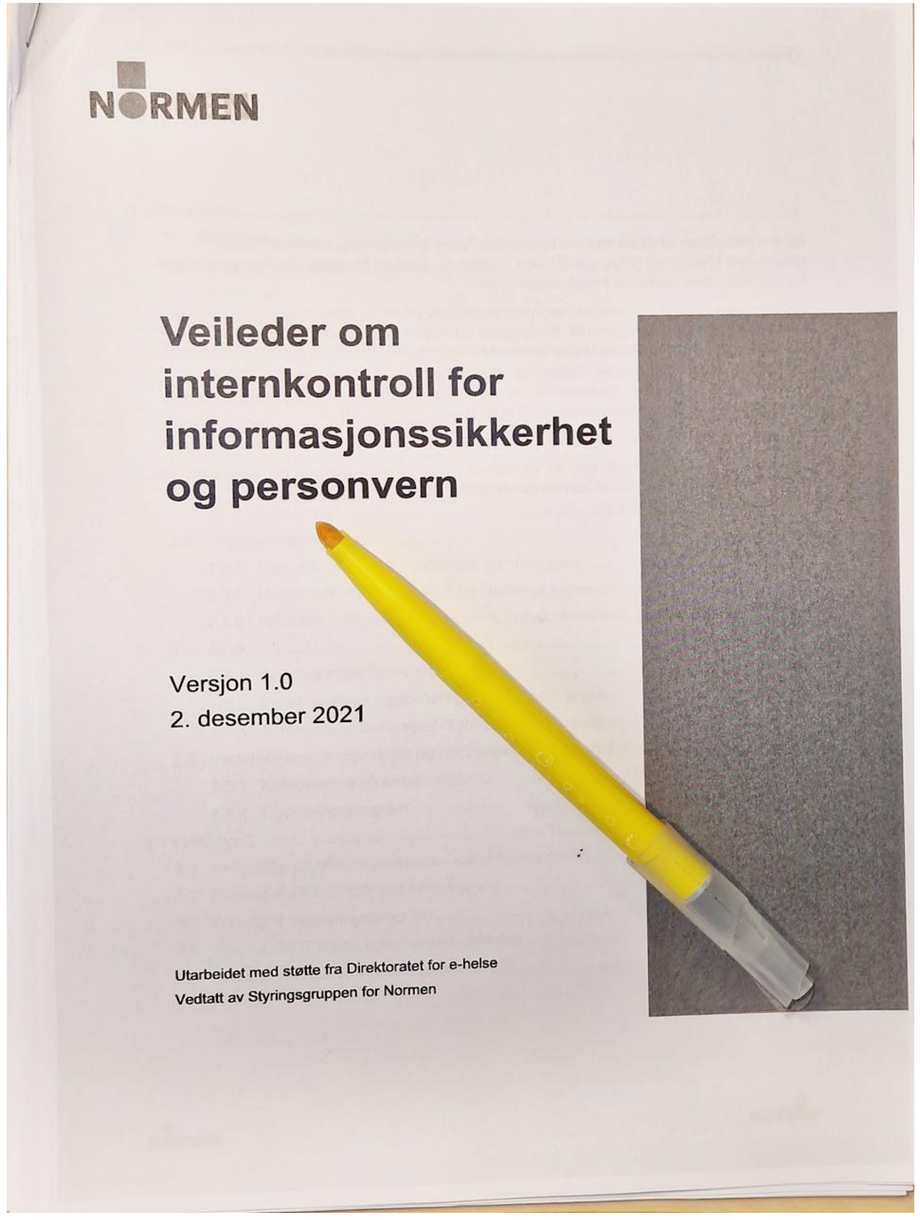
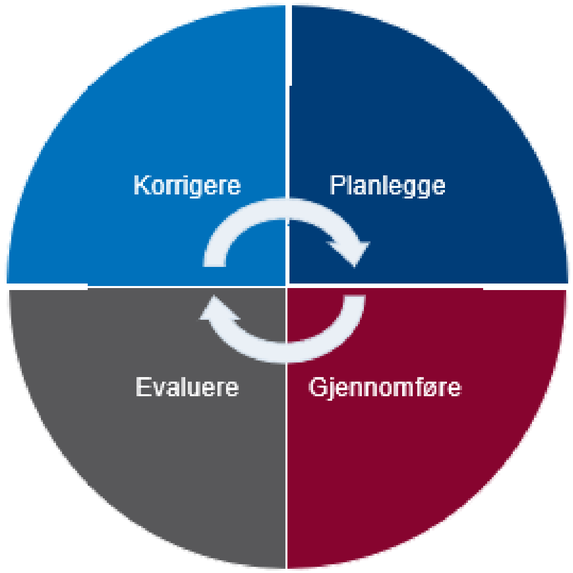
Veileder om internkontroll for informasjonssikkerhet og personvern



