Direktoratet for e-helse

Retningslinjer for logging ved data- og dokumentdeling

Versjon 1.0

HITS 1219:2019

Publikasjonens tittel:
Retningslinjer for logging ved data- og dokumentdeling

Rapportnummer
HITS 1219:2019

Utgitt:
03/2019

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

1 Innledning 5

1.1 Bakgrunn 5

1.2 Målgruppe 5

1.3 Dokumentets omfang og innhold 5

1.4 Begreper brukt i forbindelse med logging 6

2 Formål med logging 7

2.1 Sikkerhet 7

2.1.1 Bygge tillit til hverandre 7

2.1.2 Revisjon av sikkerhetsmekanismer 8

2.1.3 Avdekke unormale hendelser 8

2.2 Feilsøking 9

2.2.1 Teknisk feilsøking 9

2.3 Pasientsikkerhet og personvern 10

2.3.1 Etterprøve tjenstlig behov 10

2.3.2 Innsyn til innbygger 10

2.3.3 Gjennomgang av enkelthendelse 11

2.4 Beslutningsstøtte 12

2.4.1 Statistikk 12

3 Felles krav og prinsipper 13

3.1 Krav 13

3.2 Prinsipper 13

4 Hendelser som skal logges 14

4.1 Logghendelser i ulike rammeverk og standarder 14

4.1.1 DICOM PS3.15 Audit Trail Message Format Profile 14

4.1.2 IHE ATNA 15

4.1.3 FHIR AuditEvent 15

4.1.4 Normen 15

4.1.5 Andre standarder 16

4.2 Loggkategorier 16

4.2.1 Oversikt over loggkategorier som standarder viser til 16

4.2.2 Utvalgte loggkategorier for data- og dokumentdeling 19

4.2.3 Formål "innsyn til innbygger" - Disclosure 21

4.2.4 Formål som ikke er dekt av de valgte loggkategoriene 21
4.3 Logghendelsestyper - underordnet nivå av loggkategorier 22
4.3.1 Loggkategori: Query 22
4.3.2 Loggkategori: Export 23
4.3.3 Loggkategori: Import 23
4.3.4 Loggkategori: RESTful Operation 24
4.3.5 Loggkategori: SOAP Operation 25
4.3.6 Loggkategori: User Authentication 25
4.3.7 Loggkategori: User Authorization 26
4.3.8 Loggkategori: Security Event 26
5 Videre arbeid 27
6 Vedlegg Brukerhistorier med anvendelse av logghendelser 28
6.1 Datadeling 28
6.2 Dokumentdeling 30

1 Innledning

1.1 Bakgrunn

Data- og dokumentdeling tas i bruk på stadig flere områder innen helse- og omsorgstjenesten. En av hovedutfordringene som er meldt inn av sektoren til Direktoratet for e-helse er at krav og retningslinjer for logging tolkes og implementeres ulikt i sektoren. Ved en kartlegging av denne hovedutfordringen ble det funnet 10 konkrete utfordringer:

1. Det er uklare formål med hvorfor vi logger.
2. Det er uklart hvilke hendelser som skal logges.
3. Virksomheter har forskjellige tolkninger av hva kravene er til logging.
4. Data- og dokumentdeling kan ha lange kallkjeder med uklar ansvarfordeling for logging.
5. Ved logging kan innholdet potensielt baseres på informasjon som stammer fra mange kilder. Det er uklart hvilke kilder som skal benyttes.
6. Det kan bli potensielt veldig mange API-er å forholde seg til og logging må løses for alle.
7. Manglende standardisering av samme informasjon i ulike logger.
8. Logging håndteres som en generisk funksjon som benyttes i mange ulike use case som har ulike krav til logging.
9. Uklare retningslinjer for bruk av fødselsnummer i logger.
10. En generell utfordring er at det logges for mye for å være på den sikre siden.

Ved utarbeidelse av dette dokumentet ble de 3 første utfordringen valgt ut og dette dokumentet skal da svare ut disse utfordringene. Dokumentet vil også være et godt grunnlag for å svare ut de resterende utfordringene.

Arbeidet med dokumentet er gjort i tett samarbeid med Helsenorge, Velferdsteknologisk knutepunkt, NHN og sekretariatet for Normen. I tillegg er arbeidet forankret med sektoren.

1.2 Målgruppe

Arkitekter, prosjektledere og andre som jobber med spesifikasjon og implementering av data- og dokumentdelingsløsninger.

1.3 Dokumentets omfang og innhold

Dokumentet er begrenset til å gjelde kun for data- og dokumentdeling. De kravene og retningslinjene som beskrives i dette dokumentet gjelder for alle komponenter som er involvert ved data- og dokumentdeling. Krav og retningslinjer for logging i dette dokumentet tar utgangspunkt i disse tre utfordringer:

- Det er uklare formål med hvorfor vi logger.
- Det er uklart hvilke hendelser som skal logges.
- Virksomheter har forskjellige tolkninger av hva kravene er til logging.

Besvarelsen av de tre utfordringene skal utlede krav som skal sees på som må-krav ved logging i data- og dokumentdeling, samt til å utlede retningslinjer som skal sees på som bør-

krav. Dokumentet går ikke inn på innholdet i loggingen, dette vil bli beskrevet i et eget dokument.

1.4 Begreper brukt i forbindelse med logging

Følgende sentrale begreper er benyttet i dokumentet:

Term	Alternativ term	Beskrivelse
Logghendelse	AuditEvent, hendelse	En hendelse av en slik karakter at den skal beskrives og lagres i ett eller flere loggdatabaser for å understøtte et loggformål.
Loggkategori	EventTypeID, AuditEvent ID	Loggkategori gir et overordnet nivå av logghendelsen for å knytte tilhørende hendelsestyper til en kategori.
Logghendelsestype	EventTypeCode, Subtype	Logghendelsestype gir en beskrivelse av en konkret type logghendelse
Loggdatabase	AuditEvent Repository	Et lager som mottar loggmeldinger og lagrer de som logginnslag i en lagringsenhet. En fil kan også være en slik loggdatabase.
Logginnslag	AuditEvent Record	Ett innslag i en loggdatabase med beskrivelse av en hendelse.
Loggmelding	AuditEvent Message	En loggmelding sendes fra komponenten hvor logghendelsen oppstår og til loggdatabase hvor den lagres som et logginnslag.
Logging	Audit Trail	Fellesbegrepet på alle aktiviteter som skjer fra en logghendelse trigges til den er lagret i en loggdatabase som et logginnslag.
Sporbarhetslogg	Juridisk logg	En logg som oppfyller strenge krav til integritet, konfidensialitet og tilgjengelighet, samt lengden på lagring. Den skal være egnet som dokumentasjon i juridisk sammenheng.
(En) Logg	Sikkerhetslogg, feilsøkingslogg, innsynslogg, etc.	Den samlede mengden logginnslag som gjør at et formål kan oppnås. En logg kan hentes fra flere loggdatabaser.

Tabell 1 Begreper for logging

2 Formål med logging

En av hovedutfordringen når loggebehov skal avklares er at det er få som har samme formål bak loggebehovet i tankene. Dette fører ofte til at det er vanskelig å enes om hva og hvor mye som skal logges.

For å vite hva som skal logges, er det derfor viktig å forstå hvorfor logging utføres. Det gjelder både hvilke hendelser som skal trigge en logging og hva en logg skal inneholde.

Vi har identifisert åtte formål for logging ved bruk av data- og dokumentdeling. Disse formålene er igjen gruppert i ulike kategorier slik at formål som hører sammen blir knyttet sammen.
Følgende formål er identifisert:

1. Sikkerhet
    a. Bygge tillit til hverandre
    b. Revisjon av sikkerhetsmekanismer
    c. Avdekke unormale hendelser
2. Feilsøking
    a. Teknisk feilsøking
3. Pasientsikkerhet og personvern
    a. Etterprøve tjenstlig behov
    b. Innsyn til innbygger
    c. Gjennomgang av enkelthendelse
4. Beslutningsstøtte
    a. Statistikk

Beskrivelsen av formålene skal gi en bedre forståelse av hvorfor vi logger og hva loggene skal benyttes til slik at hvilke hendelser som skal logges for data- og dokumentdeling blir enklere å spesifisere og implementere.

