Internkontroll

17.11.21

Kurset «Intro om Normen»

Normens krav til ledelse og ansvar

- Virksomhetenes øverste ledelse har ansvar for at virksomheten følger gjeldende krav etter Normen og lovgivning

- Virksomhetens øverste ledelse skal sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver

  - Virksomheten beslutter hvilke roller og funksjoner for informasjonssikkerhet og personvern som er nødvendig

Kjært barn har mange navn

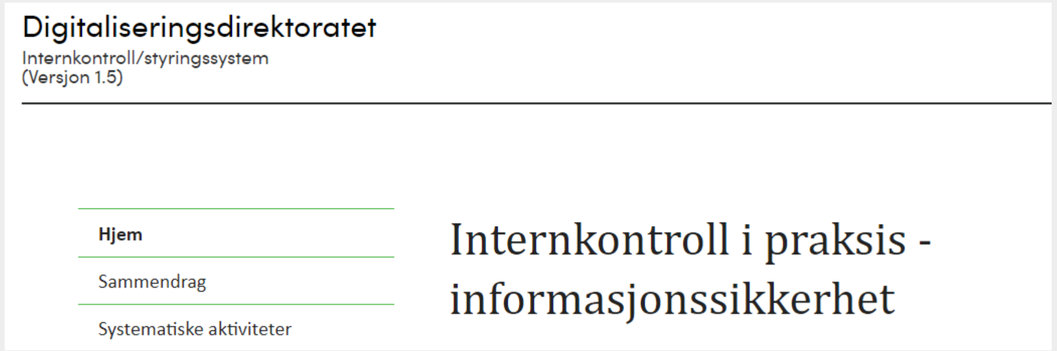
NORMEN

Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Direktoratet for e-helse

Styringssystem for informasjonssikkerhet og personvern

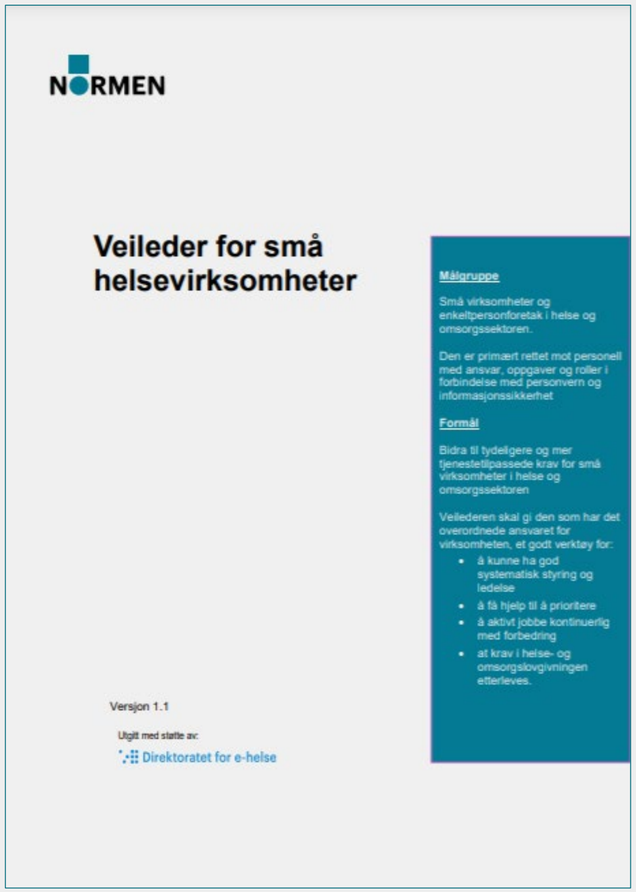
Støttedokument
Faktaark nr 2
Versjon: 3.2
Dato: 24.10.2019



Digitaliseringsdirektoratet
Internkontroll/styringssystem
(Versjon 1.5)

Hjem
Sammendrag
Systematiske aktiviteter

Internkontroll i praksis - informasjonssikkerhet



NORMEN

Veileder for små helsevirksomheter

Målgruppe

Små virksomheter og enkeltpersonforetak i helse og omsorgssektoren.

