NORMEN

# Veileder om internkontroll for informasjonssikkerhet og personvern

Versjon 1.0

2. desember 2021

Utarbeidet med støtte fra Direktoratet for e-helse

Vedtatt av Styringsgruppen for Normen

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Normen forvaltes av Styringsgruppen for Normen, etter Normens forvaltningsmodell.

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. Innbyggere og ansatte skal være trygge på at opplysninger om dem behandles på en sikker måte i helse- og omsorgssektoren. Normen skal bidra til å at virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til hverandre, ved å etablere mekanismer og regler som sørger for at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Alt om Normen, Normens krav og veiledningsmateriell finnes på www.normen.no.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knyttet til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

# Innhold

# 1 Innledning

## 1.1 Bakgrunn

Internkontroll, styringssystem, ledelsessystem, styring og kontrollaktiviteter. Det kan være utfordrende for en virksomhet å få oversikt over hva som kreves for å ivareta eget ansvar. Mange aktiviteter inngår i den overordnede prosessen, og det er behov for å se hvordan de ulike delene av den samlede internkontrollen for informasjonssikkerhet og personvern bidrar til forsvarlige helse- og omsorgstjenester.

Normens veiledningsmateriell for ulike aktiviteter som inngår i internkontrollen har vært fordelt på en rekke ulike faktaark, som

- Faktaark 01 – Ansvar og organisering
- Faktaark 02 – Styringssystem for informasjonssikkerhet og personvern
- Faktaark 08 – Avviksbehandling
- Faktaark 09 – Opplæring av ledere og medarbeidere
- Faktaark 27 – Retningslinjer for daglig informasjonssikkerhet.

Versjon 6.0 av Normen inkluderer krav til personvern i tillegg til informasjonssikkerhet, som var hovedfokus i faktaarkene nevnt over. Videre har Normen tidligere ikke hatt egen veiledning på sikkerhetskultur, et tema som får stadig mer oppmerksomhet i sektoren og som henger naturlig sammen med temaer som opplæring, kompetanse og det daglige informasjonssikkerhetsarbeidet.

På bakgrunn av denne utviklingen har det vært naturlig å oppdatere veiledningsmateriellet på internkontrollområdet for å sette de ulike delaktivitetene inn i en større sammenheng, i en egen veileder om internkontroll for helse- og omsorgssektoren.

## 1.2 Tema for veilederen

Denne veilederen skal gi veiledning til, og bidra til etterlevelse av, kravene i Normen knyttet til internkontroll.

Med internkontroll menes i Normen planlagte og systematiske tiltak som skal sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lovgivningen.

Det omfatter en formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer, kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler. Den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll).

Kravene i Normen beskrives overordnet i kapittel 1.4 Krav i Normen, mens nærmere utdypning av kravene og hvordan de kan løses i praksis følger i kapittel 2 Internkontroll i helse- og omsorgssektoren.

## 1.3 Målgruppe

Målgruppen for veilederen er virksomheter som omfattes av Normen og som skal sikre etterlevelse av Normens krav, herunder dataansvarlig.

Veilederen er nyttig for alle ledere og medarbeidere i helse- og omsorgssektoren, særlig ved behov for å forstå hvordan ulike deler av internkontrollen fungerer i egen sektor eller virksomhet. Lederansvaret får særlig fokus i kapittelet om roller og ansvar, men ledere i helse- og omsorgssektoren er en særlig viktig målgruppe for veilederen som helhet.

Veilederen kan også være nyttig for systemleverandører og andre samarbeidspartnere til helse- og omsorgssektoren, som på grunn av sin leveranse eller engasjement er omfattet av Normen 6.0 gjennom avtale med virksomheten eller Norsk Helsenett SF.

## 1.4 Krav i Normen

Denne veilederen tar i all hovedsak for seg kravene i Normens kapittel 2. Ledelse og ansvar og 5. Informasjonssikkerhet. Krav i kapittel 3. Risikostyring vil behandles kort, men først og fremst for å vise sammenhengen med Normens Veileder om risikostyring i helse- og omsorgssektoren.

Tabellen som følger, gir en oversikt over sentrale krav for internkontroll fra Normen. Merk at tabellen ikke er uttømmende for en virksomhets totale internkontroll, og at mer om hvordan kravene i tabellen kan løses i praksis følger i kapittel 2 Internkontroll i helse- og omsorgssektoren.

| Virksomheten er ansvarlig for å | Se mer om kravet i Normen |
|---|---|
| Sørge for at virksomheten følger gjeldende krav til informasjonssikkerhet og personvern, inkludert å sørge for velfungerende styring og kontroll. Dette ansvaret ligger hos virksomhetens øverste ledelse, og bør ivaretas som en del av arbeidet med virksomhetsstyring og kvalitetsforbedring. | Kapittel 2. Ledelse og ansvar |
| Ivareta ansvaret som dataansvarlig, blant annet ved å<br>- delegere myndighet og oppgaver<br>- etablere og etterleve styringssystemet<br>- gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig<br>- sikre den registrertes rettigheter<br>- etablere og dokumentere tekniske og organisatoriske tiltak<br>- inngå og følge opp avtaler<br>- håndtere avvik<br>- opptre i henhold til personvernprinsippene<br>- dokumentere virksomhetens tiltak for å etterleve personvernforordningen | Kapittel 2.2 Dataansvarliges ansvar |
| Bistå dataansvarlig med å sikre overholdelse av forpliktelser til informasjonssikkerhet i de tilfeller der | Kapittel 2. Databehandlers ansvar |

| | |
|---|---|
| virksomheten er databehandler, og være ansvarlig for at underleverandører oppfyller sine forpliktelser. Databehandler har selvstendig ansvar for informasjonssikkerhet og for ivaretakelse av den registrertes personvern. | |
| Etablere et styringssystem for informasjonssikkerhet og personvern (internkontroll). Informasjonssikkerhet og personvern bør inngå som en del av det totale styringssystemet i virksomheten. Dette ansvaret ligger hos virksomhetens øverste ledelse. | Kapittel 2.4 Styringssystem |
| Gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året. Dette ansvaret ligger hos virksomhetens øverste ledelse. | Kapittel 2.5 Ledelsens gjennomgang |
| Etablere koordinerte aktiviteter for å rettlede og kontrollere virksomheten med hensyn til risiko (risikostyring). | Kapittel 3. Risikostyring;<br>Se veileder om risikostyring for detaljering av dette kravet. |
| Kontinuerlig lære opp medarbeidere i krav om ivaretakelse av taushetsplikten, informasjonssikkerheten og personvernet. | Kapittel 5.1 Medarbeidere, kompetanse og holdningsskapende arbeid;<br>Kapittel 5.1.1 Vilkår og betingelser |
| Etablere tiltak som sørger for at alle som gis tilgang til informasjonssystemer og tilhørende informasjon, har tilstrekkelig kompetanse til å benytte systemene og til å ivareta informasjonssikkerheten og personvernet til den registrerte. | Kapittel 5.1.2 Opplæring og kompetanse |
| Behandle uønskede hendelser (for eksempel brudd på rutiner, personvernet eller informasjonssikkerheten) som avvik. Etablere rutiner for å oppdage og håndtere avvik, og behandle disse for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse. | Kapittel 5.8 Håndtering av informasjonssikkerhetsbrudd;<br>Kapittel 5.8.1 Avvikshåndtering |

## 1.5 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

Forskrift for ledelse og kvalitetsforbedring i helse- og omsorgstjenesten skal bidra til faglig forsvarlige helse- og omsorgstjenester, kvalitetsforbedring og pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves. Dette skal blant annet gjøres ved at den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter i tråd med forskriften, og at medarbeiderne i virksomheten medvirker til dette. Styringssystemet skal tilpasses

virksomhetens størrelse, egenart, aktiviteter og risikoforhold og ha det omfang som er nødvendig, og det beskrives en rekke relevante plikter i § 6-9 av denne forskriften.[1]

Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) beskriver virksomheters plikter ved behandling av helseopplysninger, og § 23 Internkontroll beskriver at dataansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med lovgivningen, og at tiltakene skal dokumenteres og være tilgjengelig både for medarbeidere og tilsynsmyndighetene.[2] Videre plikter alle virksomheter som omfattes av arbeidsmiljøloven å innføre og utøve internkontroll etter forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften).[3]

Det er flere artikler fra Lov om behandling av personopplysninger (personopplysningsloven) som er relevante for kravene som dekkes av denne veilederen. Loven gjennomfører personvernforordningen (GDPR) i Norge. Et av personvernprinsippene som beskrives i forordningens artikkel 5[4] er at den dataansvarlige er ansvarlig for og skal kunne påvise at virksomheten behandler opplysninger i samsvar med de andre prinsippene. For mer om personvernprinsippene, se Normens faktaark om temaet.[5]

Forordningens artikkel 24 beskriver dataansvarliges ansvar. Artikkelen fremhever at virksomheten skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad, for å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med kravene i forordningen. [6] Artikkelen omhandler med andre ord internkontroll, og den fordrer risikobaserte tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.

Se for øvrig vedlegget til Normen, med samlet oversikt over alle Normens krav og lovhjemmel for disse, på Normens nettsider.[7]

I tillegg til Normens krav, som er grunnlaget for Normens veiledning, baseres metoden for internkontroll på innhold blant annet fra Digitaliseringsdirektoratets veiledning Internkontroll i praksis – informasjonssikkerhet[8] samt sentrale krav og aktiviteter som beskrives i Digitaliseringsdirektoratets sammenstilling av standarden ISO/IEC 27001:2013 tilpasset norsk offentlig sektor.[9] Videre ser veilederen hen på blant annet Veiledning i helhetlig styring og kontroll av informasjonssikkerhet, som er resultatet av et samarbeid mellom Nasjonal

---

[1] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten, 2016: https://lovdata.no/dokument/LTI/forskrift/2016-10-28-1250
[2] Lov om behandling av helseopplysninger ved ytelse av helsehjelp, 2014: https://lovdata.no/dokument/NL/lov/2014-06-20-42
[3] Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter, 1997: https://lovdata.no/dokument/SF/forskrift/1996-12-06-1127
[4] Lov om behandling av personopplysninger, 2018: https://lovdata.no/dokument/NL/lov/2018-06-15-38/
[5] Normens Faktaark 57 – Personvernprinsippene, https://www.ehelse.no/normen/faktaark/faktaaark-57-personvernprinsippene
[6] Lov om behandling av personopplysninger, 2018: https://lovdata.no/dokument/NL/lov/2018-06-15-38/
[7] Normens nettsider, Oversikt over Normens krav, https://www.ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen
[8] Digitaliseringsdirektoratet, Internkontroll i praksis – informasjonssikkerhet, https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601
[9] Digitaliseringsdirektoratet, Hva sier ISO/IEC 27001?, https://www.digdir.no/informasjonssikkerhet/kva-seier-ns-isoiec-27001/3060

sikkerhetsmyndighet, Direktoratet for forvaltning og økonomistyring og Digitaliseringsdirektoratet, med bidrag fra Datatilsynet og KS.[10]

## 1.6 Avgrensning

Denne veilederen er avgrenset til internkontroll innenfor Normens temaområder i helse- og omsorgssektoren, informasjonssikkerhet og personvern. Se oversikt over krav i Normen i kapittel 1.4. Risikostyring behandles kort, først og fremst for å vise sammenhengen med Normens Veileder om risikostyring i helse- og omsorgssektoren.

Selv om risikostyring som prosess er en del av virksomhetens internkontroll, beskrives ikke kravene til denne nærmere i denne veilederen. De beskrives i Veileder om risikostyring for informasjonssikkerhet og personvern, som ble utviklet parallell med denne veilederen. Det vil være nyttig å lese også den veilederen, for å sørge for en god forståelse av hvordan disse prosessene henger sammen og utfyller hverandre.

Når anbefalingene i veilederen tas i bruk i virksomheten, må de tilpasses med utgangspunkt i virksomhetens kompleksitet og størrelse, samt konkrete behov og oppgaver. Det kan være ulike måter å etterleve enkeltkrav på.

Internkontroll for informasjonssikkerhet og personvern er en prosess som er en del av en virksomhets helhetlige internkontroll. Likevel tar ikke denne veilederen for seg øvrige krav som er en del av internkontrollen på andre områder.

