



Selvdeklareringsordning for programvare i helse- og omsorgssektoren

Deklareringsområde: Informasjonssikkerhet

Versjon: 4.1  
Dato: 17.08.2015

## VEILEDNING OG SELVDEKLARERING FOR DELOMRÅDE:

Kravnumrene nedenfor referer til Faktaark 38 - Sikkerhetskrav for systemer

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

### 1 INFORMASJON OM SELSKAP

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

<b>Leverandørnavn:</b>		
<b>Postadresse:</b>		
<b>Besøksadresse:</b>		
<b>Organisasjonsnummer:</b>		
<b>Kontaktinformasjon:</b>	<b>Navn på kontaktperson:</b>	
	<b>E-post:</b>	<b>Telefonnummer:</b>
<b>Objekt:</b>	<b>Benevnelse på system:</b>	<b>Hovedversjon:</b>
	<b>Benevnelse delsystem:<sup>1</sup></b>	<b>Versjon:</b>
	<b>Kommentar for å utdype beskrivelsen av objekt:</b>	
<b>Utfyllt:</b>	<b>Dato:</b>	<b>Utfyllt av person:</b>
		<input type="checkbox"/> Samme som kontaktperson

1. Selvdeklarasjonen kan være avgrenset til et bestemt delsystem. Om selvdeklarasjonen 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 gjentakelse av sikkerhetsbrudd.

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

<p>Krav Nr.</p> <h1>25</h1>	<p>Kravet i Normens kapittel <b>3.3.4</b> og <b>5.2.8</b> er:</p> <p><i>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.</i></p>		
<p>Hensikt med kravet</p>	<p>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.</p>		
<p>Veiledende beskrivelse</p>	<p>Systemet må kunne ta vare på hendelsesregistre i den tid databehandler fastsetter.</p>		
<p>Veiledende eksempel</p>	<p>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.</p>		
<p>Selvdeklarerer leverandøren kravet?</p>	<p>Ja <input type="checkbox"/></p>	<p>Nei <input type="checkbox"/></p>	<p>Ikke relevant <input type="checkbox"/></p>
<p>Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":</p>			

<p>Krav Nr.</p> <h1>26</h1>	<p>Kravet i Normens kapittel <b>4.4.1</b> er:</p> <p><i>Det skal registreres i hendelsesregistre i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang.</i></p> <p>Kravet i Normens kapittel <b>5.2.2</b> er:</p> <p><i>Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.</i></p>		
<p>Hensikt med kravet</p>	<p>Det er kontrollhensyn som ligger bak kravet om at det skal registreres hvem som har hatt tilgang og når tilgangen har skjedd.</p> <p>I tillegg ivaretas den registrertes rettigheter til innsyn i hendelsesregistrene.</p>		
<p>Veiledende beskrivelse</p>	<p>Hendelsesregistreringen skal være en integrert del av systemet.</p> <p>For å oppfylle kravet skal det registreres hvem som har autentisert seg for tilgang.</p> <p>Det skal registreres dato og klokkeslett for enhver slik tilgang.</p>		
<p>Veiledende eksempel</p>	<p>Informasjonselementer (jf. eksempel datamodellen) for hvem som har autentisert seg, kan være:</p> <ul style="list-style-type: none"> <li>– entydig identifikator for brukeren (for eksempel en kombinasjon av navn og ansattnummer)</li> <li>– rolle</li> <li>– virksomhet og organisatorisk tilhørighet for brukeren</li> <li>– identitet til utstyr (for eksempel laboratorieutstyr som benyttes for tilgang til helse- og personopplysinger)</li> </ul> <p>Dato og klokkeslett anbefales hentet fra operativsystemet.</p>		
<p>Selvdeklarerer leverandøren kravet?</p>	<p>Ja <input type="checkbox"/></p>	<p>Nei <input type="checkbox"/></p>	<p>Ikke relevant <input type="checkbox"/></p>
<p>Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":</p>			

