NORMEN

Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter (faktaark 20c)

Versjon 3.1

14.10.2015

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 benyttes ved innføring av nye IKT-systemer eller endringer i eksisterende systemer. IKT-ansvarlig er ansvarlig for å etablere en tilfredstillende sikkerhets- og samhandlingsarkitektur. Gjelder alle tekniske løsninger som benyttes til behandling av helse- og personopplysninger. For mindre virksomheter bør leverandørene og Norsk Helsenett sørge for en tilfredsstillende sikkerhetsarkitektur. Formålet med faktaarket er gi veiledning i hvordan. • Standardisere virksomhetens sikkerhetsfunksjoner • Etablere tilfredsstillende sikkerhet ved elektronisk samhandling med andre aktører i helse- og sosialsektoren
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • Sikkerhetsleder / sikkerhetskoordinator • IKT-ansvarlig • Databehandler • Leverandør
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen - Kapittel 5.5.3 Elektronisk samhandling
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser er spesielt relevante for faktaarket: • Pasientjournalloven § 19 Helseopplysninger ved helsehjelp • Personvernforordningen artikkel 24 Den behandlingsansvarliges ansvar • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen • Pasientjournalloven • Forskrift om tilgang til helseopplysninger mellom virksomheter

Sikkerhets- og samhandlingsarkitektur ved tilgang til helseopplysninger mellom virksomheter

Pasientjournalloven åpner for tilgang til helseopplysninger mellom virksomheter. Tilgangen skal skje innenfor rammen av taushetsplikten, og kravet til informasjonssikkerhet skal ivaretas.

Med mindre Departementet i forskrift har gitt føringer for hvordan helseopplysningene skal gjøres tilgjengelig er det dataansvarlig som bestemmer på hvilken måte dette skal skje. En slik forskrift er ikke vedtatt.

Sikkerhetskrav

1. Kryptering

Handling/Utførelse: Opplysninger sendt over åpne nett sendes i utgangspunktet over i klartekst slik at de kan leses dersom nettet avlyttes. Helse- og personopplysninger sendt over åpne nett må derfor krypteres slik at innholdet i opplysningene er uleselig for andre enn mottaker. Krypteringsstyrke skal være iht. gjeldende krav satt i ”Kravspesifikasjon for PKI (Public Key Infrastructure) i offentleg sektor ”

2. Autentisering og autorisasjon

Handling/Utførelse: Det skal benyttes sikker autentisering ved tilgang. Autorisasjonen skal sørge for at bruker kun blir gitt tilgang til opplysninger som er relevant for behandlingen. Sikkerhetsnivå 4 anbefales brukt.

3. Krav til risikovurdering

Handling/Utførelse: Både innhentende virksomhet og utleverende virksomhet skal gjennomføre risikovurderinger før det åpnes for tilgang til helseopplysninger mellom virksomheter.

Risikovurderingen skal vise at personvernet for pasienten ikke blir påvirket ved brudd på taushetsplikten og svekket informasjonssikkerhet. Det vil si at vurderingene må belyse at taushetsplikten blir ivaretatt og at løsningen for tilgang ikke medfører økt risiko. Med løsning menes både prosedyrer, organisering og teknisk løsning. For å belyse det totale risikoområdet kan det være hensiktsmessig at innhentende virksomhet og utleverende virksomhet gjennomfører risikovurderingen sammen.

4. Hendelsessregistrering

Handling/Utførelse: All autorisert bruk og forsøk på uautorisert bruk av løsningene skal registreres. Hendelsesregistrene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.

Det skal etableres prosedyrer for å analysere hendelsesregistrene slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke.

Hendelsesregistre skal kun være tilgjengelig for fastsatte roller i virksomheten.

Hendelsesregistrene skal sikres mot endring og sletting av uautorisert personell.

Alle oppføringer i hendelsesregistret skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for det.

Om det avdekkes hendelser som viser uautorisert bruk skal det opprettes en avviksmelding som skal håndteres iht. etablerte prosedyrer.

For ytterlige informasjon om hendelsesregistrering vises det til Logging og innsyn i logg (faktaark 15).

5. Oppfølging og kontroll av tilgang

Handling/Utførelse: Virksomhetene som deler informasjon plikter å samarbeide om oppfølging av tilganger. Det anbefales at virksomhetene utarbeider omforente prosedyrer for gjennomgang av handelsregisteret og håndtering av eventuelle avvik.

