdrag fra kjernejournalen eller tilsendt utskrift i posten). Dette må da registreres manuelt. - Hvilket utstyr som er brukt for påloggingen, samt lokasjonen påloggingen er gjort fra.

[12] Normen 6.0 kapittel 5.5.4 E-post og SMS
[13] NSM Grunnprinsipper for IKT-sikkerhet 2.0 – Grunnprinsipp 3.2 Etabler sikkerhetsovervåking
[14] Normen 6.0 kapittel 5.4.4 Logging
[15] Normen 6.0 kapittel 4.2.3 Innsyn

Nr	Handling
	Selv om det ikke er lovpålagt å logge punktene listet opp i b) er det sterkt anbefalt at også disse punktene inngår i loggingen der det er mulig. Dette vil lette arbeidet med å føre kontroll med tilganger, samt behandle og gjennomføre innsyn i logg. c) I tillegg til punktene over bør virksomheten vurdere å logge følgende punkter ved fjernaksess[16]: - Initiert trafikk mot IP-adresse og portnummer - Hva som er utført (kommandoer, transaksjoner, osv.). Om mulig skal angivelse av tid for utført kommando også logges. - Hvilke data/datafiler som er lastet ned til leverandør (datafiler) eller opp til virksomhet (programfiler og patcher) - IP-adresse eller annen identifikasjon av enheten som ble benyttet, samt lokasjonen påloggingen er gjort fra. d) I tillegg til punktene over bør virksomheten vurdere å logge følgende ved forsøk på uautorisert bruk: - Brukeridentiteten som ble benyttet - Tidspunkt (dato og klokkeslett) - Lokasjon for pålogging - IP-adresse eller annen identifikasjon av PC/arbeidsstasjon/mobiltelefon/ nettbrett som ble benyttet (for eksempel MAC-adresse, NAT-adresse eller mobiltelefonnummer). e) Ved behandling av helse- og personopplysninger for andre formål enn ytelse av helse- og omsorgstjenester skal kravene til logging besluttes på grunnlag av en risikovurdering.[17]

2. Oppfølging og bruk av logger

Oppfølging og analyse av logger skal benyttes som en del av kontrollen av tilgangsstyringen. Formålet med oppfølging og analyse av loggene er blant annet å avdekke uautorisert tilgang til helse- og personopplysninger. Videre vil analyse av logger gi en indikasjon på hvorvidt virksomhetens tilgangsstyring er effektiv og fungerer optimalt.

Nr	Handling
4.	**Rettslige rammer for bruk av logger** a) Logger inneholder personopplysninger[18], og all bruk av loggene (inkludert innsamling, oppbevaring og bruk i oppfølging av det enkelte helsepersonell) må oppfylle kravene i personopplysningsloven. Virksomheten som er dataansvarlig må blant annet sikre at den oppfyller informasjonsplikten, kravet til lovlighet og de øvrige personvernprinsippene i personvernforordningen artikkel 5.[19] Virksomheten

[16] Se eget veiledningsmateriell for fjernaksess mellom leverandør og virksomhet
[17] Normen 6.0 kapittel 5.4.4 Logging
[18] Personopplysninger om brukerne av systemet som logges
[19] Les mer om dette i faktaark 57 om personvernprinsippene og faktaark 56 om formål og behandlingsgrunnlag