Formålene er et utgangspunkt for å utlede krav og retningslinjer for logging. I tillegg vil de være et verktøy for prosjekter ved spesifisering av loggebehov.
De påfølgende kapitelene går igjennom formålene.

2.1 Sikkerhet

2.1.1 Bygge tillit til hverandre

Som dataansvarlig i en virksomhet, skal jeg ha den samme forståelsen for krav og retningslinjer for logging, som de virksomheter vi deler data med. Dette for at vi sammen skal kunne sikre at vi har det samme informasjonsgrunnlaget vi trenger for å ha tillit til hverandre.

For å styrke tilliten mellom samhandlingsaktørene er det hensiktsmessig å logge viktige hendelser mellom aktørene, samtidig som at partene forplikter seg til å følge felles krav og retningslinjer til logging. Dette vil sørge for at partene har det samme informasjonsgrunnlaget som skaper et tillitsforhold til hverandre. Dette vil både være tillit til at partene tar sin del av ansvaret for logging, samt at partene sørger for at de tilsammen sammen logger tilstrekkelig informasjon i henhold til lovgivningen, personvern og pasientsikkerheten.

Krav

- Beskrivelse av logging må være en del av avtalen mellom virksomhetene som deler data og dokumenter.

Retningslinjer

- Det bør gjøres en periodisk gjennomgang/test på bruk av logger for å sørge for at det henger helhetlig sammen mellom virksomhetene som deler data og dokumenter.

2.1.2 Revisjon av sikkerhetsmekanismer

Som sikkerhetsansvarlig for en data- eller dokumentdelingsløsning skal jeg kunne få informasjon om alle tilgangsbeslutninger som er gjennomført slik at jeg kan se at disse er overens med de formelle avtalene som er gjort mellom de partene vi deler informasjon med.

Når to virksomheter skal dele data eller dokumenter, må det avtales hvordan tilgangsbeslutninger skal gjennomføres. Dette gjelder både hvem som gjør hva, hvilke regler som skal gjelde og hvilke kontroller som er utført av hvem. Kontroller kan være håndhevelse av sperreregler, kontroll av virksomhetssertifikater, verifikasjon av signaturer mv.

Det er behov for å logge håndhevelse av disse reglene for å kunne gjøre en revisjon opp mot hva som er avtalt mellom samarbeidsaktørene. Slike revisjoner må gjennomføres av begge virksomhetene.

Krav

- Tilgangen til loggene skal begrenses til ansvarlige for sikkerhet i virksomhetene.
- Innbygger skal ikke ha tilgang til disse loggene.

Retningslinjer

- Loggen bør støtte bruk av verktøy og filtrering for å behandle dataene.
- Sensitive personopplysninger bør unngås i logger for dette formålet.

2.1.3 Avdekke unormale hendelser

Som sikkerhetsansvarlig skal jeg i "nær sanntid" få informasjon om unormale hendelser i data- eller dokumentdelingsløsningen slik at jeg umiddelbart kan sette i gang tiltak.

Det er flere komponenter i en data- og/eller dokumentdelingsløsning som kan bistå i å avdekke unormale hendelser i sanntid eller "nær sanntid". Et eksempel er gjentagende

brukerautorisasjoner. Dersom det gjøres autorisasjon av den samme brukeren mange ganger etter hverandre, vil dette ansees som en unormal hendelse som bør undersøkes.

Informasjon fra logging kan gi advarsler om mulige brudd på sikkerhet i "nær sanntid", slik at manuelle eller automatiske tiltak kan settes i gang for å forhindre flere sikkerhetsbrudd.

Retningslinjer

- Loggene bør benyttes av virksomhetens system for sikkerhetsovervåkning og hendelseshåndtering.
- Lagringstid på logger må avklares med det behovet virksomhetens sikkerhetsorganisasjon har for å kunne analysere logger tilbake i tid.

2.2 Feilsøking

2.2.1 Teknisk feilsøking

Som systemeier for komponentene i data- eller dokumentdelingsløsningen, skal jeg kunne få tilstrekkelig teknisk informasjon om hendelser i systemet mitt, slik at jeg kan finne årsak og hvor feilsituasjonen oppstår.

Alle tekniske komponenter i en data- eller dokumentdelingsløsning må logge med det formål om å bistå i teknisk feilsøking (eng. debugging). Dette for å både kunne finne ut hvor det feiler og hva som feiler når system eller bruker opplever en feilsituasjon. Det må logges tilstrekkelig informasjon til å kunne gjenskape feilsituasjonen.

I data- og dokumentdelingsløsninger vil det være flere systemeiere for de ulike komponentene og disse vil ha hvert sitt ansvarsområde. Det er også sannsynlig at det vil være driftspersonell og/eller leverandører som vil gjøre feilsøkingen på vegne av systemeierne.

Eksempel:

En lege gjør et søk etter et dokument vedkommende vet at finnes i en annen virksomhet, men får det ikke opp. Legen melder dette som feil i sin virksomhets interne brukerstøtte. Systemeier for dokumentregisteret får etterhvert saken og tekniske logger i dokumentregisteret brukes til å søke etter feilen. Den tekniske loggen viser en feil i mappingen av metadata ved søk.

Dette formålet har som hensikt å kunne gjøre detaljert, teknisk feilsøking i de enkelte komponentene og ikke nødvendigvis på tvers av virksomhetene.

Retningslinjer

- Innholdet i logg som skal brukes til teknisk feilsøking bør ikke inneholde sensitive personopplysninger (personvernprinsippet). Innholdet bør være detaljert, men ikke mer enn nødvendig (dataminimeringsprinsippet)
- Det bør skilles på ulike detaljeringsnivåer av feilsøkingslogging. Det bør foreligge et overordnet nivå som alltid vil være på og ett eller flere underordnede nivåer som kan slås på i en feilsituasjon for å fremskaffe en mer detaljert logg i en tidsbegrenset periode.

- Det skal ikke være behov for å lagre innholdet i denne type logg over veldig lang tid, da en feilsituasjon ofte er en tidsbegrenset hendelse. Dersom det er behov for lengre lagringstid, er det fordi loggen skal brukes til et annet formål. Det bør da vurderes å benytte ulike logger for ulike formål og lagringstid.
- En teknisk feilsøkingslogg trenger ikke oppfylle kravene til en sporbarhetslogg.

2.3 Pasientsikkerhet og personvern

2.3.1 Etterprøve tjenstlig behov

Som dataansvarlig skal jeg ha tilgang til informasjon om hvilket personell som har hatt tilgang til eller forsøkt å få tilgang til helseopplysninger om pasienter slik at jeg kan vurdere om de har hatt tjenstlig behov for innsynet.

Tilgangen som helsepersonell har til data og dokumenter på tvers av virksomheter skal alltid begrunnes ut i fra et tjenstlig behov. Hvorvidt dette stemmer, skal være mulig å etterprøve, for eksempel ved hjelp av mønstergjenkjenning over et større tidsrom eller ved stikkprøver av enkelttilganger. Første vurdering av om tilgang er gitt ut ifra tjenstlig behov, er basert på informasjon innenfor egen virksomhet. Dersom det er en mistanke som krever informasjon som er logget i andre virksomheter, kan en løsning være at logger utleveres mellom virksomhetene.

Loggen vil kun vise den informasjonen systemet har for det tjenstlige behovet. Vurderingen om den informasjonen er korrekt satt, krever andre rutiner og kunnskap enn det som kommer frem av loggen.

Krav

- Det må foreligge en felles identifikator i loggene, som gjør at flere logginnslag fra en eller flere virksomheter kan sammenstilles. Dette kan være en logghendelses-id eller sammensettingen av personidentifikasjon og tidspunkt.

Retningslinjer

- Logger etter dette formål skal følge samme retningslinjer for lagringstid som de delte helse- og personopplysningene. Se Normens faktaark 25[1].

2.3.2 Innsyn til innbygger

Som innbygger skal jeg elektronisk kunne lese og forstå hvem som har hatt tilgang til helseopplysninger om meg, eller en jeg har fullmakt for, og hvorfor slik at jeg kan vurdere om noen har hatt urettmessig tilgang.