Den er primært rettet mot personell med ansvar, oppgaver og roller i forbindelse med personvern og informasjonssikkerhet

Formål

Bidra til tydeligere og mer tjenestetilpassede krav for små virksomheter i helse og omsorgssektoren

Veilederen skal gi den som har det overordnede ansvaret for virksomheten, et godt verktøy for:

- å kunne ha god systematisk styring og ledelse
- å få hjelp til å prioritere
- å aktivt jobbe kontinuerlig med forbedring
- at krav i helse- og omsorgslovgivningen etterleves.

Versjon 1.1

Utgitt med støtte av:
Direktoratet for e-helse

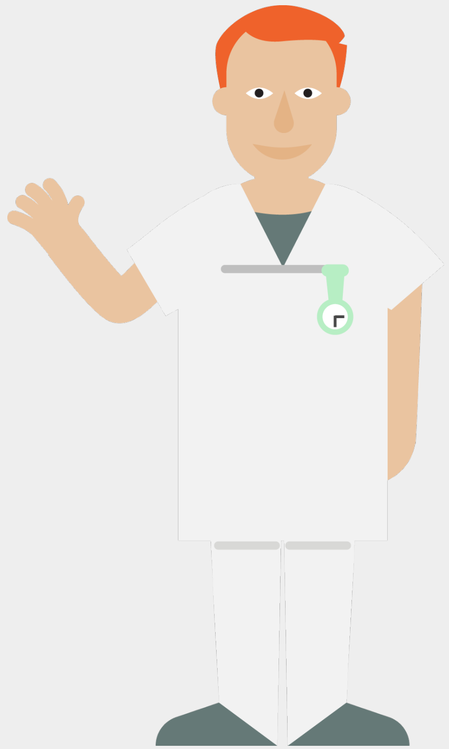
Direktoratet for e-helse

Ledelsessystem for informasjonssikkerhet

Ledelsessystem for informasjonssikkerhet i direktoratet for e-helse

Hvordan ha velfungerende styring og kontroll?

- Etablere et styringssystem / internkontroll for informasjonssikkerhet og personvern
  - Tilpasses virksomhetenes størrelse, risiko, egenart, aktiviteter og de behandlinger din virksomhet gjennomfører
  - Ledelsen har ansvaret for styringssystemet og skal sørge for å gjøre dette kjent for alle ansatte
  - Styringssystemet skal dokumenteres, angitt med løpende oppdatering og arkiveres når det erstattes

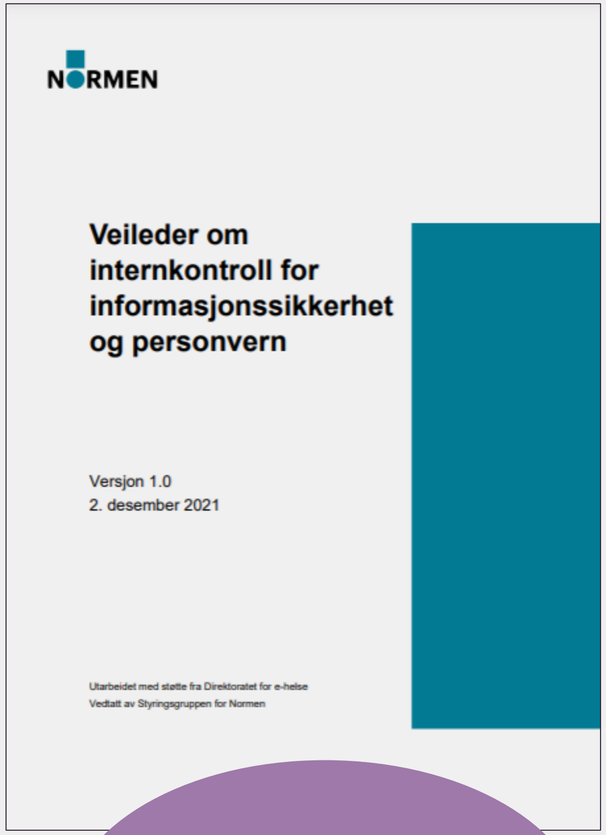


- Virksomhetens øverste ledelse skal selv gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året – Ledelsens gjennomgang
  - Ledelsens gjennomgang skal dokumenteres

Hvordan operasjonalisere et styringssystem?