Nr	Handling
	bør være særlig oppmerksom på begrensningene i muligheten til å viderebehandle personopplysninger for andre formål enn de opprinnelig ble samlet inn for.[20] b) I tillegg bør virksomheten være oppmerksom på vilkårene for bruk av kontrolltiltak overfor arbeidstakere, i arbeidsmiljøloven kapittel 9. Etablering av logging utgjør kontrolltiltak i seg selv.[21] Dataansvarlig må derfor sikre at følgende krav i arbeidsmiljøloven kapittel 9 er oppfylt: - For det første, så kan et kontrolltiltak bare benyttes når det har en saklig grunn i virksomhetens forhold. I tillegg må kontrolltiltaket ikke gi en uforholdsmessig belastning for arbeidstakerne til dataansvarlig.[22] Når det kommer til disse kravene, så kan dataansvarlig vanligvis legge til grunn at kravene er oppfylt, så lenge dataansvarlig kun benytter loggene til det opprinnelige formålet. Det opprinnelige formålet vil være å forhindre uberettiget tilgang til helse- og personopplysningene.[23] - For det andre, så må dataansvarlig sikre at egne arbeidstakere får informasjon om kontrolltiltaket. Informasjonen skal omfatte kontrolltiltakets formål, praktiske konsekvenser for arbeidstakerne (herunder informasjon om gjennomføringen) og tiltakets antatte varighet.[24] Oppfyllelse av denne informasjonsplikten kan kombineres med oppfyllelsen av informasjonsplikten i personvernforordningen artikkel 12 til 14. - For det tredje, så må dataansvarlig drøfte behov, utforming og gjennomføring kontrolltiltaket med tillitsvalgt før det etableres. Det samme gjelder ved vesentlig endring av tiltaket.[25] Behovet for kontrolltiltaket skal også reevalueres jevnlig med tillitsvalgt.[26] Det stilles ikke krav til at dataansvarlig og tillitsvalgt skal komme til enighet. Arbeidstilsynet og Datatilsynet har utarbeidet en veileder som beskriver hvordan dataansvarlig bør gå frem for å ivareta disse kravene, samt hvordan dataansvarlig bør benytte en risikobasert tilnærming for å sikre at kontrolltiltakene har ønsket effekt. Sistnevnte kan være særlig nyttig når dataansvarlig planlegger gjennomføringen av kontrollene som omtales i neste avsnitt. c) Det er etter pasientjournalloven § 22 krav om at dataansvarlig og databehandler utfører etterfølgende kontroll. Med etterfølgende kontroll menes eksempelvis gjennomgang av logger for å påse at virksomheten etterlever lovpålagte krav.
5.	**Analyse av logger**

[20] Jf. prinsippet om formålsbegrensning i personvernforordningen artikkel 5 nr. 1 bokstav
[21] Engelschiøn (2019) lovkommentar til pasientjournalloven § 22
[22] Arbeidsmiljøloven § 9-1 (1)
[23] Engelschiøn (2019) lovkommentar til pasientjournalloven § 22
[24] Arbeidsmiljøloven § 9-2 (2)
[25] Arbeidsmiljøloven § 9-2 (1)
[26] Arbeidsmiljøloven § 9-2 (2)

Nr	Handling
	a) Logger skal analyseres for å oppdage hendelser før de får alvorlige konsekvenser.[27] Dette gjelder også for manuelt førte logger. b) Elektroniske logger skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd på regelverket[28] (se også pasientjournalloven § 16 og helsepersonelloven § 21 a.). - Det anbefales å benytte standardisert format på loggene, slik at data enkelt skal kunne leses av tredjeparts logganalyseverktøy.[29][30] - Statistisk logganalyse er et eksempel på et verktøy som kan benyttes for analyse av logger for å identifisere uvanlige oppslag som videre må analyseres manuelt.[31] - Dersom virksomheten ikke har tekniske tiltak på plass for logganalyse, kan virksomheten i påvente av tekniske tiltak og etter en risikovurdering, implementere organisatoriske tiltak.[32] o Som et organisatorisk tiltak bør det utarbeides en rutine for jevnlig og systematisk gjennomgang av logger, der det tas stikkprøver på pasienter. Gjennomgangen bør utføres av personell som har en forutsetning til å kunne vurdere tjenstlig behov, og kan eksempelvis gjøres på avdelingsnivå. Det kan være aktuelt å utføre særlige stikkprøver på pasienter som er spesielt utsatt for snoking, som for eksempel kjente personer og ansatte ved sykehuset eller hos samarbeidspartnere. c) Ved fastsettelse av metode for å analysere logger bør det gjøres en totalvurdering av hva som er tilstrekkelig i hvert enkelt tilfelle. Tiltakene for analyse av logger bør være en kombinasjon av tekniske tiltak og manuelle rutiner. I tillegg kan pasientens bruk av innsynsrett (omtalt i faktaarkets del 3) medvirke til at sikkerhetsbrudd avdekkes. For ytterligere veiledning om analyse av logger vises det til grunnprinsipp 3.3[33].
6.	**Avdekking av brudd ved analyse av logger** Regelbrudd som avdekkes ved analyse av logger skal håndteres som et avvik[34]. Regelbrudd som avdekkes i denne sammenhengen kan være brudd på lov. For informasjon om hvordan regelbrudd skal behandles, vises det til kapittel om avviksbehandling i veileder om internkontroll for informasjonssikkerhet og personvern
7.	**Logger som bevis**

