NORMEN

Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter (faktaark 37)

Versjon 2.2

01.10.2018

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler krav i prosjekter ved f.eks. innføring av nytt journalsystem, ny funksjonalitet i journalsystem og gjelder ikke forskningsprosjekter. Formålet er å sikre tilfredsstillende informasjonssikkerhet og god sikkerhetsdokumentasjon i prosjekter som skal endre eller innføre nye IKT-løsninger. Påse at sikkerhetsløsninger og -dokumentasjon overføres til driftsmiljøet ved endt prosjekt. Prosjektleder vil normalt få delegert ansvar fra databehandlingsansvarlig for å påse at prosjekter gjennomføres med tilfredsstillende informasjonssikkerhet, men ved større prosjekter kan en prosjektintern sikkerhetskoordinator være hensiktsmessig Gjennomføres fra prosjekter planlegges/startes opp og til de overføres til ordinær drift.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • Virksomhetens leder/ledelse • Sikkerhetsleder / sikkerhetskoordinator • Prosjektleder • Prosjektleder forskning • Leverandør • IKT-ansvarlig • Databehandler
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 3. Risikostyring • Kapittel 5.4 Sikker IT-drift • Kapittel 5.4.6 Sikkerhetsrevisjon
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Helseregisterloven § 22.Internkontroll • Pasientjournalloven § 22.Informasjonssikkerhet • Personvernforordningen Artikkel 32.Sikkerhet ved behandlingen • Sikkerhetsrevisjon (faktaark 06) • Bruk av databehandler (faktaark 10) • Tilgangsstyring (faktaark 14) • Logging og innsyn i logg (faktaark 15)

	• Sikkerhets- og samhandlingsarkitektur (faktaark 20a) • Sikkerhets- og samhandlingsarkitektur ved intern samhandling (Faktaark 20b) • Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter (faktaark 20c) • Kommunikasjon over åpne nett (faktaark 24) • Lagringstid og sletting (faktaark 25) • Håndtering av lagringsmedia (faktaark 34) • Testing og testdata (faktaark 43)

Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter

Prosjekter som omtales i dette faktaarket gjelder prosjekter ved f.eks. innføring av nytt journalsystem eller ny funksjonalitet i journalsystem og ikke forskningsprosjekter.

1. Sikkerhetskrav og sikkerhetsdokumentasjon ved oppstart av prosjekt

a) Krav til konfidensialitet, integritet, tilgjengelighet og kvalitet er grunnleggende krav som alltid må ivaretas (jfr. Normen):

- Prosjektet må dokumentere overordnede krav til konfidensialitet, integritet, tilgjengelighet og kvalitet tilgjengelighet i løsningen
- Prosjektet må i samarbeid med systemeier sørge for at det fastsettes akseptansekriterier (ift. for eksempel oppetid, responstid, kapasitet mv.) som skal gjelde for den løsningen som prosjektet skal innføre/endre/utvide
- Krav til informasjonssikkerhet må sees i sammenheng med kritikalitet og akseptkriterier for løsningen
- Risikovurdering skal gjennomføres for løsningen som skal innføres. Dette må gjøres så tidlig at det er mulig å endre spesifikasjonen av løsingen basert på resultatene fra risikovurderingen
- Prosjektet må avklare konsekvenser ved innføring av systemet, f.eks. avhengighet av andre systemer, behov for endringer i infrastruktur og konsekvenser av dette

b) Prosjektleder må kontakte sikkerhetsleder / sikkerhetskoordinator i virksomheten for å informere om og diskutere den planlagte løsningen slik at den kan tas inn i ”porteføljen” til sikkerhetsledelsen. I større prosjekter bør det vurderes egen sikkerhetskoordinator som rapporterer til prosjektleder

c) Virksomhetens eventuelle personvernombud skal kontaktes/involveres når planlagt løsning omfatter behandling av helse- og personopplysninger

d) Prosjektleder bør gjøre en gjennomgang av hva som finnes av lignende løsninger og tidligere prosjekter for å kunne dra nytte av den kunnskap og erfaringer som finnes

e) Prosjektleder må avklare om prosjektet og/eller planlagt løsning krever konsesjon fra Datatilsynet (må gjøres før prosjektoppstart/løsningen tas i bruk). Dette gjøres med bistand fra personvernombud for de virksomheter som har dette.