[1] https://ehelse.no/Documents/Normen/Faktaark%2025%20-%20Lagringstid%20og%20sletting%20av%20helse-%20og%20personopplysninger.pdf

Logg som viser innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger er et antisnoke-tiltak for å avdekke uberettigede pasientoppslag. Pasientjournalloven § 18 beskriver ikke eksplisitt en rett til et slikt innsyn, men henviser til personvernforordningen artikkel 13 og 15 som angir hovedreglene knyttet til den registrertes innsyn. Det følger av artikkel 15 at den registrerte har rett til informasjon om mottakerne eller kategoriene av mottakere som personopplysninger har blitt utlevert til.

Innbygger vil også kunne benytte innsynsloggen til å se om helsepersonell som burde gjort innsyn ifm. tjenstlig behov, også faktisk har benyttet seg av det, men dette er ikke en del av bakgrunnen for formålet.

Krav

- Innbygger har rett på informasjon om hvilken informasjon i en virksomhet som helsepersonell i en annen virksomhet har fått innsyn i. Dette kan løses ved hjelp av at Innbygger får elektronisk innsyn i logg over bruk. Informasjonen i en slik logg må inneholde hvem som har gjort innsynet (både navn, hvilken rolle og hvor vedkommende organisatorisk jobber (det laveste nivået) på tidspunktet innsynet ble gjort), formålet for innsyn og i hvilket tidsrom innsynet ble gjort.
- Logginnslaget til dette formålet skal være lesbart og forståelig for innbygger. Det vil si at det ikke kun kan logges koder, men også beskrivende informasjon må være inkludert.
- En hendelse etter dette formålet vil potensielt resultere i mange logginnslag hos flere virksomheter. Kun et logginnslag skal lagres og det er den virksomheten som deler som er ansvarlig for å logge etter dette formålet.

Retningslinjer

- Dersom opphavet til et innsyn er en tjeneste (maskin) uten at det direkte er helsepersonell involvert, bør dette komme tydelig frem for innbygger.
- Logger etter dette formål skal følge samme retningslinjer for lagringstid som de delte helse- og personopplysningene. Se Normens faktaark 25[2].

2.3.3 Gjennomgang av enkelthendelse

Som ansvarlig for pasientsikkerhet ved en virksomhet skal jeg få samlet informasjon om en enkelthendelse slik jeg kan følge opp den konkrete hendelsen.

Det er ønskelig med en logg som gir tilstrekkelig informasjon til å gjøre en gjennomgang i etterkant av en hendelse, for å se hva som har skjedd i en konkret enkeltsituasjon.

En enkelt logg vil ikke nødvendigvis inneholde all informasjon for dette formålet. Første vurdering av en virksomhet kan være basert på informasjon fra egen logg, men dersom det er en mistanke som krever informasjon som er logget i andre virksomheter, kan en løsning være at logger utleveres mellom virksomhetene.

[2] https://ehelse.no/Documents/Normen/Faktaark%2025%20-%20Lagringstid%20og%20sletting%20av%20helse-%20og%20personopplysninger.pdf

Eksempel:

En lege har på grunn av sperring ikke fått tilgang til viktig informasjon og pasient blir feilbehandlet på bakgrunn av manglende informasjon. Gjennomgang av hendelsen og bruk av logg viser at legen ikke har skyld i dette fordi sperring er håndhevet riktig.

Krav

- Det må være en felles identifikator i loggene som gjør at flere logger fra en eller flere virksomheter kan sammenstilles for en enkelthendelse. Dette kan være en logghendelses-id eller sammensettingen av personidentifikasjon og tidspunkt.

2.4 Beslutningsstøtte

2.4.1 Statistikk

Som beslutningstager for en data- og dokumentdelingsløsning skal jeg kunne få statistisk informasjon over hvordan tjenesten benyttes slik at jeg kan fatte beslutninger på dokumentert grunnlag.

Statistikk over bruken i en data- eller dokumentdelingsløsning vil kunne gi nyttig informasjon til interessenter og beslutningstagere.

Hva slags type statistikk som er aktuelt å fremskaffe fra logger og hvilke beslutninger som kan tas på grunnlag av disse, kan være mange. Her er noen eksempler:

- For å vite om trender i løsningen og hvilke områder som bør prioriteres dersom løsningen skal utvides:
    - Hvilke data/dokumenttyper som brukes mest og minst av helsepersonell?
    - Hvilke typer dokumenter gjør innbygger mest innsyn i?
    - Hvilke samarbeidsområder gjøres det flest oppslag i?
- For å vite om ytelsen på løsningen er god nok eller om den bør forbedres:
    - Gjennomsnittlig hvor lang tid tar søkene?
    - Gjennomsnittlig hvor mange dokumenter resulterer et søk i?
    - Trendanalyser for kapasitetsplanlegging

Krav

- I logger for statistisk formål skal både innbygger og helsepersonell være anonymisert. Virksomheten som er involvert i data- og dokumentdeling trenger ikke å være anonym i en slik logg.

3 Felles krav og prinsipper

Dette kapittelet beskriver felles krav og retningslinjer er gjeldene for alle formål og som kommer i tillegg til de ovenstående kravene og retningslinjene som er gjengitt under hvert formål i kapittel 2.

I denne versjonen av dokumentet er det ikke innhentet krav og retningslinjer for logging som er beskrevet i andre kilder.

3.1 Krav

- Alle loggmeldinger med personopplysninger skal være krypterte for å sikre konfidensialitet og integritet ved overføring.
- En loggdatabase skal være beskyttet mot uautorisert tilgang og autorisert tilgang skal logges.
- Personopplysninger skal ikke behandles lenger enn det som er nødvendig for å oppnå formålet med behandlingen, jf. personopplysningsloven § 28. Det bør derfor fastsettes konkret lagringstid i normaltilfelle for samtlige logger og/eller logghendelser.
- Dersom flere logger må sammenstilles på tvers av virksomheter for å tjene et formål, må logghendelsene ha synkronisert tid slik at de kan fremstilles kronologisk.
- Logger som ihht. formålet ikke inneholder sensitiv informasjon skal holdes adskilt fra logger som inneholder sensitiv informasjon. Ut over dette, kan logging av ulikt formål samles i samme loggdatabase dersom hensiktsmessig. Det bør i slike tilfeller gjøres vurderinger av ytelse ved spørringer mot store datamengder.
- Alle logger må ha en tilhørende beskrivelse av hvilke(t) formål den understøtter, hvilke krav den tilfredsstiller og beskrivelse av lagringstid for ulike logginnslag som lagres i loggen.

3.2 Prinsipper

- Dataminimeringsprinsippet:
    - Det skal etterstrebes å ha minst mulig duplikater av informasjonen.
    - Istedenfor å duplisere logghendelser kan sikker utlevering av logginnslag erstatte behovet for dupliserte logger. I slike tilfeller bør det avtales på forhånd gode rutiner for å utlevere informasjon mellom parter når det oppstår behov for det.

4 Hendelser som skal logges

Når det oppstår en hendelse som skal rapporteres, benyttes en loggmelding for å sende denne rapporten til en loggdatabase hvor den blir til et logginnslag i en logg. Men hvilke logghendelser skal rapporteres?

Dette kapittelet gir en veiledning på hvilke hendelser innen data- og dokumentdeling som skal rapporteres for å dekke de ulike formålene som er identifisert i kapittel 2.

Informasjonen om hvilke hendelser som skal logges er kategorisert to ulike detaljeringsnivåer:

1. **Loggkategori** gir et overordnet nivå av logghendelsen for å knytte tilhørende hendelsestyper til en kategori.
2. **Logghendelsestype** gir en beskrivelse av en konkret type logghendelse.

Innholdet i en logghendelsene som skal logges, vil være på attributtnivå for logghendelsen og defineres i loggmeldingen eller i logginnslaget. Dette kan deles inn i ulike elementer:

- Informasjon om hvilken hendelse som har skjedd
- Informasjon om hvem som utførte hendelsen
- Informasjon om hvor hendelsen skjedde
- Informasjon om hvem eller hva som hendelsen omhandler

Loggkategorien og logghendelsestypen vil være en del av informasjonen i logginnslagene og gi informasjon om hvilken hendelse som har inntruffet.