[27] Normen 6.0 kapittel 5.4.4 Logging
[28] Normen 6.0 kapittel 5.4.4 Logging
[29] NSMs grunnprinsipper for IKT-sikkerhet 2.0 – 3.2.5 verifiser at innsamlingen fungerer etter hensikt
[30] Det pågår et arbeid for å få på plass en norsk implementasjonsguide basert på FHIR Audit Event
[31] Helse Sør-Øst: Statistisk logganalyse
[32] Normen 6.0 kapittel 3.4 Risikovurdering og risikohåndtering
[33] NSM Grunnprinsipper for IKT-sikkerhet 2.0 – 3.3 Analyser data fra sikkerhetsovervåking
[34] Normen 6.0 kapittel 5.4.4 Logging

Nr	Handling
	a) Logg som skal benyttes som bevis bør speilkopieres til annet medium før analyser gjennomføres. b) Speilkopieringen bør gjennomføres under påsyn av to eller flere personer. c) Det bør opprettes en skriftlig protokoll for speilkopieringen der det fremgår hva som er gjort. Protokollen bør signeres av de som var til stede og oppbevares sammen med det registrerte avviket. For å kunne benytte logger som bevis, er det avgjørende at loggene er tilstrekkelig beskyttet mot manipulering (integritetsbeskyttelse). For ytterligere veiledning om dette vises det til NSMs grunnprinsipper 3.2 og tiltak 3.2.6.[35]

3. Innsyn i logg

Den registrerte har rett til innsyn i opplysninger registrert om seg selv i behandlingsrettet helseregister. Innsynsretten gjelder også loggen over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger og på hvilket tidspunkt[36]. Enhver virksomhet som behandler helse- og personopplysninger, er pliktig til å tilrettelegge for at den registrerte på forespørsel får innsyn i opplysningene. Pasientens innsynsrett er med på å gi trygghet for at prinsippet om tjenstlig behov etterleves og bidrar til å hindre misbruk av tilgangsrettigheter.

Retten til innsyn, kravene til hvordan innsyn skal gjennomføres og unntakene fra denne rettigheten, er nærmere beskrevet i Veileder for rettigheter ved behandling av helse- og personopplysninger.

Nr	Handling
8.	**Forberedelser før innsyn** Det bør etableres rutiner for å sikre at den registrertes rettigheter til innsyn i logg blir ivaretatt. Rutinen bør som minimum sikre at den registrerte får informasjon om - opplysningene som er registrert om vedkommende - hvem som har hatt tilgang til opplysningene, når tilgangen er benyttet og til hvilken informasjon tilgangen er benyttet.
9.	**Behandling av forespørsel om innsyn** a) Forespørsel om innsyn kan mottas muntlig eller skriftlig. Dataansvarlig må forsikre seg om at innsynsforespørselen kommer fra rette vedkommende. b) Forespørsel om innsyn og rett til utskrift av dokumentasjon skal besvares uten ugrunnet opphold og sendes innen 30 dager etter henvendelsen er mottatt. - Innsyn skal være gratis. Dersom den registrerte ber om flere kopier, kan den dataansvarlig kreve et rimelig gebyr basert på administrasjonskostnadene.[37]
10.	**Gjennomføring av innsyn**

[35] NSM Grunnprinsipper for IKT-sikkerhet 2.0 – 3.2 Etabler sikkerhetsovervåking
[36] Normen 6.0 kapittel 4.2.3 Innsyn
[37] Personvernforordningen artikkel 15 nr. 3