Blant annet:

- Oversikt over behandlinger av helse- og personopplysninger
- Systemoversikt og klassifisering av systemer
- Rutine for opplæring
- Rutiner for plan, gjennomføring og oppfølging av risikovurderinger
- Oversikt over databehandlere og leverandører
- Rutine for oppretting og vedlikehold av autorisasjonsregister
- Rutine for sikkerhetskopiering
- Fysisk sikring av lokaler og områder
- Rutine for innsyn, informasjon, retting og sletting
- Rutine for tilgang til helseopplysninger
- Rutine for utlevering av helseopplysninger til kvalitetssikring
- Autentisering ved tilgang til helseopplysninger
- Avvikshåndtering



Se eksempel i vedlegg 3.2

NORMEN

3.2 Eksempel på styringssystemets innhold

I tabellen under er det listet opp et eksempel på hva styringssystemet for informasjonssikkerhet og personvern kan inneholde for en helsevirksomhet. Listene er veiledende og ikke uttømmende. Eksempelet betyr ikke at de ulike punktene som nevnes nødvendigvis bør være separate dokumenter. Det er innholdet som er viktig – styringssystemet kan fordeles på få eller mange dokumenter iht. virksomhetens størrelse behov. Hensikten med dette eksempelet er å vise de ulike temaene som naturlig inngår i styringssystem.

1. Styrende del:

- Beskrivelse av sikkerhetsmål og strategi for informasjonssikkerhet
- Overordnede føringer for bruk av informasjonsteknologi
- Beskrivelse av roller og ansvar i arbeidet med informasjonssikkerhet og personvern
- Oversikt over behandlinger av helse- og personopplysninger (protokoll, se faktaark 35)
- Vurdering av akseptabel risiko
- Systemoversikt og klassifisering av systemer
- IKT-sikkerhetsinstruks
- Rutine for plan for og gjennomføring av risikovurdering og oppfølging av resultater fra risikovurderinger

2. Gjennomførende del:

- Rutine og mal for gjennomføring av risikovurdering (se kapittel om risikovurdering i Normens veileder om risikostyring i helse- og omsorgssektoren)
- Rutine for gjennomføring av DPIA, med tilhørende mal (se kapittel om vurdering av personvernkonsekvenser i Normens Veileder om risikostyring i helse- og omsorgssektore
- Mal for databehandleravtaler
- Oversikt over databehandlere og leverandører med avtaler
- Rutine (og eventuelt sjekkliste) for oppstart og endring av behandlingsaktiviteter (herunder ivaretakelse av personvernprinsippene (se Normens faktaark om personvernprinsippene) og kravene til overføring av personopplysninger til tredjeland
- Rutine for autorisering, endring og avslutning av tilganger
- Rutine for administrasjon av nøkler og adgangskort i adgangskontrollsystemet
- Rutine for oppretting og vedlikehold av autorisasjonsregister
- Rutine for å sammenstille logger med autorisasjonsregisteret
- Rutine for bruk av mobilt utstyr og hjemmekontor
- Rutine for den registrertes innsyn i helse- og personopplysninger
- Rutine for utlevering av helse- og personopplysninger til andre
- Rutine for ivaretakelse av reservasjonsretten (kan kombineres med rutine for håndtering av protester mot behandling av personopplysninger og krav om begrenset behandling av personopplysninger)

- Rutine for å gi informasjon til den registrerte om personvernrettigheter
- Rutine for innhenting av informert samtykke
- Rutine for håndtering av helse- og personopplysninger (herunder retting, oppbevaring, lagring og sletting/makulering)
- Konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av konfigurasjonen
- Rutine for konfigurasjonskontroll og konfigurasjonsendringer
- Rutine for styring og håndtering av tekniske sårbarheter
- Rutine for endringsledelse i forbindelse med programendringer
- Regler for håndtering av passord
- Rutine for sikkerhetskopiering (back-up)
- Bruk av Norsk Helsenett (helsenettet)
- Regler for fysisk sikring av lokaler og områder
- Rutine for opplæring i informasjonssikkerhet
- Rutine for lagring av informasjon på egen brukerkonto
- Rutine for digital kommunikasjon med og om pasienter
- Rutine for bruk av e-post, telefaks og mobiltelefon
- Rutine for hendelsesregistrering
- Taushetserklæring for ansatte ved tiltredelse
- Rutine og skjema for taushets- og brukererklæring for andre som skal ha tilgang til helse- og personopplysninger
- Rutine for anonymisering av helse- og personopplysninger
- Rutiner for bruk av informasjonssystemer
- Nødrutine for alternativ drift uten bruk av informasjonssystemene
- Nødrutine for alternativ drift med delvis støtte fra informasjonssystemene
- Rutine for tilgang til helseopplysninger mellom virksomheter
- Rutine for kontroll av tilgang til helseopplysninger mellom virksomheter
- Rutine for forskning på helse- og personopplysninger
- Rutine for utlevering av helseopplysninger til kvalitetssikring og læring
- Rutine for tilkobling av teknisk utstyr til internett
- Rutine for håndtering av flyttbare datalagringsmedier
- Rutine for bruk datanettverk
- Rutine for bruk av trådløs teknologi
- Regler for sikkerhet i nettverks- og tilgangssoner
- Rutine for tilknytning av leverandør for fjernaksess
- Krav til IKT-leverandør ved service og vedlikehold