f) Prosjektleder må avklare om planlagt løsning utløser plikt til å gi pasientene informasjon om behandlingen av helse- og personopplysninger, og om nødvendig innhente samtykke, jfr. pkt. 5.3.3 i Normen

2. Sikkerhetskrav i teknisk og funksjonell løsning

a) Kravene til funksjonell og teknisk sikkerhet må ivareta de overordnede krav som er utarbeidet under punkt 1

b) Sikkerhetskravene må ta hensyn til gjennomførte risikovurderinger, slik at løsningen kommer innenfor de gitte akseptkriteriene som gjelder for løsningen

c) Krav til funksjonell og teknisk sikkerhet må tilpasses den type løsning det er snakk om. Aktuelle områder det bør stilles krav til er (for flere av områdene er det utarbeidet egne faktaark):

- Ekstern kommunikasjon (jfr. faktaark 24)
- Sikkerhets- og samhandlingsarkitektur ved meldingsformidling (jfr. faktaark 20 a)
- Sikkerhets- og samhandlingsarkitektur ved intern samhandling (jfr. faktaark 20 b)
- Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter (jfr. faktaark 20 c)
- Tilgangsstyring (jfr. faktaark 14)
- Logging og innsyn i logg (jfr. faktaark 15)
- Lagring og sletting (jfr. faktaark 25)

3. Sikkerhetsdokumentasjon for teknisk og funksjonell løsning

a) Sikkerhetsdokumentasjonen skal lagres i minimum 5 år

b) Hendelsesregistre for bruk av løsningen (autorisert bruk, forsøk på uautorisert tilgang etc.) skal lagres så lenge at det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for det

4. Sikkerhetskrav og sikkerhetsdokumentasjon ved anbudsutarbeidelse

a) Avtalen må sikre at leverandøren følger Normens krav, jfr. pkt. 5.8 i Normen.

b) Avtalen med leverandøren skal omfatte og regulere aktuelle sikkerhetskrav

c) Krav til testing av leveransen skal avtalefestes

d) Rett til å gjennomføre IKT-revisjon av leverandøren skal avtalefestes

e) Avtalen skal sikre at leverandøren leverer sikkerhetsdokumentasjon og yter rask og nødvendig support i oppstartsfasen

f) Ved testing med bruk av reelle data skal Normen følges som om systemet var i ordinær drift. Dette innebærer blant annet:

- Det må etableres avtale med databehandler
- Avtaler med andre eksterne (leverandører, utviklere, etc) må regulere sikkerhetsforholdene rundt prosjektet
- Taushetsplikten må ivaretas av alle parter i prosjektet
- Bruk av testdata jfr. Testing og testdata (faktaark 43)