4.1 Logghendelser i ulike rammeverk og standarder

Det følgende kapittelet gir en kort introduksjon til noen sentrale rammeverk og standarder, som beskriver hva som skal logges av logghendelser (AuditEvents), samt viser til kilder til mer utfyllende informasjon.

4.1.1 DICOM PS3.15 Audit Trail Message Format Profile

DICOM PS3.15 Security and System Management Profiles inneholder mange profiler rundt sikkerhet. En av profilene er *Audit Trail Message Format*-profilen[3] som beskrive ulike hendelser som skal logges. Den skiller mellom to detaljeringsnivåer; Audit Event ID[4] som er en loggkategori og Audit Event Type Code[5] som er en logghendelsestype.

[3] http://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html
[4] http://dicom.nema.org/medical/dicom/current/output/chtml/part16/sect_CID_400.html
[5] http://dicom.nema.org/medical/dicom/current/output/chtml/part16/sect_CID_401.html

Audit Trail Message Format -profilen er en videreføring av RFC3881-standarden "Security Audit & Access Accountability"[6] som kun ble gjort informativ, mens profilen er en normativ standard for logging.

4.1.2 IHE ATNA

IHE ATNA-profilen definerer en rekke overordnede logghendelser som er knyttet til aktiviteter som gjøres av IHE-aktører eller systemkomponenter (som er gruppert med sikker aktør)[7]. Disse er hovedsakelig sammenfallende med logghendelser beskrevet i DICOM PS3.15 Audit Trail Message Format, men i tillegg har IHE utvidet denne med egne logghendelser.

Ved logging på et mer detaljert nivå, viser IHE ATNA også til DICOM Audit Event Type Code, samtidig som de beskriver loggingen av IHE-transaksjoner i de ulike profilene på dette nivået.

IHE ATNA åpner også for logging av andre hendelser enn de beskrevet i DICOM eller IHE-transaksjonene. En av disse er Disclosure som beskrives i kap. 4.2.3.

4.1.3 FHIR AuditEvent

Hovedformålet med FHIR-ressursen AuditEvent er å vedlikeholde informasjon for sikkerhetslogging, samtidig skal den også kunne brukes for annen type hendelseslogging.

Ressursen AuditEvent refererer til hendelsen som er logget i attributtet *AuditEvent ID*. Hvilket lovlige hendelser som eksisterer er beskrevet i dokumentasjonen[8]. FHIR har for AuditEvent ID tatt utgangspunkt i Audit Event ID fra standarden DICOM PS3.15 Audit Trail Message Format som er de samme loggkategoriene som IHE ATNA også henviser til. I tillegg har FHIR AuditEvent utvidet DICOM standarden med en egen loggkategori; RESTful operation[9].

FHIR AuditEvent bruker attributtet *Subtype*[10] for å gi en detaljert beskrivelse av hvilken hendelsestype som logges. Attributtet er delvis knyttet til Audit Event Type Code fra DICOM PS3.15, men det er i FHIR definert en rekke nye logghendelsestyper som er mer beskrivende for loggkategorien RESTful operation[11].

4.1.4 Normen

Faktaark 15[12] i Normen beskriver krav til logging på et generelt grunnlag:

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*

---

[6] https://tools.ietf.org/html/rfc3881
[7] http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf#nameddest=3_20_Record_Audit_Event__ITI_20
[8] https://www.hl7.org/fhir/valueset-audit-event-type.html#definition
[9] https://www.hl7.org/fhir/codesystem-audit-event-type.html#4.2.12.456.2
[10] https://www.hl7.org/fhir/valueset-audit-event-sub-type.html
[11] https://www.hl7.org/fhir/codesystem-restful-interaction.html#4.2.12.null.2
[12] https://ehelse.no/Documents/Normen/Faktaark%2015%20-%20Logging%20og%20oppfølging%20av%20logger%20v3_1.pdf

b) Infrastruktur

- *Sikkerhetsrelevante hendelser i sikkerhetsbarrierer (for eksempel brannmur og ruter) slik som:*
  - *Alle forsøk på ulovlig tilgang både internt og eksternt*
  - *Alle brudd på regler som forbyr trafikk*
  - *Alle brudd på regler som slipper inn lovlig trafikk fra eksterne tilknytninger*
- *Alle forsøk på uautorisert bruk av nettverksoperativsystemer*

4.1.5 Andre standarder

ISO-standarden *Health informatics - Audit trails for electronic health records (ISO 27789:2013)* kan også ses på som en videreutvikling av *RFC 3881-standarden*[13]. Både DICOM PS3.15 Audit Trail Message Format, IHE ATNA og FHIR AuditEvent stammer fra RFC 3881, men mer som en del av et historisk perspektiv. ISO-standarden er ikke videre vurdert i dette dokumentet.

4.2 Loggkategorier

4.2.1 Oversikt over loggkategorier som standarder viser til

Basert på rammeverkene og standardene beskrevet i kapittel 4.1, viser Tabell 2 en oversikt over de loggkategoriene som standardene viser til. Oversikten gir også en vurdering av hvilke kategorier som antas å være de viktigste for data- og dokumentdeling ("DDD") på et overordnet nivå og som antas vil dekke formålene beskrevet i kapittel 1.

DICOM PS3.15 Audit Trail Message Format og IHE ATNA gir noe ulik tolkning av logghendelsen og i beskrivelsen i tabellen er det prosjektet sin tolkning. For DICOM PS3.15 Audit Trail Message Format og IHE ATNA sine beskrivelser av logghendelsene, henvises det til dokumentasjonen.

Loggkategori	Beskrivelse	Aktuell for DDD?	Kilde
Application Activity	Hendelser i denne kategorien logges når en aktør aktiveres. For DDD er ikke dette viktig, da det er hvilken aktivitet aktøren gjør som formålene trenger informasjon om.	Nei	DICOM PS3.15, FHIR, IHE ATNA
Audit Log Used	Hendelser i denne kategorien logges når en logg har blitt lest eller oppdatert av noe annet enn en innkommet loggmelding. For DDD er dette dekket av andre logghendelser. F.eks. RESTful operation.	Nei	DICOM PS3.15, FHIR, IHE ATNA

[13] https://tools.ietf.org/html/rfc3881

Loggkategori	Beskrivelse	Aktuell for DDD?	Kilde
Begin Transferring DICOM Instances	Hendelser i denne kategorien logges når lagring av en DICOM-instans starter. Ikke aktuell for DDD, men dersom dokumentdeling for bilder blir utbredt kan det vurderes.	Nei	DICOM PS3.15, FHIR, IHE ATNA
DICOM Instances Accessed	Hendelser i denne kategorien logges når en DICOM-instans opprettes, leses, oppdateres eller slettes. Ikke aktuell for DDD, men dersom dokumentdeling for bilder blir utbredt kan det vurderes.	Nei	DICOM PS3.15, FHIR, IHE ATNA
DICOM Instances Transferred	Hendelser i denne kategorien logges når lagring av en DICOM-instans er gjennomført. Ikke aktuell for DDD, men dersom dokumentdeling for bilder blir utbredt kan det vurderes.	Nei	DICOM PS3.15, FHIR, IHE ATNA
DICOM Study Deleted	Hendelser i denne kategorien logges når en DICOM-studie er slettet. Ikke aktuell for DDD, men dersom dokumentdeling for bilder blir utbredt kan det vurderes.	Nei	DICOM PS3.15, FHIR, IHE ATNA
Export (PHI-export)[14]	Hendelser i denne kategorien logges når data har blitt eksportert ut av et system. Dette kan være når et dokumentlager gir fra seg et dokument(-sett) til en dokumentkonsument.	Ja	DICOM PS3.15, FHIR, IHE ATNA
Import (PHI-Import)[15]	Hendelser i denne kategorien logges når data har blitt importert inn i et system. Dette kan være når en dokumentkonsument får et dokument(-sett) fra et dokumentlager.	Ja	DICOM PS3.15, FHIR, IHE ATNA
Network Entry	Hendelser i denne kategorien logges når et system eller maskin har entrer eller forlater et (sikkert) domene/nettverk. Ikke aktuelt da DDD forholder seg til klienter og ikke maskinen bak.	Nei	DICOM PS3.15, FHIR, IHE ATNA
Order Record	Hendelser i denne kategorien logges når en (arbeids-)order er opprettet, lest, oppdatert eller slettet. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre logghendelser ivareta logging for dette.	Nei	DICOM PS3.15, FHIR, IHE ATNA

