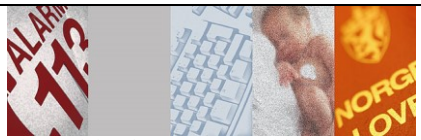

Selvdeklareringsordning for programvare i helse- og omsorgssektoren

Deklareringsområde: Informasjonssikkerhet	Versjon: 4.1 Dato: 17.08.2015

VEILEDNING OG SELVDEKLARERING FOR DELOMRÅDE:

Kravnumrene nedenfor referer til Faktaark 38 - Sikkerhetskrav for systemer

Autorisering	Autentisering	Hendelses-registrering	Pasient-rettigheter	Kvalitet
Kravnr. 1 til 18	Kravnr. 19 til 24	Kravnr. 25 - 31	Kravnr. 32 til 35	Kravnr. 36 til 37

1 INFORMASJON OM SELSKAP

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

Leverandørnavn:		
Postadresse:		
Besøksadresse:		
Organisasjonsnummer:		
Kontaktinformasjon:	***Navn på kontaktperson:***	
	E-post:	***Telefonnummer:***
Objekt:	***Benevnelse på system:***	***Hovedversjon:***
	Benevnelse delsystem:[1]	***Versjon:***
	Kommentar for å utdype beskrivelsen av objekt:	
Utfylt:	***Dato:***	***Utfylt av person:*** ☐ Samme som kontaktperson

1. *Selvdeklareringen kan være avgrenset til et bestemt delsystem. Om selvdeklareringen 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 OM SELVDEKLARERING AV PASIENTRETTIGHETER

Med pasientrettigheter menes i systemsammenheng funksjonalitet for at de grunnleggende personvernrettighetene (for eksempel innsyn i egne opplysninger) Den registrerte har, skal være opplyst om. Den registrerte skal også ha innsyn i hendelsesregistre.

Krav Nr. 32	Kravet i Normens kapittel **5.5.2** er: *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*
Hensikt med kravet	Hensikten med kravet er å gi brukeren av systemet mulighet til å sperre journalen for tilgang fra andre virksomheter, om pasienten ber om det.
Veiledende beskrivelse	Det må etableres en funksjon i et skjermbilde på den enkelte journal der en kan velge en sperrefunksjon. Sperrefunksjonen må etableres slik at nyansene nedenfor ivaretas: - sperres for enkeltpersoner - sperres for grupper - sperres for andre virksomheter Dette kravet må sees sammen med autorisering som er framført i krav 1-18.
Veiledende eksempel	Eksempler på funksjonalitet som kan finnes i programvaren for at kravet skal oppfylles: Når kravet velges f.eks. i en avkryssingsboks kan følgende valg komme opp: - Om enkeltpersoner kan søkes opp fra autorisasjonsregisteret eller brukerdatabase med angivelse av - En eller flere enkeltpersoner som velges f.eks. i en søkeboks - Om systemet benytter grupper helsepersonell kan dette knyttes til begrepet rolle slik det framkommer i krav 1-18 (jfr. datamodell i dokumentet "Veiledning i selvdeklarering av programvare") - Om virksomheter skal begrenses søkes de opp opp og velges i en søkeboks

