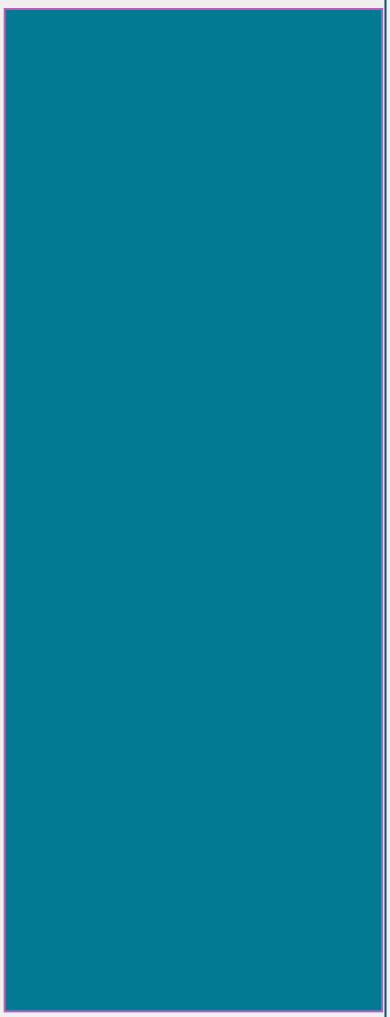
NORMEN

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

Versjon 7.0

UTGÅTT VERSJON – erstattet av versjon 7.1



Gjeldende fra 01.10.2025

Utgitt med støtte fra

Helsedirektoratet

UTGÅTT VERSJON – erstattet av versjon 7.1

Publikasjonens tittel:
Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

Versjonsnummer
7.0

Vedtatt av styringsgruppen for Normen:
03.06.2025

Gjeldende fra:
01.10.2025

Utgitt med støtte av:
Helsedirektoratet

Kontakt:
normen@helsedir.no

Publikasjonen kan lastes ned på:
www.normen.no

Forord

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.

Med bakgrunn i trussel- og risikovurderinger, ny lovgivning, teknologisk utvikling og alvorlige enkelthendelser, har det vært en økt oppmerksomhet rundt personvern og informasjonssikkerhet i helse- og omsorgssektoren.

Som en følge av dette har man også fått et økt behov for oppdatert veiledning og en modernisert og oppdatert Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen).

Denne versjonen av Normen er resultatet av et revisjons- og utviklingsarbeid hvor hovedmålene har vært å sikre at Normen er oppdatert i henhold til kravene i lov om digital sikkerhet og tilhørende forskrift. Helse- og omsorgssektoren er definert som tilbydere av samfunnsviktige og digitale tjenester, noe som innebærer at det skal spesifiseres grunnleggende krav til informasjonssikkerhet i nettverk- og informasjonssystemer, prosesser, produkter og tjenester for å forebygge, avdekke, motvirke, og håndtere uønskede hendelser. Samtidig som Normen forblir teknologinøytral og tilpasset dagens teknologiske utvikling.

UTGÅTT VERSJON - Høringsutkast av versjon 7.1

Innhold

Forord **3**
1 Om Normen **7**
1.1 Hva er informasjonssikkerhet og personvern? 7
1.2 Hva er Normen? 8
1.3 Hvem gjelder Normen for? 9
1.4 Normens forhold til lovverket 9
1.5 Om Normens krav 9
1.6 Normens utvikling og forvaltning 10
2 Ledelse og ansvar **11**
2.1 Roller og ansvar for informasjonssikkerhet og personvern 11
2.2 Dataansvarliges ansvar 12
2.3 Databehandlers ansvar 13
2.4 Styringssystem 13
2.5 Ledelsens gjennomgang 14
3 Risikostyring **16**
3.1 Forholdsmessighet ved valg av informasjonssikkerhetstiltak 16
3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet 16
3.3 Oversikt over teknologi og behandling av helse- og personopplysninger 17
3.4 Risikovurdering og risikohåndtering 18
3.4.1 Risikovurdering 18
3.4.2 Risikohåndtering 19
3.5 Vurdering av personvernkonsekvenser 19
3.5.1 Personvernkonsekvensvurdering (DPIA) 19
4 Grunnleggende om behandling av helse- og personopplysninger **21**
4.1 Behandlingsgrunnlag 21
4.2 Plikter og krav ved behandling av helse- og personopplysninger 22
4.2.1 Taushetsplikten 22
4.2.2 Informasjon til den registrerte 23
4.2.3 Innsyn 23
4.2.4 Retting og sletting 24
4.2.5 Tilgjengeliggjøring og utlevering av opplysninger i behandlingsrettet helseregister 25
4.2.6 Oppbevaring av helse- og personopplysninger 26
4.3 Innebygd personvern 27
5 Informasjonssikkerhet **28**
5.1 Medarbeidere, kompetanse og holdningsskapende arbeid 28

UTGÅTT VERSJON – erstattet av versjon 7.1

5.1.1 Vilkår og betingelser 28
5.1.2 Opplæring og kompetanse 28
5.1.3 Opphør av arbeidsforhold 29
5.2 Tilgangsstyring 29
5.2.1 Autorisering 30
5.2.2 Autentisering 31
5.2.3 Kontroll av tilganger 31
5.3 Fysisk sikkerhet og håndtering av utstyr 32
5.3.1 Nøkler/adgangskort 32
5.3.2 IKT-utstyr 32
5.3.3 Infrastruktur 32
5.3.4 Mobilt utstyr, hjemmekontor og fjernarbeid 33
5.3.5 Kryptering 33
5.3.6 Medisinsk utstyr og velferdsteknologi 34
5.4 Sikker IT-drift 34
5.4.1 Konfigurasjonskontroll 34
5.4.2 Endringsstyring 35
5.4.3 Sikkerhetskopiering 35
5.4.4 Logging 35
5.4.5 Styring og håndtering av tekniske sårbarheter 36
5.4.6 Sikkerhetsrevisjon 37
5.5 Kommunikasjonssikkerhet 37
5.5.1 Styring av informasjonssikkerhet i nettverk- og informasjonssystemer 37
5.5.2 Tilkobling til eksterne nett 38
5.5.3 Elektronisk samhandling 38
5.5.4 E-post og SMS 40
5.5.5 Tilkobling til Internett 40
5.6 Digital kommunikasjon til den registrerte 40
5.7 Leverandørforhold og avtaler 41
5.7.1 Krav til leverandørers taushetsplikt 41
5.7.2 Generelt om avtaler og leverandøroppfølging 41
5.7.3 Tjenesteutsetting 42
5.7.4 Databehandler 42
5.7.5 Vedlikehold, fjernaksess eller fysisk service 43
5.7.6 Systemleverandører 44
5.7.7 Leverandøroppfølging 44
5.7.8 Overføring av opplysninger til utlandet 44
5.7.9 Skytjenester 45
5.8 Håndtering av informasjonssikkerhetsbrudd 45

UTGÅTT VERSJON – erstattet av versjon 7.1

5.8.1 Avvikshåndtering 45
5.8.2 Brudd på personopplysningssikkerhet 46
5.8.3 Varsel til Statens helsetilsyn 46
5.8.4 Varsel til Nasjonal sikkerhetsmyndighet 47
5.9 Beredskap 47
6 Vedlegg 49
6.1 "Oversikt over Normens krav" 49
6.2 Definisjoner 49
6.3 Støttedokumenter 56
6.3.1 Faktaark 56
6.3.2 Veiledere 56
6.3.3 Maler 56
6.4 Referanser 56
6.5 Normens historikk 57

UTGÅTT VERSJON – erstattet av versjon 7.1

1 Om Normen

1.1 Hva er informasjonssikkerhet og personvern?

Gode helsetjenester forutsetter at relevante pasientopplysninger kan deles. Opplysningene trengs for å gi helsehjelp, til kvalitetssikring av helsehjelpen og til læring. Forskere har behov for opplysningene for å utvikle bedre helsetjenester.

God pasientsikkerhet krever at opplysninger lagres og deles mellom helsepersonell, at opplysningene er 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.

Se også " https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049"

Informasjonssikkerhet handler om å beskytte helse- og personopplysninger, samt sikre nettverk og informasjonssystemer som er nødvendige for å kunne tilby trygge og forsvarlige helse- og omsorgstjenester. Dette omfatter både tekniske, organisatoriske, fysiske, personellmessige og juridiske tiltak for å ivareta informasjonens integritet, tilgjengelighet og konfidensialitet – uavhengig av hvor og hvordan informasjonen behandles.

Et sentralt mål er å bygge robuste systemer og prosesser som tåler både kjente og uforutsette trusler. Informasjonssikkerhet skal bidra til å redusere risiko og forebygge, oppdage og håndtere uønskede hendelser – enten de skyldes menneskelige feil, teknisk svikt eller tilsiktede angrep.

Med «integritet» menes i Normen at helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting. Integritet er en forutsetning for god og forsvarlig helsehjelp.

Med «tilgjengelighet» menes i Normen at helse- og personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene. Tilgjengelig informasjon for helsepersonell er en forutsetning for god og forsvarlig helsehjelp.

Med «konfidensialitet» menes i Normen at helse- og personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene. Konfidensialitet bidrar til ivaretakelse av taushetsplikt og personvern, noe som er viktig for innbyggernes tillit til helse- og omsorgstjenesten.

Med sikkerhetstiltak menes tekniske, organisatoriske, fysiske og personellmessige tiltak som anses egnet for å oppnå tilfredsstillende informasjonssikkerhet og personvern i sektoren basert på risikovurdering.

Personvernforordningen bruker også begrepet robusthet i tillegg til integritet, tilgjengelighet og konfidensialitet. Med «robusthet» menes i Normen organisasjonens og informasjonssystemenes evne til å gjenopprette normaltilstand etter for eksempel en fysisk eller teknisk hendelse. Robusthet oppnås gjennom egnede tekniske og organisatoriske tiltak

UTKAST VERSJON - forslag til ny versjon 7.1

som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting av personopplysningssikkerheten og informasjonssikkerheten for øvrig.