[14] IHE ATNA sin term på hendelsen. PHI står for Protected Health Information.
[15] Se fotnote over

Loggkategori	Beskrivelse	Aktuell for DDD?	Kilde
Patient Record	Hendelser i denne kategorien logges når informasjon om en pasient er opprettet, lest, oppdatert eller slettet. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre logghendelser ivareta logging for dette.	Nei	DICOM PS3.15, FHIR, IHE ATNA
Procedure Record	Hendelser i denne kategorien logges når informasjon om en prosedyre er opprettet, lest, oppdatert eller slettet. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre logghendelser ivareta logging for dette.	Nei	DICOM PS3.15, FHIR, IHE ATNA
Query (Query Information)[16]	Hendelser i denne kategorien logges når et søk utføres. Dette kan være når en dokumentkonsument gjør et søk etter dokumenter for en pasient, enten via et koblingspunkt (XCA) eller mot et dokumentregister.	Ja	DICOM PS3.15, FHIR, IHE ATNA
Security Alert	Hendelser i denne kategorien logges når en gjør endringer på sikkerhetsmekanismene i applikasjoner (eller maskinvare) som prosesserer sikkerhetsinformasjon.	Nei	DICOM PS3.15, FHIR, IHE ATNA, Normen
User Authentication	Hendelser i denne kategorien logges når en brukerautentisering er forsøkt. Både de som blir godkjent og ikke godkjent skal logges.	Ja	DICOM PS3.15, FHIR, IHE ATNA
RESTful operation	Hendelser i denne kategorien logges når en RESTful-operasjon blir utført ihht. FHIR.	Ja	FHIR
Health-service-event	Hendelser i denne kategorien logges når en helsetjeneste blir gjennomført. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre loggkategorier ivareta logging for dette.	Nei	IHE ATNA
Medication	Hendelser i denne kategorien logges når medikamenter administreres. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre loggkategorier ivareta logging for dette.	Nei	IHE ATNA

[16] IHE ATNA sin term på hendelsen.

Loggkategori	Beskrivelse	Aktuell for DDD?	Kilde
Patient-care-assignment	Hendelser i denne kategorien logges når behandlere knyttes til en helsehjelpsepisode. Både ved oppstart, men også endring i roller eller autorisasjon. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre loggkategorier ivareta logging for dette.	Nei	IHE ATNA
Patient-care-episode	Hendelser i denne kategorien logges når spesielle hendelser skjer i en helsehjelpsepisode. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre loggkategorier ivareta logging for dette.	Nei	IHE ATNA
Patient-care-protocol	Hendelser i denne kategorien logges ved ulike aktiviteter for timeoppfølging for en pasient. Det kan være innkalling, oppdateringer og endringer, kanselleringer etc. Dette er ikke aktuelt i dokumentdeling, og for datadeling vil andre loggkategorier ivareta logging for dette.	Nei	IHE ATNA
User Authorization	Hendelser i denne kategorien logges når det gjøres en autorisasjon på en bruker. Både positivt og negativ autorisasjon skal logges.	Ja	Normen
Security Event	Hendelser i denne kategorien skal logges når det skjer en aktivitet i sikkerhetsmekanismer i data- og dokumentdelingsløsningen.	Ja	Normen

Tabell 2 Loggkategorier - overordnede logghendelser

4.2.2 Utvalgte loggkategorier for data- og dokumentdeling

Oppsummert er det valgt ut syv loggkategorier fra standardene som skal benyttes ved logging for data- og dokumentdeling:

1. Export
2. Import
3. Query
4. User Authentication
5. RESTful operation
6. User Authorization
7. Security Event

I tillegg er det behov for en loggkategori som dekker SOAP operations.

Tabell 3 oppsummerer de lovlige loggkategoriene for data- og dokumentdeling.

Logg-kategori	Beskrivelse	Benyttes for	Skal dekke formål
Export	Hendelser i denne kategorien logges når data har blitt eksportert ut av et system når dokumentdeling benyttes.	Dokumentdeling	Etterprøve tjenstlig behov Gjennomgang av enkelthendelse Bygge tillit til hverandre
Import	Hendelser i denne kategorien logges når data har blitt importert inn i et system når dokumentdeling benyttes	Dokumentdeling	Etterprøve tjenstlig behov Gjennomgang av enkelthendelse Bygge tillit til hverandre
Query	Hendelser i denne kategorien logges når et søk utføres når dokumentdeling benyttes. Dette kan være når en dokumentkonsument gjør et søk etter dokumenter for en pasient, enten via et koblingspunkt (XCA) eller mot et dokumentregister.	Dokumentdeling	Etterprøve tjenstlig behov Gjennomgang av enkelthendelse Bygge tillit til hverandre
User Authentication	Hendelser i denne kategorien logges når en brukerautentisering er forsøkt. Både de som blir godkjent og ikke godkjent skal logges.	Data- og dokumentdeling	Revisjon av sikkerhetsmekanismer Avdekke unormale hendelser Gjennomgang av enkelthendelse Bygge tillit til hverandre
RESTful operation	Hendelser i denne kategorien logges når en RESTful-operasjon blir utført. Skal dekke både vanlige REST-operasjoner og FHIR-baserte REST-operasjoner.	Datadeling	Etterprøve tjenstlig behov Gjennomgang av enkelthendelse Bygge tillit til hverandre

Logg-kategori	Beskrivelse	Benyttes for	Skal dekke formål
User Authorization	Hendelser i denne kategorien logges når det gjøres en autorisasjon på en bruker. Både positivt og negativ autorisasjon skal logges.	Data- og dokumentdeling	Revisjon av sikkerhetsmekanismer Avdekke unormale hendelser Gjennomgang av enkelthendelse
Security Event	Hendelser i denne kategorien skal logges når det skjer en aktivitet i sikkerhetsmekanismer i data- og dokumentdelingsløsningen.	Data- og dokumentdeling	Revisjon av sikkerhetsmekanismer Avdekke unormale hendelser Gjennomgang av enkelthendelse
SOAP operation	Hendelser i denne kategorien logges når en SOAP-basert operasjon blir utført og det ikke inngår i en dokumentdelingstransaksjon.	Datadeling	Etterprøve tjenstlig behov Gjennomgang av enkelthendelse

Tabell 3 Lovlige loggkategorier for data- og dokumentdeling.

4.2.3 Formål "innsyn til innbygger" - Disclosure

Det skal benyttes en spesifikk logghendelse knyttet til formålet om "Innsyn til innbygger". Logghendelsestypen som skal benyttes kalles Disclosure. Logghendelser tilsvarer formålet som skal gi innbygger mulighet til å se hvem som har hatt tilgang til sine helseopplysninger. En disclosure-hendelse er i henhold til IHE ATNA en hendelse som logges spesifikt for å vises pasienten. Denne logghendelsen kommer i tillegg til de andre definerte logghendelsene. Det er viktig at denne type hendelse kun logges én gang hos én aktør. Fordelen er at det blir enkelt å hente ut slike logginnslag for f.eks. Helsenorge, men ulempen er at data dupliseres.

Logghendelsestypen skal kunne benyttes i de loggkategoriene som er relevante.

4.2.4 Formål som ikke er dekt av de valgte loggkategoriene

Fra Tabell 3 kan det utledes at to formål ikke er dekt:

1. Teknisk feilsøking
2. Statistikk

Logging for å dekke disse formålene må den enkelte virksomhet selv løse og vil ikke bli videre behandlet i dette dokumentet.