Eksempel i vedlegg 3.2

3. Kontrollerende del:

- Rutine for avviksbehandling (se kapittel 2.4 i denne veilederen)
- Rutine for ledelsens gjennomgang (gjennomføres minimum en gang i året) (Se Normen kapittel 2.5/kapittel 2.3 i denne veilederen)
- Rutine for regelmessig gjennomføring av sikkerhetsrevisjoner (Se faktaark 6)
- Rutine for oppfølging av resultater av risikovurdering
- Rutine for oppfølging av logger i behandlingsrettede helseregistre (se Normens veileder om tilgangsstyring)

Normens krav til ledelse og ansvar – Dataansvar

Normens krav 2.2

2.2 Dataansvarliges ansvar

Dataansvarlig er den som alene eller sammen med andre virksomheter bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke midler som skal benyttes.

I personvernforordningen benyttes begrepet behandlingsansvarlig, som er det samme som dataansvarlig i helsesektoren.

Dataansvarlig skal

- delegere myndighet og oppgaver (jf. kap. 2.1)
- etablere og etterleve styringssystemet (jf. kap. 2.4)
- gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig (jf. kap. 3)
- sikre den registrertes rettigheter (jf. kap. 4)
- etablere og dokumentere tekniske og organisatoriske tiltak (jf. kap. 5)
- inngå og følge opp avtaler (jf. kap. 5.7)
- håndtere avvik (jf. kap. 5.8)

NORMEN

Ansvarlighetsprinsippet etter personvernforordningen

Normens krav 2.2

Dataansvarlig er ansvarlig for å opptre i henhold til personvernprinsippene. Dette innebærer at helse- og personopplysninger skal

- behandles på en lovlig måte (gyldig behandlingsgrunnlag)
- behandles på en rettferdig måte (med respekt for de registrertes interesser og rettigheter)
- behandles på en åpen måte (oversiktlig, forutsigbar og forståelig informasjon) med hensyn til den registrerte (pasienten/brukeren)
- bare registreres for bestemte formål som skal være legitime (som dokumentasjon av helsehjelp)
- være tilgjengelige for helsepersonell når dette er nødvendig for å kunne gi forsvarlig helsehjelp
- bare benyttes til de formål de er registrert for, med mindre det finnes behandlingsgrunnlag for andre formål
- være relevante, adekvate, korrekte og om nødvendig oppdaterte for de formål de er registrert for
- lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene
- sikres mot uautorisert tilgang, endring, ødeleggelse og spredning

Dataansvarlig skal dokumentere at virksomheten har gjennomført tiltak for å etterleve personvernforordningen.

NORMEN

Personvernforordningen

«Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige **gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov**.»

Artikkel 24:
Den behandlingsansvarliges (dataansvarliges) ansvar

= **Internkontroll**

Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten

- Med formål om å bidra til forsvarlige helse- og omsorgstjenester, pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves

- Den med det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter
  - Plikt til å planlegge
  - Plikt til å gjennomføre
  - Plikt til å evaluere
  - Plikt til å korrigere

§ 2.Virkeområde

Forskriften gjelder virksomheter som er pålagt internkontrollplikt etter

a) helsetilsynsloven § 5

b) spesialisthelsetjenesteloven § 2-1a tredje ledd

c) helse- og omsorgstjenesteloven § 3-1 tredje ledd eller

d) tannhelsetjenesteloven § 1-3a.