Personvern kan defineres og beskrives på ulike måter. Uansett hvilken innfallsvinkel som velges, står det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, respekt for egen integritet og privatlivets fred sentralt. Personvern er derfor nær knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse.[1]

Tema for Normen er den delen av personvernet som handler om personopplysningsvern. Personvernforordningen (GDPR) regulerer personopplysningsvernet. Personopplysninger skal behandles etter prinsippene i personvernforordningen art. 5, se kap 2.2, og de registrertes rettigheter skal sikres.

En viktig del av dette er det personvernforordningen art. 32 kaller personopplysningssikkerhet. Det er det samme som informasjonssikkerhet for personopplysninger.

Normen skal, innenfor lovverkets rammer, søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet.

1.2 Hva er Normen?

Normen er en bransjenorm som er utarbeidet og forvaltes av organisasjoner og virksomheter i helse- og omsorgssektoren.

Denne versjonen av Normen har ikke status som atferdsnorm etter personvernforordningen artikkel 40 (lovdata.no)

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern hos den enkelte virksomhet, i infrastruktur, nettverk- og informasjonssystemer i sektoren generelt. Normen skal også bidra til å forebygge, avdekke, motvirke og håndtere uønskede hendelser i nettverk- og informasjonssystemer, tjenester og produkter som brukes for å levere digitale tjenester i sektoren. Videre skal Normen bidra til å sikre at en virksomhet som etterlever og innretter seg etter Normen, har egnede tekniske, organisatoriske, fysiske og personellmessige tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

Videre skal Normen bidra til at virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. De som samhandler med en virksomhet som har forpliktet seg til å innrette seg etter Normens krav, skal kunne stole på at denne virksomheten har egnede tekniske, organisatoriske, fysiske og personellmessige tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

Normen skal bidra til at pasienter, brukere, ansatte og andre registrerte sikres et godt personvern. Normen er et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet og personvern, og skal bidra til å understøtte gode helsetjenester, god pasientsikkerhet, kvalitetssikring, helsepersonellets læring, godt personvern og pasientens helsetjeneste.

DRAFT-VERSION – erstattet av versjon 7.1

1.3 Hvem gjelder Normen for?

Normen gjelder for enhver virksomhet som ved avtale har forpliktet seg til å følge den.

1.4 Normens forhold til lovverket

Lovgivningen stiller krav til informasjonssikkerhet og personvern som gjelder uavhengig av Normen. Relevante tilsynsmyndigheter kan kontrollere den enkelte virksomhets etterlevelse av disse lovkravene.

Normen dekker ikke alle lovkrav til informasjonssikkerhet, personvern og behandling av helse- og personopplysninger.

Lovgivningen har flere krav til informasjonssikkerhet, personvern og behandling av helse- og personopplysninger enn det som er hovedtema for Normen. Dette inkluderer problemstillinger rundt bruk av helse- og personopplysninger for andre formål enn ytelse av helse- og omsorgstjenester. Dette omfatter spesifikke krav til registre som har egne forskrifter, rettsgrunnlag for behandling av helse- og personopplysninger samt plikt til og krav til journalføring. Informasjonssikkerhet er også regulert i annet lovverk enn det som gjelder behandling av personopplysninger.

Lovgivningen stiller krav til informasjonssikkerhet i nettverk- og informasjonssystemer, produkter, tjenester og prosesser som benyttes for å levere helse- og omsorgstjenester og beskytte personopplysninger. Kravene i lov om digital sikkerhet og tilhørende forskrift gjelder for virksomheter som blant annet omfatter de regionale helseforetakene, nasjonale e-helseløsninger som systemer for rekvirering og utlevering av legemidler, samt kommuner med over 50 000 innbyggere eller flere enn 20 000 brukere som er avhengige av tjenesten. Målet er å forebygge, avdekke og motvirke uønskede hendelser, og sikre at virksomheter har forsvarlig tekniske, organisatoriske, fysiske og personellmessige sikkerhetstiltak på plass. Øvrige krav i Normen gjelder for alle virksomheter i helse- og omsorgssektoren som gjennom avtale har forpliktet seg til å følge den. Normen er avgrenset mot sikkerhetsloven.

Normens krav utdyper og supplerer gjeldende regelverk. Overholdelse av kravene i Normen kan brukes for å påvise at virksomhetens forpliktelser etter regelverket overholdes.

Normen har i liten grad lovhenvisninger i dokumentet. Lov- og forskriftshjemler til Normens krav finnes i vedlegget "Oversikt over Normens krav".

Kommentert [GJ1]: Lenke til oppdatert mapping

1.5 Om Normens krav

Normen beskriver organisatoriske, tekniske, fysiske og personellmessige sikkerhetstiltak som anses egnet for å oppnå tilfredsstillende informasjonssikkerhet og personvern i sektoren.

Ved valg av organisatoriske, tekniske, fysiske og personellmessige sikkerhetstiltak skal virksomheten vurdere tiltakene i forhold til virksomhetens størrelse, art, kompleksitet og omfang for behandling av helse- og personopplysninger, pasientsikkerhet og risikobildet mv. Tiltakene skal velges basert på risikovurderinger, og tiltakene skal være forholdsmessige. Dette kan bety at større virksomheter som behandler personopplysninger i større omfang,

UTGÅTT VERSJON - Erstattet av Version 7.1

bør etablere flere tiltak enn mindre virksomheter som behandler personopplysninger i mindre omfang, og der risikoen er mindre kompleks og lettere håndterbar.

Normen har en veileder for små helsevirksomheter som gir nærmere veiledning for hvordan små virksomheter kan jobbe med informasjonssikkerhet og personvern i praksis.

Normen skiller mellom «skal»- og «bør»-krav. «Skal»-krav gjelder for alle. «Bør»-krav må virksomheten selv vurdere om er «egnet» for virksomheten.

Normen er ikke uttømmende for behandling av helse- og personopplysninger der formålet ikke er ytelse av helse- og omsorgstjenester (f.eks. behandling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten.), men relevante krav til informasjonssikkerhet og personvern som beskrives i Normen, gjelder også her. Kravene til informasjonssikkerhet og personvern er i hovedsak like i lovgivning som regulerer både behandlingsrettede helseregistre og annen bruk av helse- og personopplysninger. Virksomheten skal vurdere hvilke krav fra Normen som gjelder basert på den konkrete behandlingen av helse- og personopplysninger (kapittel 3.1 Forholdsmessighet ved valg av tiltak).

En virksomhet håndterer i tillegg personopplysninger om egne ansatte. Normen er ikke uttømmende for behandling av opplysninger om ansatte. Virksomheten skal ivareta de ansattes personvern iht. gjeldende lover og forskrifter. Det er spesielt viktig at opplysninger om de ansattes bruk av informasjonssystemene (logging) kun gjøres med hjemmel i lov, slik at unødvendig overvåking av de ansatte unngås. Den ansatte har rett til innsyn i opplysninger som gjelder den ansatte selv (jf. personvernforordningen artikkel 15).

Normen har krav som dekker de fleste temaer innen informasjonssikkerhet og personvern: mennesker, prosesser, teknologi samt nettverk- og informasjonssystemer, tjenester og produkter. Normen har også støttedokumenter i form av veiledningsmateriell. Veiledningsmateriellet gir veiledning og eksempler på tiltak, se kapittel 6.2

Vedlegget "Oversikt over Normens lovkrav" inneholder alle Normens "skal-krav", med hjemmel i lov eller forskrift, samt referanser til ISO 27001:2023 og 27002:2022.

Kommentert [GJ2]: Lenke til oppdatert mapping

1.6 Normens utvikling og forvaltning

Normen er utarbeidet og forvaltes av en styringsgruppe fra helse- og omsorgstjenesten. I prinsipielle spørsmål som behandles i styringsgruppen, søkes enstemmighet.

Helsedirektoratet er sekretariat for styringsgruppens arbeid, med fast deltakelse fra Norsk Helsenett.

UTGÅTT VERSJON - erstattes av versjon 7.0

2 Ledelse og ansvar

Virksomhetens øverste leder har ansvaret for å sikre at virksomheten har et sikkerhetsnivå som oppfyller gjeldende krav til informasjonssikkerhet og personvern. For virksomheter som er underlagt Lov om digital sikkerhet, innebærer dette å etablere og opprettholde et forsvarlig sikkerhetsnivå i tråd med lovens krav.

For virksomheter som ikke er omfattet av lov om digital sikkerhet, gjelder Normens krav om at virksomhetens informasjonsbehandling skal ha et sikkerhetsnivå som er egnet med hensyn til risikoen og behandlingens art.

Der Normen benytter begrepet «egnet» sikkerhetsnivå, skal dette for virksomheter som er underlagt lov om digital sikkerhet forstås som «forsvarlig» sikkerhetsnivå. Det vil si et sikkerhetsnivå som er tilpasset risikoen og er i tråd med lovens krav.

Videre skal ledelsen sikre at alle nødvendige organisatoriske, tekniske, fysiske og personellmessige sikkerhetstiltak blir gjennomført for å redusere risiko og opprettholde et egnet sikkerhetsnivå i virksomheten. Ansvaret bør ivaretas som en del av arbeidet med virksomhetsstyring og kvalitetsforbedring.

Ansvaret inkluderer å:

- sette føringer for vurdering og håndtering av risiko,[2] inkludert fastsettelse av kriterier for å akseptere risiko
- sørge for velfungerende styring og kontroll.

Virksomheten skal dokumentere alle tiltak som iverksettes for å opprettholde informasjonssikkerhet og personvern.

Virksomheter som er omfattet av både Normens krav og forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten, bør legge denne forskriftens bestemmelser til grunn for å sikre at helse- og omsorgslovgivningens krav til informasjonssikkerhet og personvern etterleves.

UTGÅTT VERSJON – erstattet av versjon 7.1

2.1 Roller og ansvar for informasjonssikkerhet og personvern

Virksomhetens øverste ledelse skal sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver for å ivareta ansvaret for informasjonssikkerhet og personvern. Oppgavene kan utføres av egne ansatte eller av eksterne.

