

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h2>Sikkerhetskrav for systemer</h2>	<b>Støttedokument Faktaark nr. 38</b> Versjon: 3.0 Dato: 01.12.2011

<b>Målgruppe</b>  Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens leder er ansvarlig for at systemer som tas i bruk for behandling av helse- og personopplysninger inneholder nødvendige sikkerhetsløsninger.		
<b>Gjennomføring</b>	Ved anskaffelse av systemer i helse-, sosial og omsorgssektoren skal leverandøren dokumentere at nødvendige sikkerhetsløsninger er etablert. Innkjøper kan benytte sjekklisten i faktaarket som grunnlag for dokumentasjonen.		
<b>Formål</b>	Gi innkjøper av systemer i helse-, sosial og omsorgssektoren et hjelpemiddel for å sikre at systemene inneholder løsninger iht kravene i Normen. Faktaarket skal benyttes som grunnlag for selvdeklareringsordningen for programvare i helse-, omsorgs- og sosialsektoren. Ifm selvdeklareringsordningen utarbeides det detaljerte beskrivelser av hvordan leverandøren kan oppfylle kravene.		
<b>Omfang</b>	Gjelder alle fagsystemer som benyttes til behandling av helse- og personopplysninger i helse-, sosial og omsorgssektoren. For eksempel elektronisk pasientjournal, pasientadministrasjon, laboratoriesystem, rekvisisjon og svar og medisinsk teknisk utstyr som inneholder helse- og personopplysninger		
<b>Hjemmel</b>	Kravene i faktaarket er hjemlet i lov og forskrift (jf. Normen kapittel 1.2). Enkelte tilleggskrav er fastsatt i Normen		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Norm for informasjonssikkerhet</li> <li>• Faktaark 14 - Tilgangsstyring</li> <li>• Faktaark 15 - Hendelsesregistrering og oppfølging</li> <li>• Faktaark 31 - Passord og passordhåndtering</li> </ul>		

### Sikkerhetskrav som skal ivaretas i systemer som behandler helse- og personopplysninger

Kravene nedenfor følger av Normen. For enkelte krav er det angitt en utdypning av kravet som ikke direkte kan leses ut av Normen. Disse er angitt som "Utdypning av kravet:".

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke relevant
<b>Autorisering</b>					
1.	Tilgangsstyring skal etableres for alle behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer	5.2			
2.	Autorisering skal skje selvstendig for hver enkelt rolle	5.2.1			
3.	Ulike ansettelsesforhold skal identifiseres	5.2.1			
4.	All tildeling av autorisasjon skal registreres i et autorisasjonsregister	5.5.2			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke relevant
5.	<p>Databehandlingsansvarlig skal sørge for at det opprettes et autorisasjonsregister. Registeret skal som minimum inneholde:</p> <ul style="list-style-type: none"> <li>- informasjon om hvem som er tildelt autorisasjon</li> <li>- til hvilken rolle autorisasjonen er tildelt</li> <li>- formålet med autorisasjonen</li> <li>- tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt</li> <li>- informasjon om hvilken virksomhet den autoriserte er knyttet til</li> </ul> <p>Utdypning av kravet: Det skal også registreres hvem (fysisk identifiserbar person) som har opprettet (registrert) autorisasjonen</p>	5.2.2			
6.	<p>5 års lagring minimum fra det tidspunkt dokumentet ble tatt ut av bruk:</p> <ul style="list-style-type: none"> <li>- Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregister)</li> </ul>	3.3.4			
7.	<p>Tildelt autorisasjon skal sikre at den enkelte kan få tilgang til nødvendige helse- og personopplysninger i samsvar med personellets ansvar og oppgaver</p> <p>Utdypning av kravet: Tildelt autorisasjon skal kunne tidsavgrenses</p>	5.2.2			
8.	<p>For personer som har ulike roller i virksomheten, skal autorisering skje for hver rolle uavhengig av vedkommendes øvrige roller</p>	5.2.2			
9.	<p>Autorisasjon for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov</p>	5.2.2			
10.	<p>Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger</p>	5.2.2			
11.	<p>Tilgang til behandlingsrettede helseregistre skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten</p>	5.2.3			
12.	<p>Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger</p>	5.5.2			
13.	<p>Hendelsesregistrene, autorisasjonsregister og tilstedeværelsesregister skal sikres mot endring og sletting av uautorisert personell.</p> <p>Hendelsesregistrene skal sikres mot endring og sletting av uautorisert personell</p>	5.2.6 5.5.2			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke relevant
14.	Dersom det er åpnet for nødrettstilgang, skal tekniske tiltak etableres på en slik måte at helsepersonell i nødrettssituasjoner, kan få tilgang til nødvendige helse- og personopplysninger. Slik tilgang skal grunnngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))	5.5.2			
15.	Nødrettstilgang kan etableres som en mulighet for autoriserte brukere til å gi seg selv tilgang uten å følge fastsatte prinsipper for å få tilgang til helse- og personopplysninger	4.4.2			
16.	Begrunnelsen for nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som et avvik.	4.4.2			
17.	Virksomhetens ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister (inkl elektronisk pasientjournal (EPJ)) eller i et fagsystem  Utdypning av kravet: Behandlingsrettet helseregister inkl elektronisk pasientjournal (EPJ) eller fagsystem må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	6.5			
<b>Autentisering</b>					
18.	Autentisering må sikre identifisering i korrekt rolle i hvert enkelt tilfelle.	5.2.1			
19.	Ulike roller skal identifiseres og ved behov gis ulike autentiseringskriteria.	5.2.1			
20.	Ved tilgang til behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer skal ulike ansettelsesforhold identifiseres og gis ulike autentiseringskriteria.	5.2.1			
21.	Flere personer skal ikke benytte samme autentiseringskriteria.  Utdypning av kravet der det ikke benyttes PKI: - Passordet skal kunne byttes enkelt av bruker - Tvunget skifte av passord skal være teknisk mulig - Passordets kvalitet og varighet skal kunne konfigureres	5.2.1			
22.	Tekniske tiltak skal iverksettes slik at personer i eller utenfor virksomheten uansett ressurser og kunnskap ikke skal kunne endre opplysninger uten at det registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har endret og hva som er endret.  Utdypning av kravet der det ikke benyttes PKI: - Passordfil skal krypteres	5.5.2			
23.	Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger	5.5.2			
<b>Hendelsesregistrering</b>					