Virksomheter i helse- og omsorgssektoren må ta hensyn til virksomhetens interne systemer som håndterer blant annet ansattopplysninger, på samme måte som virksomheter i andre sektorer. Denne veilederen avgrenser ikke mot behandling av ansattopplysninger, men har heller ikke fokus på det. Prinsipper for behandling av helse- og personopplysninger som beskrives i denne veilederen vil kunne være nyttige også med tanke på behandling av opplysninger om egne ansatte.

Veilederen tar heller ikke for seg krav til internkontroll for informasjonssikkerhet og personvern utover det som faller inn under Normens virkeområde, som er helse- og omsorgssektoren.

[10] Digitaliseringsdirektoratet, Helhetlig styring og kontroll av informasjonssikkerhet, https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

# 2 Internkontroll i helse- og omsorgssektoren

Den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll).

Internkontroll skal være formalisert, og det er et krav i Normen at dokumentasjon om internkontrollen til enhver tid skal være oppdatert og lett tilgjengelig for alle ansatte. Det må også etableres rutiner for å sikre at styrende dokumenter til enhver tid er oppdaterte i tråd med krav i gjeldende lovverk, beslutninger, organisatoriske løsninger, rutiner og andre relevante styringsdokumenter. Informasjonssikkerhet og personvern bør inngå som en integrert del av den totale internkontrollen i virksomheten.

Internkontroll i helse- og omsorgssektoren består av planlagte og systematiske tiltak som skal sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lovgivningen. Det inkluderer både helselovgivningen og lovgivning som ikke kun gjelder for helse- og omsorgssektoren, som personopplysningsloven.

I helse- og omsorgssektoren behandles det store mengder opplysninger som grunnlag for gode helse- og omsorgstjenester, helseregistre, forskning og innovasjon. Opplysningene må behandles slik at helse- og omsorgstjenester kan tilbys på en forsvarlig måte og samtidig ivaretar innbyggernes tillit til sektoren. God informasjonssikkerhet og godt personvern er en forutsetning for digitalisering. Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur.[11] Tilstrekkelig internkontroll er en forutsetning for dette.

God pasientsikkerhet krever at opplysninger lagres og deles mellom helsepersonell, at opplysningene er tilgjengelige, korrekte og oppdaterte, samt at pasient, bruker og helsepersonell har tillit til systemer og personell. Mangelfull informasjon og svikt i overganger innad og mellom helsetjenestenivåer er dokumentert som et av de største risikoområdene for god pasientsikkerhet. Informasjonssikkerhet handler blant annet om å vurdere og håndtere risiko relatert til informasjon, herunder behandling av helse- og personopplysninger. Informasjonens integritet, tilgjengelighet og konfidensialitet skal sikres. God informasjonssikkerhet er viktig for å kunne utøve forsvarlige helsetjenester,[12] og internkontroll er et av de mest sentrale verktøyene som understøtter dette målet.

For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig og se informasjonssikkerhet som en del av virksomhetsstyringen. Internkontroll for informasjonssikkerhet og personvern må være en integrert del av virksomhetens øvrige internkontroll. Ved å se på informasjonssikkerhet og personvern som integrerte deler av virksomhetens øvrige prosesser vil man kunne oppnå balanse og avstemme mellom ulike fagområder på tvers av virksomheten, og blant annet kunne se samspillet mellom

[11] Helse- og omsorgsdepartementet, Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten, 2019: https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

[12] Helse- og omsorgsdepartementet, Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten, 2019: https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

informasjonssikkerhet, personvern og pasientsikkerhet. Virksomhetens ledelse vil gjennom god, helhetlig virksomhetsstyring få en totaloversikt over virksomhetens aktiviteter med sikte på å evaluere og drive kontinuerlig forbedring. For mer om helhetlig styring og kontroll av informasjonssikkerhet som en del av virksomhetsstyringen, se Digitaliseringsdirektoratets veiledningsmateriell på temaet.[13]

## 2.1 Roller og ansvar

Virksomhetene i helse- og omsorgssektoren er dataansvarlig[14] for all behandling av helse- og personopplysning som skjer i eller på vegne av virksomheten. Dataansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten.

Dataansvarlig er ansvarlig for informasjonssikkerheten i virksomheten og skal påse at nødvendige tiltak er iverksatt for å ivareta denne.

Dataansvarlig skal videre påse at behandlingen av helse- og personopplysninger og informasjonssikkerheten organiseres slik at det er tydelig hvem som har ansvar for de ulike deler av behandlingen. Ansvar og organisering skal dokumenteres før behandling av helse- og personopplysninger begynner. Dette inkluderer all behandling, også opplysninger om f.eks. pasienters pårørende og ansatte.

Ansvaret for informasjonssikkerhet innebærer både et overordnet ansvar for at virksomheten har tilfredsstillende og dekkende informasjonssikkerhet iht. Normen, og et ansvar for at ledere på alle nivåer, ansatte/medarbeidere, innleid personell og leverandører følger de spesifikke krav og plikter som gjelder i virksomheten.

Det er virksomhetens øverste ledelse som har ansvaret for styringssystemet for informasjonssikkerhet og personvern, herunder etablering, implementering og forvaltning av styringssystemet.[15] Dette ansvaret omfatter blant annet å sikre at det gis tilstrekkelige økonomiske rammer og ressurser for gjennomføring av nødvendige aktiviteter.[16] Videre har virksomhetens øverste ledelse et ansvar for å sikre at kravene til informasjonssikkerhet og personvern etterleves på alle nivåer i virksomheten, samt sørge for at styringssystemet kommuniseres og tilgjengeliggjøres for samtlige ansatte i virksomheten.[17]

Risikostyringsprosessen er en sentral del av internkontrollen, og roller og ansvar tilknyttet de ulike delprosessene som denne består av er beskrevet i nærmere detaljer i Veileder om risikostyring i helse- og omsorgssektoren. Virksomhetens øverste ledelse har også ansvar for hensiktsmessig risikostyring i virksomheten.

---

[13] Digitaliseringsdirektoratet, Helhetlig styring og kontroll av informasjonssikkerhet, https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

[14] I helse- og omsorgssektoren benyttes begrepet «dataansvarlig» der det i personvernforordningen kalles «behandlingsansvarlig».

[15] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 3.

[16] Normen 6.0 kapittel 2.4 femte avsnitt.

[17] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten §§ 6, 7 og 8, samt Normen 6.0 kapittel 2.4 femte avsnitt.

Databehandler har et selvstendig ansvar for at Normen følges slik det er regulert i avtale med virksomheten eller Norsk Helsenett SF. Databehandler har som alle andre virksomheter i helse- og omsorgssektoren plikt til å dokumentere sitt eget ansvar og sin egen organisering av arbeidet med informasjonssikkerhet og personvern.

Tabellen som følger viser eksempler på roller og ansvar innen internkontroll for informasjonssikkerhet og personvern. Den er ikke uttømmende, og enhver virksomhet kan ha andre roller som også er sentrale avhengig av intern organisering og type virksomhet. Eksempler på hvordan ulike roller, ansvar og oppgaver kan detaljeres ligger i vedlegg 3.1.

| Type virksomhet | Eksempel på roller og ansvar i virksomheten |
|---|---|
| Store virksomheter<br><br>(f.eks. sykehus, kommuner, mv.) | **Virksomhetens leder**<br>- Ivareta virksomhetens ansvar og oppgaver som dataansvarlig<br>- Fastsette mål og strategi for informasjonssikkerhet<br>- Fastsette akseptabel risiko<br>- Beskrive ansvar og myndighetsforhold<br>- Fastsette hvilke behandlinger av helse- og personopplysninger som skal utføres i virksomheten og sørge for at slik behandling dokumenteres (iht. artikkel 30)<br>- Be om forhåndsdrøfting med Datatilsynet ved behov<br>- Følge opp og kontrollere informasjonssikkerheten (inklusive databehandler og andre leverandører)<br>I en virksomhet som har et styre så er virksomhetens leder administrerende direktør. Styret har et ansvar for å følge opp at virksomheten har tilstrekkelige rutiner på særlig viktige strategiske områder. |
| | **Leder**<br>- Følge opp virksomhetsleders ansvar i egen avdeling<br>- Følge opp og kontrollere informasjonssikkerheten<br>- Prioritere og gjennomføre tiltak |
| | **Fagansvarlig informasjonssikkerhet**[18]<br>- Koordinere arbeidet med informasjonssikkerheten i virksomheten<br>- Rådgiver til ledelsen og virksomheten for øvrig på informasjonssikkerhetsområdet |
| | **Fagansvarlig personvern**<br>- Koordinere arbeidet med personvern i virksomheten<br>- Rådgiver til ledelsen og virksomheten for øvrig på personvernområdet |
| | **Fagansvarlig IKT**<br>- Sørge for at informasjonssystemet driftes og sikres iht. fastsatte krav |

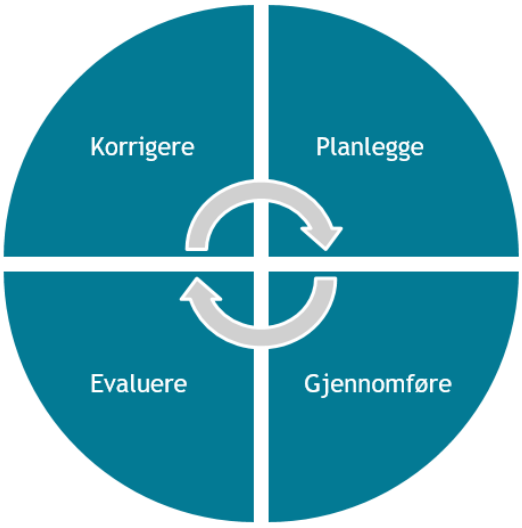
[18] Denne rollen kalles ofte informasjonssikkerhetsleder eller CISO.

| | |
|---|---|
| | - Etablere nødvendig beredskap og sikre at slik beredskap øves<br>- Følge opp leverandører og databehandler<br>I IKT-organisasjonen bør det også etableres en rolle som kontaktpunkt mot ekstern IKT-leverandør, dersom dette benyttes. |
| | **Systemeier**<br>- Sørge for at sitt informasjonssystem oppfyller Normens krav<br>- Sørge for at informasjonssystemet fungerer som besluttet<br>- Definere tilgangsroller<br>- Rapportere til IKT-ansvarlig |
| | **Risikoeier**<br>- Definert av virksomheten som ansvarlig for måloppnåelse og tilhørende risiko på et definert område etter forhåndsdefinerte kriterier. For særlig høy risiko vil risikoeier ofte være virksomhetens leder. |
| | **Personvernombud**<br>- Rådgiver til ledelsen på personvernområdet |
| | **Ansatt/medarbeider**<br>- Følge virksomhetens sikkerhetsprosedyrer |
| Små virksomheter<br><br>(f.eks. legekontor, tannlegekontor, fysioterapeutpraksis, psykologfellesskap, kiropraktor, manuellterapeut, bedriftshelsetjeneste) | **Virksomhetens leder**<br>- Definere mål og strategi for informasjonssikkerhet<br>- Fastsette akseptabel risiko<br>- Beskrive ansvar og myndighetsforhold (benytt vedlagte eksempel til å definere ansvarsområder)<br>- Fastsette hvilke behandlinger av helse- og personopplysninger som skal utføres i virksomheten og sørge for at slik behandling dokumenteres (iht. artikkel 30)<br>- Melde til og eventuelt be om forhåndsdrøfting med Datatilsynet<br>- Vurdere eventuell løsning for fjernaksess opp mot Normens krav og veiledning<br>- Følge opp og kontrollere informasjonssikkerheten (inklusive databehandler og andre leverandører)<br>- Prioritere tiltak og sørge for kontroll med at tiltak etterleves |
| | **Ansatt/medarbeider**<br>- Følge virksomhetens sikkerhetsprosedyrer |

## 2.2 Styringssystem for informasjonssikkerhet og personvern

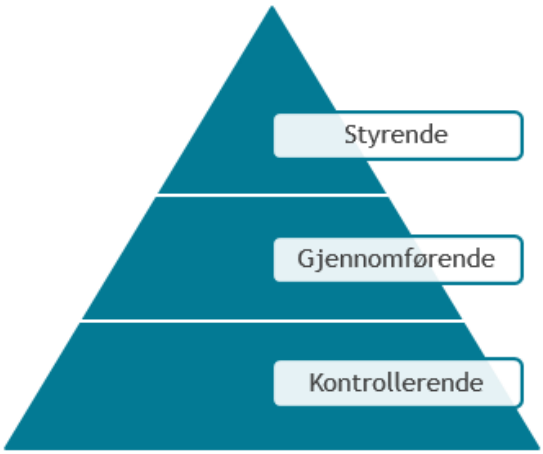
Alle virksomheter i helse- og omsorgstjenesten skal etablere styringssystem[19] for informasjonssikkerhet og personvern.[20] Med styringssystem menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer og korrigerer etterlevelse av relevante eksterne og interne føringer, som eksempelvis føringer i lov og forskrift, tildelingsbrev, avtaler med leverandører og kunder, og interne policyer, retningslinjer og krav. Et godt styringssystem bidrar til at virksomheter i helse- og omsorgssektoren oppnår sine virksomhetsmål om å levere gode tjenester for pasienter og brukere, i tillegg til etterlevelse.[21]

Styringssystemet kan fremstilles som en syklus, som i figuren under.