Den som har ansvar for en funksjon eller en enhet, bør også ha ansvaret med å følge opp informasjonssikkerhet og personvern i funksjonen eller enheten.

Virksomheten beslutter hvilke roller og funksjoner for informasjonssikkerhet og personvern som er nødvendig. Det skal være tydelig hvem som er ansvarlig, og hva de er ansvarlig for.

Alle skal være kjent med hvilke oppgaver de har, i tillegg til å ha tilstrekkelig kunnskap om andres relevante ansvar og oppgaver, og hvem som har myndighet til å ta beslutninger.

En større virksomhet bør ha en egen informasjonssikkerhetsleder eller sikkerhetsorganisasjon knyttet opp mot virksomhetens ledelse.

Offentlige virksomheters øverste ledelse skal sørge for at det utpekes et personvernombud. For en privat virksomhet skal øverste ledelse utpeke et personvernombud når informasjonsbehandlingens omfang, art og formål krever det. Dette gjelder også små virksomheter. Personvernombudet kan være ansatt i virksomheten eller ekstern og utføre oppgavene på grunnlag av en tjenesteavtale.

Personvernombudet skal gis tilstrekkelige ressurser og tilgang på relevant kompetanse til å utføre sine plikter. Ombudet skal ikke ha interessekonflikt med eventuelle andre roller som vedkommende har i virksomheten, og skal ikke motta instruksjoner om hvordan oppgavene skal utføres.

2.2 Dataansvarliges ansvar

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

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

Dataansvarlig skal:

- delegere myndighet og oppgaver (jf. kap. 2.1)
- etablere, vedlikeholde og etterleve styringssystemet (jf. kap. 2.4)
- gjennomføre risikovurderinger og utarbeide en plan for håndtering av risiko (jf. kap. 3)
- gjennomføre personvernkonsekvensvurderinger (DPIA) for behandlinger der det er nødvendig (jf. kap. 3)
- sikre den registrertes rettigheter (jf. kap. 4)
- etablere, dokumentere og iverksette organisatoriske, tekniske, fysiske og personellmessige sikkerhetstiltak (jf. kap. 5)
- inngå og følge opp avtaler (jf. kap. 5.7)
- rapportere og håndtere avvik (jf. kap. 5.8)
- iverksette tiltak for fysisk sikkerhet (jf. kap. 5.2)
- sørge for at sikkerhetstiltak er gjort kjent for personell og leverandører (jf. kap. 5.1.2)
- sikre tilstrekkelig kompetanse innenfor informasjonssikkerhet og personvern, og nødvendig opplæring ved behov (jf. kap. 5.1.2)
- etablere og dokumentere beredskapsplaner og gjennomføre øvelser (jf. kap. 5.9)

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

- behandles på en lovlig måte (gyldig behandlingsgrunnlag)
- behandles på en rettferdig måte (med respekt for de registrertes interesser og rettigheter)
- behandles på en åpen måte (oversiktlig, forutsigbar og forståelig informasjon) med hensyn til den registrerte (pasienten/brukeren)

UTKAST VERSJON 7.0 – erstatter av versjon 7.1

- bare registreres for bestemte formål som skal være legitime (som dokumentasjon av helsehjelp)
- være tilgjengelige for helsepersonell når dette er nødvendig for å kunne gi forsvarlig helsehjelp
- bare benyttes til de formål de er registrert for, med mindre det finnes behandlingsgrunnlag for andre formål
- være relevante, adekvate, korrekte og om nødvendig oppdaterte for de formål de er registrert for
- lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene
- sikres mot uautorisert tilgang, endring, ødeleggelse og spredning

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

2.3 Databehandlers ansvar

En databehandler er en virksomhet som behandler helse- og personopplysninger på vegne av dataansvarlig. Databehandler har på lik linje med dataansvarlig et selvstendig ansvar for informasjonssikkerhet og for ivaretakelse av den registrertes personvern.

Databehandler skal
- bare behandle helse- og personopplysninger etter instruks fra dataansvarlig
- ikke bruke underdatabehandler uten at det er godkjent av dataansvarlig
- være ansvarlig for at underleverandører oppfyller sine forpliktelser
- bistå dataansvarlig med å sikre overholdelse av forpliktelser til informasjonssikkerhet

Databehandler skal bistå dataansvarlig med personvern og informasjonssikkerhet ved å sørge for en risikobasert tilnærming. Dette innebærer at databehandler skal bidra til at et egnet sikkerhetsnivå blir ivaretatt og nødvendige tiltak blir implementert.

Se nærmere om databehandler i kap. 5.7.4.

2.4 Styringssystem

Alle virksomheter skal ha et styringssystem for informasjonssikkerhet og personvern (internkontroll). Med styringssystem menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer, kontrollerer og korrigerer etterlevelse av relevant regelverk, sikkerhetskrav, avtaler, tjenester og produkter.

Informasjonssikkerhet og personvern bør inngå som en del av det totale styringssystemet i virksomheten. Styringssystemet skal tilpasses virksomhetens størrelse og ha en risikobasert tilnærming. Det skal ta hensyn til virksomhetens risiko, egenart og aktiviteter, samt informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i. For mindre virksomheter betyr det at de ikke trenger et like omfattende styringssystem som store virksomheter.

UTKAST VERSJON – erstattet av versjon 7.1

Se nærmere i Normens veileder om internkontroll for informasjonssikkerhet for veiledning om hva som bør inngå i et styringssystem og Normens veileder for små helsevirksomheter.

Virksomhetens ledelse har ansvaret for å fastsette mål og strategi for informasjonssikkerhet, etablere styringssystem, sikkerhetsorganisering med roller og ansvar, og sørge for at det inngå som en del av den overordnede virksomhetsstyringen. Virksomhetens leder skal gi tilstrekkelige økonomiske rammer og ressurser for gjennomføring av alle nødvendige aktiviteter for å etablere og opprettholde et egnet sikkerhetsnivå i virksomheten.

Styringssystemet skal godkjennes av virksomhetens leder og gjennomgås minst årlig med sikte på å forbedre virksomhetens sikkerhetsarbeid.

Styringssystemet skal gjøres kjent for samtlige ansatte med tjenstlig behov samt leverandører og underleverandører.

Styringssystemet skal dokumenteres. Dokumenter angitt i styringssystemet skal holdes løpende oppdatert, kontinuerlig forbedres og arkiveres fra det tidspunktet dokumentet ble erstattet med en ny gjeldende versjon. Dette kan f.eks. være rutiner for sikkerhetsrevisjoner, risikovurderinger, driftsrutiner, avvik og hvordan de håndteres, ledelsens gjennomgang, databehandleravtaler mv.

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. Dokumentasjonen skal til enhver tid være oppdatert og tilgjengelig.

Alle offentlige virksomheter skal beskrive mål og etablere strategi for informasjonssikkerhet. Dette skal danne grunnlaget for styringssystemet.

2.5 Ledelsens gjennomgang

Virksomhetens øverste ledelse har ansvar for å sikre at virksomheten opprettholder et egnet sikkerhetsnivå og følger gjeldende krav til informasjonssikkerhet og personvern. Ledelsen skal gjennomgå virksomhetens styringssystem for informasjonssikkerhet og personvern minst en gang i året.

Grunnlag for gjennomgangen skal omfatte vurdering av:

- status på aktiviteter fra tidligere ledelsens gjennomgang
- endringer i behandlinger av helse- og personopplysninger (protokoll)
- endringer i organiseringen av arbeidet
- resultatene fra risikovurderinger og status for planer for risikobehandling
- resultat av personvernkonsekvensvurderinger (DPIA)
- resultater fra revisjoner
- resultat av avviksbehandling
- oppfølging av leverandører og databehandleravtaler
- endring i akseptabel risiko

Resultatene fra ledelsens gjennomgang skal omfatte beslutninger om eventuelle behov for endringer i styringssystemet. Dersom gjennomgangen avdekker at virksomhetens risiko ikke

UTKAST VERSJON - erstattet av Version 7.1

er akseptabel, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar. Ledelsens gjennomgang skal dokumenteres.

UTGÅTT VERSJON – erstattet av versjon 7.1

3 Risikostyring

Risikostyring innebærer koordinerte aktiviteter for å rettlede og kontrollere en virksomhet med hensyn til risiko. Det omfatter å få oversikt over informasjon og teknologi i virksomheten, identifisere trusler, sårbarheter og konsekvenser ved mulige uønskede hendelser for både virksomheten og de registrerte, analysere risikoen og etablere tiltak for å opprettholde et egnet sikkerhetsnivå.

Virksomheten skal etablere og iverksette sikkerhetstiltak som er egnet for å håndtere risiko på en tilfredsstillende måte. Dette inkluderer å sikre både konfidensialitet, integritet, tilgjengelighet og robusthet i nettverk- og informasjonssystemene. Disse hensynene skal balanseres.

Det skal tas hensyn til den tekniske utviklingen, gjennomføringskostnader og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i, når det vurderes om en risiko kan aksepteres. Arbeidet med risikostyring skal ta hensyn til for eksempel type og mengde opplysninger, virksomhetens størrelse og behandlingens kompleksitet.

UTGÅTT VERSJON - erstattet av versjon 7.1

3.1 Forholdsmessighet ved valg av informasjonssikkerhetstiltak

Ved vurderinger og valg av sikkerhetstiltak skal virksomheten vurdere tiltakene opp mot virksomhetens art, omfang og kompleksitet for behandling av helse- og personopplysninger og pasientsikkerhet. Ved vurdering av teknologiske sikkerhetstiltak skal det også tas hensyn til virksomhetens driftsmiljø, brukermiljø, funksjon og risiko ved virksomhetens nettverk- og informasjonssystemer.

Sikkerhetstiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikobildet, og skal bidra til å forebygge, avdekke, håndtere og redusere konsekvensen av hendelser. Dette gjelder særlig i vurderingen av egnet sikkerhetsorganisasjon, arbeidsoppgaver, kontrolloppgaver og tiltak innen informasjonssikkerhet, nettverk- og informasjonssystemer, tjenester, produkter og prosesser (for eksempel tilgangsstyring, logging, hendelseshåndtering, fysisk sikring, leverandørkjeder, anskaffelser mv.).

Virksomheten skal sørge for at det er forholdsmessighet mellom risiko og tiltakets kostnad.

3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet

Virksomheten skal sørge for at virksomhetens behandlinger av helse- og personopplysninger har et egnet sikkerhetsnivå i tråd med Normens minimumskrav til informasjonssikkerhet og eventuelt egne informasjonssikkerhetsmål. Normen stiller følgende overordnede minimumskrav til informasjonssikkerhet (konfidensialitet, integritet, tilgjengelighet og robusthet):

Krav for å sikre konfidensialitet

Virksomheten skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger.

- hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
- avgrense tilgang for autorisert personell iht. tjenstlig behov
- ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten

Krav for å sikre integritet
Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er sikret mot utilsiktet eller uautorisert endring eller sletting. Integritet er en forutsetning for god og forsvarlig helsehjelp

- logge hvem som har rettet, registrert, endret og slettet
- hindre utilsiktet eller uautorisert endring eller sletting
- sikre at helse- og personopplysninger registreres på rett person
- sikre at helse- og personopplysninger føres i henhold til relevant kodeverk og terminologi
- sikre at helse- og personopplysninger er korrekte og om nødvendig oppdaterte
- hindre at kopier av data blir en kilde til utdatert informasjon

Krav for å sikre tilgjengelighet og robusthet
Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er tilgjengelig til rett tid.

- sikre at helse- og personopplysninger er tilgjengelig iht. tjenstlig behov
- sikre sikker og stabil drift av nettverks- og informasjonssystemer, inkludert motstandsdyktighet og evne til å gjenopprette normaltilstand ved hendelser.
- sikre at det er etablert tekniske, organisatoriske, fysiske og personellmessige tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting
- sikre at informasjonssystemene er tilgjengelig iht. virksomhetens tilgjengelighetskrav

Brudd på kravene skal behandles som avvik.

UTGÅTT VERSJON - erstattet av versjon 7.1

3.3 Oversikt over teknologi og behandling av helse- og personopplysninger

Ved å etablere og vedlikeholde oversikt over helse- og personopplysningene som behandles, og teknologi som brukes, skal virksomheten identifisere potensielle risikoområder den bør være spesielt oppmerksom på.

Virksomheten skal ha:

- protokoll over behandlinger av helse- og personopplysninger, se Normens faktaark for protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)
- oversikt over informasjonssystemer, IKT-prosesser, IKT- tjenester, infrastruktur, og annen informasjon med betydning for informasjonssikkerheten, mv. Virksomheten skal også kartlegge konsekvenser av bortfall av systemer og klassifisere systemene, jf. kap. 5.9. Oversikten bør være dokumentert.

Områder for risikovurdering bør ta utgangspunkt i oversikten over helse- og personopplysningene som behandles, og oversikten over informasjonssystemene som brukes samt identifisering av potensielle trusler og sårbarheter. Risikovurderingen bør også inkludere vurdering av organisatoriske, tekniske, fysiske og personellmessige tiltak for å sikre integritet, tilgjengelighet og robusthet.

3.4 Risikovurdering og risikohåndtering

3.4.1 Risikovurdering

Risikovurdering er et verktøy og skal være av et slikt omfang at virksomheten kan identifisere nødvendige sikkerhetstiltak. Virksomhetene skal utarbeide, vedlikeholde og dokumentere risikovurderinger. Ved endringer i virksomheten som kan påvirke informasjonssikkerhet, skal risikoen som disse endringene medfører vurderes.

Risikovurderinger skal minst inneholde:

- kartlegging av virksomhetens nettverk- og informasjonssystemer, samt deres betydning for leveransen av samfunnsviktige tjenester.
- identifikasjon av potensielle hendelser som kan påvirke virksomhetens nettverk- og informasjonssystemer.
- analyse av sårbarheter knyttet til virksomhetens nettverk- og informasjonssystemer.
- vurdering av sannsynligheten for at en hendelse kan inntreffe.
- vurdering av konsekvensene av hendelser
- analyse av virksomhetens avhengighet av andre virksomheter for å fungere optimalt

Risikovurderingen bør ta utgangspunkt i en kartlegging av informasjonsverdier og hva som vil bli konsekvensen av hendelser som rammer tilgjengeligheten, integriteten og konfidensialiteten til informasjonsverdiene. Virksomheten skal vurdere sannsynligheten for at en hendelse kan inntreffe og konsekvensen av hendelsen. Dersom risikoen er uakseptabel, skal virksomheten gjennomføre tiltak for å redusere risikoen. Les mer i Normens veileder om risikostyring for informasjonssikkerhet og personvern

Virksomheten skal gjennomføre risikovurderinger, og de skal som minimum gjennomføres før:

- etablering av eller endring i behandling av helse- og personopplysninger
- etablering av nye informasjonssystemer eller registre som inneholder eller benytter helse- og personopplysninger
- endringer i eksisterende informasjonssystemer eller registre som inneholder eller benytter helse- og personopplysninger
- det etableres organisatoriske, tekniske, fysiske, personellmessige tiltak eller andre endringer med betydning for informasjonssikkerheten
- det etableres eller endres tilgang til helseopplysninger mellom virksomheter

UTGÅTT VERSJON – erstattet av versjon 7.1

Risikovurdering bør oppdateres ved endring i trusselbildet. I tillegg skal virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten.

3.4.2 Risikohåndtering

Basert på risikovurderingen skal virksomhetene ha en plan for å håndtere risiko. Som en del av risikohåndteringen skal virksomhetene iverksette nødvendige sikkerhetstiltak for å redusere risiko og opprettholde et egnet sikkerhetsnivå.

Risikohåndtering skal gjennomføres med utgangspunkt i minimumskravene for konfidensialitet, integritet, tilgjengelighet og robusthet, og virksomhetens akseptkriterier. Det skal tas avgjørende hensyn til konsekvenser for pasient/ bruker og forsvarlig helsehjelp i risikovurderingene.

Når det er nødvendig å gjennomføre tiltak for å oppnå akseptabel risiko, skal tiltakene fremgå av en plan med tydelig frist og hvem som er ansvarlig for gjennomføring. Planen skal forankres hos virksomhetens ledelse.

Dersom planlagte tekniske tiltak for å oppnå akseptabel risiko ikke kan innføres umiddelbart, bør risikoreduserende administrative tiltak f.eks. i form av rutine vurderes.

Virksomheten skal sikre at den har tilstrekkelig kompetanse tilgjengelig for å kunne vurdere risiko. Representanter for de som yter helsehjelp skal søkes involvert der det er relevant. De som utfører risikovurderingene, skal ha en tydelig eskaleringsvei til ledelsen/styret. Resultater fra risikovurderingen og plan for oppfølging av tiltak skal kommuniseres på rett detaljnivå til virksomhetens ledelse og ev. styret der dette er relevant.

3.5 Vurdering av personvernkonsekvenser

Virksomheter skal alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte. Virksomheten skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering, DPIA, Data Protection Impact Assessment.

3.5.1 Personvernkonsekvensvurdering (DPIA)

Personvernkonsekvensvurderingen (DPIA) skal gjøres før behandlingen av personopplysninger starter. For mer informasjon og veiledning om når man må gjennomføre en vurdering av personvernkonsenser, se Datatilsynets nettsider (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/).

Høy risiko for personvernet kan oppstå:

- når helseopplysninger behandles i stor skala
- ved bruk av ny teknologi

UTGÅTT VERSJON - erstattet av versjon 7.1

- når personopplysninger behandles på en automatisert, systematisk og omfattende måte, og dette danner grunnlag for avgjørelser som har rettsvirkning eller påvirker den registrerte i betydelig grad
- dersom behandlingens art, omfang, formål og sammenhengen den utføres i, tilsier det

Datatilsynet har laget en liste over behandlingsaktiviteter som alltid krever at det gjennomføres en personvernkonsekvensvurdering (DPIA).

Personvernkonsekvensvurdering (DPIA) skal minst inneholde:

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger
- beskrivelse av formålet med behandlingen av personopplysninger
- en vurdering av om behandlingene av helse- og personopplysninger er nødvendige og står i rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er utpekt, i forbindelse med utførelsen av en personvernkonsekvensvurdering.

Det skal planlegges tiltak som reduserer risikoen for personvernet. Dersom behandlingen av helse- og personopplysninger medfører en høy risiko som ikke kan reduseres ved hjelp av rimelige tiltak, skal den dataansvarlige be om forhåndsdrøftelse med Datatilsynet før behandlingen av opplysningene starter.

UTGÅTT VERSJON – Oppdatert av versjon 7.1

4 Grunnleggende om behandling av helse- og personopplysninger

Pasientbehandling forutsetter behandling av helseopplysninger om pasienten. Dokumentasjonsplikten i pasientbehandlingen skal bidra til at pasienter og brukere gis helse- og omsorgstjenester av god kvalitet, og være til støtte for helsepersonell ved ytelse av helsehjelp til den enkelte pasient. Ivaretakelse av pasientens personvern er også viktig for pasientsikkerheten ved at journalopplysningene skal være relevante, korrekte og oppdaterte.

Helsesektoren har flere lover og forskrifter med særregler om behandling av helse- og personopplysninger, og de utfyller kravene i personopplysningslovgivningen. Helselovgivningen bygger i stor grad på pasienter og brukeres rettigheter og virksomheters plikter. Normen er avgrenset til å omhandle viktige rettigheter og plikter i lovgivningen som gjelder behandling av personopplysninger.

Se Helsedirektoratets rundskriv om helsepersonelloven og pasient- og brukerrettighetsloven

Helsepersonellets taushetsplikt er en viktig del av personvernet og er en forutsetning for det nødvendige tillitsforholdet mellom pasienter og helsepersonell.