<p>Krav Nr.</p> <h1>27</h1>	<p>Kravet i Normens kapittel 4.4.2 er:</p> <p><i>Det skal registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting.</i></p>		
<p>Hensikt med kravet</p>	<p>Det er kontrollhensyn som ligger bak kravet om at det skal registreres hvem som har foretatt registrering, endring, retting og sletting.</p>		
<p>Veiledende beskrivelse</p>	<p>Hendelsesregistreringen skal være en integrert del av systemet.</p> <p>Med ”hvem”, i kravet, menes hvilken person i hvilken rolle og en systemgenerert identitet.</p> <p>For å oppfylle kravet skal det registreres hvem som har utført en spesifikk registrering, endring, retting og sletting av helse- og personopplysninger.</p> <p>Bruken av den enkelte funksjonen (registreringen, endringen, rettingen og / eller sletting) skal identifiseres og registreres.</p>		
<p>Veiledende eksempel</p>	<p>Informasjonselementer som skal registreres om hvem som har utført en spesifikk registrering, endring, retting og sletting, kan være:</p> <ul style="list-style-type: none"> <li>– entydig identifikator for brukeren (for eksempel en kombinasjon av navn og ansatt-nummer)</li> <li>– rolle</li> <li>– virksomhet og organisatorisk tilhørighet for brukeren</li> <li>– identitet til utstyr (for eksempel laboratoriestyr som benyttes for tilgang til helse- og personopplysninger)</li> </ul> <p>Informasjonselementer som skal registreres om den spesifikke bruken av funksjonen (registreringen, endringen, rettingen og slettingen), kan være</p> <ul style="list-style-type: none"> <li>– unik funksjons-id</li> <li>– funksjonsvalg</li> <li>– kvittering for gjennomført oppgave</li> </ul>		
<p>Selvdeklarerer leverandøren kravet?</p>	<p>Ja <input type="checkbox"/></p>	<p>Nei <input type="checkbox"/></p>	<p>Ikke relevant <input type="checkbox"/></p>
<p>Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:</p>			

<p>Krav Nr.</p> <h1>28</h1>	<p>Kravet i Normens kapittel 5.5.2 er:</p> <p><i>For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres hendelsesregistre over følgende:</i></p> <ul style="list-style-type: none"> <li>- <i>Autorisert bruk av informasjonssystemene skal registreres.</i></li> <li>- <i>Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk.</i></li> <li>- <i>Bruk av nødretts tilgang til behandlingsrettet helseregister skal registreres.</i></li> </ul>		
<p>Hensikt med kravet</p>	<p>Hensikten med hendelsesregistrering er å forebygge, avdekke og forhindre gjentakelse av sikkerhetsbrudd i informasjonssystemene.</p> <p>Hensikten med å hendelsesregistrere bruk av nødretts tilgang, er å kunne følge opp enhver slik bruk som avvik.</p>		
<p>Veiledende beskrivelse</p>	<p>For å ivareta kravet, må systemet ha funksjonalitet for hendelsesregistrering av:</p> <ol style="list-style-type: none"> <li>1. All autorisert bruk</li> </ol> <p>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.</p> <ol style="list-style-type: none"> <li>2. All bruk av nødretts tilgang</li> <li>3. Alle forsøk på uautorisert bruk</li> </ol> <p>Uautorisert bruk (eller forsøk på uautorisert bruk) inntreffer når en bruker forsøker å logge på systemet med ukorrekte autentiseringskriteria.</p>		
<p>Veiledende eksempel</p>			
<p>Selvdeklarerer leverandøren kravet?</p>	<p>Ja <input type="checkbox"/></p>	<p>Nei <input type="checkbox"/></p>	<p>Ikke relevant <input type="checkbox"/></p>
<p>Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":</p>			