Styringssystemet kan også fremstilles som et tredelt hierarki, med en styrende, gjennomførende og kontrollerende del. Dette illustreres i figuren som følger.

[19] Begrepene styringssystem, ledelsessystem og internkontroll benyttes om hverandre i faglitteraturen. Styringssystem og ledelsessystem benyttes typisk når det er snakk om informasjonssikkerhet, og begrepet internkontroll benyttes når det er snakk om personvern.
[20] Se også personvernforordningen artikkel 24 og 32, pasientjournalloven §§ 22 og 23, helseregisterloven §§ 21 og 22 og forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten §§ 3 og 5 til 9.
[21] NS-ISO/IEC 27701 beskriver informasjonshåndteringssystem for personvern (PIMS) basert på ledelsesstandarden for informasjonssikkerhet, NS-EN ISO/IEC 27001, og kan være et nyttig verktøy for å integrere styringssystem også på personvernområdet.




Formålet med et styringssystem for informasjonssikkerhet og personvern er å:

- sikre at virksomheten har tilstrekkelig styring og kontroll på informasjonssikkerheten, herunder sikring av informasjonens konfidensialitet, integritet og tilgjengelighet
- sikre og påvise virksomhetens etterlevelse av personvernlovgivningen i samsvar med kravene som beskrives i personvernforordningen artikkel 5 og artikkel 24, pasientjournalloven § 23 og helseregisterloven § 22
- sikre at arbeidet med informasjonssikkerhet og personvern ivaretas på en systematisk måte
- være et verktøy for sikre at nødvendige sikkerhetstiltak etableres i virksomheten mot tilsiktede og utilsiktede hendelser som kan påvirke behandlingen av helse- og personopplysninger.

For alle offentlige virksomheter i sektoren skal det beskrives mål og etableres en strategi for informasjonssikkerhet.[22] Dette er med på å danne grunnlaget for styringssystemet. Også private virksomheter bør beskrive mål og etablere en informasjonssikkerhetsstrategi i samsvar med god praksis.[23] Risikostyringsprosessen er en svært viktig del av styringssystemet, og danner grunnlag for å avklare hvilke eksisterende tiltak som er tilfredsstillende, samt hvilke tiltak som må gjennomføres for å oppnå tilstrekkelig informasjonssikkerhet og personvern. Flere detaljer om denne prosessen finnes i Veileder om risikostyring i helse- og omsorgssektoren.

At oppbyggingen av styringssystem for personvern og informasjonssikkerhet skal være risikobasert, følger av personvernforordningen artikkel 24 og 32, pasientjournalloven §§ 22 og 23, helseregisterloven §§ 21 og 22. Dette har også støtte i forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 5, som uttrykkelig pålegger virksomheten

[22] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 beskriver videre at internkontroll på informasjonssikkerhetsområdet skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet.
[23] ISO/IEC 27001 kapittel 6.2

å ta hensyn til risikoforhold når den utarbeider styringssystem som skal sikre ivaretakelse av krav i helse- og omsorgslovgivningen.

Omfanget av styringssystemet og valg av egnede sikkerhetstiltak skal tilpasses virksomhetens størrelse, egenart og aktiviteter og behandlingene av helse- og personopplysningenes art, omfang, formål og sammenhengen den utføres i. Dette innebærer at styringssystemet i mindre helsevirksomheter ikke trenger å være like omfattende som styringssystemet til mer komplekse virksomheter.[24]

### 2.2.1 Kontinuerlig forbedring

Styringssystem for informasjonssikkerhet og personvern skal sikre at arbeidet med personvern og informasjonssikkerhet blir en kontinuerlig prosess. Det betyr at virksomheten hele tiden bør søke å forbedre seg og videreutvikle systemet i takt med endringer som påvirker informasjonssikkerhet og personvern i virksomheten. Virksomheten må også følge opp svakheter i styringsaktiviteter og tiltak må identifiseres og korrigeres.

For å sikre en helhetlig styring av risiko, anbefales det at styringssystemet for informasjonssikkerhet og personvern integreres i det totale styringssystemet i virksomheten.[25] Virksomheten oppnår flere fordeler knyttet til effektivitet og samordning ved å gjøre dette. Eksempelvis vil virksomheten unngå å operere med, og vedlikeholde, flere parallelle styringssystemer som i verste fall kan være motstridende på enkelte punkter. Videre er det enklere for ledelse å prioritere ressursfordeling ved å se på det helhetlige risikobildet virksomheten står overfor.

De aller fleste prosesser og aktiviteter som utføres i helse- og omsorgsvirksomheter involverer behandling av informasjon med beskyttelsesbehov i større eller mindre grad. Det er naturlig at den største oppmerksomheten rettes mot informasjon som behandles av helsepersonell ifm. ytelse av helsehjelp. Det er imidlertid viktig med oppmerksomhet om informasjonssikkerhet og personvern også der informasjonen brukes «sekundært», som for eksempel ved betaling og fakturering, forskning og som arbeidsgiver.

### 2.2.2 Krav til dokumentasjon

Det er krav til at styringssystemet dokumenteres, og at dokumentene holdes løpende oppdatert og eldre versjoner arkiveres.[26] Avslutningsvis i dette kapitlet vises et eksempel på hvilke typer dokumenter som skal eller bør utarbeides i virksomhetens styringssystem.

Dokumentasjon av risiko og tiltak knyttet til informasjonssikkerhet skal sikres ut fra de behov for sikkerhet som foreligger. Dersom dokumentasjon skal deles med annen virksomhet må dataansvarlig vurdere om detaljert informasjon som kan ha sikkerhetsmessig betydning skal fjernes før utlevering. Dette kan være for eksempel være informasjon om sårbarheter i egne virksomhetsprosesser eller systemer.

[24] Normen 6.0 kapittel 2.4 fjerde avsnitt
[25] Normen 6.0 kapittel 2.4 tredje avsnitt.
[26] Normen 6.0 – Kapittel 2.4 Styringssystem; Et dokumentert styringssystem vil også bidra til etterlevelse av kravet til å sikre og påvise egen etterlevelse av personvernlovgivning i samsvar med kravene i personvernforordningen artikkel 5 og artikkel 24, pasientjournalloven § 23 og helseregisterloven § 22

I dette kapitlet presenteres et eksempel på oppbygging av dokumentasjonen for et styringssystem for informasjonssikkerhet og personvern hos en helsevirksomhet. Dette eksempelet tar utgangspunkt i en hierarkisk oppbygning, med en styrende, gjennomførende og kontrollerende del.

Den styrende dokumentasjonen inneholder ledelsens krav til informasjonssikkerhet og personvern og beskriver de overordnede føringene som gjelder i virksomheten. Videre beskrives sikkerhetsorganisasjonen med hvilke roller som er ansvarlig for oppgavene på ulike nivåer. Som utgangspunkt for arbeidet med informasjonssikkerhet og personvern skal det utarbeides og vedlikeholdes en oversikt over hvilke behandlinger av helse- og personopplysninger virksomheten utfører.

Den gjennomførende dokumentasjonen inneholder detaljerte rutiner, instrukser og prosessbeskrivelser som skal sikre etterlevelse av kravene til informasjonssikkerhet og personvern som er beskrevet i den styrende dokumentasjonen. Reglene og kravene gjelder både ledelsen, den enkelte medarbeider og ansvarlige for informasjonsteknologi. Det handler ikke nødvendigvis om å beskrive nye rutiner, instrukser og prosessbeskrivelser, det kan like gjerne være dokumentasjon av allerede eksisterende aktiviteter. I sin enkleste form kan en prosessbeskrivelse være en sjekkliste.

Den kontrollerende dokumentasjonen beskriver kontrollmekanismene som skal benyttes for å kontrollere at målene oppnås, kravene etterleves samt at rutinene følges. Den kontrollerende dokumentasjonen kan for eksempel være rutine for ledelsens gjennomgang, revisjonsplaner og -rapporter, logger fra systemene og avviksrapporter.

I Vedlegg 3.2 er det listet opp et eksempel på hva styringssystemet for informasjonssikkerhet og personvern kan inneholde for en helsevirksomhet.

## 2.3 Ledelsens gjennomgang

Normen stiller krav om at virksomhetens ledelse selv skal gjennomgå virksomhetens aktiviteter innen informasjonssikkerhets og personvern.[27] Dette er en viktig del av lederansvaret i helse- og omsorgssektoren.

Formålet med ledelsens gjennomgang er å sikre at styringssystemet for informasjonssikkerhet og personvern er tilstrekkelig og virkningsfullt ut ifra formålet, kravene og risikoene til virksomheten. Gjennomgangen skal gi ledelsen et grunnlag for å fatte velinformerte strategiske beslutninger om hva som skal gjøres for å utvikle og forbedre informasjonssikkerheten og personvernet.

### 2.3.1 Hva som bør inngå i ledelsens gjennomgang

Virksomhetens øverste ledelse skal selv gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året. Følgende forhold vil normalt inngå i beslutningsgrunnlaget:

- Resultat fra risikovurderinger og personvernkonsekvensvurderinger
- Resultat av avviksbehandling
- Oppfølging av leverandører og databehandleravtaler

[27] Normen 6.0 kapittel 2.5

- Vurderinger av akseptabel risiko[28]

Hva som er akseptabelt risikonivå vil variere, og vil bero på de konkrete omstendighetene. I henhold til personvernforordningens artikkel 32 skal det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

I tillegg bør også en del andre forhold inngå i beslutningsgrunnlaget, for eksempel:[29]

- Status for tiltak besluttet under tidligere ledelsens gjennomganger
- Status for tiltak fastsatt i planer for risikohåndtering
- Oppnåelse av beskrevne sikkerhetsmål (f.eks. i målrapporteringen, ofte formulert som «Key Performance Indicators» (KPIer) på området)
- Endringer i eksterne krav innen informasjonssikkerhet og personvern (f.eks. lover, forskrifter og tildelingsbrev, samt avtaler med kunder, leverandører og andre samarbeidspartnere)
- Endringer innen infrastruktur, informasjonssystemer og behandlinger av helse- og personopplysninger
- Resultat fra interne målinger og evalueringer, herunder fra inntrengningstester i informasjonssystemer, målinger av sikkerhetskultur og evalueringer etter øvelser, samt antall deltakere på kompetansetiltak om informasjonssikkerhet og personvern
- Resultat fra interne revisjoner og offentlige tilsyn
- Relevante vurderinger og råd fra nasjonale sikkerhetsmyndigheter eller sektormyndigheter (årlige rapporter eller temarapporter)
- Muligheter for forbedring av styringssystemet.

Dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar. Fordi tiltak innen informasjonssikkerhet og personvern ofte har økonomiske kostnader, og prioritet opp imot andre tiltak må avklares, bør tiltaksplanen inngå i budsjettprosessen til virksomheten.

### 2.3.2 Hvem som skal eller bør delta i ledelsens gjennomgang

Det fremgår av Normens krav om ledelsens gjennomgang, at gjennomgangen skal foretas av virksomhetens øverste ledelse. I tillegg bør ledere og sentrale fagpersoner på områder av betydning for informasjonssikkerhet og personvern, delta.

Gjennomgangen fasiliteres ofte av informasjonssikkerhetsleder, men denne oppgaven kan også være hensiktsmessig for personell med roller innen f.eks. personvern, virksomhetsstyring eller internrevisjon.