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 33	Kravet i Normens kapittel **5.3.4** er: *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.*
Hensikt med kravet	Hensikten med kravet er å sikre at Den registrerte har innsyn i at tilgang til egne helse- og personopplysninger er i henhold til et tjenstlig behov. Velger leverandøren å inkludere funksjonalitet for disse prosedyrene i systemet er det kravene nedenfor som skal selvdeklareres.
Veiledende beskrivelse	Det er den databehandlingsansvarlige som skal etablere prosedyrer slik kravet beskriver. I forbindelse med selvdeklarering menes det at systemet har funksjonalitet som gjør at databehandlingsansvarlig kan ivareta kravet. Leverandøren kan velge å lage funksjonalitet for å ivareta kravet. I så fall må det finnes funksjonalitet for at den registrerte får informasjon om hvem som har hatt tilgang eller har fått utlevert Den registrertes helse- og personopplysninger og hvor ofte den aktuelle tilgangen faktisk er benyttet.
Veiledende eksempel	Eksempler på funksjonalitet som kan finnes i programvaren for at kravet skal oppfylles: - Informasjonssystemet må ha funksjon for å søke frem til den registrerte - Når den registrerte er funnet i systemet, kan det angis for hvilken tidsperiode den registrerte ønsker innsyn. Hvis det ikke finnes funksjonalitet for angivelse av tidsperiode, vil resultatet vise tilganger fra første gangs oppføring i hendelsesregisteret til dags dato - Systemet kan ha funksjonalitet som gir følgende informasjon på skjerm og / eller utskrift: o Navn, rolle og organisatorisk tilhørighet til den som har hatt tilgang o Hvor ofte denne tilgangen er benyttet (dvs. konkret antall ganger / tilfeller tilgangen er benyttet) o Alle opplysinger knyttet til bruker / pasientens navn eller fødselsnummer eller noe som indirekte kan knyttes til individet

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 34	*Kravet i Normens kapittel **5.3.4** er:* *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*
Hensikt med kravet	Hensikten med kravet er å sikre at Den registrerte har innsyn i at tilgang til egne helse- og personopplysninger er i henhold til et tjenstlig behov. Dette kravet må sees sammen med krav 33 som tilleggsinformasjon om det er gitt tilgang fra andre virksomheter.
Veiledende beskrivelse	Se krav 33
Veiledende eksempel	Se krav 33 med tillegg av: Systemet kan ha funksjonalitet som gir følgende informasjon på skjerm og / eller utskrift: – Person og organisatorisk tilhørighet til den som har hentet fram opplysningene – Hvorfor helseopplysningene er hentet fram – Hvilke tidsperioder vedkommende har hentet fram helseopplysningene

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 35	Kravet i Normens kapittel **5.3.3** er: *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.*
Hensikt med kravet	Hensikten med kravet er å sikre at Den registrerte er kjent med virksomhetens behandling av helse- og personopplysninger og om behandlingen er i samsvar med gjeldende regler. Kravet skal også sikre at Den registrerte er kjent med, og kan benytte, sine rettigheter knyttet til innsyn i, retting, sletting og sperring av opplysninger om seg selv. Velger leverandøren å inkludere funksjonalitet for disse prosedyrene i systemet er det kravene nedenfor som skal selvdeklareres.
Veiledende beskrivelse	Det er den databehandlingsansvarlige som skal etablere prosedyrer slik kravet beskriver. I forbindelse med selvdeklarering menes det at systemet har funksjonalitet som gjør at databehandlingsansvarlig kan ivareta kravet. Det må finnes funksjonalitet som ivaretar at hver enkelt registrert som ber om det, får informasjon om: – virksomhetens behandling av helse- og personopplysninger – rettigheter til innsyn i, retting, sletting og sperring av registrerte opplysninger om seg selv
Veiledende eksempel	For eksempel kan et skjermbilde inneholde et avkrysningsfelt om informasjon om rettighetene er gitt til den registrerte. Systemet kan ha funksjonalitet der en kan skrive ut en mal med informasjon om rettigheter, flettet med Den registrertes navn og adresse fra systemet. Eksempler på informasjonselementer som skal gis for å dokumentere virksomhetens behandling av helse- og personopplysninger: – navn og adresse på den databehandlingsansvarlige – formålet med behandlingen av helse- og personopplysninger om den registrerte – hvilke helse- og personopplysninger om den registrerte som behandles – hvor helse- og personopplysningene er hentet fra – om det er frivillig for Den registrerte å gi fra seg helse- og personopplysningene – om helse- og personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker – hvilke sikkerhetstiltak som er etablert omkring behandlingen av helse- og personopplysningene om den registrerte (så langt innsyn ikke svekker sikkerheten) – informasjon om retten til å kreve innsyn, retten til å kreve retting, og retten til å kreve sletting

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":