Hva er 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.



Krav til internkontroll - Myndighetskrav

Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten

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

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

§ 2.Virkeområde

Forskriften gjelder virksomheter som er pålagt internkontrollplikt etter

a) helsetilsynsloven § 5

b) spesialisthelsetjenesteloven § 2-1a tredje ledd

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

d) tannhelsetjenesteloven § 1-3a.

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

a) spesialisthelsetjenesteloven § 3-4a eller

b) helse- og omsorgstjenesteloven § 4-2.

NORMEN

Krav til internkontroll - Myndighetskrav
Personvernforordningen

Behandlingsansvarlig og databehandler sitt ansvar.

Artikkel 24:
Den behandlingsansvarliges (dataansvarliges) ansvar

Gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen

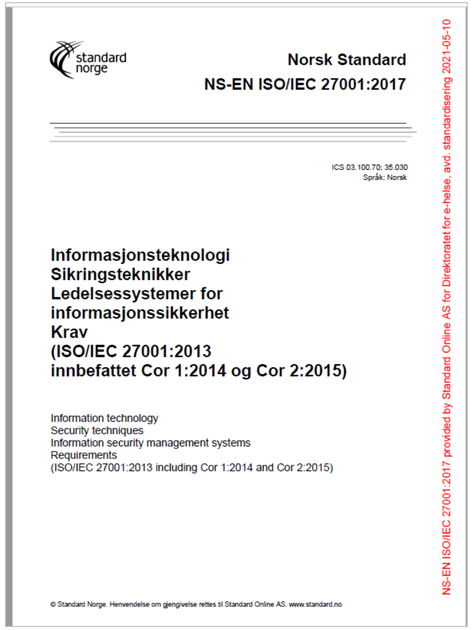
Artikkel 32 :
Sikkerhet ved behandlingen

Styringssystem

- Med styringssystem menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.
- Informasjonssikkerhet og personvern bør inngå som en **del av det totale** styringssystemet i virksomheten
- Styringssystemet skal **dokumenteres**
- Alle **offentlige virksomheter** skal beskrive mål og etablere strategi for informasjonssikkerhet. Dette skal danne grunnlaget for styringssystemet.

Internkontroll / Styringssystem / Ledelsessystem
Kjært barn har mange navn

- Internkontroll for informasjonssikkerhet
- Styringssystem for informasjonssikkerhet (SSIS)
- Kvalitetssystem for informasjonssikkerhet
- Ledelsessystem for informasjonssikkerhet
- Information Security management system (ISMS)


standard norge

Norsk Standard

NS-EN ISO/IEC 27001:2017

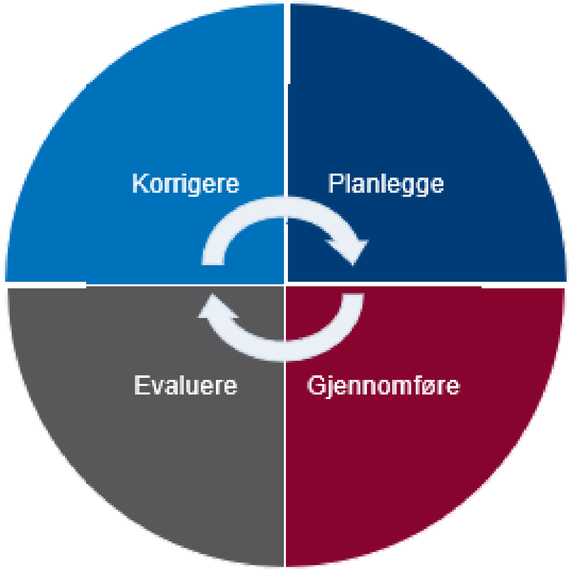
ICS 03.100.70; 35.030
Språk: Norsk

**Informasjonsteknologi
Sikringsteknikker
Ledelsessystemer for
informasjonssikkerhet
Krav
(ISO/IEC 27001:2013
innbefattet Cor 1:2014 og Cor 2:2015)**