For små og mellomstore virksomheter som f.eks. en behandlingsklinikk eller et privat sykehus, kan det være naturlig at også ledergruppen er involvert i hele gjennomgangen. For

[28] Les mer om akseptabel risiko i Normens veileder om risikostyring for informasjonssikkerhet og personvern.
[29] Mange av disse forholdene fremgår av NS-ISO/IEC 27001 kapittel 9, som må anses å uttrykke beste praksis på området.

de aller minste virksomhetene vil det kanskje være realistisk at alle de ansatte «tar sikkerhetspraten» i felleskap.

I store virksomheter som f.eks. et helseforetak, vil ansvarsområdet kunne omfatte mange og komplekse forhold. Mens selve ledelsens gjennomgang skal være på et overordnet nivå tilpasset toppledelsen, vil det være særlig viktig å gjennomgå detaljer med berørte enheter i virksomheten som en del av prosessen.

### 2.3.3 Hvordan ledelsens gjennomgang bør gjennomføres og dokumenteres

Ledelsens gjennomgang bør være på agendaen i et møte. Den som er gitt ansvaret for å fasilitere gjennomgangen bør utarbeide en agenda og sørge for at det blir avsatt tilstrekkelig tid.

Grunnlagsinformasjonen til møtet kan bestå av mange dokumenter med mye informasjon – spesielt i store virksomheter. Et tips kan være å ikke fremlegge dokumentene i sin helhet. Men i stedet utarbeide et saksfremlegg med en liste over hvilke dokumenter eller datauttrekk som utgjør grunnlaget, en oppsummering av de viktigste resultatene og utviklingstrekkene, og med tydelige anbefalinger om beslutninger.

Det er mulig å gjennomføre ledelsens gjennomgang for alle de ulike områdene i én og samme prosess, spesielt der mye er integrert i et stort helhetlig styringssystem. Fordelen er at det da er lettere å se indre sammenhenger og gjøre mer helhetlige tiltak, for eksempel mellom informasjonssikkerhet, personvern og pasientsikkerhet. I praksis kan imidlertid en full gjennomgang av alle områdene i én og samme prosess bli for omfattende og lett føre til en for overfladisk behandling av hvert av områdene. Her må virksomhetene selv vurdere hva som blir mest hensiktsmessig i praksis.

I noen tilfeller kan de som fasiliterer og forbereder gjennomgangen oppdage at det er lite strukturert informasjon å basere seg på, typisk hvis styringssystemet er umodent og har vesentlige mangler. Dette vil være et funn i seg selv som er nyttig for ledelsen å vite om. Da vil de sentrale temaene under gjennomgangen kunne handle om å forbedre bl.a. risikostyring, måling, avviksrapportering eller revisjoner, slik at neste ledelsens gjennomgang får et bedre beslutningsgrunnlag.

Ledelsens gjennomgang skal dokumenteres. I tillegg til at agendaen og saksfremlegget bør være skriftlig, må det dokumenteres hvilke temaer som faktisk ble gjennomgått og hvilke beslutninger som ble fattet. Normalt bør det derfor utarbeides et møtereferat der dette, samt hvem som deltok på møtet, fremgår. Det må utarbeides en tiltaksplan, f.eks. som vedlegg til referatet eller som et eget dokument.

Når det gjelder frekvensen på ledelsens gjennomgang, er minstekravet i Normen én gang i året. Virksomheten må selv vurdere om det er behov for noe utover dette. Det kan være særlig relevant når virksomheten gjennomgår endringer som for eksempel ved oppstart av nye oppgaver, omorganiserer, endret infrastruktur eller behandling av helse- og personopplysninger.

**Eksempel:**
Normland Helsesenter skal ta sikkerhetspraten – de skal gjennomføre ledelsens gjennomgang for første gang, i forbindelse med et møte for de ansatte. Helsesenterets leder Lena leder møtet. Helsesekretær Maren lager referat.

Hovedpunkter fra møtet:

- Sjekkliste for sikkerhet: Må supplere oversikt over eksterne avtalepartnere med leverandør som håndterer makulering av papirdokumenter. Det mangler rutine for håndtering av elektroniske meldinger. Hva gjør vi hvis vi får feilmeldinger ved sending av f.eks henvisninger? Tiltak: Maren og kollega Morten lager forslag til rutine. Lena har overordnet ansvar for at det blir utført.
- Avvik: Det har flere ganger ligget igjen sensitive dokumenter som pasienter har glemt igjen på venterommet. Tiltak er instruks til renholder: Finner man slike dokumenter skal de låses inn på resepsjonskontoret. Til Maren og kollega Morten lager forslag til rutine. Lena har overordnet ansvar for at det blir utført.
- Risiko: Scenarioer gjengitt i veiledningsmateriell fra Normen er gjennomgått. Avdekket et scenario med ikke akseptabel risiko: Papirdokumenter scannes inn på feil pasient. Tiltak: Maren og kollega Morten lager forslag til rutine. Lena har overordnet ansvar for at det blir utført.
- Oversikter (bl.a. ansvar, funksjoner og oppgaver): Ingen endringer utover makulering som nevnt over • Oppfølging av leverandører og databehandlere: Dårlig tilgjengelighet på support hos EPJ-tjenesteleverandør. Følges opp av Lena mot kontaktperson.

Maren lagrer referatet i internkontrollsystemet etter at det er godkjent av Lena.

## 2.4 Avvik

Avvik, eller uønskede hendelser, er sikkerhetsbrudd og/eller når behandling av helse- og personopplysninger er utført i strid med gjeldende regelverk, retningslinjer eller rutiner.

For å sikre at regelverket følges skal det etableres avviksrutiner slik at avvik oppdages og at årsak til avviket, korrigerende tiltak, læring og rapportering blir dokumentert. Avvikshåndtering kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige rutiner.

Virksomheten skal samle inn fakta om hendelsesforløpet for etablering av korrigerende tiltak og effekten av korrigerende tiltak skal vurderes og eventuelle andre tiltak skal settes i verk ved behov.

Formålet med avviksbehandling er å:

- Håndtere sikkerhetsbrudd og andre uønskede hendelser på en systematisk måte
- Gjenopprette normaltilstanden etter et sikkerhetsbrudd eller en annen uønsket hendelse

- Vurdere endringer i sikkerhetsarbeidet for å hindre fremtidige sikkerhetsbrudd og andre uønskede hendelser (læring)
- Sikre at interessenter som ledelsen, Datatilsynet og den registrerte varsles ved brudd på personopplysningssikkerheten
- Sikre at politiet ved Kripos blir varslet ved hendelser tilknyttet adressesperre FORTROLIG og STRENGT FORTROLIG (kode 7 og 6)

Den enkelte medarbeider er ansvarlig for å rapportere avvik. Virksomhetens ledelse er ansvarlig for å behandle avvik og iverksette tiltak.

### 2.4.1 Sentrale roller i avvikshåndteringen

Den følgende tabellen beskriver ulike roller i avvikshåndteringen, med tilhørende bekrivelse og eksempler.

| Rolle | Beskrivelse |
|---|---|
| Avviksmelder | Den som melder inn avvik. Dette kan være alle ansatte i virksomheten og hos underleverandører/databehandlere. |
| Avviksbehandler | Den som er satt til å følge opp avvik i henhold til virksomhetens interne rutine. Dette kan være nærmeste leder, virksomhetens leder, prosesseier, fagansvarlig for personvern, informasjonssikkerhetsleder, IKT-ansvarlig. |
| Avvikseier | Den som eier avviket. Hvem som har denne rollen avhenger av årsaken til avviket. Eksempler kan være som følger:<br>- Ansatt har ikke fulgt etablert rutine, avviket kan eies av nærmeste leder<br>- Rutine mangler eller det er avdekket feil eller mangler i etablert rutine, avviket kan eies av prosesseier<br>- En digital sikkerhetshendelse som et dataangrep eller et svindelforsøk oppstår, avviket kan eies av IKT-leder<br>- Utdatert programvare og utstyr som ikke oppdateres, avviket kan eies av toppledelsen som dataansvarlig (med ansvar for økonomiske rammer til nødvendige endringer og oppdateringer)<br>- Manglende rutine for å ivareta den registrertes rettigheter, avviket kan eies av informasjonssikkerhetsansvarlig eller fagansvarlig for personvern |
| Tiltaksansvarlig | Den som får ansvar for å iverksette et konkret tiltak på vegne av avviksbehandler og/eller avvikseier. |

Ulike typer avvik krever at ulike roller er involvert i avvikshåndteringen.

Er årsaken til avviket mangler i virksomhetens overordnede styringssystem/ledelsessystem vil tiltakene iverksettes på et overordnet nivå (eier av prosessen ansvarlig) og ikke i linjen. Eksempel på slike typer avvik kan være manglende informasjonssikkerhetspolicy, manglende eller uklare regler/prosedyrer og prosesser eller manglende eller uklare rollebeskrivelser.

Dersom årsaken til avviket er en menneskelig feilhandling, dvs. at medarbeidere opptrer i strid med bestemmelser i virksomhetens styringssystem, bør tiltakene iverksettes i linjen gjennom nærmeste leder. Menneskelige feilhandlinger kan for eksempel skje fordi medarbeidere har manglende kunnskap/kjennskap til etablerte policyer, prosedyrer, prosesser, roller og ansvar, eller at medarbeidere kjenner til regelverket, men har manglende respekt for etablerte prosedyrer og prosesser, og etterlever derfor ikke regelverket. Om én ansatt gjør en slik feil er imidlertid sannsynligheten stor for at det er behov for tiltak i større deler av organisasjonen. Det er sjelden at den personen var den eneste som «ikke visste», sannsynligvis var det bare den som ble oppdaget.

### 2.4.2 Virksomhetens rapportering og melding til andre

I Normen omtales rapportering av avvik og brudd på personvern og informasjonssikkerhet til både Datatilsynet og Statens helsetilsyn, i tillegg til plikten til å underrette den registrerte.

**Datatilsynet**

Dersom det har skjedd et brudd på personopplysningssikkerheten i virksomheten og det er sannsynlig at bruddet vil medføre en risiko for de registrerte sine rettigheter og friheter, skal dataansvarlig **rapportere bruddet til Datatilsynet** innen 72 timer.[30] Datatilsynet beskriver på sine nettsider hvordan dette skal gjøres.[31]

Meldingen skal inneholde en beskrivelse av bruddet:

- Hovedårsaken
- Tidsrommet
- Når det ble oppdaget,
- Antall personer som er berørt
- Beskrivelse av hva som har skjedd
- Hvordan det oppstod
- Beskrivelse av hva slags personopplysninger som ble berørt
- Hvilken relasjon virksomheten har til de berørte personene (f.eks. ansatte, pasienter, pårørende eller leverandør)
- Beskrivelse av hvor personopplysningene befinner seg

I tillegg skal meldingen inneholde til beskrivelse av de sannsynlige konsekvensene av bruddet, beskrivelse av tiltak som er gjort og planlagt for å hindre gjentakelse, og hva som er gjort for å redusere skadevirkninger.

Utover brudd på personopplysningssikkerheten kan virksomheten velge å rapportere også andre typer avvik til Datatilsynet. Dette kan gjøres for å bistå tilsynet i deres arbeid, og for å redusere eventuelle gebyr, jf. at gebyr kan ilegges også uten at det er sikkerhetsbrudd, og da vil rapportering kunne være gebyrreduserende.

[30] I henhold til personvernforordningens artikkel 33.
[31] Datatilsynet, Melding avvik til Datatilsynet, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/meld-avvik-til-datatilsynet/; Her melder du avvik: https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/

### Den registrerte

Dataansvarlig skal **underrette den registrerte** dersom det er sannsynlig at et brudd på personopplysningssikkerheten vil medføre høy risiko for de registrerte (typisk pasienten eller brukeren).[32] Unntak til dette er dersom:

- Det er gjennomført tekniske og organisatoriske sikkerhetstiltak for de personopplysningene som er berørt, f.eks. tiltak som gjør opplysningene uleselige.
- Det er truffet tiltak i etterkant som gjør at det er lite trolig at bruddet har ført til utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert tilgjengeliggjøring av eller tilgang til personopplysninger.
- Om varslingen innebærer en uforholdsmessig stor innsats (f.eks. ved at bruddet berører et stort antall individer) skal allmennheten underrettes slik at den registrerte likevel underrettes på en effektiv måte.

