

 	Utgitt med støtte av:  HelseDirektoratet
Norm for informasjonssikkerhet www.normen.no	
<h1>Sikkerhetskrav for systemer</h1>	Støttedokument Faktaark nr. 38 Versjon: 2.1 Dato: 15.12.2010

Målgruppe 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
Ansvar	Virksomhetens leder er ansvarlig for at systemer som tas i bruk for behandling av helse- og personopplysninger inneholder nødvendige sikkerhetsløsninger.		
Gjennomføring	Ved anskaffelse av systemer i helsesektoren skal leverandøren dokumentere at nødvendige sikkerhetsløsninger er etablert. Innkjøper kan benytte sjekklisten i faktaarket som grunnlag for dokumentasjonen.		
Formål	Gi innkjøper av systemer i helsesektoren et hjelpemiddel for å sikre at systemene inneholder sikkerhetsløsninger iht personopplysningsforskriften og Normen		
Omfang	Gjelder alle systemer som benyttes til behandling av helse- og personopplysninger i helsesektoren.		
Hjemmel	Personopplysningsforskriften §§ 2-8, 2-11, 2-12, 2-13 og 2-14.		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet • Faktaark 14 - Tilgangsstyring • Faktaark 15 - Hendelsesregistrering og oppfølging • Faktaark 31 - Passord og passordhåndtering • Faktaark 37 - Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter • Elektronisk pasientjournal standard, Arkitektur, arkivering og tilgangsstyring, Del I: Funksjonsrettet beskrivelse, KITH (EPJ-Standard): http://kith.no/templates/kith_WebPage_842.aspx. 		

Om sikkerhetskrav for systemer i helsesektoren

Personopplysningsforskriften og Normen setter krav til sikkerhet i systemer i helsesektoren. Eksempler på systemer er elektronisk pasientjournal, pasientadministrasjon, laboratoriesystem, rekvisisjon- og svar og medisinsk teknisk utstyr som inneholder helse- og personopplysninger. Faktaarket dekker kun sikkerhetsmessige krav.

Dette faktaarket samler kravene på en oversiktlig måte som en hjelp til leverandører og innkjøper av slike systemer ifm. anskaffelser. Kravene må sees på som en hjelp til leverandører og til virksomheten som et utgangspunkt for å tydeliggjøre hvordan de ulike kravene blir oppfylt i systemløsningen. Kravene er ikke nødvendigvis komplette i forhold til alle systemer. Innkjøper kan selv spesifisere ytterligere krav og eventuelt be om mer detaljert spesifisering på de foreliggende kravene i en anbudsforespørsel.

Faktaarket kan gjerne benyttes direkte i anskaffelsesdokumenter som innkjøper sender potensielle leverandører.

I tilfeller hvor det skal anskaffes systemløsning for elektronisk pasientjournal (EPJ), bør innkjøper i tillegg benytte krav i Pasientjournalforskriften og EPJ-Standarden.

Sjekkliste med sikkerhetskrav som skal ivaretas i systemer som behandler helse- og personopplysninger

Forklaring til tabellen

Krav = krav som skal ivaretas i system for behandling av helse- og personopplysninger

Ref. = referanse til hvor i Normen (Norm), personopplysningsforskriften (POF) eller faktaark (F) kravet er beskrevet

Nr.	Krav	Sikkerhetsområde	Forslag til hvordan kravet kan dokumenteres	Ref.
1.	Det skal registreres når autorisasjon tildeles og avsluttes og hvem som utfører dette, med mindre risikovurdering avdekker at dette ikke er nødvendig.	Konfidensialitet Integritet	Beskrive hvordan dette er løst i systemet.	Norm 5.2.2
2.	All autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene skal registreres og registeret skal lagres i elektronisk form i minimum 2 år.	Konfidensialitet Integritet	Beskrive hvilke data som hendelsesregistreres og hvordan 2 års fristen er løst.	Norm 5.5.2 F14 F15 Norm 5.2.6 POF §2-8 POF §2-14
3.	Det skal føres hendelsesregistre over alle oppslag (lesing), utskrifter, endring, retting og sletting av helse- og personopplysninger.	Konfidensialitet Integritet Kvalitet	Beskriv hvordan dette er løst i systemet.	Norm 5.5.2 F15
4.	Det skal ikke kunne endres opplysninger uten at det registreres hvem som har endret og hva som er endret. Dette krever for eksempel validering av alle felter i systemet.	Konfidensialitet Integritet Kvalitet	Beskrive hvordan dette er løst i systemet.	Norm 5.5.2
5.	Nødrettstilgang skal kunne etableres som en mulighet for spesielt autoriserte brukere til å gi seg selv tilgang.	Tilgjengelighet	Beskrive hvordan dette er løst i systemet.	Norm 4.4.2
6.	Årsak for bruk av nødrettstilgang skal registreres.	Konfidensialitet Integritet	Beskrive hvordan dette er løst i systemet.	Norm 5.5.2
7.	Helse- og personopplysninger skal henføres til rett identifisert person. For eksempel ved bruk av farger for å illustrere hvilken journal som er åpen, bilde av pasient i journalen og i forbindelse med skanning og kobling til rett journal.	Kvalitet	Beskrive hvordan dette er løst i systemet.	Norm 4.4.4
8.	Helse- og personopplysninger skal føres i henhold til kodeverket.	Kvalitet	Beskrive hvordan dette er løst ift hvilke kodeverk systemet har løsninger for.	Norm 4.4.4

