| Deklareringsområde: Informasjonssikkerhet | Versjon: 4.1<br>Dato: 17.08.2015 |
|---|---|

# VEILEDNING OG SELVDEKLARERING FOR DELOMRÅDE:

Kravnumrene nedenfor referer til Faktaark 38 - Sikkerhetskrav for systemer

| Autorisering | Autentisering | Hendelses-registrering | Pasientrettigheter | Integritet |
|---|---|---|---|---|
| Kravnr. 1 til 18 | Kravnr. 19 til 24 | Kravnr. 25 - 31 | Kravnr. 32 til 35 | Kravnr. 36 til 37 |

## 1 INFORMASJON OM SELSKAP

Tabellen nedenfor bør fylles ut av leverandøren med informasjon om virksomheten og objektet.

| | | |
|---|---|---|
| ***Leverandørnavn:*** | | |
| ***Postadresse:*** | | |
| ***Besøksadresse:*** | | |
| ***Organisasjonsnummer:*** | | |
| ***Kontaktinformasjon:*** | ***Navn på kontaktperson:*** | |
| | ***E-post:*** | ***Telefonnummer:*** |
| ***Objekt:*** | ***Benevnelse på system:*** | ***Hovedversjon:*** |
| | ***Benevnelse delsystem:***[1] | ***Versjon:*** |
| | ***Kommentar for å utdype beskrivelsen av objekt:*** | |
| ***Utfylt:*** | ***Dato:*** | ***Utfylt av person:***<br>☐ Samme som kontaktperson |

1. *Selvdeklareringen kan være avgrenset til et bestemt delsystem. Om selvdeklareringen gjelder hele systemet med alle sine eventuelle delsystemer skal ikke hvert enkelt delsystem beskrives. I slike tilfeller angis kun systemet med en eventuelt utdypende kommentar. Eksempler på delsystem kan være: en modul i systemet, en integrasjon som hører inn under systemet og som leveres med systemet.*

# 2 SELVDEKLARERING AV HENDELSESREGISTRERING

Med hendelsesregistrering menes registrering av tilgang, bruk og forsøk på uautorisert bruk av systemet. Målet er å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

Med hendelsesregister menes et logisk register der hendelser i systemet er ført.

| Krav Nr. 25 | Kravet i Normens kapittel **3.3.4** og **5.2.8** er:<br><br>*Hendelsesregistre med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene, skal tas vare på til det av helsehjelpens karakter ikke lenger antas å bli bruk for.* |
|---|---|
| Hensikt med kravet | Hensikten med kravet er at den databehandlingsansvarlige skal kunne gå så langt tilbake i tid som det er nødvendig og som ikke er tidsmessig bestemt. |
| Veiledende beskrivelse | Systemet må kunne ta vare på hendelsesregistre i den tid databehandler fastsetter. |
| Veiledende eksempel | Det kan om nødvendig etableres en funksjon som muliggjør å "fjernarkivere" hendelsesregistre om databehandlingsansvarlig beslutter å oppbevare disse til evig tid. Hensikten er å unngå for store datasett og eventuelle databaser. |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

| Krav Nr. 26 | Kravet i Normens kapittel **4.4.1** er:<br><br>*Det skal registreres i hendelsesregistre i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang.*<br><br>Kravet i Normens kapittel **5.2.2** er:<br><br>*Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.* |
|---|---|
| Hensikt med kravet | Det er kontrollhensyn som ligger bak kravet om at det skal registreres hvem som har hatt tilgang og når tilgangen har skjedd.<br><br>I tillegg ivaretas den registrertes rettigheter til innsyn i hendelsesregistrene. |
| Veiledende beskrivelse | Hendelsesregistreringen skal være en integrert del av systemet.<br><br>For å oppfylle kravet skal det registreres hvem som har autentisert seg for tilgang.<br><br>Det skal registreres dato og klokkeslett for enhver slik tilgang. |
| Veiledende eksempel | Informasjonselementer (jf. eksempel datamodellen) for hvem som har autentisert seg, kan være:<br><br>– entydig identifikator for brukeren (for eksempel en kombinasjon av navn og ansattnummer)<br><br>– rolle<br><br>– virksomhet og organisatorisk tilhørighet for brukeren<br><br>– identitet til utstyr (for eksempel laboratorieutstyr som benyttes for tilgang til helse- og personopplysinger)<br><br>Dato og klokkeslett anbefales hentet fra operativsystemet. |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

