Innholdsfortegnelse

Veiledning i selvdeklarering av programvare

Støttedokument
Versjon: 4.1
Dato: 17.08.2015

1. Innledning

Dette dokumentet gir informasjon om de veiledende dokumenter som skal brukes ifm. deklareringsområdet informasjonssikkerhet.

Selvdeklarasjonsordningen skal bidra til at programvare som leveres til helse- og omsorgstjenesten ivaretar krav stilt i Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen).

2. Om selvdeklarering

Selvdeklarering er et frivillig tilbud som den enkelte leverandør av programvare kan ta i bruk for å dokumentere etterlevelse av Normens krav i programvaren.

Det kan selvdeklareres at programvaren inneholder nødvendig og tilstrekkelig funksjonalitet slik at den databehandlingsansvarlige kan oppfylle lovbestemte krav.

Eksempler på bruk av dokumentasjonen er:
- Ovenfor kunder i anbudsprosesser
- Kunders behov i den daglige driften
- Tilsynsmyndigheter
- En del av programvarens systemdokumentasjon og kvalitetsdokumentasjon

3. Programvare som selvdeklareringen anbefales brukt på

Tilbudet kan benyttes på alle typer programvare. Med programvare menes i denne sammenhengen:
- Helhetlige informasjonssystemer
- Delsystemer/moduler
- Programvarekomponenter i tilknytning til informasjonssystemet
- Databaser i tilknytning til informasjonssystemet

Eksempler på programvare som kan selvdeklareres:
- Journalsystem (for eksempel elektronisk pasientjournalsystem)
- Pasientadministrative systemer (for eksempel demografisk informasjon, timebok, fakturering, opphold)
- Røntgensystemer (for eksempel røntgen informasjonssystem, PACS)
- Laboratoriesystemer (for eksempel immunologi, klinisk/kjemisk, mikrobiologi)
- Planleggingssystemer (for eksempel operasjonsplanlegging)
- Beslutningsstøttesystemer (for eksempel blodbanksystem)
- Saksbehandlingssystemer (for eksempel sak-/arkivsystem)
- Underliggende støttesystemer (for eksempel SMS-system, rapportgeneratorer)
- Systemer for meldingsutveksling (for eksempel løsninger for meldingsformatering, signering, kryptering og sending/mottak)

4. Veiledningsdokumenter

Deklareringsområdet informasjonssikkerhet er delt opp i seks delområder iht. tabellen nedenfor.

Veiledningsdokumentene er uavhengig av type system, type delsektor, profesjon og teknologi.

Tabellen viser dokumenter ifm. selvdeklareringen. Dokumentene bygger på kravene i Faktaark 38, som er en oppsummering av Normens sikkerhetskrav for systemer.

Nr	Delområde	Krav i faktaark 38, versjon 4.1
1.	Autorisering	1-18
2.	Autentisering	19-24
3.	Hendelsesregistrering	25-31
4.	Pasientrettigheter	32-35
5.	Integritet	36-37

Hvert dokument er strukturert slik:

Kap.	Tittel	Innhold
1.	Informasjon om selskap	Tabell leverandøren skal fylle ut med informasjon om leverandøren og hva som selvdeklareres
2.	Om selvdeklarering av <Delområde>	Beskrivelse av krav, hensikt, veiledning og eksempler

Enkelte begrep som benyttes i veiledningsdokumentene er definert i Normen, se www.normen.no.

5. Utfylling av skjematikk

For hvert krav skal leverandøren fylle ut tabellen nedenfor (og som er satt inn på slutten av hvert enkelt krav i veiledningsdokumentene):

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:			

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

- Ved ”Ja”: Skriv inn hvor og i hvilket av leverandørens dokument ivaretakelse av kravet er beskrevet. Det er ikke et krav at leverandøren skal utarbeide særskilt dokumentasjon for selvdeklareringen. Det er imidlertid et krav at leverandøren skal i systemets dokumentasjon (for eksempel systemdokumentasjon, brukerhåndbøker mv.) kunne vise at kravet er ivaretatt. Dokumentasjonens tekst og illustrasjoner må være av en slik karakter at personer som ikke har kompetanse i systemmodellering og programmering skal kunne forstå dokumentasjonen
- Ved ”Nei”: Skriv en kort begrunnelse
- Ved ”Ikke relevant”: Eksempel på tekst kan være: ”Leveres ikke som en del av systemet”

6. Eksempel datamodell

Dette avsnittet viser et eksempel på en datamodell. Datamodellen er ment å kunne tjene som et felles begrepsapparat og som visualisering av dataelementer og avhengigheter mellom dataelementene.

Forklaring til datamodellen nedenfor:

- Bruker er en person som innehar en rolle i en organisatorisk enhet i en virksomhet. De tre forbindelser mellom bruker og innehar rolle, representerer den som er ansatt i rollen, den som har registrert ansettelsen og den som har godkjent ansettelsen
- Roller har tilknyttet rettigheter. Rettighetene som er tilknyttet en rolle kan endres over tid
- Autorisasjonsregisteret fremkommer ved en kombinasjon av bruker, ansettelse i rolle, rolle, rolle har tilknyttet rettigheter, formål og rettigheter
- Hver bruker kan ha flere sett med autentiseringskriteria (brukernavn/passord). Hvert autentiseringskriterium er knyttet til en eller flere roller brukeren er autorisert til
- Brukere autentiserer seg i en rolle. Når det velges hvilken Den registrerte brukeren skal lese, endre, rette eller slette opplysninger etc. om, gis en begrunnelse for beslutning om ytelse. Hvis brukeren i en autentisering velger flere Den registrerte gis en ny begrunnelse for hvert valg. Brukeren får deretter tilgang til helseopplysninger for Den registrerte i henhold til rettighetene tilknyttet rollen som brukeren er autentisert i
- Hendelsesregisteret fremkommer ved kombinasjon av bruker, autentiseringskriteria, autentisering i rolle, beslutning om tilgang, Den registrerte og helseopplysninger

Utgitt med støtte av:
Helsedirektoratet

Veiledning i selvdeklarering av programvare

Støttedokument
Versjon: 4.1
Dato: 17.08.2015