4.3 Logghendelsestyper - underordnet nivå av loggkategorier

En loggkategori er knyttet til en gruppe logghendelsestyper som er et underordnet nivå av en kategori. DICOM PS3.15, FHIR og IHE ATNA er enige om en mengde logghendelsestyper som er beskrivende for enkelthendelser som skal logges[17]. DICOM PS3.15, FHIR og IHE ATNA har derimot ikke gjort en generell kobling av logghendelsestypene opp mot de ulike loggkategoriene. Det er noen få unntak:

- I sine dokumentdelingsprofiler kobler IHE sine definerte transaksjoner opp mot loggkategorier og logghendelsestyper som IHE ATNA har definert. Følgende loggkategorier benyttes i dokumentdeling:
    - Query
    - Export
    - Import
- FHIR AuditEvent beskriver på samme måte hvilke logghendelsestyper som inngår i loggkategorien RESTful operation.

Basert på formålene med logging i data- og dokumentdeling, beskrives det i dette kapittelet en kobling av loggkategorier og logghendelsestyper som forventes å være aktuelle for data- og dokumentdeling. Ved implementering kan det være behov for at dette tilpasses.

I resten av dette kapittelet oppsummeres aktuelle logghendelsestyper for data- og dokumentdeling samt en kategorisering av logghendelsestyper basert på IHE, FHIR og en tolkning gjort som en del av arbeidet med utarbeidelsen av dette dokumentet.

4.3.1 Loggkategori: Query

Logghendelsestype	Beskrivelse	Kilde
ITI-18 Registry Stored Query	Hendelsen logges når transaksjonen IHE XDS ITI-18 sendes fra en dokumentkonsument til et dokumentregister eller et koblingspunkt	IHE ATNA/XDS
ITI-38 Cross Gateway Query	Hendelsen logges når transaksjonen IHE XCA ITI-38 sendes fra et koblingspunkt til et annet.	IHE ATNA/XCA
Disclosure	Hendelsen logges med formål "innsyn til innbygger". Hendelsen skal logges i tillegg de de overnevnte hendelsestypene, men kun en gang av en aktør.	IHE ATNA

Tabell 4 Logghendelsestyper for Query

[17] http://dicom.nema.org/medical/dicom/current/output/chtml/part16/sect_CID_401.html

4.3.2 Loggkategori: Export

Logghendelsestype	Beskrivelse	Kilde
ITI-39 Cross Gateway Retrieve	Hendelsen logges når transaksjonen IHE XCA ITI-39 sendes fra koblingspunktet som leverer fra seg dokument(er) til koblingspunktet som mottar.	IHE ATNA/XCA
ITI-41 Provide and Register Document Set-b	Hendelsen logges når transaksjonen IHE XDS ITI-41 benyttes av en dokumentkilde for å levere fra seg dokument(er) til et dokumentlager.	IHE ATNA/XDS
ITI-42 Register Document Set-b	Hendelsen logges når et dokumentlager leverer fra seg metadata om et dokument(sett) til et dokumentregister ved bruk av transaksjonen IHE XDS ITI-42	IHE ATNA/XDS
ITI-43 Retrieve Document Set	Hendelsen logges når et dokumentlager leverer fra seg et dokument(sett) til en dokumentkonsument ved bruk av transaksjonen IHE XDS ITI-43	IHE ATNA/XDS
Disclosure	Hendelsen logges med formål "innsyn til innbygger". Hendelsen skal logges i tillegg de de overnevnte hendelsestypene, men kun en gang av en aktør.	IHE ATNA

Tabell 5 Logghendelsestyper for Export

4.3.3 Loggkategori: Import

Logghendelsestype	Beskrivelse	Kilde
ITI-39 Cross Gateway Retrieve	Hendelsen logges når transaksjonen IHE XCA ITI-39 mottas i koblingspunktet som får dokument(er) fra koblingspunktet som leverer fra seg.	IHE ATNA/XCA
ITI-41 Provide and Register Document Set-b	Hendelsen logges når transaksjonen IHE XDS ITI-41 gjennomføres og et dokumentlager mottar dokument(er) fra en dokumentkilde.	IHE ATNA/XDS
ITI-42 Register Document Set-b	Hendelsen logges når et dokumentlager mottar metadata om et dokument(sett) fra et dokumentlager ved bruk av transaksjonen IHE XDS ITI-42	IHE ATNA/XDS
ITI-43 Retrieve Document Set	Hendelsen logges når en dokumentkonsument mottar et	IHE ATNA/XDS

Logghendelsestype	Beskrivelse	Kilde
	dokument(sett) fra et dokumentlager ved bruk av transaksjonen IHE XDS ITI-43	
Disclosure	Hendelsen logges med formål "innsyn til innbygger". Hendelsen skal logges i tillegg de de overnevnte hendelsestypene, men kun en gang av en aktør.	IHE ATNA

Tabell 6 Logghendelsestyper for Import

4.3.4 Loggkategori: RESTful Operation

FHIR AuditEvent-ressursen beskriver et litt mer detaljert nivå av logghendelsen i attributtet SubType[18].

"RESTful operation" dekker REST med FHIR, men de underordnede logghendelsene vil også være dekkende for vanlig REST-operasjoner også.

Logghendelsestype	Beskrivelse	Kilde
Read	Hendelsen logges når den nåværende statusen til en ressurs leses	FHIR AuditEvent
Vread	Hendelsen logges når en spesifikk versjon av statusen til en ressurs leses	FHIR AuditEvent
Update	Hendelsen logges når det gjøres en oppdatering av en eksisterende ressurs ved bruk av dens id (eller opprettelse om den er ny)	FHIR AuditEvent
Patch	Hendelsen logges når det gjøres en oppdatering av en eksisterende ressurs ved at det postes ett sett av endringer til den	FHIR AuditEvent
Delete	Hendelsen logges når en ressurs slettes	FHIR AuditEvent
History	Hendelsen logges når endringshistorikken til en spesiell ressurs, en type ressurs eller et helt system, hentes ut.	FHIR AuditEvent
History-instance	Hendelsen logges når endringshistorikken til en spesiell ressurs hentes ut	FHIR AuditEvent
History-type	Hendelsen logges når endringshistorikken til alle ressurser av en spesiell type hentes ut	FHIR AuditEvent
History-system	Hendelsen logges når endringshistorikken til alle ressurser i et system hentes ut	FHIR AuditEvent

[18] https://www.hl7.org/fhir/valueset-audit-event-sub-type.html

Logghendelsestype	Beskrivelse	Kilde
Create	Hendelsen logges når det opprettes en ny ressurs ved bruk av en serveropprettet id	FHIR AuditEvent
Search	Hendelsen logges når det gjøres et søk på en ressurstype eller alle ressurser, basert på et filterkriterie	FHIR AuditEvent
Search-type	Hendelsen logges når det gjøres et søk på en ressurstype basert på et filterkriterie	FHIR AuditEvent
Search-system	Hendelsen logges når det gjøres et søk på alle ressurser basert på et filterkriterie	FHIR AuditEvent
Capabilities	Hendelsen logges når man får en kapabilitetsuttalelse for et system	FHIR AuditEvent
Transaction	Hendelsen logges når det oppdateres, opprettes eller slettes ett sett av ressurser som en enkelttransaksjon	FHIR AuditEvent
Batch	Hendelsen logges når det utføres et sett med separate interaksjoner i en enkelt http-operasjon	FHIR AuditEvent
Operation	Hendelsen logges når det utføres en operasjon som definert av en "OperationDefinition"	FHIR AuditEvent
Disclosure	Hendelsen logges med formål "innsyn til innbygger". Hendelsen skal logges i tillegg de de overnevnte hendelsestypene, men kun en gang av en aktør.	IHE ATNA

Tabell 7 Logghendelsestyper for RESTful operation

4.3.5 Loggkategori: SOAP Operation

Dokumentdeling er basert på SOAP-tjenester og loggkategoriene Query, Export og Import skal dekke transaksjoner tilknyttet disse. For andre SOAP-tjenester skal denne loggkategorien benyttes. Det er foreløpig ikke meldt inn behov for bestemte logghendelser.

