Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Sikkerhetsrevisjon

Støttedokument
Faktaark nr 6
Versjon: 4.1
Dato: 19.09.2018

Formål	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		
Ansvar	Virksomhetens ledelse har et ansvar for at det gjennomføres sikkerhetsrevisjoner. Databehandler har et selvstendig ansvar for å gjennomføre sikkerhetsrevisjoner.		
Gjennomføring	Gjennomføres jevnlig og minimum årlig		
Omfang	Alle virksomheter som behandler helse- og personopplysninger er pålagt å gjennomføre sikkerhetsrevisjoner. Sikkerhetsrevisjonen må tilpasses omfanget av virksomheten.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☐ Prosjektleder forskning ☒ Sikkerhetsleder	☐ Ansatt / medarbeider ☐ Forsker ☒ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☒ Leverandør
Hjemmel	• Personvernforordningen artikkel 32, første ledd bokstav d. • Pasientjournalloven § 23		
Referanser	• Norm for informasjonssikkerhet, kap. 5.4.6 • Faktaark 6b – Sikkerhetsrevisjon - sjekkliste		

Merknad 19.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

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 ift. 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 ifm 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 iht 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 ila 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 Faktaark 6b – Sikkerhetsrevisjon – sjekkliste benyttes. Faktaarket kan benyttes som grunnlag for å utarbeide egne revisjonslister for eksempel ift de 4 områdene faktaarket er delt opp i.