Information technology
Security techniques
Information security management systems
Requirements
(ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

- **ISO/IEC 27001** er den mest **anerkjente** standarden for informasjonssikkerhet i verden.

- PDCA hjulet



NORMEN

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).
  - Informasjonssikkerhet og personvern bør inngå som en integrert del av den totale internkontrollen i virksomheten.

- 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, og **internkontroll er et av de mest sentrale verktøyene som understøtter dette målet**.

ENISA THREAT LANDSCAPE: HEALTH SECTOR

Map of incidents observed (January 2021 to March 2023)

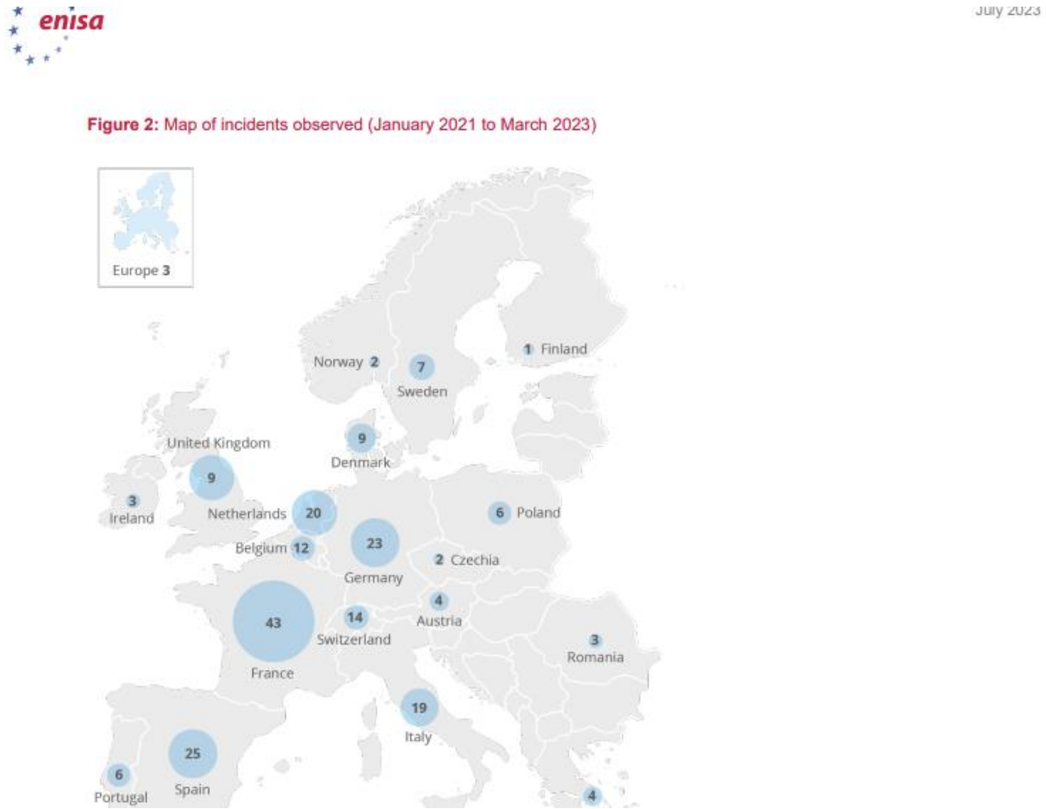
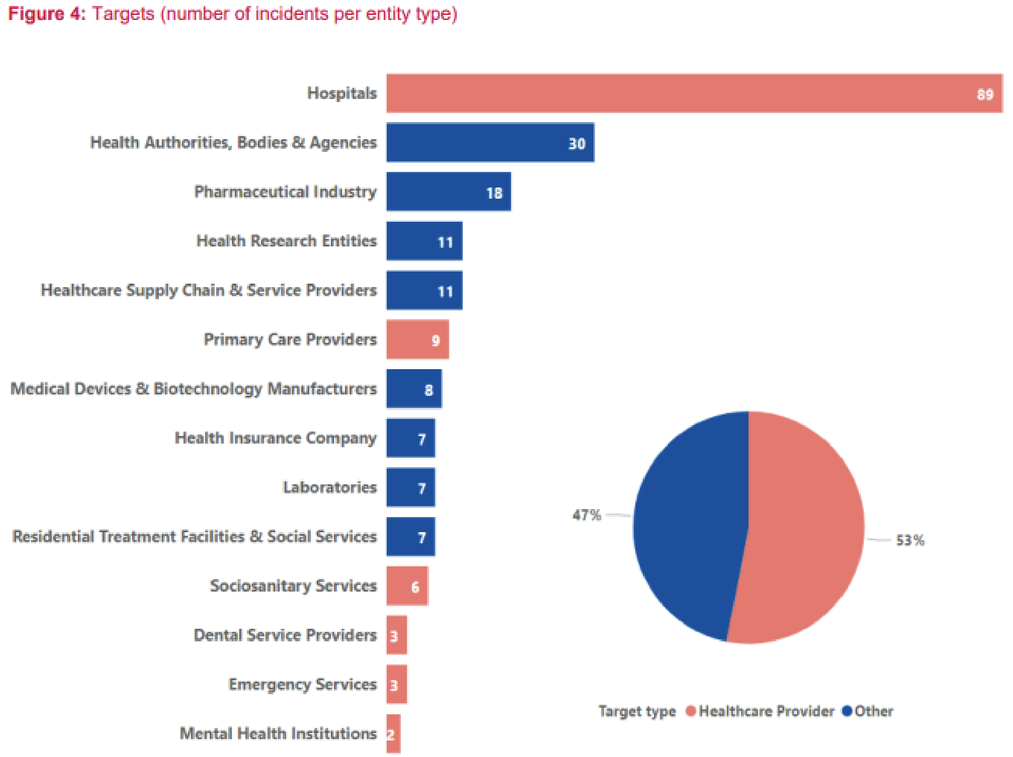