Virksomheten skal som minimum gi den registrerte følgende informasjon:

- Beskrivelse av bruddet
- Navn og kontaktinformasjon til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes
- Beskrivelse av de sannsynlige konsekvensene av bruddet
- Beskrivelse av de tiltakene som virksomheten har truffet eller foreslår å sette i gang for å håndtere bruddet, inkludert (dersom det er relevant) tiltak for å redusere eventuelle skadevirkninger som følge av bruddet

### Statens helsetilsyn

Virksomheter som yter helse- og omsorgstjenester, skal **varsle Statens helsetilsyn** om avvik som følge av feil og avvik på informasjonssystemer.

Varslingsplikten utløses ved dødsfall eller svært alvorlig skade på pasient eller bruker som følge av ytelse av helse- og omsorgstjenester når utfallet er uventet ut fra påregnelig risiko.[33]

Ved hendelser som medfører varsling til Statens helsetilsyn, skal virksomheten:

- følge opp og informere pasienter og pårørende
- gjennomgå hendelsen
- identifisere og følge opp risikoreduserende tiltak

Eksempelet som følger beskriver en situasjon der virksomheten må vurdere hvorvidt avvik skal meldes og rapporteres, både til tilsyn og de registrerte.

[32] I henhold til personvernforordningens artikkel 34.
[33] I henhold til lov om statlig tilsyn med helse- og omsorgstjenesten mv. (helsetilsynsloven) § 6

**Eksempel:**

Pasient NN er 16 år og er innlagt på Normland sykehus. I forbindelse med en oppdatering av sykdomsbildet, skal sykehuset sende informasjon til de pårørende. Pasienten har samtykket til at denne informasjonen gis. Ved en feil sendes denne informasjonen til en rekke andre pårørende i tillegg til rett mottaker. Pårørende til NN får vite dette via andre som har mottatt informasjonen, da lokalsamfunnet er lite, og alle kjenner alle.

Pårørende til NN blir svært opprørte, og kontakter sykehuset for å få informasjon om det som har skjedd. Sykehuset har ikke oppdaget feilen, men tar affære og melder avviket til Datatilsynet. De vurderer avviket til å ikke være så alvorlig at det er nødvendig å varsle de registrerte.

De pårørende kontakter sykehusets personvernombud for å få bistand. De mener at de har rett på mer informasjon om det som har skjedd, og synes det er svært ubehagelig at andre i lokalsamfunnet har fått sensitiv informasjon om sønnen deres. De vil derfor, i tillegg til informasjon om avviket, ha kontaktinformasjon til de andre mottakerne.

Personvernombudet kontakter egen virksomhet og argumenterer for at de pårørende bør få varsel etter artikkel 34, da de allerede er kjent med at avviket har skjedd og hva slags informasjon som er på avveie. Videre er det et viktig å demonstrere at man tar hendelsen på alvor og at man gjør det man kan for å ivareta pasienten og de pårørende. I en ubehagelig situasjon som denne er det avgjørende at pårørende og NN føler at de blir sett og at deres ubehag ikke bagatelliseres. Personvernombudet anbefaler at virksomheten tar hensyn til dette i sin kontakt med NN og de pårørende. Ombudet mener likevel at man ikke kan gi ut informasjon om andre mottakere, da disse har en selvstendig rett til å få sitt personvern ivaretatt.

Hendelsen resulterer i at sykehuset gjør endringer i sine informasjonsrutiner, og heretter sender informasjon via andre kanaler der risikoen for feilsending vurderes å være mye lavere. Sykehuset følger opp NN og hans pårørende ved å kontakte de direkte og informere om rutineendringen, for å gjøre de trygge på at dette ikke vil skje igjen.

### 2.4.3 Avviksprosessen – system for avvikshåndtering


Etablering av system for avvikshåndtering er et lovpålagt krav innen en rekke områder som kvalitet; helse, miljø og sikkerhet; ytre miljø; personvern; og informasjonssikkerhet. De fleste virksomheter har en felles prosess for avvikshåndtering og forbedringsarbeid. I store virksomheter benyttes ofte egne elektroniske avvikssystem og egne fagavdelinger med

overordnet ansvar for internkontrollen på de ulike områdene. I små virksomheter vil det ofte være de samme personene som fyller flere roller.

Denne veilederen tar utgangspunkt i en standard prosess for avvikshåndtering som er gjenkjennelig og overførbar til både små og store virksomheter, samt vektlegger kravene i Normen til avvikshåndtering og kontinuerlig forbedring. Den kan slik skaleres opp eller ned basert på type virksomhet og ikke minst størrelsen på virksomheten.

Avvik kan avdekkes på ulike måter, blant annet følgende:

- Ansatte oppdager at informasjon er kommet på avveie, IKT-driftspersonell avdekker sikkerhetsbrudd som manglende tilgang, uautorisert tilgang, etc. og melder om avvik i virksomheten.
- Melding om avvik kommer til dataansvarlig fra databehandler eller gjennom automatiske varslingsfunksjoner.
- Avvik rapporteres i forbindelse med mottatt klage fra pasient/bruker, mottatt rapport fra ekstern revisor (f.eks. ISO-revisjon, eller kunderevisjon) eller når internrevisor påpeker feil eller mangler i virkshetens ledelsessystem (som prosedyre, rutiner, ansvarsforhold, etc.)

Alle som har observert eller vært involvert i et avvik plikter å melde fra.

Det kan ofte være vanskelig å vite hva som skal rapporteres som avvik. I alle tilfeller skal brudd på minimumskravene for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet som beskrives i Normens kapittel 3.2 meldes som avvik. Det er alltid bedre å melde avvik en gang for mye, enn en gang for lite, og det er viktig at virksomhetens ledelse oppfordrer de ansatte til å melde avvik så fort de avdekkes.

**Hvordan melde avvik?**

Avvik skal meldes via de kanaler som er etablert i virksomheten. I større virksomheter som sykehus benyttes ofte egne elektroniske avvikssystem, mens andre mindre virksomheter benytter avviksskjema eller andre kanaler. Avviksmeldingen skal beskrive avviket og hvor det har skjedd. Dersom avviksmelder har iverksatt strakstiltak eller har forslag til tiltak skal dette følge av avviksmeldingen. Meldingen skal ikke inneholde personopplysninger knyttet til navn eller annen type informasjon der det kan være behov for konfidensialitet. Det er viktig å ha god veiledning til melder i de kanaler som skal benyttes til avviksmelding slik en blir minnet på å ikke ta med sensitiv informasjon i avviksmeldingen. Avviksmeldingen skal også beskrive hva som eventuelt kan være konsekvensen av bruddet.

**Vurdere avvik og beslutte tiltak**

Når avvik mottas, må risiko og de konkrete omstendighetene rundt vurderes. En må vurdere om det er brudd på konfidensialitet, integritet, tilgjengelighet eller robustheten, og hva konsekvensene av det vil være. På samme måte som ved øvrig håndtering av risiko er kartlegging av årsaker til avviket en viktig kilde til å identifisere gode og effektfulle tiltak.

Det er forskjell på om årsaken til avviket er brudd på eller manglende etterlevelse av policy, prosesser og prosedyrer, eller om årsaken er mangler i styringssystemet. Skal det iverksettes tiltak i avdelingen som følges opp av nærmeste leder løses avviket på det laveste nivået. Er det behov for å iverksettes tiltak på overordnet nivå og endringen omfatter hele organisasjonen bør dette følges opp av virksomhetens leder. Avviket skal alltid først vurderes av nærmeste leder.

Når årsakene er kartlagt danner dette utgangspunkt for å beslutte hvilke tiltak som skal iverksettes. Skal tiltaket virke forebyggende eller skadebegrensende og skal det gjelde hele organisasjonen (endring i prosess) eller bare for avdelingen avviket oppstod.

**Iverksette og evaluere tiltak**

Hovedhensikten med all avviksbehandling, er å iverksette tiltak for å hindre gjentagelse. For om mulig hindre at hendelsen skal skje igjen, må tiltakene rette seg mot de aktuelle årsakene til avviket. Flere tiltak kan iverksettes for å behandle det samme avviket, så det kan være flere tiltaksansvarlige som implementerer avvik på vegne av avviksbehandler og/eller avvikseier.

For å sikre gjennomføring av tiltaket anbefales å sette ansvarlig for gjennomføringen, tidsfrist og estimerte kostnader knyttet til gjennomføringen. Det er viktig at de som får ansvar for gjennomføring har forankring, myndighet og ressurser til å implementere tiltakene.

Tiltaksansvarlig bør varsle avvikseier dersom tiltaket blir overført til annen tiltaksansvarlig, og som et minimum når alle besluttede tiltak er iverksatt/gjennomført.

**Lukking av avvik, kvalitetssikring og -forbedring**

Når tiltakene er gjennomført kan avvikseier vurdere om avviket kan lukkes. I noen tilfeller kan ikke avviket lukkes før det er gjort en evaluering av om tiltaket fungerer etter hensikten. Dette gjelder spesielt avvik med alvorlig konsekvens som for pasientsikkerhet, liv og helse og stor konsekvens for personvernet. Har avviket vært omfattende bør det også gjennomføres en risikovurdering for å avklare om etablerte tiltak er tilstrekkelige.

Når tiltakene er gjennomført og risikoen er på et akseptabelt nivå kan avviket lukkes. Ved lukking av avvik skal det skrives en avsluttende vurdering av avviket. Ved lukking av avviket vil det også ha en stor verdi å vurdere sannsynlighet for gjentagelse av avviket som en del av den endelige behandlingen. Det kan også være nyttig å forsøke å dokumentere de faktiske kostnader avviket har medført for å senere kunne benytte dette i en kost/nyttevurdering av implementerte tiltak.

Tiltakene som er innført bør vurderes etter en tid. Dette kan gjøres i en sikkerhetsrevisjon. Det bør vurderes om tiltakene har vært hensiktsmessige, hvorvidt de er effektive for å hindre sikkerhetsbrudd og om de har hatt utilsiktede konsekvenser som eksempelvis mangelfull tilgang til systemer, redusert funksjonalitet i IKT-systemene, mv. Denne vurderingen bør være en del av ledelsenes årlige gjennomgang av informasjonssikkerhet og personvern.

**Eksempel:**
Eksempler på avvik innen informasjonssikkerhet og brudd på personvernet i helse- og omsorgssektoren kan være:

- En ansatt på legekontoret feilsender e-post med vedlegg med helse- og personopplysninger som innhold
- En kommune gjennomfører en spørreundersøkelse blant ansatte som inneholder personopplysninger i et skjemaverktøy der virksomheten ikke har databehandleravtale med leverandøren
- En psykolog sender en vurdering som inkluderer helse- og personopplysninger til en annen av sine pasienter enn intendert mottaker
- Et sykehus opplever feil i tilganger, utstyr eller programvare som gjør at de ansatte ikke får tilgang til de helse- og personopplysningene de trenger for å yte helsehjelp
- Et rehabiliteringssenter har behandlet helse- og personopplysningen uten å vurdere hvorvidt de har tilstrekkelig rettslig grunnlag (behandlingsgrunnlag)
- En fysioterapeut sender en pasients fødselsnummer ukryptert per e-post til en ekstern mottaker (et enkelt dokument som inneholder et fødselsnummer sendt mellom ansatte i samme virksomhet er imidlertid ikke et avvik, da det ikke forlater virksomhetens datanettverk)
- En ansatt i helseforetaket forlater innlogget PC for å spise lunsj mens en kollega bistår med feilsøking
- En tannlege skriver ut deler av tannlegejournalen til en pasient, men glemmer å hente utskriften på tannlegepraksisens felles nettverksprinter
- En jurist som jobber med anskaffelser deler en risikovurdering med beskrivelser av sårbarheter i et internt system fra én leverandør med en annen leverandør

## 2.5 Medarbeidere, kompetanse og holdningsskapende arbeid

Det er menneskene i virksomheten som vurderer risiko, beslutter hvordan risikoen skal håndteres og skal følge rutinene i internkontrollen. Den menneskelig faktor kan være en barriere som forhindrer brudd på informasjonssikkerheten og personvernet – men kan også være en årsak til slike brudd. Utfallet avhenger av sikkerhetsbevisstheten til medarbeidere, deres kompetanse og holdninger. Sikkerhetsadferden til enkeltpersoner og sikkerhetskulturen i virksomheten er dermed grunnmuren for å ivareta informasjonssikkerhet og personvern i virksomheten.

