NORMEN

Sikkerhetsrevisjon (faktaark 06)

Versjon 4.1
19.09.2018

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 sikkerhetsrevisjon og hvordan virksomheten skal og bør gjennomføre en sikkerhetsrevisjon. Alle virksomheter som behandler helse- og personopplysninger, er pålagt å gjennomføre sikkerhetsrevisjoner. Sikkerhetsrevisjonen må tilpasses omfanget av virksomheten. Det er virksomhetens ledelse som har et ansvar for at det gjennomføres sikkerhetsrevisjoner. Databehandler har et selvstendig ansvar for å gjennomføre sikkerhetsrevisjoner. Sikkerhetsrevisjonen skal gjennomføres jevnlig og minimum årlig. Formålet med å gjennomføre sikkerhetsrevisjon er å: • Kontrollere at det er gjennomført nødvendige sikkerhetstiltak ift gjennomførte risikovurderinger • Vurdere om sikkerhetstiltakene er tilstrekkelige • Kontrollere at lover og regler ift. informasjonssikkerhet følges • Sikre at etablerte prosedyrer for sikkerhet benyttes og fungerer etter hensikten
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • Virksomhetens leder/ledelse • Sikkerhetsleder • Personvernombud • IKT-ansvarlig • Databehandler • Leverandør
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen: • Kapittel 5.4.6 Sikkerhetsrevisjon i Normen
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser er spesielt relevante for faktaarket: • Personvernforordningen artikkel 32, første ledd bokstav d. • Pasientjournalloven § 23.

Sikkerhetsrevisjon

Virksomhetens ledelse er ansvarlig for at det gjennomføres sikkerhetsrevisjon. For mindre virksomheter bør daglig leder selv gjennomføre sikkerhetsrevisjonene, i samarbeid med andre som har roller tilknyttet sikkerhet og drift av datasystemene. I større virksomheter kan den praktiske gjennomføringen gjøres av for eksempel sikkerhetsleder eller personvernombud. Det presiseres at det ikke er krav om bruk av ekstern revisor.

Resultater fra sikkerhetsrevisjonen skal dokumenteres og gjennomgås i forbindelse med ledelsens gjennomgang. I tillegg skal det i etterkant av den enkelte revisjon vurderes gjennomføring av tiltak for å rette opp avvik som er avdekket. Identifiserte avvik skal behandles i samsvar med prosedyre for avviksbehandling. I den årlige sikkerhetsrevisjon skal det kontrolleres at alle avvik er håndtert.

Omfanget av sikkerhetsrevisjoner skal tilpasses virksomhetens størrelse og behov og dekke relevante områder som har betydning for tilfredsstillende informasjonssikkerhet. Det anbefales å gjennomføre mindre revisjoner som dekker enkeltområder og som til sammen dekker hele området i løpet av en periode. For eksempel kan en sikkerhetsrevisjon dekke:

- fysisk sikring av lokaler som benyttes til behandling av helse- og personopplysninger
- prosedyre for kontroll av hendelsesregistre
- prosedyre ved fratredelse av ansatt / medarbeider
- tilgang til helseopplysninger mellom virksomheter
- gjennomgang og kontroll av oppføringer i autorisasjonsregisteret

Databehandler skal gjennomføre sikkerhetsrevisjon av egen behandling av helse- og personopplysninger. For å ivareta dataansvarliges plikt til å forsikre seg om at informasjonssikkerheten er tilfredsstillende bør databehandler utlevere resultat fra gjennomførte sikkerhetsrevisjoner til dataansvarlig. Dette avtales i databehandleravtalen.

For en komplett sikkerhetsrevisjon av alle Normens krav kan vedlegget til Normens krav benyttes. Vedlegget kan benyttes som grunnlag for å utarbeide egne revisjonslister tilpasset virksomhetens art og omfang.