6. Sikkerhetskrav og sikkerhetsdokumentasjon ved overføring av system til drift og forvaltning

a) Beskrive ansvarsforhold

b) Opplæring av driftspersonale og brukere som skal bruke løsningen

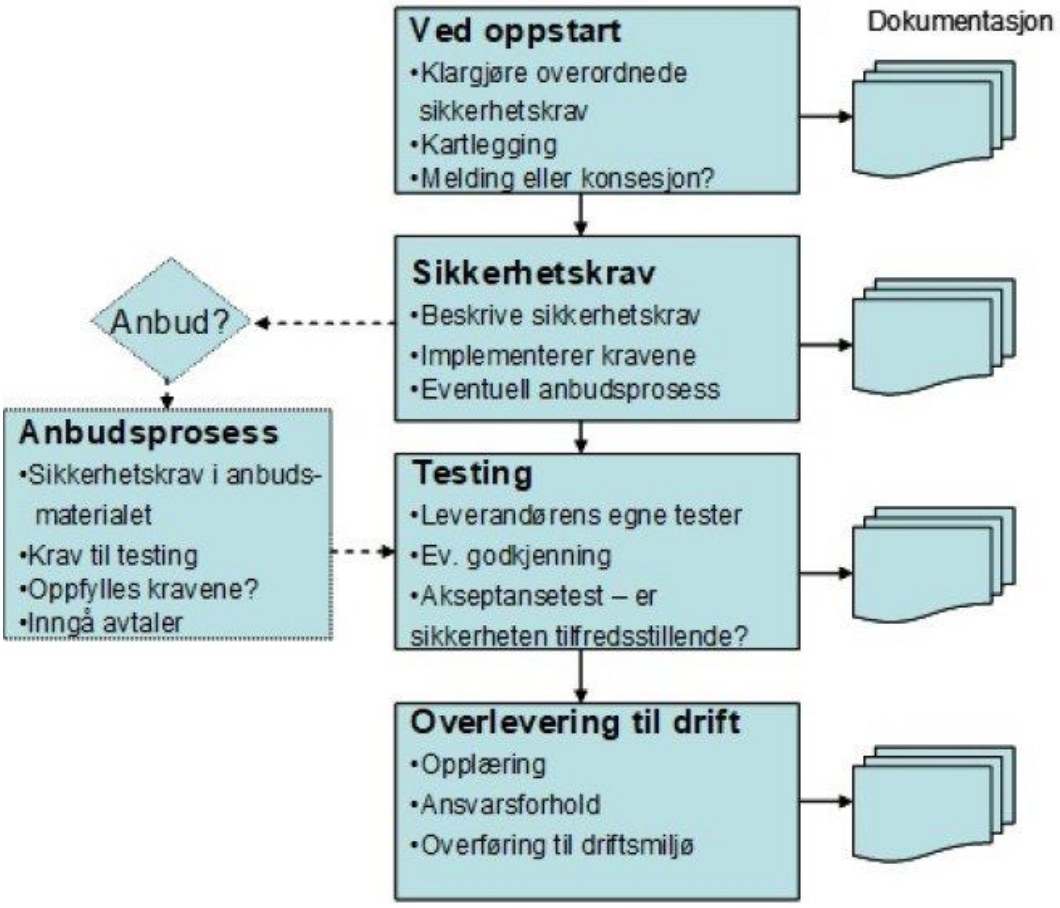
- Kompetansebehovet for å overta løsningen
- Evt. behov for superbrukere eller lignende
- Opplæring av brukerstøtte
- Tilfredsstillende opplæring av brukere og driftspersonale
- Opplæring skal skje med bruk av opplæringsdata så fremt det ikke er innhentet samtykke fra pasient om bruk av reelle pasientdata (jfr. pkt. 5.3.3 i Normen)

c) Ved avslutning av prosjektet skal følgende dokumentasjon minimum foreligge:

- Driftsprosedyrer
- Sikkerhetsdokumentasjon for løsningen (konfigurasjonsoversikt etc.)
- Rapporter fra utførte risikovurderinger
- Relevante avtaler med leverandører, databehandler etc.
- Oversikt over data som er behandlet i prosjektperioden (hendelsesregistre, tilganger etc.)
- Autorisasjoner som er gitt i systemet i prosjektperioden
- Evt. melding til/konsesjon fra Datatilsynet

d) Ved overgang fra prosjekt til drift skal kopier av helse- og personopplysninger som ikke lenger skal brukes i samsvar med sitt formål (for eksempel testing og opplæring) slettes på en tilfredsstillende måte jfr. Lagringstid og sletting (faktaark 25) og Håndtering av lagringsmedia (faktaark 34)

e) Ved overgang fra prosjekt til drift, må det sikres at den innførte løsningen og aktuell sikkerhetsdokumentasjon er blitt en del av "porteføljen" til sikkerhetsledelsen.



Skisse over sikkerhets- og dokumentasjonskrav i prosjektet