Mørketallsundersøkelsen 2020[34] viser at blant de som er utsatt for sikkerhetsbrudd i norske virksomheter, anses de vanligste årsakene til bruddene å være tilfeldigheter eller uflaks, menneskelige feil, mangel på sikkerhetsbevissthet hos ansatte eller at eksisterende prosesser ikke blir fulgt. Det er ikke grunn til å tro at dette skulle være annerledes i helse- og omsorgssektoren enn i resten av samfunnet. Kompetansebyggende og holdningsskapende

[34] Mørketallsundersøkelsen 2020, Næringslivets sikkerhetsråd, NSR, https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

arbeid er derfor naturlige komponenter i internkontroll i helse- og omsorgssektoren, og er videre beskrevet i de neste kapitlene.

I Normen er følgende krav relatert direkte til medarbeidere og kompetanse:

- Kontinuerlig lære opp medarbeidere i krav om ivaretakelse av taushetsplikten, informasjonssikkerheten og personvernet.[35]
- Etablere tiltak som sørger for at alle som gis tilgang til informasjonssystemer og tilhørende informasjon, har tilstrekkelig kompetanse til å benytte systemene og til å ivareta informasjonssikkerheten og personvernet til den registrerte.[36]

I tillegg er det mange krav spredd utover i Normen om bl.a. organisatoriske tiltak. Det følger av definisjonene i Normen at organisatoriske tiltak også omfatter opplæring.

### 2.5.1 Kompetanse og sikkerhetskultur

Det finnes en rekke definisjoner av kompetansebegrepet, avhengig av kontekst og bruksområde. Utdanningsdirektoratet definerer kompetanse som følger:

> *Kompetanse er å kunne tilegne seg og anvende kunnskaper og ferdigheter til å mestre utfordringer og løse oppgaver i kjente og ukjente sammenhenger og situasjoner. Kompetanse innebærer forståelse og evne til refleksjon og kritisk tenkning.*[37]

Kompetanse kan altså anses at dannes av kunnskap, forståelse og ferdigheter. Enklere sagt av «å vite», «å skjønne» og «å gjøre».[38] For å øke kompetanse innen informasjonssikkerhet og personvern i helse- og omsorgssektoren, handler det derfor om følgende:

- Tilføre og tilegne (ny) *kunnskap* om hvilke verdier som skal beskyttes, hvilke metoder som typisk brukes av trusselaktører for å skade informasjonsverdiene i sektoren og ikke minst hvordan verdiene kan beskyttes – også av den enkelte i virksomheten.
- Skape *forståelse* for hvorfor informasjonssikkerhet og personvern er viktig for helse- og omsorgssektoren, hvilke konsekvenser et kan sikkerhetsbrudd få for pasienter og brukere, den enkelte medarbeider, virksomheten og andre interessenter. Det gjelder også forståelse for hvorfor sikkerhet gjelder alle, samt hvordan hver medarbeider i sektoren kan bli en robust sikkerhetsbarriere rundt informasjonsverdiene og ikke en sårbarhet. Det vil kunne gi bevissthet og indre motivasjon som styrker sikkerhetsadferden og videre sikkerhetskulturen i virksomheten.
- Opparbeide *ferdigheter* i beskyttelse av informasjon og personvern. Repetisjon gir evne til å automatisere ferdigheter.[39] Ved å bryte ned kunnskap til enkelte emner som kan repeteres jevnlig, etableres det et nytt tankemønster som vil kunne føre til nye vaner og endret adferd. Det kan være en motorisk handling, som f.eks. å låse PC-en hver gang man forlater den. Dette er en bevisst handling som etter hvert blir til automatikk i ubevisstheten. Det kan også være ny kunnskap som drøftes med andre eller reflekteres over gjentatte ganger, til det etableres som en selvfølge. Et eksempel er samtaler og vurderinger om rotårsaken til gjentatte sikkerhetsbrudd på et område.

[35] Normen 6.0 kapittel 4.2.1 og 5.1.1
[36] Normen 6.0 kapittel 5.1.2 og 5.4.2 andre avsnitt siste kulepunkt
[37] Utdanningsdirektoratet, https://www.udir.no/lk20/overordnet-del/prinsipper-for-laring-utvikling-og-danning/kompetanse-i-fagene/?curriculum-resources=true
[38] Regjeringen, https://www.regjeringen.no/no/dokumenter/nou-2018-2/id2588070/?ch=3
[39] KS, https://www.ks.no/fagomrader/barn-og-unge/ks-led/fagstoff/nevroplastisitet--video/

Kunnskapen som medarbeidere får og innehar, risiko- og konsekvensforståelsen de etablerer og ferdigheter de utvikler, vil påvirke sikkerhetskulturen i virksomheten. Sikkerhetskultur er hvordan den samlede kompetansen i virksomheten brukes i hverdagen. NSM definerer sikkerhetskultur på følgende måte:

> *Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.*[40]

Sikkerhetskulturen er en del av virksomhetens organisasjonskultur. Kulturen påvirkes av flere elementer, som ledelse, kommunikasjon, styringssystem, ansvarliggjøring, motivasjon og selvsagt kompetanse.

For å ha en sterk sikkerhetskultur, er det avgjørende at ledelsen både har fokus på sikkerhet, prioriterer sikkerhetsrelaterte spørsmål, og ikke minst selv viser ønskelig sikkerhetsadferd (ledelse ved eksempel). Hvordan ledere i sektoren prioriterer og engasjerer seg, samt deres kompetansenivå innen sikkerhet, har betydning for de ansattes sikkerhetsadferd.[41] Sikkerhetsfokus hos toppledelsen har en direkte innvirkning på hvordan sikkerhetsorganisasjonen ser ut, om sikkerhetsroller og sikkerhetsansvar er definert og fordelt, og ikke minst om det er satt av tid og ressurser til kompetansehevende aktiviteter i virksomheten. Ledelsen og deres felles risikoforståelse danner et grunnlag for og innhold til et opplæringsopplegg.

Ledelsen på alle nivåer bør kommunisere informasjonssikkerhet og personvern både seg imellom og ut til organisasjonen, slik at medarbeidere oppfatter viktigheten av å fokusere på disse temaene. Her vil det være særlig relevant å kommunisere at informasjonssikkerhet og personvern er viktige komponenter i å ivareta pasientsikkerheten og det å kunne yte forsvarlig helsehjelp. Kommunikasjonskanaler skal kunne nå alle medarbeidere og budskapet skal kunne oppleves som forståelig og relevant.

En forutsetning for å oppnå en ønsket felles sikkerhetskultur er at medarbeidere og ledere er innforstått med hvilke krav de må forholde seg til. Virksomheten må derfor ha tilstrekkelige og tydelige retningslinjer og rutiner. For å sikre at hver enkelt medarbeider kjenner til retningslinjene og rutinene, og kan finne dem ved behov, er det viktig at disse er gjort lett tilgjengelige og kommunisert ut til organisasjonen.

Motivasjon og eierskap er drivkraften i en adferdsendring. Det er derfor viktig at den enkelte medarbeider føler et ansvar for å etterleve gjeldende krav og bidra til å opprettholde og videreutvikle sikkerhetskulturen. Indre motivasjon skapes blant annet av å kjenne på eierskap og ansvar, og av risiko- og konsekvensforståelse. En opplevd hendelse og egen erfaring påvirker viljen til å endre adferd. Ytre motivasjon som ros for ønsket adferd og sanksjoner ved uansvarlige handlinger, kan også ha en viss påvirkning. Rapportering av eventuelle sikkerhetsbrudd og avvik, som er beskrevet tidligere i veilederen, bidrar til økt ansvarsfølelse og bevisstgjøring blant de ansatte. Kartlegging av sikkerhetskultur[42] og måling av kompetanseutviklingen over tid, vil også kunne gi økt sikkerhetsbevissthet i virksomheten, øke eierskap og motivasjonen hos medarbeiderne, samt gi indikatorer for videre kompetanseheving og kulturutvikling.[43]

---

[40] NSM, Sikkerhetskultur, Årsmelding 2010

[41] NHO, https://arbinn.nho.no/hms/sikkerhet-og-beredskap/sikkerhet/sikkerhet/sikkehetskultur/

[42] NorSIS, https://norsis.no/sikkerhetskultur/

[43] Digitaliseringsdirektoratet, https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2141

For mer om kompetanse- og kulturutvikling innen informasjonssikkerhet generelt, har Digitaliseringsdirektoratet eget veiledningsmateriell på dette.[44]

### 2.5.2 Opplæringsprogram

Opplæring av ledere og medarbeidere krever forankring i organisasjonen og at det stilles krav til både innhold og kvalitet. Opplæringen anbefales basert på en opplæringsplan slik at det settes av tid besluttet av ledelsen. Det anbefales at opplæringen i informasjonssikkerhet og personvern knyttes til annen opplæring i virksomheten. Det anbefales å ta utgangspunkt i styringssystemet for informasjonssikkerhet som inneholder alle retningslinjer og rutiner for virksomheten. På den måten får den enkelte opplæring i hvor styringssystemet finnes, hvordan det er bygget opp og hvilke prosedyrer som er utarbeidet.

Virksomheten bør etablere en rutine for opplæring i informasjonssikkerhet og personvern. En slik rutine skal tilpasses størrelsen og behovene til virksomheten, samt risikoer den står overfor. En slik rutine bør inneholde:

- Roller og ansvar for utarbeidelse og gjennomføring av opplæringsprogram
- Tidsrom for opplæringsprogram
- Målgruppe(r) og opplæringsnivå(er)
- Forslag til et opplæringsløp – tidspunkt for gjennomføring og opplæringsformat
- Forslag til måletiltak
- Dato for neste revisjon

For store virksomheter er det naturlig at denne rutinen er relativt detaljert for ulike målgrupper og roller, mens for små virksomheter vil disse punktene med en kort beskrivelse trolig være tilstrekkelig.

Det anbefales videre å etablere et årshjul for kompetanseheving. I store og mellomstore virksomheter bør det i programmet være flere opplæringsløp, ett for hver målgruppe. Opplæringen bør tilpasses målgruppen både i innhold og format.

Følgende opplæring bør gjennomføres:

- Grunnleggende opplæring av alle medarbeidere som også inkluderer helsepersonell, kontorpersonale, ledere og studenter, samt løpende opplæringstiltak for vedlikehold og utvikling av kompetansen.
- Opplæring i sikkerhetsstyring av ledere, risikoeiere og fagpersoner innen informasjonssikkerhet og personvern, samt løpende opplæringstiltak for vedlikehold og utvikling av kompetansen.
- Kurs i sikkerhets- eller personvernfag for spesialister som er tildelt roller, ansvar eller oppgaver innen informasjonssikkerhet eller personvern.
- Tilpasset opplæring av personell med spesielle oppgaver (for eksempel IT-drift, sikkerhetskopiering, anskaffelser av/til informasjonssystemer, tildeling av autorisasjon, tilbaketrekking av autorisasjon)
- Opplæring ved tilgang til helse- og personopplysninger mellom virksomheter

[44] Digitaliseringsdirektoratet, https://www.digdir.no/informasjonssikkerhet/kompetanse-og-kulturutvikling-innen-informasjonssikkerhet/2187

Avhengig av størrelsen på virksomheten og behov, kan årshjulet justeres og utvides til flere målgrupper, eksempelvis systemeiere, utviklere, nyansatte, innleid personell og tilsvarende.[45] I små virksomheter som ikke har ansatte dedikert til informasjonssikkerhet og personvern, vil ledere eller personer med dette som tilleggsroller måtte tilegne seg nok kunnskap til selv å utføre sikkerhets- og personvernoppgaver eller sette det ut til andre (bestillerkompetanse ved kjøp av tjenester som f.eks. sikkerhetsrevisjon eller personvernombud).

I utarbeidelsen og gjennomføringen av et opplæringsprogram, er det viktig å beholde fokuset på effekten av tiltakene og ikke selve tiltaket. Risikoen ved et for omfattende opplegg kan være at sikkerheten i virksomheten forblir svekket, fordi de ansatte kan oppfatte opplæringen som for vanskelig og tidkrevende å gjennomføre. Dette gjelder særlig for de små virksomhetene i helse- og omsorgssektoren. Et annet eksempel er at effekten av et pålagt e-læringsprogram som gir høy gjennomføringsgrad, ikke nødvendigvis gir ønsket effekt hvis de ansatte bare «klikker» seg gjennom, uten at de faktisk tar innover seg innholdet som formidles. Det er derfor viktig med enkle og kontinuerlige tiltak som også kan måles underveis.