4.3.6 Loggkategori: User Authentication

Logghendelsestype	Beskrivelse	Kilde
Authentication Decision	Hendelsen logges når det gjøres en autentiseringsavgjørelse for en bruker	DICOM PS3.15, IHE ATNA

Tabell 8 Logghendelsestyper for User Authentication

4.3.7 Loggkategori: User Authorization

Logghendelsestype	Beskrivelse	Kilde
Authorization Decision	Hendelsen logges når det gjøres en autorisasjonsavgjørelse for en bruker	DICOM PS3.15, IHE ATNA

Tabell 9 Logghendelsestyper for User Authorization

4.3.8 Loggkategori: Security Event

Logghendelsestype	Beskrivelse	Kilde
Node Authentication	Hendelsen logges når en node-autentisering er forsøkt. Både negativt og positivt utfall logges.	DICOM PS3.15, FHIR, IHE ATNA
Emergency Override Started	Hendelsen logges når det tas en avgjørelse om å bruke blålysfunksjonalitet	DICOM PS3.15, FHIR, IHE ATNA
Emergency Override Stopped	Hendelsen logges når en blålyshendelse avsluttes	DICOM PS3.15, FHIR, IHE ATNA
Authentication Decision	Hendelsen logges når en autentiserings-avgjørelse er tatt	DICOM PS3.15, IHE ATNA
Authorization Decision	Hendelsen logges når en autorisasjons-avgjørelse er tatt	DICOM PS3.15, IHE ATNA
Access Control Decision	Hendelsen logges når en adgangskontroll-avgjørelse er tatt	DICOM PS3.15, IHE ATNA
Login	Hendelsen logges når en brukerpålogging er forsøkt.	DICOM PS3.15, FHIR, IHE ATNA
Logout	Hendelsen logges når en brukerutlogging er forsøkt.	DICOM PS3.15, FHIR, IHE ATNA

Tabell 10 Logghendelsestyper for Security Event

5 Videre arbeid

Det er mange utfordringer knyttet til logging ved bruk av data- og dokumentdeling som ikke er besvart i dette dokumentet. Flere av dem er beskrevet kort i innledningen til dokumentet, mens andre er kommet til underveis.

Ett av hovedfokusene har vært å definere formålene for hvorfor det er viktig å logge. Det er utledet en del krav og retningslinjer knyttet til disse formålene. Flere vil fremkomme ved modning og bruk av formålene i diskusjoner i blant annet implementeringsprosjekter. Det vil være behov for å fange opp disse slik at dokumentet kan oppdateres med erfaringer.

De kravene og retningslinjene som er kort beskrevet i kapitel 2 og 3, er kun de som er kommet frem i diskusjoner i utarbeidelsen av dette dokumentet. Det finnes andre krav og retningslinjer tilknyttet logging som er beskrevet i andre normerende dokumenter for både data -og dokumentdeling og for andre anvendelser. Det bør vurderes å samle alle krav og retningslinjer til logging i ett dokument.

Det andre hovedfokuset i dette dokumentet er hvilke logghendelser som er viktige for data- og dokumentdeling. Disse er beskrevet på to nivå og noen av kombinasjonene av disse nivåene er delvis basert på vurderinger sett opp imot formål og gjennomgang av praktiske scenarioer. Gjennom erfaringer fra implementeringsprosjekter kan det være behov for å legge til samt å justere logghendelsestypene og i hvilken loggkategori de bør tilhøre.

Standardene vi har sett på dekker ikke andre tjenester som benytter SOAP. Vi har valgt å definere "SOAP operations" som en ny loggkategori. Det må vurderes om det må defineres egne logghendelsestyper for "SOAP operations".

I videre arbeid må det beskrives hva som skal logges for hver logghendelse slik at det dekker formålet med loggingen. Det vil for eksempel være ulike detaljer som skal logges for "Security Event – Access Control Decision " for formålet "Revisjon av sikkerhetsmekanismer" enn for formålet "Statistikk". Det er derfor behov for å profilere innholdet i logginnslagene slik at det vil være enklere å utvikle loggeløsninger.

De to brukerhistoriene som er beskrevet i vedlegget, tar kun for seg "happy-flow". Det vil si et hendelsesforløp uten feil og problemer. I veien videre er det naturlig å gå igjennom brukerhistorier som feiler underveis, samt se på kjente problemstillinger. En kjent problemstilling er hvor et søk resulterer i en begrenset liste med dokumenter fordi noen av dokumentene som det søkes etter er sperret for den som gjør søket. For formålet "Gjennomgang av enkelthendelse" vil det være interessant å vite hvorfor resultatlisten så ut som den gjorde. Per i dag er det ingen klar løsning for dette basert på logghendelsene som er beskrevet, men svaret kan ligge i detaljene for en logghendelse og at man må utvide logghendelsestypene slik at de dekker håndhevelse av personvernregler.

6 Vedlegg Brukerhistorier med anvendelse av logghendelser

Vi har gjennomgått to brukerhistorier for å se på anvendelsen av logghendelsene i data- og dokumentdeling.

Det er definert noen forutsetninger ved anvendelse av logghendelsene som gjelder for begge:

- Det er en synkron flyt og logging av hendelsen skjer når responsen mottas
- Loggingen beskriver ikke feilsituasjoner, kun positiv flyt.

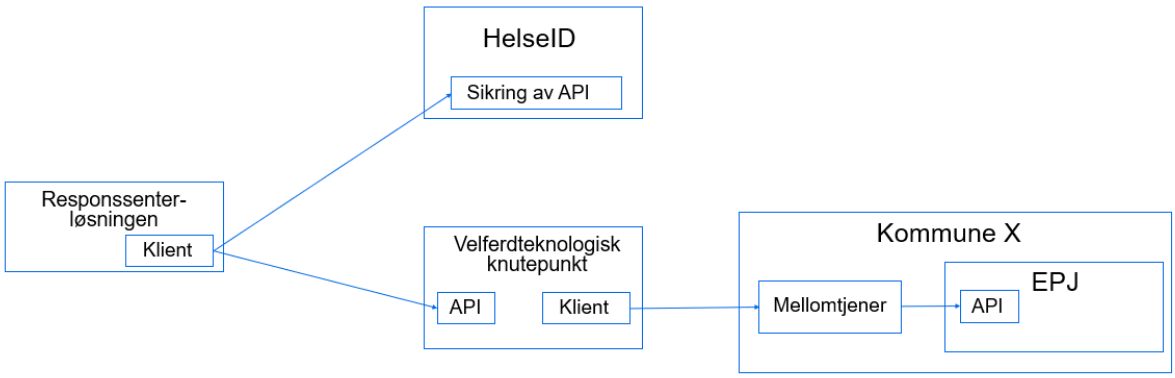
I tillegg er det beskrevet forutsetninger som gjelder for hver av brukerhistoriene.

6.1 Datadeling

Brukerhistorie: Responssentertjenesten (RT) ønsker å sende en forespørsel til velferdsteknologisk knutepunkt (VKP), om å hente ut basisopplysninger om alle tjenestemottakere som har aktiv GPS-lokaliseringstjeneste fra samarbeidskommunenes EPJ-systemer. Dette for å unngå å registrere disse opplysningene manuelt.

Forutsetninger:

- Kommune X er dataansvarlig og har delegert ansvaret til VKP å administrere og godkjenne hvilke responssentre som skal få benytte VKP sine API'er og kommunens EPJ-API'er.
- VKP har igjen delegert ansvaret til HelseID for å håndheve hvilke klienter som skal ha tilgang til hvilke API. VKP må administrere hvilke klienter som skal få tilgang
- Det benyttes kun TLS mellom VKP og Kommune X - ingen token. En naturlig videreføring er at Kommune X får støtte for å behandle tilgangstoken.
- Det er kun en EPJ bak hver HER-ID som kontaktes.