Figure 3: Incidents per country and year (2021, 2022, Q1 2023)



Må gjenopprette over 1000 datamaskiner etter hackerangrep

LENA (NRK): Hackerne kom seg innenfor brannmuren og 1300 ansatte jobber må med penn og papir. Ekspert sier småkommuner er ekstra utsatt for dataangrep.

STOR JOBB: IKT- lærlingene Mathias Johansen Kirkeby (t.v.) og Edvard Olafsen Elnæs har en enorm oppgave foran seg. De skal gjennomføre en teknisk oppvask på hundrevis av datamaskiner som tilhører Østre Toten kommune.

FOTO: ANDERS BAKKERUD LARSEN / NRK

Sigrid Havig Berge
Journalist

Ole Martin Sponberg
Journalist

Anders Bakkerud Larsen
Journalist

Publisert 14. jan. 2021 kl. 13:50
Oppdatert 8. feb. 2021 kl. 12:51

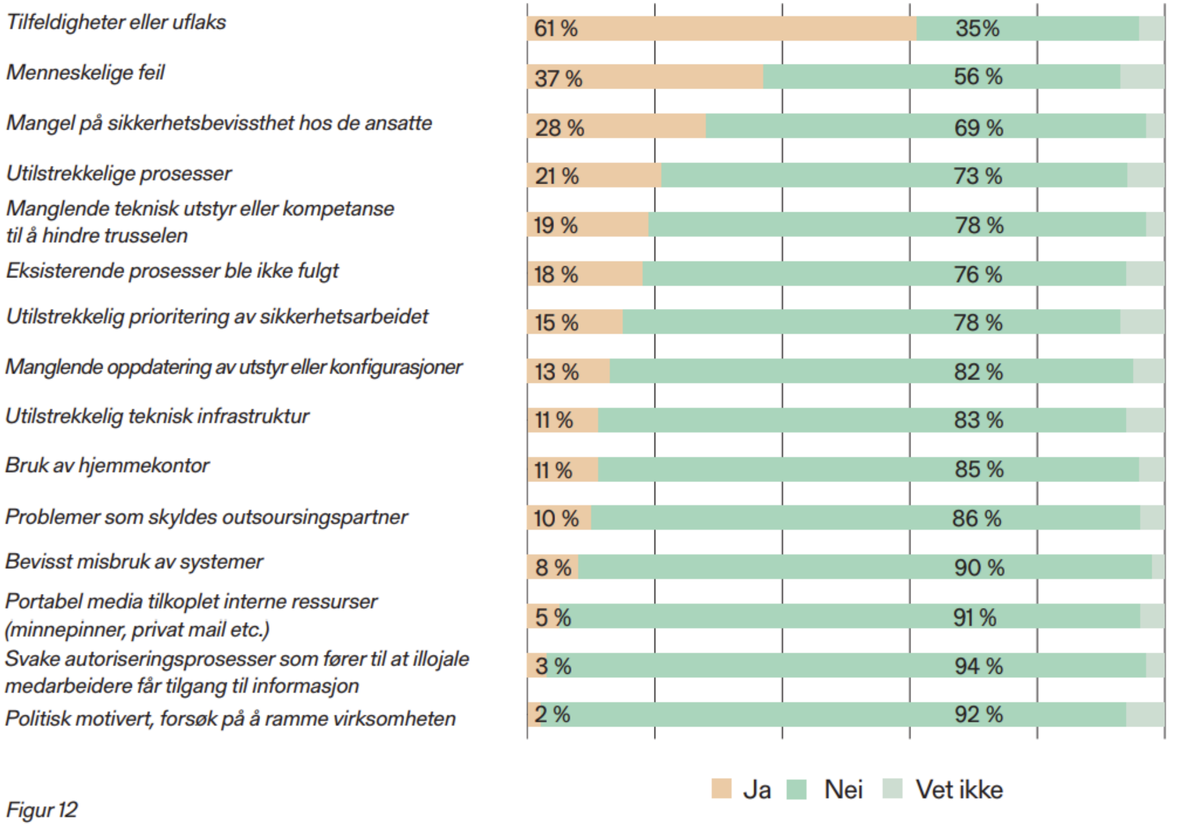
Artikkelen er mer enn to år gammel.

Kilde: NRK.no

3.1 Hvorfor sikkerhetsbrudd oppsto

I størst grad mener norske virksomheter at sikkerhetsbruddene har oppstått som en følge av tilfeldigheter eller uflaks.

Figur 12. Var noen av følgende faktorer medvirkende til at sikkerhetsbruddet oppsto?
Total sample; base n = 550; total n = 2500; 1950 missing



Figur 12

Næringslivets Sikkerhetsråd - Mørketallsundersøkelsen 2022

2.1 Roller og ansvar

- Virksomhetene i helse- og omsorgssektoren er dataansvarlig 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.

- …

- …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.

Ansvar

- Virksomhetens leder
- Leder
- Fagansvarlig informasjonssikkerhet
- Fagansvarlig personvern
- Fagansvarlig IKT
- Systemeier
- Risikoeier
- Personvernombud
- Ansatt/medarbeider

TYPE VIRKSOMHET	EKSEMPEL PÅ ROLLER OG ANSVAR I VIRKSOMHETEN
	Virksomhetens leder
Store virksomheter (f.eks. sykehus, kommuner, mv.)	• Ivareta virksomhetens ansvar og oppgaver som dataansvarlig • Fastsette mål og strategi for informasjonssikkerhet • Fastsette akseptabel risiko • Beskrive ansvar og myndighetsforhold • Fastsette hvilke behandlinger av helse og personopplysninger som skal utføres i virksomheten og sørge for at slik behandling