Forskriften gjelder også virksomheter som er pålagt plikt til å arbeide systematisk for kvalitetsforbedring og pasient- og brukersikkerhet etter

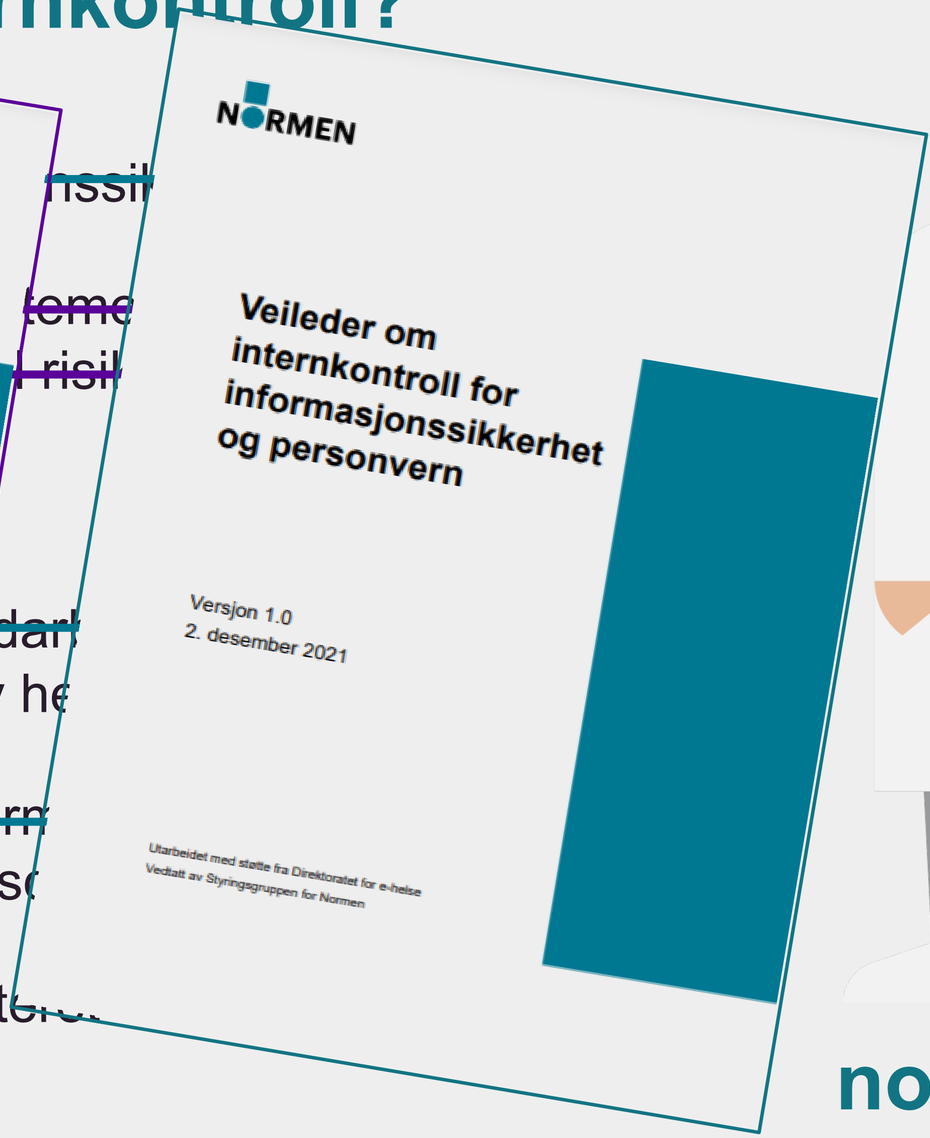
a) spesialisthelsetjenesteloven § 3-4a eller

b) helse- og omsorgstjenesteloven § 4-2.

NORMEN

Hvor finn[illegible] jeg mer om internkontroll?

- ~~Faktaark 01~~
- ~~Faktaark 0[illegible]~~ [illegible]nssik
  ~~personverr~~
- ~~Faktaark 0~~ [illegible]teme
- ~~Faktaark [illegible]~~ [illegible]risik
- Faktaark
- ~~Faktaark~~
- ~~Faktaark~~
- ~~Faktaark~~ [illegible]edark
- Faktaar [illegible]av he
  person
- ~~Faktaa~~ [illegible]nform
- Faktaa [illegible]hetsc
  prosje
- Faktaark 55 ~~– Opp~~ [illegible]egistre
- Veileder for små helsevirksomhe



normen.no