4.1 Behandlingsgrunnlag

Personopplysninger kan bare behandles når lovgivningen tillater det. All behandling av personopplysninger skal ha et lovlig grunnlag. I personvernforordningen kalles dette et behandlingsgrunnlag.

Behandling av særlige kategorier personopplysninger, for eksempel helseopplysninger, er i utgangspunktet forbudt etter personvernforordningen. Unntak gjelder likevel blant annet når det er gitt samtykke, når det ytes helsehjelp og sosialtjenester underlagt taushetsplikt, når allmenne folkehelsehensyn gjør det nødvendig, og til forskningsformål.

Se mer om behandlingsgrunnlag (www.datatilsynet.no) ref. personvernforordningens artikkel 6 Behandlingens lovlighet og artikkel 9 Behandling av særlige kategorier av personopplysninger.

Før behandling av helse- og personopplysninger starter, eller ved endringer i slik behandling, skal dataansvarlig sørge for å ha et gyldig behandlingsgrunnlag. Behandlingsgrunnlaget skal dekke alle typer behandling som utføres: innsamling, registrering, lagring, sletting, utlevering, mv. Skal opplysningene brukes til et annet formål enn opprinnelig, må dette ha et eget behandlingsgrunnlag.

Personvernforordningen artikkel 6 viser til seks ulike behandlingsgrunnlag

- Den registrerte har samtykket til behandlingen
- Behandling er nødvendig for å oppfylle en avtale med den registrerte
- Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse (med hjemmel i lov)
- Behandling er nødvendig for å verne den registrertes eller en annen persons vitale interesser

UTGÅTT VERSJON – erstattet av versjon 7.1

- Behandling er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som dataansvarlige er pålagt.
- Behandling er nødvendig for å ivareta en berettiget interesse som veier tyngre enn hensynet til den enkeltes personvern.

I vurderingen av behandlingsgrunnlag er følgende spørsmål relevante:

- hva er formålet med behandlingen?
- er behandlingen regulert i lov eller forskrift?
- hvilken behandling skal utføres?
- er behandlingen nødvendig for å yte forsvarlige helse- og omsorgstjenester?

Plikten til å føre journal gir virksomheten en rettslig forpliktelse til å behandle helse- og personopplysninger. Størstedelen av behandlinger av personopplysninger i helse- og omsorgssektoren er dermed lovpålagt. I tillegg til krav om dokumentasjon har lovverket også en rekke andre regler om behandling, f.eks. om utlevering av opplysninger

Andre behandlinger av personopplysninger i virksomheten kan ha andre behandlingsgrunnlag. Eksempler på dette er at i arbeidet med å følge opp ansatte kan "avtale med den registrerte" være riktig behandlingsgrunnlag, og dersom virksomheten utfører oppdrag som ikke er helsehjelp, kan både samtykke og avtale være riktige behandlingsgrunnlag.

Dersom flere behandlingsgrunnlag kan passe, skal virksomheten bestemme seg for ett grunnlag per formål.

Det er dataansvarlige som skal vurdere behandlingsgrunnlaget.

Behandlingsgrunnlaget skal dokumenteres. Dette kan gjøres i protokollen.

Se kap.3.3. Oversikt over teknologi og behandling av helse- og personopplysninger og Normens faktaark for protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)

UTSÅTT VERSJON – erstattet av versjon 7.1

4.2 Plikter og krav ved behandling av helse- og personopplysninger

Den registrerte har en rekke rettigheter ved behandling av helse- og personopplysninger. Virksomheten skal legge til rette for tekniske, organisatoriske, fysiske og personellmessige tiltak, slik at den registrerte kan få innfridd sine rettigheter.

Dette kapittelet omhandler plikter og krav både etter personvernlovgivningen og helselovgivningen. Det er presisert i kapitteloverskrift der teksten kun gjelder for behandlingsrettet helseregister.

4.2.1 Taushetsplikten

Virksomheten skal sørge for at alt personell som gis tilgang til helse- og personopplysninger og annen informasjon underlagt taushetsplikt, er kjent med sin taushetsplikt.

Virksomheten skal legge til rette for at personellet ivaretar taushetsplikten. Dette bør minst sikres gjennom

- tilgangsstyring, logging og etterfølgende kontroll
- sikring av nettverk- og informasjonssystemer
- rutiner, opplæring og informasjon
- utforming av fysiske lokaler

Brudd på taushetsplikten er et avvik, og er forbundet med både forvaltningsmessige og strafferettslige sanksjoner.

4.2.2 Informasjon til den registrerte

Virksomheten har plikt til å gi informasjon til den registrerte på en kortfattet, åpen, forståelig og lett tilgjengelig måte og med et klart og enkelt språk. Her må det også tas hensyn til krav om universell utforming.

Informasjonen skal gis skriftlig eller på en annen måte, herunder elektronisk dersom det er hensiktsmessig. På anmodning fra den registrerte kan informasjonen gis muntlig, forutsatt at den registrerte identifiserer seg.

Ved innsamling av opplysninger skal den dataansvarlige på en forståelig måte gi den registrerte informasjon om sine rettigheter og hvordan personopplysningene behandles.

4.2.3 Innsyn

Begrepet innsyn brukes i flere sammenhenger. Innsynsrett kan gjelde etter helselovgivningen, etter personvernlovgivningen og etter offentleglova. Innsyn etter offentleglova omtales ikke i Normen.

Virksomheten skal sikre at den registrerte kan få innsyn i opplysninger registrert om seg selv. Dette innsynet gjelder også loggen over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.

Virksomheten skal sikre at den registrerte kan få kunnskap om hvilke personopplysninger om seg selv som virksomheten behandler. Dette omfatter også kunnskap om hvem fra andre virksomheter som har tilegnet seg opplysningene.

Virksomheten skal sikre seg at den som gjør sine rettigheter gjeldende, er identifisert.

4.2.3.1 Innsyn i behandlingsrettet helseregister

Pasienten har som utgangspunkt rett til innsyn i alle opplysninger i behandlingsrettet helseregister som omhandler seg selv. Dette gjelder også lydopptak, røntgenbilder, videoopptak etc.

Helsepersonell skal på anmodning gi forklaring på faguttrykk mv. Det skal legges til rette for at samiskspråklige, fremmedspråklige og personer med funksjonshemninger kan utøve innsynsretten. Tiltakene skal dokumenteres.

UTKAST VERSJON – erstattet av versjon 7.1

Utgangspunktet er at alle pasienter over 16 år har selvstendig innsynsrett. Barn mellom 12 og 16 år har selvstendig innsynsrett i en viss grad, idet de har rett til å bli hørt og kan begrense eller nekte innsyn for foreldre elle andre med foreldreansvar for barnet. Barn under 12 år har ikke innsynsrett, men foreldre eller andre med foreldreansvar for barnet har innsynsrett på barnets vegne.

Pasienter kan nektes innsyn i opplysninger i hele eller deler av behandlingsrettet helseregister dersom det er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller innsyn er klart utilrådelig av hensyn til personer som står vedkommende nær. Det skal mye til for at innsyn skal nektes, og det må være en reell fare for konsekvenser av et visst omfang.

Dataansvarlig skal gi innsyn innen 30 dager, uten kostnad for pasienten.

4.2.4 Retting og sletting

Den registrerte har rett til å få uriktige eller ufullstendige opplysninger rettet uten ugrunnet opphold.

Arkivlovgivningen har regler om lagring og oppbevaring. Normen omtaler ikke dette temaet her.

4.2.4.1 Retting og sletting i behandlingsrettet helseregister

Rettingen skal skje ved at oppføringen føres på nytt, eller ved at en datert rettelse tilføyes. Retting skal ikke skje ved at opplysninger slettes.

Dersom opplysningene er feilaktige eller misvisende og føles belastende for den det gjelder, eller de åpenbart ikke er nødvendige for å gi helsehjelp, kan pasienten kreve at opplysningene slettes.

Retting og sletting skal som hovedregel utføres av den som har signert opplysningene. Dersom slik retting eller sletting vanskelig kan gjøres av helsepersonellet som har signert opplysningene, kan retting eller sletting gjøres av helsepersonell utpekt av den dataansvarlige.

Opplysninger som er ført på feil person, skal slettes med mindre allmenne hensyn tilsier at sletting ikke bør foretas.

Se mer i Helsedirektoratets rundskriv til helsepersonelloven

Dataansvarlig skal underrette enhver mottaker som har fått utlevert personopplysninger som i etterkant er rettet eller slettet, om enhver retting eller sletting av personopplysningene. Dataansvarlig skal underrette den registrerte om nevnte mottakere dersom den registrerte anmoder om det.

Dersom krav om retting eller sletting avslås, skal pasienten orienteres om klageadgangen.

Dataansvarlig bør gi elektronisk svar dersom personopplysninger behandles elektronisk.

UTKAST VERSJON - erstattet av versjon 7.1

4.2.5 Tilgjengeliggjøring og utlevering av opplysninger i behandlingsrettet helseregister

4.2.5.1 Retten til å motsette seg tilgjengeliggjøring og utlevering

Pasienten eller brukeren har rett til å motsette seg at opplysninger utleveres eller tilgjengeliggjøres. Dette kan gjelde overføring eller tilgjengeliggjøring av opplysninger både til pasienten selv, til verger og /eller til helsepersonell. Virksomheten har et overordnet ansvar for at pasientens rettighet blir ivaretatt.

Opplysninger kan som hovedregel ikke overføres eller tilgjengeliggjøres dersom det er grunn til å tro at pasienten eller brukeren ville motsette seg det dersom den ble spurt.

Overføring og tilgjengeliggjøring kan likevel skje dersom tungtveiende grunner taler for det.

Pasienten eller brukeren kan ikke motsette seg lovpålagt overføring. Dette gjelder også lovpålagt overføring av opplysninger til sentrale registre.