| Krav Nr. 27 | Kravet i Normens kapittel **4.4.2** er:<br><br>*Det skal registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting.* |
|---|---|
| Hensikt med kravet | Det er kontrollhensyn som ligger bak kravet om at det skal registreres hvem som har foretatt registrering, endring, retting og sletting. |
| Veiledende beskrivelse | Hendelsesregistreringen skal være en integrert del av systemet.<br><br>Med "*hvem*", i kravet, menes hvilken person i hvilken rolle og en systemgenerert identitet.<br><br>For å oppfylle kravet skal det registreres hvem som har utført en spesifikk registrering, endring, retting og sletting av helse- og personopplysinger.<br><br>Bruken av den enkelte funksjonen (registreringen, endringen, rettingen og / eller sletting) skal identifiseres og registreres. |
| Veiledende eksempel | Informasjonselementer som skal registreres om hvem som har utført en spesifikk registrering, endring, retting og sletting, kan være:<br><br>– entydig identifikator for brukeren (for eksempel en kombinasjon av navn og ansatt-nummer)<br><br>– rolle<br><br>– virksomhet og organisatorisk tilhørighet for brukeren<br><br>– identitet til utstyr (for eksempel laboratorieutstyr som benyttes for tilgang til helse- og personopplysinger)<br><br>Informasjonselementer som skal registreres om den spesifikke bruken av funksjonen (registreringen, endringen, rettingen og slettingen), kan være<br><br>– unik funksjons-id<br><br>– funksjonsvalg<br><br>– kvittering for gjennomført oppgave |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|
| Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant": | | | |

| Krav Nr. 28 | Kravet i Normens kapittel **5.5.2** er:<br><br>*For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres hendelsesregistre over følgende:*<br>- *Autorisert bruk av informasjonssystemene skal registreres.*<br>- *Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk.*<br>- *Bruk av nødrettstilgang til behandlingsrettet helseregister skal registreres.* |
|---|---|
| Hensikt med kravet | Hensikten med hendelsesregistrering er å forebygge, avdekke og forhindre gjentagelse av sikkerhetsbrudd i informasjonssystemene.<br><br>Hensikten med å hendelsesregistrere bruk av nødrettstilgang, er å kunne følge opp enhver slik bruk som avvik. |
| Veiledende beskrivelse | For å ivareta kravet, må systemet ha funksjonalitet for hendelsesregistrering av:<br><br>1. All autorisert bruk<br><br>Autorisert bruk innebærer at en bruker som har autentisert seg i korrekt rolle utfører lesing (inkl. utskrift), registrering, redigering, retting, sletting og/eller sperring av helse- og personopplysninger.<br><br>2. All bruk av nødrettstilgang<br><br>3. Alle forsøk på uautorisert bruk<br><br>Uautorisert bruk (eller forsøk på uautorisert bruk) inntreffer når en bruker forsøker å logge på systemet med ukorrekte autentiseringskriteria. |
| Veiledende eksempel | |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|
| Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant": | | | |