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke relevant
24.	2 års lagring minimum: Hendelsesregistre med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene. Dersom oppføringer i hendelsesregistre kan knyttes til enkeltpersoner, skal hendelsesregistrene slettes når de sikkerhetsmessige formål er oppfylt, men først etter 2 år.	3.3.4			
	All autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene skal registreres og registeret skal lagres i minimum 2 år	5.2.6			
25.	Det skal registreres i hendelsesregistre i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang.	4.4.1			
	Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.	5.2.2			
26.	Det skal registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting	4.4.3			
27.	For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres hendelsesregistre over følgende: <ul style="list-style-type: none"> <li>- Autorisert bruk av informasjonssystemene skal registreres.</li> <li>- Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk.</li> <li>- Bruk av nødrettstilgang til behandlingsrettet helseregister skal registreres.</li> </ul>	5.5.2			
28.	Følgende skal som minimum registreres i hendelsesregistre: <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>- grunnlaget for tilgangen</li> <li>- tidspunkt og varighet for tilgangen</li> </ul>	5.5.2			
29.	Alle hendelsesregistre skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister og tilstedeværelsesregister.	5.5.2			
<b>Pasientrettigheter</b>					
30.	Det skal etableres prosedyrer for å sikre at den registrertes rettigheter for innsyn i hendelsesregistre blir ivaretatt. Prosedyrene skal som et minimum sikre at den registrerte får informasjon om: <ul style="list-style-type: none"> <li>- Hvem som har hatt tilgang.</li> <li>- Hvor ofte tilgangen er benyttet.</li> </ul>	5.3.4			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke relevant
31.	Det skal etableres prosedyrer og gjennomføres tiltak for å sikre at: - Pasienten/brukeren får informasjon om virksomhetens behandling av helse- og personopplysninger, og sine rettigheter til innsyn i, retting, sletting og sperring av registrerte opplysninger om seg selv.	5.3.3			
<b>Kvalitet</b>					
32.	Helse- og personopplysninger skal henføres til rett identifisert person	4.4.4			
33.	Helse- og personopplysninger skal føres i henhold til kodeverket	4.4.4			

#### Tilleggskrav for særskilte fagsystemer

Nr	Krav	Hjemmel	Krav ivaretatt		
			Ja	Nei	Ikke relevant
<b>Tilleggskrav for fagsystemer innen psykisk helsevern</b>					
1.	System som benyttes innen psykisk helsevern skal ha funksjonalitet for å kunne gi medlemmer av kontrollkommisjonen lesetilgang til journalen til enkeltpasienter	Forskrift om kontrollkommisjonenes virksomhet § 1-8			