Figur 1 Enkel skisse for brukerhistorie til datadeling

1. Responssenterløsningen spør VKP om oppdatert informasjon om tjenestemottakere i en gitt kommune (for en gitt HER-ID).
    a. RT kaller HelseID for å få et tilgangstoken.
    b. HelseID godkjenner klient og utsteder tilgangstoken.
        i. HelseID logger: Security Event – Authentication Decision
        ii. HelseID logger: Security Event – Authorization Decision
    c. RT mottar tilgangstoken fra HelseID
        i. RT logger: Security Event – Authorization Decision
    d. RT kaller VKP sitt API
    e. VKP sjekker om tilgangstoken er gyldig og om HER-ID stemmer
        i. VKP logger: Security Event – Access Control Decision
        ii. VKP logger: Security Event – Authorization Decision
2. VKP spør kommune X sin EPJ om liste med ID'er for mottakere av GPS-lokaliseringstjeneste og mottar svar.
    a. VKP kaller Kommune X sin mellomtjener[19].
    b. Mellomtjeneren i Kommune X godkjenner klient fra VKP
        i. Mellomtjener logger: Security Event – Node Authentication
    c. EPJ mottar kall fra mellomtjener og kontrollerer at det kommer fra riktig klient
        i. EPJ logger: Security Event – Node Authentication
    d. EPJ behandler henvendelsen
    e. EPJ sender svar til VKP med liste over ID'er
        i. EPJ logger: RESTful operation - Search
    f. VKP mottar liste med ID'er fra EPJ
        i. VKP logger: RESTful operation - Search
3. VKP spør deretter om basis personinformasjon for hver tjenestemottaker og samler opp denne informasjonen i form av forekomster av FHIR-ressursen Patient.
    a. VKP kaller Kommune X sin mellomtjener. Forutsetter at sesjonen fra 2b fortsatt er gyldig.
    b. EPJ mottar kall fra VKP og behandler det.
    c. EPJ sender svar til VKP med basis personinformasjon om tjenestemottaker X.
        i. EPJ logger: RESTful operation – Read
    d. VKP mottar basis personinformasjon fra EPJ
        i. VKP logger: RESTful operation – Read
    e. For alle ID'er mottatt i 2e gjentar VKP og EPJ operasjonene 3a til 3d.
4. VKP returnerer listen med tjenestemottakere til RT som svar på kallet i 1d.
    a. VKP bundler informasjonen med tjenestemottakere og sender den til RT
        i. VKP logger: RESTful operation – Batch
    b. RT mottar bundle med oppdatert informasjon om tjenestemottakere av GPS-lokaliseringstjeneste i Kommune X.
        i. RT logger: RESTful operation – Batch

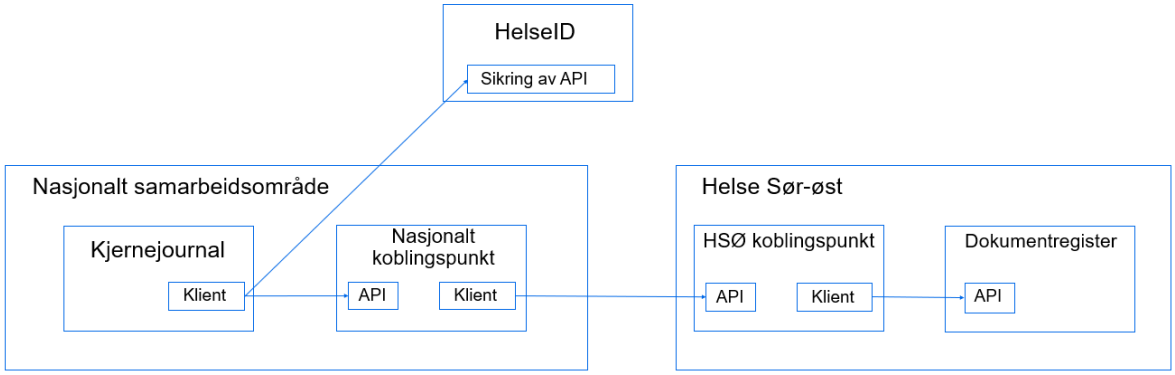
[19] Proxy, API-gateway, e.l.

6.2 Dokumentdeling

Brukerhistorie: Som innlogget helsepersonell i Kjernejournal ønsker jeg å søke etter dokumenter produsert av Helse Sør-øst som inneholder relevante helseopplysninger om en pasient slik at jeg har best mulig oversikt over pasientens helsetilstand og utførte behandlinger/undersøkelser.

Forutsetninger:

- Helsepersonell er allerede pålogget i Kjernejournal



Figur 2 Enkel skisse for brukerhistorie til dokumentdeling

1. Innlogget helsepersonell i Kjernejournal spør fra dokumentdelingsfanen om det finnes dokumenter i andre virksomheter som inneholder relevante helseopplysninger for pasient X.
    a. Kjernejournal kaller HelseID for å få et XUA sikkerhetsbillett.
    b. HelseID godkjenner klient og utsteder XUA sikkerhetsbillett
        i. HelseID logger: Security Event – Authentication Decision
        ii. HelseID logger: Security Event – Authorization Decision
    c. Kjernejournal mottar XUA sikkerhetsbillett.
        i. Kjernejournal logger: Security Event – Authorization Decision
    d. Kjernejournal kaller sitt koblingspunkt for nasjonal dokumentdeling med XUA sikkerhetsbillett (ITI-40[20]) og IHE XDS-transaksjonen ITI-18[21].
2. Koblingspunktet i nasjonalt samarbeidsområde mottar spørringen og oversender den til koblingspunktet i Helse Sør-øst.
    a. Koblingspunktet mottar transaksjonen ITI-40 og sjekker om XUA sikkerhetsbillett er gyldig
        i. Nasjonalt koblingspunkt logger: Security Event – Access Control Decision

[20] IHE ITI-40 Provide X-User Assertion
[21] IHE ITI-18 Registry Stored Query

   b. Koblingspunktet mottar ITI-18 og transformerer den til transaksjonen IHE XCA ITI-38[22] og kaller koblingspunkt for nasjonal dokumentdeling i samarbeidsområdet til Helse Sør-øst
   c. Koblingspunktet mottar transaksjonen ITI-40 og sjekker om XUA sikkerhetsbillett er gyldig
      i. Koblingspunkt Helse Sør-øst logger: Security Event – Access Control Decision
   d. Koblingspunktet kontrollerer klienten som spør (når en TLS-forbindelse opprettes)
      i. Koblingspunktet logger: Security Event – Node Authentication
3. Koblingspunktet i Helse Sør-øst oversender søket til samarbeidsområdets dokumentregister og returnerer svaret til koblingspunktet i nasjonalt samarbeidsområde.
   a. Koblingspunktet mottar ITI-38 og transformerer den til transaksjonen IHE XDS ITI-18 og kaller dokumentregisteret i samarbeidsområdet sammen med XUA sikkerhetsbillett.
   b. Dokumentregisteret mottar ITI-40 og sjekker om XUA sikkerhetsbillett er gyldig
      i. Dokumentregisteret logger: Security Event – Access Control Decision
   c. Dokumentregisteret kontrollerer klienten som spør (når en TLS-forbindelse opprettes)
      i. Koblingspunktet logger: Security Event – Node Authentication
   d. Dokumentregisteret mottar ITI-18 og behandler transaksjonen.
   e. Dokumentregisteret returnerer svar på søket til koblingspunktet
      i. Dokumentregisteret logger: Query – ITI-18
   f. Koblingspunktet i Helse Sør-øst mottar svar på ITI-18 og transformerer transaksjonen til ITI-38
      i. Koblingspunkt Helse Sør-øst logger: Query – ITI-18
   g. Koblingspunktet i Helse Sør-øst sender svar på ITI-38 til koblingspunktet i nasjonalt samarbeidsområde
      i. Koblingspunkt Helse Sør-øst logger: Query – ITI-38
4. Koblingspunktet i nasjonalt samarbeidsområde mottar svar på spørringen og returnerer dette til Kjernejournal for fremvisning til helsepersonell.
   a. Koblingspunktet mottar svar på ITI-38 fra koblingspunktet i Helse Sør-øst og transformerer transaksjonen til ITI-18.
      i. Nasjonalt koblingspunkt logger: Query – ITI-38
   b. Koblingspunktet i nasjonalt samarbeidsområde sender svar på ITI-18 til Kjernejournal
      i. Nasjonalt koblingspunkt logger: Query – ITI-18
   c. Kjernejournal mottar svar på ITI-18 som ble forespurt i 1d og fremviser dette til innlogget helsepersonell.
      i. Kjernejournal logger: Query – ITI-18.

[22] IHE ITI-38 Cross Gateway Query