Vedlegg 3.3 viser forslag til opplæringsprogram for alle medarbeidere, ledere og fagpersoner med særskilte roller, ansvar og oppgaver innen informasjonssikkerhet og personvern.

Vedlegg 3.4 viser eksempler på momenter (i materiell) for opplæring og bevisstgjøring i praktisk informasjonssikkerhet og personvern for både ledere, ansatte og innleide, samt tips og råd om hvordan de i praksis kan etterleves og øves på. Disse kan være nyttige i utformingen av opplæringstiltak.

Vedlegg 3.5 viser et eksempel på hva en instruks om bruk av informasjonsteknologi som retter seg til brukerne (ansatte og innleide) i virksomheten kan inneholde. Denne kan også bidra til å fremheve hvilke temaer som brukerne har behov for opplæring innenfor.

[45] Digitaliseringsdirektoratet, https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-og-kulturutvikling-innen-digital-sikkerhet/2141#velge_maalgruppe

*Endringshistorikk*

| Dato | Versjon | Endring |
|---|---|---|
| 02.12.21 | 1.0 | Ny veileder om internkontroll i helse- og omsorgssektoren bygger på oppdatert innhold fra faktaarkene:<br>- Faktaark 01 – Ansvar og organisering;<br>- Faktaark 02 – Styringssystem for informasjonssikkerhet og personvern;<br>- Faktaark 08 – Avviksbehandling;<br>- Faktaark 09 – Opplæring av ledere og medarbeidere;<br>- Faktaark 27 – Retningslinjer for daglig informasjonssikkerhet.<br>Personvern er integrert som tema, i tillegg til nytt materiale om en rekke relevante temaer innen internkontroll i sektoren, som blant annet sikkerhetskultur. |

# 3 Vedlegg

## 3.1 Eksempler på sikkerhetsansvar, -roller og oppgaver

Eksemplene under er basert på virksomheter i sektoren, og gir en oversikt over mulige roller og ansvarsområder. Eksemplene er ment til inspirasjon slik at ansvarsområder blir vurdert og ansvaret plassert. Matrisene må tilpasses lokale forhold og utvides med relevante roller for akkurat din virksomhet, for eksempel med personvernrådgiver, forsker, prosjektleder og/eller systemkoordinator.

**Eksempel 1 på sikkerhetsansvar, -roller og -oppgaver internt i virksomheten**

**Matrisen må tilpasses lokale forhold**

**<Virksomhet>**

| Funksjon: | Virksomhetens leder | Leder | Ansatt/medarbeider | Fagansvarlig IKT | Fagansvarlig sikkerhet | Systemeier |
|---|---|---|---|---|---|---|
| **Ansvar** | - Sørge for at det er etablert et styringssystem for informasjonssikkerhet og at dette vedlikeholdes<br>- Sørge for at informasjonssikkerheten er tilfredsstillende<br>- Bestemme formålet med behandlingen av personopplysninger<br>- Bestemme hvilke hjelpemidler som skal brukes | - Sørge for opplæring av ansatte<br>- Beredskap<br>- Tildele, vedlikeholde og inndra roller/ tilgang<br>- Rapportere avvik i samsvar med virksomhetens prosedyrer for dette<br>- Følge opp forskningsprosjekt | - Gjøre seg kjent med og følge lover, regler og prosedyrer<br>- Melde avvik | - Sørge for at informasjonssystemet er tilgjengelig<br>- Sørge for at informasjonssystemet oppfyller Normens krav<br>- Sørge for at informasjonssystemet fungerer som besluttet<br>- Etablere ansvarskart for informasjonssystemet | - Overvåke at informasjonssystemet benyttes i samsvar med bestemmelser og prosedyrer<br>- Rapportere til dataansvarlig | - Sørge for at sitt informasjonssystem er tilgjengelig<br>- Sørge for at sitt informasjonssystem oppfyller Normens krav<br>- Sørge for at informasjonssystemet fungerer som besluttet<br>- Definere tilgangsroller<br>- Rapportere til IKT-ansvarlig |
| **Rolle** | *Dataansvarlig* | *Leder med personalansvar* | *Systembruker* | *Bestiller* | *Fagansvarlig informasjonssikkerhet* | *Systemeier for et system* |
| **Oppgaver** | - Vedta, implementere, vedlikeholde og følge opp bruken av styringssystem for informasjonssikkerhet | - Sørge for at det gis opplæring i nødvendige systemer og i informasjonssikkerhet | - Lese og følge gjeldende regler | - Utarbeide og vedlikeholde prosedyrer rundt egen funksjon<br>- Utarbeide og inngå serviceavtale om drift og | - Utarbeide og vedlikeholde prosedyrer rundt egen funksjon<br>- Utforming av styrende, utførende og kontrollerende dokument i | - Utarbeide og vedlikeholde prosedyrer rundt egen funksjon<br>- Bistå IKT-ansvarlig i å utarbeide vedlegg til serviceavtale |

| | | | | | | |
|---|---|---|---|---|---|---|
| | - Gjennomføre ledelsens gjennomgang<br>- Melde brudd på personopplysnings-sikkerheten til Datatilsynet | - Lage og teste beredskapsprosedyrer for systemsvikt<br>- Sørge for risikovurderinger og overvåke risiko<br>- Tildele den enkelte medarbeider korrekt rolle og bestille tilgang til nettverk og system<br>- Vedlikeholde medarbeidernes tilgangsnivå<br>- Inndra tilgang ved opphør av arbeidsforhold<br>- Sørge for at forskningsprosjekt blir meldt til den regionale etiske komité (REK)<br>- Følge opp at forskningsprosjekt følger plan<br>- Behandle avvik<br>- Etablere og følge opp tilganger og evt. avtaler om tilgang på tvers | - Gjøre seg kjent med styringssystem for informasjonssikkerhet | vedlikehold av informasjonssystemet<br>- Utarbeide beredskapsplan<br>- Ivareta konfigurasjonskontroll ved endringer av informasjonssystemet<br>- Sørge for risikovurderinger og overvåke risiko<br>- Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess<br>- Følge opp partnere, leverandør og databehandlere i forhold til informasjonssikkerhet<br>- Håndtere meldte avvik<br>- Rådgiving<br>- Sørge for at det blir utpekt systemeier for det enkelte system og holde oversikt over disse | styringssystemet for informasjonssikkerhet<br>- Forberede ledelsens gjennomgang<br>- Følge opp iverksetting av tiltak som er besluttet gjennomført<br>- Samordne og gjennomføre sikkerhetsrevisjoner<br>- Vurdere rapporterte avvik<br>- Forestå risikovurderinger<br>- Godkjenne dokument til styringssystemet for informasjonssikkerhet<br>- Erverve og vedlikeholde kunnskap om trusler, sårbarhet, sikkerhetstiltak og -teknikker, sikkerhetskrav<br>- Opplæring<br>- Rådgiving | - Bistå IKT-ansvarlig i å utarbeide avtaler om endringer av sitt systems konfigurasjon<br>- Definere tilgangsroller for sitt system og gjøre disse kjent<br>- Sørge for risikovurderinger og overvåke risiko<br>- Følge opp partnere, leverandør og databehandlere i forhold til informasjonssikkerhet<br>- Håndtere meldte avvik<br>- Følge opp tilgang på tvers |

**Eksempel 2 på sikkerhetsansvar, -roller og -oppgaver internt i virksomheten**

## Matrisen må tilpasses lokale forhold

## <Virksomhet>

**Sikkerhetsansvar, -roller og -oppgaver *internt* i virksomheten**

| **Avdelingsleder**<br>*(Personalansvar)* | **Bruker**<br>*(av IKT-system)* | **Fagansvarlig IKT** | **Fagansvarlig IKT-sikkerhet**<br>*(tilsyns- og rådgiverfunksjon)* | **Systemeier**<br>*(ett eller flere system)* | **Personvernombud** |
|---|---|---|---|---|---|
| Sørge for:<br>- at eget personell har riktige tilganger/ autorisasjoner/roller<br>- behandling av personopplysninger i egen avdeling er meldt til rette instanser<br>- at det er gjennomført obligatorisk sikkerhetsopplæring og at sikkerhetskrav blir overholdt<br>- å gjøre seg kjent med og implementere beredskapsplaner for bortfall av IKT i egen avdeling<br>- at avvik blir behandlet i samsvar med virksomhetens rutiner | - Gjøre seg kjent med og overholde IKT sikkerhetsinstruksen og IKT rutiner<br>- gjennomføre obligatorisk opplæring i informasjons-sikkerhet<br>- gjøre seg kjent med og overholde IKT avviksrutiner | Sørge for:<br>- at informasjonssystemene oppfyller lovbestemte og andre krav<br>- at informasjonssystemene er tilgjengelig, herunder å utarbeide, inngå og følge opp tjenesteavtale (SLA) om drift og vedlikehold av informasjonssystemene<br>- å etablere ansvarskart for informasjonssystemene<br>- å utarbeide og implementere overordnede beredskapsplaner for IKT<br>- at risikovurderinger blir utført<br>- at risiko overvåkes<br>- å følge opp partnere, leverandør og databehandlere i forhold til sikkerhet | - Overvåke risiko (vurdere, handle, tiltak, varsle, osv..) og at informasjonssystemet benyttes i samsvar med bestemmelser og rutiner<br>- Følge opp IKT sikkerhetsavvik<br>- Utforming av styrende, utførende og kontrollerende IKT sikkerhetsdokument i foretakets Internkontrollsystem<br>- Delta i og kvalitetssikre risikovurderinger<br>- Forberede og følge opp ledergruppens årlige gjennomgang<br>- Gjennomføre sikkerhetsrevisjoner<br>- Delta i regionalt sikkerhetsutvalg<br>- Rapporterer til Dataansvarlig | - Sørge for at det er etablert drift og forvaltningsavtale (ref. SLA)<br>- Sørge for at informasjonssystemet oppfyller lovbestemte og andre krav og er meldt til pålagte instanser<br>- Definere og vedlikeholde tilgangsroller<br>- Sørge for risikovurderinger og overvåke risiko<br>- Følge opp partnere, leverandører og databehandlere i forhold til sikkerhet<br>- Håndtere meldte IKT sikkerhetsavvik<br>- Utarbeide og implementere beredskapsrutiner for bortfall av systemet | - Gi råd og veiledning om behandling av personopplysninger<br>- Føre oversikt over all behandling av personopplysninger<br>- Motta meldinger om behandling av personopplysninger og vurdere om disse er melde- eller konsesjonspliktige<br>- Påse at meldinger/søknader i tilknytning til behandling av personopplysninger blir sendt til aktuelle instanser (unntatt i det som kommer inn under lov om medisinsk og helsefaglig forskning) |

## 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 og behov. Hensikten med dette eksempelet er å vise de ulike temaene som naturlig inngår i et styringssystem.

| **1. Styrende del:** |
|---|
| • Beskrivelse av sikkerhetsmål og strategi for informasjonssikkerhet<br>• Overordnede føringer for bruk av informasjonsteknologi<br>• Beskrivelse av roller og ansvar i arbeidet med informasjonssikkerhet og personvern<br>• Oversikt over behandlinger av helse- og personopplysninger. Se Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)<br>• Vurdering av akseptabel risiko<br>• Systemoversikt og klassifisering av systemer<br>• IKT-sikkerhetsinstruks<br>• 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)<br>• Rutine for gjennomføring av DPIA, med tilhørende mal (se kapittel om vurdering av personvernkonsekvenser i Normens Veileder om risikostyring i helse- og omsorgssektoren)<br>• Mal for databehandleravtaler<br>• Oversikt over databehandlere og leverandører med avtaler<br>• Rutine (og eventuelt sjekkliste) for oppstart og endring av behandlingsaktiviteter (herunder ivaretakelse av personvernprinsippene. Se Personvernprinsippene (faktaark 57) og kravene til overføring av personopplysninger til tredjeland<br>• Rutine for autorisering, endring og avslutning av tilganger<br>• Rutine for administrasjon av nøkler og adgangskort i adgangskontrollsystemet<br>• Rutine for oppretting og vedlikehold av autorisasjonsregister<br>• Rutine for å sammenstille logger med autorisasjonsregisteret<br>• Rutine for bruk av mobilt utstyr og hjemmekontor<br>• Rutine for den registrertes innsyn i helse- og personopplysninger<br>• 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

**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 Sikkerhetsrevisjon (faktaark 06).
- Rutine for oppfølging av resultater av risikovurdering
- Rutine for oppfølging av logger i behandlingsrettede helseregistre (se Normens veileder om tilgangsstyring)

## 3.3 Forslag til opplæringsprogram

Følgende er et forslag til opplæringsprogram for henholdsvis alle ansatte, ledere, og fagpersoner med roller, ansvar og oppgaver innen informasjonssikkerhet og personvern.