2.2 Styringssystem for informasjonssikkerhet og personvern

- Alle virksomheter i helse- og omsorgstjenesten skal etablere styringssystem

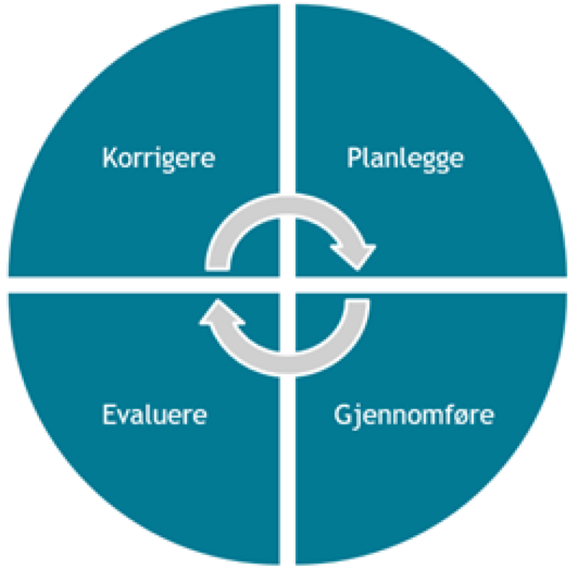
- Formålet med et styringssystem for informasjonssikkerhet og personvern er å:

  - sikre at virksomheten har tilstrekkelig styring og kontroll på informasjonssikkerheten, herunder sikring av informasjonens konfidensialitet, integritet og tilgjengelighet

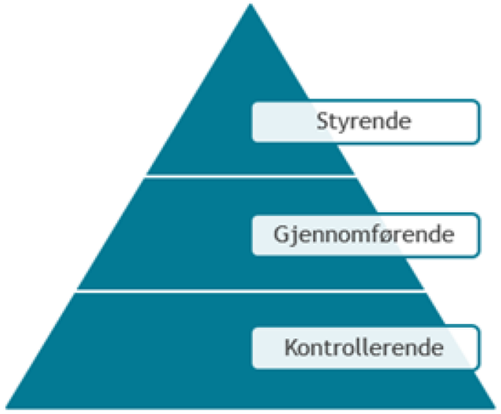
  - Sikre og påvise virksomhetens etterlevelse av personvernlovgivningen i samsvar med kravene som beskrives i personvernforordningen artikkel 5 og artikkel 24, pasientjournalloven § 23 og helseregisterloven § 22

  - 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.



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



Her vises styringssystemet som et tredelt hierarki.

- 2.2.1 Kontinuerlig forbedring
  - ... 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

2.3 Ledelsens gjennomgang

- 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:
    - 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

… 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.

- 2.3.3 Hvordan ledelsens gjennomgang bør gjennomføres og dokumenteres
  - 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.**

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.

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

- …Det er sjelden at den personen var den eneste som «ikke visste», sannsynligvis var det bare den som ble oppdaget.

- ... Har avviket vært omfattende bør det også gjennomføres en risikovurdering for å avklare om etablerte tiltak er tilstrekkelige

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.

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

- Kontinuerlig lære opp medarbeidere i krav om ivaretakelse av taushetsplikten, informasjonssikkerheten og personvernet.

- 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.

2.5.1 Kompetanse og sikkerhetskultur

«Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd – NSM»

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.

- 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.

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 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.

- …

Kultur


Fertilitetsseksjonen [redacted]
Fertilitetsseksjonen [redacted]
5. januar 2022 ·
🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟Gladmelding:
Fra 10.januar åpner vi for pasienter også i helg. Dette betyr at timer til ultralyd, egginnsett, inseminering og egguttak må påberegnes å legges til lørdag/søndag. Dette er en stor forbedring for alle som tidligere har fått eggløsning på «feil» dag.
Utredningstimer og andre kontroller blir kun hverdager.
🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟🌟
100
4 kommentarer 5 delinger
Liker
Kommenter
Del
Mest relevante
Linda [redacted]
Fantastiske nyheter!!
Liker Svar 2 år
Ann [redacted]
Fantastisk! 🤩
Liker Svar 2 år
Tina [redacted]
Hurra!! 🥳👏
Liker Svar 2 år
Ann [redacted]
Yey!!!!
Liker Svar 2 år

SPØRSMÅL?