Virksomheten har derfor et ansvar for å sikre at pasienten gjøres oppmerksom på retten til å motsette seg tilgjengeliggjøring og utlevering. Det kan være hensiktsmessig å inkludere denne informasjonen i annen informasjon pasienten har rett til.

Det skal alltid dokumenteres hvem det er utlevert opplysninger til, og hvilken virksomhet denne tilhører.

4.2.5.2 Tilgjengeliggjøring og utlevering av helseopplysninger mellom virksomheter ved ytelse av helsehjelp

Med mindre pasienten eller brukeren motsetter seg det, skal helsepersonell gi tilgang til nødvendige og relevante helseopplysninger til samarbeidende personell i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte.

Ved utskriving fra helseinstitusjon bør pasienten gis anledning til å opplyse hvem epikrise skal sendes til.

4.2.5.3 Til virksomhetens ledelse og til administrative systemer

Når det er nødvendig for å gi helsehjelp, eller for internkontroll og kvalitetssikring av tjenesten, kan den som yter helsehjelp, gi opplysninger til virksomhetens ledelse. Opplysningene skal være nødvendig og relevant for formålet.

Opplysningene skal så langt det er mulig, gis uten individualiserende kjennetegn.

Helsepersonell skal gi pasientens fødselsnummer og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data til virksomhetsinterne pasientadministrative systemer.

4.2.5.4 Til læring og kvalitetssikring

Når formålet er læring og kvalitetssikring for helsepersonell som tidligere har ytet helsehjelp til pasienten i et konkret behandlingsforløp, men som ikke skal medvirke i den videre helsehjelpsytelsen kan det tilgjengeliggjøres taushetsbelagte helseopplysninger. Dette kan bare skje hvis pasienten ikke motsetter seg det. Dette kan bl.a. omfatte situasjoner der ambulansepersonell har fraktet en pasient til sykehus, personell har behandlet pasient på

UTGÅTT VERSJON - erstattet av versjon 7.1

akuttmottak ved sykehus eller tilsatte ved et sykehjem har medvirket til at pasient blir innlagt på sykehus. Ved å få opplysningene kan behandler vurdere om undersøkelsene, vurderingene og behandlingstiltakene som ble gjort var korrekte (jf. helsepersonelloven § 29c).

Tilgjengeliggjøring skal begrenses til de opplysninger som er nødvendige og relevante for formålet. I pasientens journal skal det dokumenteres hvilke opplysninger som er tilgjengeliggjort og hvem de er tilgjengeliggjort til.

4.2.6 Oppbevaring av helse- og personopplysninger

Hovedregelen etter personvernforordningen er at personopplysninger skal lagres til formålet er oppfylt. Deretter skal opplysningene slettes eller anonymiseres.

4.2.6.1 Lagringstid ved ytelse av helsehjelp

Helseopplysninger skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å være bruk for dem. Det samme gjelder opplysninger om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logger).

Hvis ikke opplysningene deretter skal bevares etter arkivloven, helsearkivloven eller annen lovgivning, skal de slettes.

4.2.6.2 Tilintetgjøring av dokumenter i behandlingsrettet helseregister mv. etter digitalisering

Når dokumenter på papir er digitalisert på forsvarlig måte, kan fysiske originaldokumenter tilintetgjøres. Med forsvarlig digitalisert menes at all tekst er lesbar, og at all tekst, alle sider, bilder og figurer er skannet inn. Elektronisk behandlingsrettet helseregister skal gjenspeile originalen.

4.2.6.3 Behandlingsrettet helseregister ved opphør og overdragelse av virksomhet mv.

Ved overdragelse eller opphør av virksomhet kan behandlingsrettet helseregister overføres til en annen virksomhet.

Pasient/bruker kan motsette seg overføring av sin journal og i stedet kreve at registeret overføres til en annen bestemt virksomhet.

Det som ikke skal overføres til et bestemt helsepersonell eller til en bestemt virksomhet, og virksomheten ikke selv skal ta vare på, kan avleveres til offentlig arkivdepot, deponeres i annen oppbevaringsinstitusjon eller leveres til fylkesmannen. Opplysninger som leveres til fylkesmannen, oppbevares i ti år, og kan deretter tilintetgjøres etter samråd med Riksarkivaren eller avleveres til offentlig arkivdepot.

UTKAST VERSJON 1 – erstattet av versjon 7.1

4.3 Innebygd personvern

Innebygd personvern er et sentralt krav i personvernforordningen. Virksomheten, både dataansvarlig og deres leverandører, skal stille krav til og ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Virksomheten skal sørge for at informasjonssystemene oppfyller personvernprinsippene, se kap. 2.2, og at de ivaretar de registrertes rettigheter.

Dataansvarlig skal velge leverandører som er i stand til å levere tjenester som oppfyller lovbestemte krav og krav i Normen. Leverandører skal bidra til at dataansvarlig som tar i bruk leverandørens produkter og tjenester, kan oppfylle disse kravene. Om nødvendig skal partene gå i dialog for å finne riktige tiltak for å kunne oppfylle kravene.

UTGÅTT VERSJON – erstattet av versjon 7.0

5 Informasjonssikkerhet

Dette kapitlet beskriver sentrale sikkerhetstiltak som skal sikre beskyttelse av helse- og personopplysninger, og gir en oversikt over nødvendige tiltak for å oppnå et tilstrekkelig sikkerhetsnivå. Sikkerhetstiltakene skal vurderes og iverksettes på grunnlag av risikovurderinger.

De fleste sikkerhetskravene i kapittel 5 gjelder også for behandling av helse- og personopplysninger med andre formål enn ytelse av helse- og omsorgstjenester. Virksomheten skal, med bakgrunn i risikovurdering, vurderer hvilke sikkerhetstiltak som er nødvendige, og om det er behov for å gjennomføre mer omfattende tiltak enn det som er beskrevet i dette kapittelet.

UTGÅTT VERSJON – erstattet av versjon 7.1

5.1 Sikkerhetstiltak for medarbeidere

5.1.1 Vilkår og betingelser

Alle medarbeidere i virksomheten skal jevnlig læres opp i krav om ivaretakelse av taushetsplikten, informasjonssikkerheten og personvernet. Dette bør inkluderes i arbeidsavtalen eller avtales skriftlig på annen måte.

Virksomheten bør innhente taushetserklæring for den enkelte medarbeider.

Virksomheten bør utarbeide en instruks for informasjonssikkerhet og personvern som omfatter de vesentlige kravene.

Virksomheten skal ha retningslinjer for privat bruk av informasjonssystemer og utstyr.

5.1.2 Opplæring og kompetanse

Virksomheten skal sørge for at medarbeidere som gis tilgang til virksomhetens informasjon, infrastruktur og/eller systemer har tilstrekkelig kompetanse, og er gjort kjent med relevante sikkerhetstiltak.

Kompetansebygging skal være kontinuerlig og tilpasset ulike roller og brukergrupper. Det bør følges opp at opplæringstiltakene gir ønsket effekt. Gjennomført opplæring og vurdering av effekt bør dokumenteres. Nye opplæringstiltak skal vurderes ved teknologiske endringer eller endring i rutiner.

Virksomheten bør ha en oppdatert oversikt over medarbeideres kompetanse og behov for opplæring.

5.1.3 Opphør av arbeidsforhold

Når et arbeidsforhold opphører, skal alle medier (herunder digitalt, papir, osv.) som kan inneholde helse- og personopplysninger, leveres tilbake. Adgangskort skal leveres tilbake og deaktiveres. All tilgang til virksomhetens nettverk- og informasjonssystemer skal sperres for å sikre at den tidligere ansatte, leverandører og oppdragstakere ikke lenger har tilgang. Virksomheten skal ha rutiner for å rydde opp i informasjon den ansatte kan ha lagret på egen brukerkonto.

Virksomheten bør gjennomføre tiltak for å gjøre medarbeideren oppmerksom på at taushetsplikten gjelder etter at arbeidsforholdet er opphørt.

5.2 Tilgangsstyring

Tilgangsstyring handler om hvordan virksomheten gjennomfører

- autorisering for tilgang til nettverk- og informasjonssystemer
- autorisering for tilgang til behandlingsrettet helseregister, som innebærer tildeling av tillatelser til å kunne lese, registrere, redigere, rette, slette eller sperre helse- og personopplysninger
- autentisering, som sikrer identifisering av autorisert bruker
- tilgjengeliggjøring av helse- og personopplysninger om bestemte pasienter/brukere for autorisert personell
- tilgjengeliggjøring av helse- og personopplysninger til annet personell enn virksomhetens eget personell
- kontrollerende tiltak

Virksomheten skal ha rutiner for autorisering, endring og avslutning av tilganger. Innenfor rammen av taushetsplikten skal virksomheten sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte.

Virksomheten bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten og personvernet.

Tilgangsstyring skal etableres for alle tilganger til nettverk- og informasjonssystemer. Det gjelder også for administrator- og systembrukere.
Bare autorisert personell med tjenstlige behov skal få tilgang til helse- og personopplysninger.

Tilgang til behandlingsrettede helseregistre skal gis etter en konkret beslutning basert på om det er eller skal etableres tiltak for medisinsk behandling av pasienten. Tilgang skal styres slik at taushetspliktreglene ivaretas, og at tilgang til helse- og personopplysninger ikke gis til andre enn dem som har tjenstlig behov.

Virksomheten skal også iverksette nødvendige sikkerhetstiltak for ansatte, leverandører og innleid personell som kan få tilgang til virksomhetens nettverk- og informasjonssystemer. Tiltak for adgangskontroll, brukerautentisering og tilgangskontroll skal sikre egnet tilgangsstyring til nettverk- og informasjonssystemer.

UTGÅTT VERSJON – erstattet av versjon 7.1

5.2.1 Autorisering

Virksomheten er ansvarlig for at autorisasjoner tildeles, administreres og kontrolleres. Ved tildeling av autorisasjon skal lovbestemt taushetsplikt vurderes og ivaretas.