6. Pasientens rettigheter

Handling/Utførelse:

- Pasienten skal få informasjon om at helsepersonell i andre virksomheter, enn der de får behandling, kan få tilgang til journalopplysningene
- Pasienten har rett til informasjon og innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (hendelsesregistre).
- Pasienten har rett til å kunne sperre informasjon i journalsystemet. (Reservasjonsrett) Det skal være en teknisk løsning som muliggjør sperring av hele eller deler av journalsystemet for enkeltpersoner, grupper eller helsepersonell i andre virksomheter.

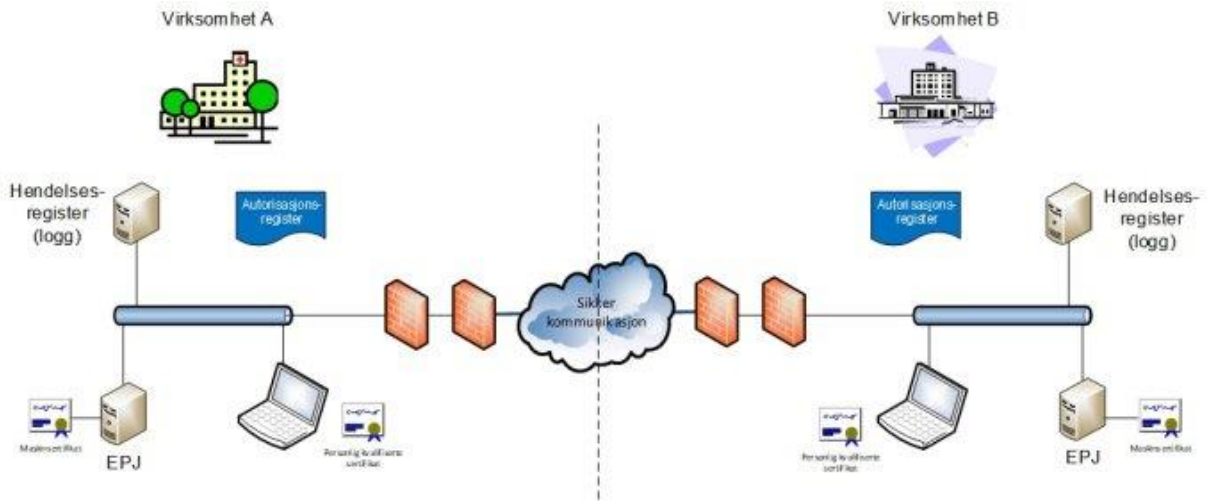
7. Avtaler

Handling/Utførelse:

- Tilgang mellom virksomheter skal ikke etableres før det er utarbeidet en avtale som regulerer samarbeidet. Minstekravet til innhold i en slik avtale er nærmere beskrevet i forskrift om tilgang til helseopplysninger mellom virksomheter.

Sikkerhetsarkitektur ved samhandling mellom virksomheter

Tilgang mellom virksomheter forutsetter at man har etablert en sikkerhetsarkitektur som sikre at kun autorisert personell får tilgang til helse- og personopplysninger.



Eksempel: Sikkerhetsarkitektur, tilgang mellom virksomheter

- Virksomheten har etablert minst to tekniske tiltak for å hindre uautorisert tilgang. I eksempelet har vi følgende tekniske tiltak:
  - Kommunikasjon mellom EPJ sikres med maskinsertifikat. Sertifikatet benyttes til to formål.
    - Gjensidig autentisere EPJ serverne for å sikre at trafikken kommer fra riktige servere plassert i sikker sone hos virksomhetene.
    - Sikrer at trafikken mellom serverne er kryptert ende til ende.
  - Brannmurer som styrer hvilken trafikk som slipper inn og ut av virksomheten.
  - Personlige sertifikater på brukernivå for sikker autentisering av den som skal hente informasjon.

- Hendelsesregistrering hos begge virksomhetene sikrer muligheten for etterkontroll av tilganger.
- Autorisasjonsregister hos begge virksomhetene sikrer muligheten for rollebasert tilgangsstyring og lovpålagt lagring av autorisasjonsregisteret.