Nr	Handling
	a) Forespørselen om innsyn avgjøres av den som har fått fullmakt fra den dataansvarlige. Innsynsforespørselen og hvilken beslutning som ble fattet skal dokumenteres. b) Hvis innsyn er besluttet, skal minimum følgende opplysninger meddeles den som har forespurt om innsyn: - Identitet og organisatorisk tilhørighet til den som har hatt tilgang - Tidspunkt for den enkelte tilgang - Hvilke opplysninger det ble gitt tilgang til ved det enkelte tilfelle - Registreringsdato for den enkelte opplysning det er gitt tilgang til ved det enkelte tilfelle. c) Ved innsyn i logg skal innholdet gjøres forståelig for den registrerte. Dette innebærer følgende: - Ved behov skal virksomhetens autorisasjonsregister sammenstilles med logg i det behandlingsrettede helseregisteret - Dersom den registrerte ber om det, skal det gis en kortfattet forklaring på hva loggen inneholder, mulige årsaker til at helsepersonell har brukt tilgangen til et behandlingsrettet helseregister, og tekniske uttrykk og lignende. d) Den registrerte har rett til å få utskrift av dokumentasjonen. Ved utskrift skal det kunne foretas sortering i henhold til den registrertes ønske. - Dersom den registrerte inngir anmodningen elektronisk, og med mindre den registrerte anmoder om noe annet, skal informasjonen gis i en vanlig elektronisk form.[38] De fleste helseregioner har tilrettelagt for at innsyn kan utføres gjennom innlogging på helsenorge.no[39]

[38] Personvernforordningen artikkel 15 nr. 3
[39] https://www.helsenorge.no/rettigheter/innsyn-pasientjournal/

4. Sikring, oppbevaring og sletting av logger

Nr	Handling
11.	**Sikring av logger** Logger skal sikres mot innsyn, endring og sletting av uautorisert personell[40]. - Det er kun et fåtall personer som bør ha tilgang til loggene. Tilgangen bør være avgrenset til en spesifikk rolle (f.eks. loggadministrator) som ikke har andre administrative tilganger. - Det bør implementeres funksjonalitet som forebygger og oppdager forsøk på manipulering eller sletting av logger. For ytterligere veiledning om dette vises det til NSMs grunnprinsipper 3.2 og tiltak 3.2.6.[41]
12.	**Oppbevaring av logger** a) I behandlingsrettet helseregister skal helseopplysninger oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem. Det samme gjelder også opplysninger om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens navn eller fødselsnummer.[42] Logger av sikkerhetsmessig betydning bør oppbevares så lenge det er nødvendig for å oppnå formålet.[43]
13.	**Sletting av logger** a) Når loggene ikke lenger er nødvendig, skal de slettes. Loggene skal likevel ikke slettes dersom opplysningene er omfattet av en arkivplikt (for eksempel etter arkivloven eller helsearkivforskriften). b) Virksomheten må selv vurdere når loggene skal slettes. I store informasjonssystemer kan logging medføre et stort volum av data. Dette taler for at logger bør lagres i begrenset tid. Samtidig må virksomheten ta hensyn til behovet for å kontrollere tilganger i ettertid. Selv om nødvendig behandling er gitt og behovet for helsehjelp ikke lenger er til stede, kan det bli behov for å bevise eller motbevise et brudd på personopplysningssikkerheten. For logger over tilgang i behandlingsrettet helseregister, er det et gjennomgående behov for lang lagringstid.[44] c) Virksomheten bør vurdere lagringstid for logger i sammenheng med lagringstid for autorisasjonsregisteret. Loggene viser hvem som har hatt tilgang til helse- og personopplysninger, mens autorisasjonsregisteret gir en oversikt over hvilke tilganger ansatte skulle hatt. Det er derfor nødvendig å se disse opplysningene i sammenheng for å kunne oppklare brudd på personopplysningssikkerheten.

[40] Normen 6.0 kapittel 5.4.4 Logging
[41] NSM Grunnprinsipper for IKT-sikkerhet 2.0 – 3.2 Etabler sikkerhetsovervåking
[42] Pasientjournalloven § 25
[43] Normen 6.0 kapittel 5.4.4 Logging
[44] Engelschiøn og Vigerust (2021) lovkommentar til pasientjournalloven § 22