Dataansvarlig kan delegere myndighet for å tildele autorisasjon til den enkelte enhets leder. I dette ligger at leder, innen eget ansvarsområde, vurderer og godkjenner autorisasjonen. Tildelt autorisasjon skal sikre at medarbeideren kan få tilgang til nødvendige og relevante helse- og personopplysninger i samsvar med personellets ansvar og oppgaver, så langt lovbestemt taushetsplikt ikke er til hinder for det. Autorisasjonen skal vurderes på nytt når det oppstår endringer i ansvarsområder, ansettelsesforhold eller langvarig fravær.

Dersom tilgangsstyringen er basert på roller, skal autorisering skje for hver rolle uavhengig av medarbeiderens øvrige roller. Autorisasjonen for tilgang til behandlingsrettede helseregister skal tidsbegrenses og angi hvilke virksomheter autorisasjonen omfatter.

For autorisering av teknisk personell med særskilt behov for tilgang til større mengder helse- og personopplysninger skal det etableres tiltak slik at mulig misbruk skal kunne avdekkes.

For å hindre uautorisert tilgang skal følgende tiltak etableres:

- dersom det er åpnet for selvautorisering, skal tilgang grunngis og registreres.
- tekniske tiltak skal sikre at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i informasjonssystemene hvem som har endret, og hva som er endret.
- all tildeling av autorisasjon skal registreres i et autorisasjonsregister (jf. 5.2.1.1).
- tekniske tiltak skal også sikre at personer i eller utenfor virksomheten ikke skal kunne endre konfigurasjon og programvare uten at det logges (jf. 5.4.4).
- bruker med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver. Driftspersonell skal ha personlige brukerkontoer for oppgaver som ikke krever administratortilganger.
- risikovurdering skal begrunne behovet for ulike administratorbrukere.

5.2.1.1 Autorisasjonsregister

Virksomheten skal sørge for at det opprettes et autorisasjonsregister. Registeret skal som minimum inneholde:

- informasjon om hvem som er tildelt autorisasjon
- informasjon om til hvilken rolle autorisasjonen er tildelt (om rollen benyttes i virksomheten)
- formålet med autorisasjonen
- tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt
- Informasjon om hvilken virksomhet den autoriserte er knyttet til
- Helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk)

UTGÅTT VERSJON - Erstattet av versjon 7.1

5.2.1.2 Tilgang til helse- og personopplysninger mellom virksomheter

Virksomheten skal ha kontroll og oversikt over all behandling av helse- og personopplysninger som den er ansvarlig for, inkludert tilgjengeliggjøring av opplysninger til andre virksomheter:

- det skal gjennomføres risikovurdering ved oppstart eller endring av tilgjengeliggjøring av opplysninger for andre virksomheter.
- dataansvarlig og virksomhetene som gis tilgang til opplysninger hos dataansvarlig, skal avklare gjennom avtale eller på annen måte hvordan
    - brukerautentisering skal foregå på sikker måte (f.eks. to- eller flerfaktorautentisering)
    - autorisering til helseopplysninger hos dataansvarlig skal foregå
    - logging og oppfølging av logger skal foregå

UTGÅR VED NESTE – erstattes av versjon 7.1

5.2.2 Autentisering

Autentisering skal som minimum ivareta følgende:

- Tilgang til nettverk- og informasjonssystemer, både for vanlige brukere og administratorer, skal sikres gjennom brukerautentisering som gir tilstrekkelig beskyttelse. Den som gis tilgang, skal bekrefte sin identitet på en sikker måte. Hva som anses som en sikker autentiseringsmetode, skal vurderes og besluttes på bakgrunn av en risikovurdering.
- Ulike ansettelsesforhold skal identifiseres.
- Flere personer skal ikke benytte samme autentiseringskriterier.
- Tildeling av brukerautentiseringskriterier (for eksempel passord) skal gjennomføres på en betryggende måte.
- Tilgang fra hjemmekontor eller mobilt utstyr (og mobilnettverk) skal sikres ved sikker autentiseringsløsning (f.eks. to- eller flerfaktorautentisering).
- Dette gjelder også for lokasjoner som kommuniserer ved hjelp av linjer virksomheten ikke har fysisk kontroll over.
- Alle standardpassord (fabrikkinnstillinger) på systemer og utstyr skal endres før behandling av helse- og personopplysninger starter.
- Ved bruk av trådløse nettverk for behandling av helse- og personopplysninger skal den autoriserte brukeren autentiseres med sikker autentiseringsløsning (f.eks. to- eller flerfaktorautentisering).

Benyttes roller, skal ulike roller identifiseres, og ved behov gis ny autentisering.

5.2.3 Kontroll av tilganger

Virksomhetens ledelse skal påse at det jevnlig gjennomføres styring og kontroll av hvem som har elektronisk tilgang til og bruker virksomhetens nettverk- og informasjonssystemer. Gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner, skal foretas av den enkelte leder:

- ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde.
- minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon).
- ved sikkerhetsbrudd for det som blir berørt av bruddet.

Dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang, skal virksomhetens ledelse varsles. For øvrig skal hendelsen behandles iht. etablerte rutiner for avviksbehandling, særlig med henblikk på å få avklart om eksisterende tilgangskontroll er god nok. Misbruk av selvautorisering skal følges opp som avvik. Dersom kontrollen viser at det har skjedd en urettmessig tilgang, skal dette behandles som et avvik.

Ved bruk av tilgang til helseopplysninger mellom virksomheter skal avtalepartene samarbeide om kontroll av tilganger. Den dataansvarlige som har adgang til å autorisere helsepersonell for tilgang, skal løpende kontrollere:

- hvem i egen virksomhet som elektronisk har hentet frem helseopplysninger fra annen virksomhet.
- hvorfor dette er gjort.
- tidsperioden helseopplysningene er hentet frem.

Dersom kontrollen viser at noen urettmessig har hentet frem helseopplysninger, skal virksomheten opplysningene er hentet fra, og pasienten/brukeren opplysningene gjelder, varsles. Avviket skal behandles iht. etablerte rutiner for avviksbehandling.

UTGÅTT VERSJON – erstattet av versjon 7.1

5.3 Fysisk sikkerhet og håndtering av utstyr

5.3.1 Nøkler/adgangskort

Det skal etableres rutine for administrasjon av nøkler/adgangskort i adgangskontrollsystemet.

5.3.2 IKT-utstyr

Sikkerhetstiltak skal hindre at uautoriserte får tilgang til helse- og personopplysninger. Dette kan løses ved adgangskontroll av lokaler med utstyr og ved at utstyret sikres mot misbruk eller uautorisert innsyn.

5.3.3 Infrastruktur

Sikkerhetstiltak skal hindre at annet enn autorisert personell får adgang til virksomhetens infrastruktur, nettverk- og informasjonssystemer.
Det skal etableres prosedyrer, retningslinjer og iverksette tiltak for fysisk sikkerhet for å opprettholde egnet sikkerhet til nettverk- og informasjonssystemer.

Fysiske sikkerhetstiltak skal minst omfatte:

- tiltak for å forhindre at uvedkommende får tilgang til lokasjoner, fysisk og teknisk infrastruktur som nettverk- og informasjonssystemer benytter eller er avhengig av
- tiltak for å identifisere og beskytte bygninger, rom og tilstøtende lokaler og områder som har betydning for sikkerhetsnivået til nettverk- og informasjonssystemer
- tiltak for å ivareta eksterne avhengigheter, herunder datakommunikasjon og strømtilførsel

Alle lagringsmedier skal slettes forsvarlig når de tas ut av bruk. Dette gjelder også for helse- og opplysninger som ikke lenger er nødvendige for formålet de ble samlet inn for. Plikt til lagring og arkivering av helse- og personopplysninger skal uansett overholdes i henhold til helselovgivningen og arkivlovens bestemmelser.

5.3.4 Mobilt utstyr, hjemmekontor og fjernarbeid

Det skal gjennomføres risikovurdering før mobilt utstyr, hjemmekontor og annet fjernarbeid. tas i bruk, og ved endringer som kan påvirke informasjonssikkerheten. Det skal etableres prosedyrer og retningslinjer for fjernarbeid eks. hjemmekontor og mobilt fjernarbeid fra ulike lokaler og geografiske steder. Det skal videre iverksettes sikkerhetstiltak når ansatte, leverandører og innleid personell utfører fjernarbeid, for å beskytte informasjon, nettverk- og informasjonssystemer, produkter og tjenester som behandles eller lagres utenfor virksomhetens lokaler.

Helse- og personopplysninger skal bare lagres lokalt på utstyret når dette er nødvendig ut fra tjenstlig behov, og skal alltid lagres kryptert.

5.3.5 Kryptering

Tekniske tiltak skal defineres og etableres slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres. Kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr virksomheten har kontroll med. Kontrollen kan ivaretas gjennom avtale.

All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer, skal sikres ved kryptering.

Se for eksempel dokumentet "NSM Cryptographic recommendations Version 1.0" (www.nsm.no)

Kryptering av lagrede helse- og personopplysninger kan vurderes som et sikkerhetstiltak.

I registre som er etablert med hjemmel i helseregisterloven §§ 10 og §11, skal direkte personidentifiserende kjennetegn lagres kryptert.

UTGÅTT VERSJON – erstattet av versjon 7.0

5.3.6 Medisinsk utstyr og velferdsteknologi

Medisinsk utstyr og velferdsteknologi som behandler helse- og personopplysninger, skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring, endringskontroll og rutiner for bruk, på linje med andre informasjonssystemer.

5.4 Sikker IT-drift

5.4.1 Konfigurasjonskontroll

Det er en forutsetning at virksomheten har oversikt over dataflyt, datakommunikasjon og integrasjoner og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger. Dette gjelder også utstyr ved avdelingskontor og hjemmekontor og mobilt utstyr.