**Alle ansatte**

Opplæringsopplegg for alle ansatte skal kunne gi den grunnleggende kunnskapen, forståelsen og ferdighetene som sikrer at krav i Normen blir etterlevd. Budskapet i opplæringen bør være enkelt formulert og bli kommunisert til medarbeidere gjennom kanaler som når dem og som brukes aktivt av hver av dem. Det kan eksempelvis være fellesmøter, intranett, e-post eller e-læringskurs. Budskapet bør brytes ned i helt konkrete oppgaver som er enkelt å huske og repetere over en viss tid, eksempelvis «Tips og råd til daglig informasjonssikkerhet» i denne veilederen. Opplæringen bør gi spisset kunnskap om hvordan hver medarbeider helt konkret kan ivareta informasjonssikkerhet og personvern. Historiefortelling («storytelling») basert på ekte hendelser fra egen eller andres virksomhet kan gi en nødvendig følelse av relevans og med det eierskap og økt bevissthet. Det er viktig at de ansatte skal kunne kjenne seg igjen i budskapet som formidles.

Forslag til virkemidler i opplæringen av alle medarbeidere:

- Informasjonsbrosjyre med de viktigste områdene innen personvern og informasjonssikkerhet medarbeiderne skal ha kunnskap om. Denne bør deles ut til alle medarbeidere. Nærmeste leder bør følge opp med en samtale omkring temaene som informasjonsbrosjyren tar opp.
- Plakater («one-pagere») for ulike tema, med få viktige punkter på hver, som er lett tilgjengelig og lett å forstå, med et budskap som er lett å huske. Disse kan tilgjengeliggjøres på utvalgte steder som f.eks. venterom, ekspedisjoner og personalrom. Bruk gjerne illustrasjoner/fotografier fra arbeidssituasjoner i egen virksomhet. Temaer kan eksempelvis være taushetsplikt, makulering, låse PC med skjermsparer, melde avvik, hente utskrift og ikke åpne e-post fra ukjente.
- Foredrag, allmøter og avdelingsmøter der nye retningslinjer, andre viktige endringer eller påminnelser informeres om.
- Frokostseminarer og læring i spisepauser («lunch and learn»-aktiviteter) der det i uformelle samlinger, gjerne med enkel matservering, gis foredrag eller gjennomgås samtaleemner innen informasjonssikkerhet og personvern.
- Diskusjonskort med korte beskrivelser av ulike temaer innen personvern og informasjonssikkerhet.
- E-læring for sektoren (se bl.a. nettsidene www.legeforeningen.no og www.tannlegeforeningen.no). E-læring kan også bestå av spillorienterte digitale verktøy («gamification»).
- Korte videoklipp som viser konsekvenser og treffer «en nerve» hos mottakeren som skaper refleksjon.
- Quiz og andre uformelle engasjerende målingstiltak. Dette vil kunne gi indikasjon på effekten av opplæringstiltak.
- Kartlegging av sikkerhetskultur ved å ta i bruk spørreundersøkelse (kvantitativ måling) og intervjuer med nøkkelpersoner (kvalitativ måling). Det kan gjennomføres eksempelvis hvert tredje år eller delvis inngå i årlig medarbeiderundersøkelse.

### Ledere

Ledere skal til enhver tid inneha oppdatert kompetanse for å kunne ta stilling til risikohåndtering i virksomheten. De skal kjenne til og forstå gjeldende krav til informasjonssikkerhet og personvern på området de har ansvar for, være i stand til å beskrive sikkerhetsmål og beslutte hvilken risiko virksomheten kan akseptere. Ledere skal også inneha kunnskap om styringssystemet for informasjonssikkerhet, avtaler og prosedyrer som regulerer tilgang til helseopplysninger mellom virksomheter.

Forslag til virkemidler i opplæringen av ledere:

- Eksterne og interne kurs og seminarer
- Systematisk og kontinuerlig kommunikasjon med fagpersoner, internt og eksternt
- Deltagelse i risikovurdering og andre relevante workshops
- Gjennomføring av sikkerhetsøvelser

### Fagpersoner som er tildelt roller, ansvar og oppgaver innen informasjonssikkerhet og personvern

Kompetanseheving hos fagpersoner forutsetter kontinuerlig vedlikehold, hvor det er nødvendig å hente kunnskap eksternt, samt være oppdatert på trusler og angrepsmetoder, sårbarheter, risikobildet og utviklingen i sikkerhetsfaget. Dette for at fagpersoner skal kunne tilpasse sikkerhetsarbeidet i virksomheten til de eksterne omgivelsene, og etter behov justere retningslinjer og opplæringsopplegg internt.

Forslag til virkemidler i opplæringen av fagpersoner:

- Eksterne kurs og seminarer.
- Delta i faglig nettverk for kompetanseoverføring både internt i helse- og omsorgssektoren, men også på andre relevante arenaer.
- Gjennomlesning av ferske rapporter, artikler og annet faglitteratur for kontinuerlig oppdatering av sin fagkompetanse.

## 3.4 Tips og råd til daglig informasjonssikkerhet

Tabellen som følger viser eksempler på momenter (i materiell) for opplæring og bevisstgjøring om praktisk informasjonssikkerhet og personvern for både ledere, ansatte og innleide, samt tips og råd om hvordan de i praksis kan etterleves og øves på. Disse kan være nyttige i utformingen av opplæringstiltak.

| Momenter | Tips og råd |
|---|---|
| Du skal ikke dele brukernavn og passord med andre | • Ansvar og aktivitet knyttet til journal skal knyttes til enkeltperson<br>• Et passord er lett å huske for meg, men ikke av andre<br>• Du kan bli beskyldt for feil eller aktiviteter som andre som låner passordet ditt har gjort. |
| Tilgang til og bruk av pasientjournal skal begrunnes ut fra tjenstlige behov, skal kun sendes dit pasienten selv angir, utleveres til pasienten selv eller etter fullmakt. Journal kan også sendes ny fastlege etter ønske fra pasienten | • Journalen eies av pasienten<br>• Pasienten bestemmer – vi forvalter |
| Du skal alltid logge av PC, og lås alltid når du går i fra | • Windows knapp og L<br>• Ctrl+Alt+Delete<br>• Fjerne smartkort |
| Du skal ikke lagre pasientopplysninger og andre personopplysninger andre steder enn på områder som er tiltenkt slik lagring. Slik informasjon skal for eksempel ikke lagres lokalt på PC (med mindre det er godkjent) eller ukryptert på bærbart utstyr som for eksempel minnepinne | • Det er vanskelig for virksomheten å ivareta krav til for eksempel tilgangskontroll, sikkerhetskopiering og sletting, hvis opplysninger lagres på andre områder enn tiltenkt.<br>• Minnepinne er lett å miste og skal merkes og oppbevares forsvarlig<br>• Ta ikke med bærbart utstyr med ukrypterte pasientopplysninger utenfor kontoret/arbeidsplassen<br>• Lagre pasientopplysninger slik arbeidsgiver har bestemt |
| Du skal ha kontroll på dokumentene dine | • Hente utskrifter med en gang<br>• Skriv ut kun det du må<br>• Ikke legge igjen dokumenter på møterom<br>• Ha gode makuleringsrutiner |

| | |
|---|---|
| Du vet hva du kan og ikke kan lese | • Det er forbudt å lese, søke eller på annen måte tilegne seg eller bruke opplysninger uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift<br>• Ikke lov å åpne i ektefelles, slektningers eller din egen journal, uten grunn. |
| Du vet hva og med hvem du kan dele pasientinformasjon | • Taushetsplikt gjelder også mellom helsepersonell<br>• Pass på at ikke uvedkommende lytter når du snakker om pasienter med en kollega, i telefon eller på offentlig sted<br>• Pass på at uvedkomne ikke har innsyn<br>• Når du deler pasientopplysninger med andre må du forsikre deg om at vedkommende du kommuniserer med har rett til å få opplysningene. Mottar du f.eks. telefonsamtaler om pasienter, og du er i tvil om identiteten til innringer, kan du be om å få ringe vedkommende tilbake. |
| Du sender ikke pasientinformasjon på SMS eller på e-post | • Dobbeltsjekk at e post/SMS du sender ikke inneholder pasientinformasjon<br>• Ikke svar pasienter på e post/SMS<br>• Benytt godkjente løsninger |
| Du kommenterer ikke jobb på sosiale medier og er forsiktig når du bruker nettsamfunn | • Husk taushetsplikten<br>• Vær forsiktig og ikke røp sensitiv informasjon<br>• Det er ingen angreknapp på internett<br>• Avslå venneforespørsler fra pasienter for å unngå å komme i konflikt med taushetsplikten |
| Du vet hvordan du melder avvik innen informasjonssikkerhet og personvern | • Bruk avvikssystemet<br>• Se på det som et forbedringstiltak som gjør at man lærer av feil og kan endre rutiner<br>• Meld avvik med en gang, slik at det er mulig å overholde fristen til å varsle Datatilsynet (innen 72 timer) |

| | |
|---|---|
| Vær kritisk til lenker og innhold i e-post | • Obs uærlige aktører med baktanker<br>• Du kan få virus og infisere datamaskinen<br>• Ramme arbeidsgiver |
| Du har et bevisst forhold til hvordan du bruker helse- og personopplysninger | • Unngå å samle inn helse- og personopplysninger som ikke er nødvendige for arbeidsoppgaven du skal utføre<br>• Ikke gjenbruk helse- og personopplysninger til nye formål, uten å avklare at det er lov<br>• Bidra til å sikre at helse- og personopplysninger er oppdaterte og korrekte |

## 3.5 Instruks for bruk av informasjonsteknologi

Tabellen som følger inneholder et eksempel på hva en instruks om bruk av informasjonsteknologi som retter seg til brukerne (ansatte og innleide) i virksomheten, kan inneholde.

**Instruks for bruk av informasjonsteknologi i Normvik sykehus:**

a. Privat bruk av informasjonssystemet skal godkjennes
b. Bruk av informasjonssystemet fra hjemmekontor eller på reise skal godkjennes
c. Flytting/kopiering av helse- og personopplysninger (over på minnepinne, CD mv.) skal godkjennes
d. Alle data skal sikkerhetskopieres
b. Utskrifter med helse- og personopplysninger skal oppbevares i låsbart skap og makuleres etter bruk
f. Elektronisk forsendelse av helse- og personopplysninger (e-post, meldingsutveksling mv.) skal krypteres
g. Ved fravær fra arbeidsplass og ved arbeidsdagens slutt skal bruker logge ut av alle systemer
h. Alle brukere skal ha egne brukernavn og passord til alle systemer
i. Oppbevaring, bruk og sikring av passord/PIN-kode/sikkerhetskoder for elektronisk ID skal være iht. fastlagte prosedyrer
j. Brukernavn og passord skal ikke oppgis på telefon eller e-post
k. Forespørsler om pasient via e-post skal ikke besvares
l. Det er ikke tillatt å søke etter informasjon man ikke har behov for eller ikke er autorisert for
m. Kun jobbrelatert informasjon fra Internett kan lastes ned
n. Programvare skal ikke installeres uten godkjennelse
o. E-post og vedlegg til e-post fra mistenkelig ukjent avsender skal ikke åpnes
p. Nødprosedyrer skal være etablert, kjent og ved behov følges
q. Feilsituasjoner skal håndteres iht. fastlagte prosedyrer
r. Avvik skal rapporteres i avvikssystemet
s. Virksomheten kan ha innsynsrett i arbeidstakers e-postkasse som arbeidsgiver har stilt til disposisjon til bruk i arbeidet. Tilsvarende har arbeidsgiver adgang til gjennomsøking av og innsyn i arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet.