Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Sikkerhetskrav for systemer

Støttedokument
Faktaark nr. 38
Versjon: 5.0
Dato: 21.11.2018

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 - Logging og oppfølging av logger • Faktaark 31 - Passord og passordhåndtering		

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

Faktaarket er à jour med utgave 5.3 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:”.

Faktaarket dekker ikke samtlige krav ved tilgang til helseopplysninger mellom virksomheter. Grunnen er at flere av kravene kan løses utenfor systemene.

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
Autorisering					
1.	Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregisteret) skal oppbevares i minimum 5 år fra det tidspunkt autorisasjonen ble tatt ut av bruk	2.3			
2.	Selvautorisering 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	3			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
3.	Tilgangsstyring skal etableres for alle behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer	5.2			
4.	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			
5.	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	5.2.1			
6.	Benyttes det roller i virksomheten skal autorisering for hver rolle skje uavhengig av personellets øvrige roller	5.2.1			
7.	Autorisasjon for å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov	5.2.1			
8.	Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger	5.2.1			
9.	Det skal iverksettes tiltak slik at mulig misbruk av teknisk personell skal kunne avdekkes	5.2.1			
10.	Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger	5.2.1			
11.	Dersom det er åpnet for selvautorisering, skal tekniske tiltak etableres på en slik måte at helsepersonell kan få tilgang til nødvendige helse- og personopplysninger.	5.2.1			
12.	Tilgang ved selvautorisering skal grunngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))	5.2.1			
13.	All tildeling av autorisasjon skal registreres i et autorisasjonsregister	5.2.1			
14.	Misbruk av selvautorisering skal følges opp som avvik	5.2.1			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
15.	Dataansvarlig 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 (om rolle benyttes i virksomheten) - 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	5.2.1.1			
16.	Ved tilgang til helseopplysninger mellom virksomheter skal autorisasjonen tidsbegrenses	5.2.1.3			
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.	5.2.3			
18.	Ved tilgang til helseopplysninger mellom virksomheter skal dataansvarlige, som har adgang til å autorisere helsepersonell for tilgang, løpende kontrollere: - hvem i egen virksomhet som elektronisk har hentet frem helseopplysninger fra annen virksomhet - hvorfor dette er gjort - tidsperioden helseopplysningene er hentet frem	5.2.3			
Autentisering					
19.	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	5.2.1			
20.	Om det benyttes roller skal den enkelte rolle identifiseres	5.2.2			
21.	Om det benyttes roller skal den enkelte rolle ved behov gis ulike autentiseringskriteria.	5.2.2			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
22.	Ved tilgang til behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer skal ulike ansettelsesforhold identifiseres.	5.2.2			
23.	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	5.2.2			
Logging					
24.	Logger 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.	2.3			
25.	Det skal registreres i logger i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang.	3			
26.	Det skal registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting	3			
27.	Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.	5.2.1			
28.	For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logg over: - Autorisert bruk av informasjonssystemene skal registreres. - Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk. - Bruk av selvautorisering til behandlingsrettet helseregister skal registreres.	5.4.4			
29.	Autorisasjonsregister skal sikres mot endring og sletting av uautorisert personell	5.4.4			
30.	Logger skal sikres mot endring og sletting av uautorisert personell	5.4.4			
31.	Følgende skal som minimum registreres i loggene: - entydig identifikator for den autoriserte brukeren - rollen den autoriserte brukeren har ved tilgangen (om det benyttes roller) - virksomhetstilhørighet - organisatorisk tilhørighet til den som er autorisert - 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	5.4.4			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
32.	Ved tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende logges: - person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene - hvorfor helseopplysningene er hentet frem - hvilke tidsperioder vedkommende har hentet frem helseopplysningene	5.4.4			
33.	Alle logger skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister	5.4.4			
Pasientrettigheter					
34.	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.	4.2			
35.	Dersom den registrerte sender en anmodning elektronisk, skal informasjonen om mulig gis elektronisk	4.2			
36.	Det skal etableres prosedyrer for å sikre at den registrertes rettigheter for innsyn i logger blir ivaretatt. Prosedyrene skal som et minimum sikre at den registrerte får informasjon om: - Person og organisatorisk tilhørighet til den som har behandlet helseopplysningene - Hvilke behandlinger av helse- og personopplysninger som er utført - Når behandlingene av helse- og personopplysninger er gjort.	4.2.1			
37.	Ved bruk av tilgang til helseopplysninger mellom virksomheter skal 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	4.2.1			
38.	Det skal fremgå av journalen når helse- og personopplysninger er gitt til annet personell enn virksomhetens eget personell	4.3.1			
39.	Når helseopplysningene utleveres til ledelsen skal de så langt som mulig behandles uten at den registrertes navn og fødselsnummer fremgår	4.3.2			
40.	Når helseopplysninger tilgjengeliggjøres for læring og kvalitetssikring skal de begrenses til de opplysninger som er nødvendige og relevante for formålet	4.3.3			
41.	Det skal dokumenteres i pasientens journal hvilke opplysninger som er tilgjengeliggjort for ledelsen og for læring og kvalitetssikring og hvem de er tilgjengeliggjort for	4.3.3			

Nr	Krav	Kapittel i Normen	Krav ivaretatt		
			Ja	Nei	Ikke rele-vant
42.	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.	5.2.1.3			
Integritet					
43.	Helse- og personopplysninger skal være korrekte og knyttes til rett identifisert person	3			
44.	Helse- og personopplysninger skal føres i henhold til relevant kodeverk	3			