<p>Krav Nr.</p> <h1>29</h1>	<p>Kravet i Normens kapittel 5.2.2 er:</p> <p><i>Følgende skal som minimum registreres i hendelsesregistre:</i></p> <ul style="list-style-type: none"> <li>- entydig identifikator for den autoriserte brukeren</li> <li>- rollen den autoriserte brukeren har ved tilgangen</li> <li>- virksomhetstilhørighet</li> <li>- organisatorisk tilhørighet til den som er autorisert</li> <li>- hvilke type opplysninger det er gitt tilgang til</li> <li>- hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer</li> <li>- grunnlaget for tilgangen</li> <li>- tidspunkt og varighet for tilgangen</li> </ul>		
<p>Hensikt med kravet</p>	<p>Det er kontrollhensyn som ligger bak kravet om at det skal registreres opplysninger om tilgangen.</p>		
<p>Veiledende beskrivelse</p>	<p>Det må etableres en funksjonalitet som i et hendelsesregister registrerer følgende opplysninger i forbindelse med bruk av systemet:</p> <ul style="list-style-type: none"> <li>- entydig identifikator for brukeren (for eksempel en kombinasjon av navn og ansattnummer) eller en systemgenerert identitet</li> <li>- rollen den autoriserte brukeren har ved tilgangen</li> <li>- virksomhetstilhørighet for den autoriserte brukeren (enten angivelse av intern tilhørighet, dvs. virksomheten selv eller angivelse av ekstern virksomhet, f.eks. databehandler eller leverandør)</li> <li>- organisatorisk tilhørighet til den som er autorisert (f.eks. avdelingsnavn eller avdelingskode). Kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur</li> <li>- hvilke type opplysninger det er gitt tilgang til. Med "type" opplysninger menes overordnet: Enten personopplysninger alene eller også helseopplysninger</li> <li>- hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer</li> <li>- grunnlaget for tilgangen (for eksempel yte helsehjelp, nødrettstilgang, administrativ bruk)</li> <li>- tidspunkt og varighet for tilgangen (dato og klokkeslett)</li> </ul>		
<p>Veiledende eksempel</p>	<p>Eksempelvis kan " <i>hvilke type opplysninger</i> ", i kravet, være gitt gjennom:</p> <ul style="list-style-type: none"> <li>- særlover, forskifter, rundskriv eller spesielle regelverk</li> <li>- nasjonale og internasjonale standarder fagsystemet er knyttet opp til</li> <li>- typer opplysninger fra normer i det enkelte faget (for eksempel blodbank, medisinskgenetikk, klinisk kjemisk lab)</li> </ul>		
<p>Selvdeklarerer leverandøren kravet?</p>	<p>Ja <input type="checkbox"/></p>	<p>Nei <input type="checkbox"/></p>	<p>Ikke relevant <input type="checkbox"/></p>
<p>Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":</p>			

Krav Nr.  <h1 style="margin: 0;">30</h1>	Kravet i Normens kapittel <b>5.2.2</b> er:  <i>Ved tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende hendelsesregistreres:</i> <ul style="list-style-type: none"> <li>- <i>hvorfor helseopplysningene er hentet fram</i></li> <li>- <i>hvilke tidsperioder vedkommende har hentet fram helseopplysningene</i></li> </ul>		
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.  Det må i tillegg til listen i krav 29 etableres funksjonalitet som i et hendelsesregister registrerer følgende opplysninger i forbindelse med bruk av systemet: <ul style="list-style-type: none"> <li>– hvorfor helseopplysningene er hentet fram</li> <li>– hvilke tidsperioder vedkommende har hentet fram helseopplysningene</li> </ul>		
Veiledende eksempel	Se krav 29		
Selvdeklarerer leverandøren kravet?	Ja <input type="checkbox"/>	Nei <input type="checkbox"/>	Ikke relevant <input type="checkbox"/>
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":			



Krav Nr.  <h1 style="margin: 0;">31</h1>	Kravet i Normens kapittel <b>5.5.2</b> er:  <i>Alle hendelsesregistre skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister og tilstedeværelsesregister.</i>		
Hensikt med kravet	Hensikten er å identifisere avvik, avdekke sikkerhetsbrudd og forhindre gjentakelse av uønskede hendelser.  Kravet sikrer også at den registrerte kan ivareta innsynsrettigheter.  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 selvdeklarerer.  For å oppfylle krevet, skal det være mulig å gjennomføre definerte søk i registrene.  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).  Eksport til datafil bør skje til vanlig brukte dataformater (for eksempel kommaseparert, tab-separert, dollarfil, regneark).		
Selvdeklarerer leverandøren kravet?	Ja <input type="checkbox"/>	Nei <input type="checkbox"/>	Ikke relevant <input type="checkbox"/>
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":			