Nr.	Krav	Sikkerhetsområde	Forslag til hvordan kravet kan dokumenteres	Ref.
9.	Autorisering skal skje selvstendig for hver enkelt rolle og autentisering må sikre identifisering i korrekt rolle i hvert enkelt tilfelle.	Konfidensialitet Integritet	Beskrive hvordan dette er løst med hvilke roller som er mulig eller ferdig definert i systemet. Hver rolle må også beskrives ift hvordan den kan bygges opp med tilgang til funksjoner, skjermbilder, enkeltdokumenter, osv.	Norm 5.2.1
10.	Ulike ansettelsesforhold (samme person kan ha ulike roller innenfor samme virksomhet) skal identifiseres og ved behov gis ulike autentiseringskriteria.	Konfidensialitet Integritet	Beskrive hvordan dette er løst og begrensninger som finnes; antall ansettelsesforhold per medarbeider, osv.	Norm 5.2.1
11.	Hendelsesregistrene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.	Konfidensialitet Integritet	Beskrive hvordan analyse av hendelsesregistre utføres.	Norm 5.2.6 POF §2-14
12.	Hendelsesregistrene skal sikres mot endring og sletting av uautorisert personell.	Konfidensialitet Integritet Tilgjengelighet	Beskrive tilgangsstyring til hendelsesregistre.	Norm 5.2.6
13.	Systemet skal støtte muligheten for innsyn i (for å ivareta innsynsretten), retting, sletting og sperring av hele/deler av journaler.	Konfidensialitet Integritet	Beskrive hvordan dette er løst i systemet.	Norm 5.3.3 F14
14.	Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger.	Konfidensialitet Integritet	Beskrive hvordan dette er løst i systemet.	Norm 5.5.2
15.	Autentisering av bruker fra og i interne systemer skal skje med minimum brukernavn og passord.	Konfidensialitet Integritet	Beskrive hvordan dette er løst i systemet. Har systemet egen autentisering. Kan autentisering samkjøres med operativsystem.	Norm 5.2.1 F14
16.	Passordfil skal krypteres.	Konfidensialitet	Beskrive hvordan dette er løst og hvilken styrke på kryptering som benyttes.	F31
17.	Tildelt autorisasjon skal kunne tidsavgrenses.	Konfidensialitet Integritet	Beskrive hvordan dette er løst.	F14

Nr.	Krav	Sikkerhetsområde	Forslag til hvordan kravet kan dokumenteres	Ref.
18.	Det skal være mulig å gjøre en avsjekk av tildelte autorisasjoner.	Konfidensialitet Integritet Kvalitet	Beskrive hvordan dette er løst og hvilke lister, oversikter på skjerm, etc. som kan benyttes og hvordan disse kan plukkes ut ift avdelinger, roller, osv.	Norm 5.3.2
19.	Passordet bør kunne byttes enkelt av bruker og tvunget skifte bør være teknisk mulig.	Konfidensialitet Integritet Kvalitet	Beskrive hvordan dette er løst.	F31
20.	System som benyttes innen psykisk helsevern bør ha funksjonalitet for å kunne gi medlemmer av kontrollkommissjonen lesetilgang til journalen til enkeltpasienter, jf EPJ-standarden.	Konfidensialitet	Beskrive hvordan dette er løst.	F39