Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Sikkerhetskrav for systemer

Støttedokument
Faktaark nr. 38
Versjon: 4.3
Dato: 1.11.2016

Formål	Gi innkjøper av systemer i helse- og omsorgstjenesten et hjelpemiddel for å sikre at systemene inneholder løsninger iht kravene i Normen. Faktaarket skal benyttes som grunnlag for selvdeklareringsordningen for programvare i helse- og omsorgstjenesten, hvor det er utarbeidet detaljerte beskrivelser av hvordan leverandøren kan oppfylle kravene.		
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 helse- og omsorgstjenesten skal leverandøren dokumentere at nødvendige sikkerhetsløsninger er etablert. Innkjøper kan benytte sjekklisten i faktaarket som grunnlag for dokumentasjonen.		
Omfang	Gjelder alle fagsystemer som benyttes til behandling av helse- og personopplysninger i helse- og omsorgstjenesten. For eksempel elektronisk pasientjournal, pasientadministrasjon, laboratoriesystem, rekvisisjon og svar og elektromedisinsk utstyr som inneholder helse- og personopplysninger		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☐ Prosjektleder forskning ☒ Sikkerhetsleder	☐ Ansatt / medarbeider ☐ Forsker ☐ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☒ Leverandør
Hjemmel	Kravene i faktaarket er hjemlet i lov og forskrift (jf. Normen kapittel 1.2). Enkelte tilleggskrav er fastsatt i Normen		
Referanser	• Faktaark 14 - Tilgangsstyring • Faktaark 15 - Hendelsesregistrering og oppfølging • Faktaark 31 - Passord og passordhåndtering		

Merknad 17.08.18: Faktaarket er ikke oppdatert ut fra siste versjon av Normen (5.3), ny personopplysningslov, endringer i helselovgivningen eller EUs personvernforordning. Oppdatering pågår.

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

Faktaarket er à jour med 5. utgave av Normen**.**

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
Autorisering					
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 rele-vant
5.	Databehandlingsansvarlig skal sørge for at det opprettes et autorisasjonsregister. Registeret skal som minimum inneholde: - informasjon om hvem som er tildelt autorisasjon - til hvilken rolle autorisasjonen er tildelt - formålet med autorisasjonen - tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt - informasjon om hvilken virksomhet den autoriserte er knyttet til - helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk) Utdypning av kravet: Det skal også registreres hvem (fysisk identifiserbar person) som har opprettet (registrert) autorisasjonen	5.2.2			
6.	Ved tilgang til helseopplysninger mellom virksomheter skal autorisasjonen tidsbegrenses	5.5.2			
7.	5 års lagring minimum fra det tidspunkt dokumentet ble tatt ut av bruk: - Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregister)	3.3.4			
8.	Tildelt autorisasjon skal sikre at den enkelte kan få tilgang til relevante og nødvendige helse- og personopplysninger i samsvar med personellets ansvar og oppgaver Utdypning av kravet: Tildelt autorisasjon skal kunne tidsavgrenses	5.2.2			
9.	For personer som har ulike roller i virksomheten, skal autorisering skje for hver rolle uavhengig av vedkommendes øvrige roller	5.2.2			
10.	Autorisasjon for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov	5.2.2			
11.	Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger	5.2.2			
12.	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	5.2.3			
13.	Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger	5.5.2			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
14.	Hendelsesregistrene, autorisasjonsregister og tilstedeværelsesregister skal sikres mot endring og sletting av uautorisert personell Hendelsesregistrene skal sikres mot endring og sletting av uautorisert personell	5.2.6 5.5.2			
15.	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 grunngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))	5.5.2			
16.	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	4.4.3			
17.	Begrunnelsen for nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som et avvik.	4.4.3			
18.	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. Ved tilgang til helseopplysninger mellom virksomheter skal det i tillegg kontrolleres hvorfor tilgangen er benyttet og tidsperioden helseopplysningene er hentet fram. Utdypning av kravet: Behandlingsrettet helseregister inkl elektronisk pasientjournal (EPJ) eller fagsystem må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	6.5			
Autentisering					
19.	Autentisering må sikre identifisering i korrekt rolle i hvert enkelt tilfelle.	5.2.1			
20.	Ulike roller skal identifiseres og ved behov gis ulike autentiseringskriteria.	5.2.1			
21.	Ved tilgang til behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer skal ulike ansettelsesforhold identifiseres.	5.2.1			
22.	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			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
23.	Tekniske tiltak skal iverksettes slik at personer i eller utenfor virksomheten 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			
24.	Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger	5.5.2			
Hendelsesregistrering					
25.	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.	3.3.4 5.2.8			
26.	Det skal registreres i hendelsesregistre i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang. Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.	4.4.1 5.2.2			
27.	Det skal registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting	4.4.2			
28.	For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres hendelsesregistre over følgende: - Autorisert bruk av informasjonssystemene skal registreres. - Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk. - Bruk av nødrettstilgang til behandlingsrettet helseregister skal registreres.	5.5.2			
29.	Følgende skal som minimum registreres i hendelsesregistre: - entydig identifikator for den autoriserte brukeren - rollen den autoriserte brukeren har ved tilgangen - virksomhetstilhørighet - organisatorisk tilhørighet til den som er autorisert - hvilke type opplysninger det er gitt tilgang til - hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer - grunnlaget for tilgangen - tidspunkt og varighet for tilgangen	5.5.2			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
30.	Ved tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende hendelsesregistreres: - hvorfor helseopplysningene er hentet fram - hvilke tidsperioder vedkommende har hentet fram helseopplysningene	5.5.2			
31.	Alle hendelsesregistre skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister og tilstedeværelsesregister.	5.5.2			
Pasientrettigheter					
32.	Ved tilgang til helseopplysninger mellom virksomheter skal det være en funksjon for å sperre tilgang til helseopplysninger for helsepersonell fra andre virksomheter Med sperring menes en teknisk løsning der hele eller deler av journalen gjøres utilgjengelige for helsepersonell. Opplysningene skal kunne sperres overfor både enkeltpersoner, grupper av helsepersonell og virksomheter.	5.2.2			
33.	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: - Hvem som har hatt tilgang eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer eller på noen annen måte direkte eller indirekte kan knyttes til pasienten eller brukeren - Hvor ofte tilgangen er benyttet.	5.3.4			
34.	Ved tilgang til helseopplysninger mellom virksomheter skal i tillegg den registrerte få informasjon om: - Person og organisatorisk tilhørighet til den som har hentet fram opplysningene - Hvorfor helseopplysningene er hentet fram - Hvilke tidsperioder vedkommende har hentet fram helseopplysningene	5.3.4			
35.	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			
Integritet					
36.	Helse- og personopplysninger skal henføres til rett identifisert person	4.4.2			
37.	Helse- og personopplysninger skal føres i henhold til kodeverket	4.4.2			