| Krav Nr. 29 | Kravet i Normens kapittel **5.2.2** er:<br><br>*Følgende skal som minimum registreres i hendelsesregistre:*<br>- *entydig identifikator for den autoriserte brukeren*<br>- *rollen den autoriserte brukeren har ved tilgangen*<br>- *virksomhetstilhørighet*<br>- *organisatorisk tilhørighet til den som er autorisert*<br>- *hvilke type opplysninger det er gitt tilgang til*<br>- *hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer*<br>- *grunnlaget for tilgangen*<br>- *tidspunkt og varighet for tilgangen* |
|---|---|
| Hensikt med kravet | Det er kontrollhensyn som ligger bak kravet om at det skal registreres opplysninger om tilgangen. |
| Veiledende beskrivelse | Det må etableres en funksjonalitet som i et hendelsesregister registrerer følgende opplysninger i forbindelse med bruk av systemet:<br><br>– entydig identifikator for brukeren (for eksempel en kombinasjon av navn og ansattnummer) eller en systemgenerert identitet<br>– rollen den autoriserte brukeren har ved tilgangen<br>– virksomhetstilhørighet for den autoriserte brukeren (enten angivelse av intern tilhørighet, dvs. virksomheten selv eller angivelse av ekstern virksomhet, f.eks. databehandler eller leverandør)<br>– organisatorisk tilhørighet til den som er autorisert (f.eks. avdelingsnavn eller avdelingskode). Kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur<br>– hvilke type opplysninger det er gitt tilgang til. Med ”type” opplysninger menes overordnet: Enten personopplysninger alene eller også helseopplysninger<br>– hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer<br>– grunnlaget for tilgangen (for eksempel yte helsehjelp, nødrettstilgang, administrativ bruk)<br>– tidspunkt og varighet for tilgangen (dato og klokkeslett) |
| Veiledende eksempel | Eksempelvis kan ” *hvilke type opplysninger”*, i kravet, være gitt gjennom:<br>– særlover, forskifter, rundskriv eller spesielle regelverk<br>– nasjonale og internasjonale standarder fagsystemet er knyttet opp til<br>– typer opplysninger fra normer i det enkelte faget (for eksempel blodbank, medisinskgenetikk, klinisk kjemisk lab) |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|
| Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”: | | | |

| Krav Nr. 30 | Kravet i Normens kapittel **5.2.2** er:<br><br>*Ved tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende hendelsesregistreres:*<br>- *hvorfor helseopplysningene er hentet fram*<br>- *hvilke tidsperioder vedkommende har hentet fram helseopplysningene* |
|---|---|
| Hensikt med kravet | Det er kontrollhensyn som ligger bak kravet om at det skal registreres opplysninger om tilgangen som er gitt til annen virksomhet. |
| Veiledende beskrivelse | Dette kravet kan sees sammen med krav 29.<br><br>Det må i tillegge til listen i krav 29 etableres funksjonalitet som i et hendelsesregister registrerer følgende opplysninger i forbindelse med bruk av systemet:<br><br>– hvorfor helseopplysningene er hentet fram<br>– hvilke tidsperioder vedkommende har hentet fram helseopplysningene |
| Veiledende eksempel | Se krav 29 |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|
| Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant": | | | |

| Krav Nr. 31 | Kravet i Normens kapittel **5.5.2** er:<br><br>*Alle hendelsesregistre skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister og tilstedeværelsesregister.* |
|---|---|
| Hensikt med kravet | Hensikten er å identifisere avvik, avdekke sikkerhetsbrudd og forhindre gjentakelse av uønskede hendelser.<br><br>Kravet sikrer også at den registrerte kan ivareta innsynsrettigheter.<br><br>Det er ikke et krav at analyseverktøyene er elektroniske - analysen kan også utføres manuelt. |
| Veiledende beskrivelse | Velger leverandøren å inkludere analyseverktøyet i systemet, er det kravene nedenfor som skal selvdeklareres.<br><br>For å oppfylle krevet, skal det være mulig å gjennomføre definerte søk i registrene.<br><br>Søkene skal resultere i lesbare data, og skal kunne eksporteres til en datafil (for eksempel for å kunne sammenholdes med autorisasjonsregistre og tilstedeværelsesregistre). |
| Veiledende eksempel | Funksjonalitet for predefinerte søk, for eksempel søk etter bruk av nødrettstilgang og søk etter forsøk på uautorisert bruk (for eksempel kjent brukernavn og ukjent passord).<br><br>Eksport til datafil bør skje til vanlig brukte dataformater (for eksempel kommaseparert, tab-separert, dollarfil, regneark). |

| Selvdeklarerer leverandøren kravet? | Ja ☐ | Nei ☐ | Ikke relevant ☐ |
|---|---|---|---|

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":