Følgende skal ivaretas:

- konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjonene som er formålsbestemt
- virksomheten skal sørge for at all dataflyt, datakommunikasjon og integrasjoner kartlegges og dokumenteres.
- kun godkjent utstyr og programvare skal benyttes til behandling av helse- og personopplysninger. Virksomheten skal fastsette hvem som har godkjenningsmyndighet.
- maskin- og programvare skal oppdateres slik at den nyeste og mest tidsaktuelle sikkerhetsfunksjonaliteten følger med og nødvendige sikringstiltak benyttes. Oppdateringer bør verifiseres og testes før oppdateringen gjennomføres. Verifisering og testing skal dokumenteres som ledd i virksomhetens endringsstyring (se kap. 5.4.2).
- planlagte endringer skal følge virksomhetens rutine for konfigurasjonsendringer.
- det skal benyttes separate miljøer for utvikling, test og produksjon slik at helse- og personopplysninger som benyttes ved ytelse av helsehjelp, ikke blir påvirket ved feil i utvikling og test.
- konfigurasjonen av utstyr og programvare skal jevnlig sjekkes slik at den kun utfører formålsbestemte funksjoner.
- konfigurasjonen skal beskyttes mot skadelig programvare
- konfigurasjonen skal beskyttes mot utilsiktede handlinger.

Konfigurasjonsendringer, dvs. endringer i utstyr eller programvare, skal ikke settes i drift før følgende tiltak er gjennomført:

- risikovurdering som viser at risiko er akseptabel
- test som sikrer at forventede funksjoner er ivaretatt
- implementering som sikrer mot uforutsette hendelser
- ny konfigurasjon er dokumentert
- konfigurasjonsendringer er godkjent av virksomhetens leder eller den ledelsen bemyndiger

UTGÅTT VERSJON – erstattet av versjon 7.1

Konfigurasjonskontroll skal reguleres gjennom avtale ved

- bruk av databehandler.
- bruk av fjernaksess for vedlikehold og oppdateringer. Fjernaksess skal kun gjøres over kanaler virksomheten har kontroll med.

5.4.2 Endringsstyring

Alle endringer med betydning for informasjonssikkerheten i organisasjon, nettverk- og informasjonssystemer og infrastruktur skal forankres på relevant ledernivå.

Virksomheten skal utarbeide rutiner og iverksette sikkerhetstiltak for endringsledelse som skal omfatte følgende temaer:

- identifisering av vesentlige endringer
- planlegging og testing av endringer
- vurdering av potensielle konsekvenser, for eksempel ved å gjennomføre en risikovurdering og eventuelt en personvernkonsekvensvurdering
- godkjennelsesrutiner for endringer
- kommunikasjon av plan til aktuelle personer/roller
- reserverutiner om endringen må avbrytes, feiler eller uønskede hendelser oppstår
- endringslogg med relevante opplysninger
- opplæring av berørte brukere/roller
- sikre at nettverk- og informasjonssystemer videreutvikles kontinuerlig, herunder at oppdateringer kvalitetssikres, installeres og testes fortløpende

5.4.3 Sikkerhetskopiering

Virksomhetens ledelse skal sørge for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal drift.

Sikkerhetskopier skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret.

Det skal jevnlig testes at sikkerhetskopiene er korrekte og kan tilbakeføres.

Minimum en sikkerhetskopi skal beskyttes mot skadelig programvare og uønskede hendelser.

5.4.4 Logging

For å oppdage brudd eller forsøk på brudd skal det som minimum logges:

- autorisert bruk av informasjonssystemene
- all system- og administratorbruk til nettverk- og informasjonssystemer og infrastrukturen
- endring av konfigurasjon og programvare
- sikkerhetsrelevante hendelser i sikkerhetsbarrierer
- forsøk på uautorisert bruk av nettverk- og informasjonssystemer og infrastrukturen
- bruk av selvautorisering

UTGÅTT VERSJON – erstattet av versjon 7.1

Følgende skal som minimum registreres i loggene ved autorisert bruk av behandlingsrettet helseregister:

- identiteten til den som har lest, rettet, registrert, endret eller slettet helse- og personopplysninger
- organisatorisk tilhørighet
- grunnlaget for tilgjengeliggjøringen
- tidsperioden for tilgjengeliggjøringen

Ved behandling av helse- og personopplysninger for andre formål enn ytelse av helse- og omsorgstjenester skal kravene til logging besluttes på grunnlag av en risikovurdering.

Følgende bør vurderes logget i tillegg til minimumskravene:

- rollen den autoriserte brukeren har ved tilgangen
- virksomhetstilhørighet
- type opplysninger det er gitt tilgang til
- hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer

Loggene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.

Det skal etableres rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser. Dersom brudd avdekkes, skal dette håndteres som et avvik.

Det skal etableres rutiner for ved behov å kunne sammenholde loggene med autorisasjonsregister.

Loggene og autorisasjonsregister skal sikres mot endring og sletting.

Logger skal ha korrekt tidsstempel.

Logger som genereres ved ytelse av helsehjelp, skal lagres til det ikke antas å være bruk for dem.

Logger av sikkerhetsmessig betydning bør oppbevares så lenge som nødvendig for å oppnå formålet.

UTGÅTT VERSJON – erstattet av versjon 7.1

5.4.5 Styring og håndtering av tekniske sårbarheter

Styring og håndtering av tekniske sårbarheter skal følge rutinene for endringsstyring. Virksomheten skal ha rutine for å skaffe seg informasjon om tekniske sårbarheter i nettverk- og informasjonssystemer, utstyr og programvare.

Utgangspunktet for styring og håndtering er oversikt over:

- IKT-utstyr
- programvare: programvaren, leverandør, versjonsnumre, hvilken versjon som er installert hvor, og hvem som har ansvaret for programvaren

Det skal etableres rutiner og operative tiltak som ivaretar:

- ansvaret for overvåkning, risikovurdering, korrigering og koordinering
- ansvaret for sikkerhetsovervåkning av nettverk- og informasjonssystemer for å avdekke hendelser
- hvordan virksomheten skal reagere og varsle om sårbarheter
- prioritering og etablering av tidslinje for korrigering
- at alle korrigeringer bør testes før de implementeres

5.4.6 Sikkerhetsrevisjon

Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner. Formålet med sikkerhetsrevisjon er å gjennomføre kontrollaktiviteter og kvalitetssikring av etablerte tiltak og fastsatte rutiner. Det skal foreligge en godkjent plan for sikkerhetsrevisjoner.

For å gjennomføre tilstrekkelige sikkerhetsrevisjoner i virksomheter bør vurderingene som minimum omfatte:

- plassering av ansvar og organisering av sikkerhetsarbeidet
- overholdelse av rutiner for bruk av nettverk- og informasjonssystemer og behandling av helse- og personopplysninger
- vurdering av hvor effektive sikkerhetstiltakene er
- tilgang til helse- og personopplysninger og tiltak mot uautorisert innsyn
- opplæring og kompetanse i personvern og informasjonssikkerhet
- gjennomgang av dokumentasjon for ivaretakelse av informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og leverandører

Resultatene, konklusjonene og avvik fra sikkerhetsrevisjonene skal dokumenteres og håndteres av virksomheten.

5.5 Kommunikasjonssikkerhet

5.5.1 Styring av informasjonssikkerhet i nettverk- og informasjonssystemer

Informasjonssikkerhet i nettverk- og informasjonssystemer er et sentralt tiltak for å sikre behandling av helse- og personopplysninger.

Virksomheten skal tydelig definere hvilke sikkerhetskrav som gjelder for nettverk- og informasjonssystemer. Tiltakene som etableres skal være basert på risikovurdering og inkludere teknologiske sikkerhetstiltak tilpasset omfang, kompleksitet, driftsmiljø, brukermiljø, funksjon og risiko ved virksomhetens nettverk- og informasjonssystemer.

Sikkerhetstiltakene for nettverk- og informasjonssystemer skal minst inkludere:

- bruk av to- eller flerfaktorautentisering for å sikre tilgang for både brukere og administratorer

UTGÅTT VERSJON – erstattet av versjon 7.1

- tilgangskontroll basert på tjenstlig behov for å beskytte innholdet i nettverk- og informasjonssystemer
- kontroll over hvem som har tilgang til virksomhetens nettverk- og informasjonssystemer
- segmentering av tjenester basert på prinsippet om minste nødvendige rettigheter
- tiltak som sikrer at systemene kan håndtere avbrudd og gjenopprettes raskt uten betydelig reduksjon i tjenestekvaliteten
- kapasitetsstyring for å tåle overbelastning og utstyrssvikt
- kontinuerlig videreutvikling og kvalitetssikring av oppdateringer, inkludert installasjon og testing
- overvåkning av nettverk- og informasjonssystemer for å oppdage sikkerhetshendelser

5.5.2 Tilkobling til eksterne nett

Ved tilkobling til eksterne nett skal det etableres tekniske tiltak som ivaretar at kun eksplisitt angitt tillatt trafikk kan passere utenfra og inn eller motsatt, og at annen trafikk stoppes.

Tiltaket skal minst omfatte to uavhengige tekniske tiltak for å redusere risikoen for at personer utenfor virksomheten kan få uautorisert tilgang til eller kunne endre eller slette helse- og personopplysninger.

5.5.3 Elektronisk samhandling

Referansekatalogen for e-helse som er hjemlet i forskrift om standarder og nasjonale e-helseløsninger, gir oversikt over obligatoriske og anbefalte standarder for helse- og omsorgstjenesten. Forskriften skal bidra til at virksomheter i helse- og omsorgstjenesten som yter helsehjelp, bruker IKT-standarder for å fremme sikker elektronisk samhandling.

Nedenfor beskrives krav til samhandling som ellers ikke fremgår av Normens øvrige kapitler.

5.5.3.1 Krav til elektronisk samhandling

Det skal etableres klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler, og ansvarsforholdene skal fremgå av avtalene mellom virksomhetene og meldingsformidler. Alle avtaler skal være skriftlige.

Avsender/tilbydende virksomhet er ansvarlig for:

- egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging
- at tjenesten ikke skal kunne formidle program som inneholder skadelig programvare e.l.
- sikker overføringskryptering ende-til-ende

Mottaker/anvendende virksomhet er ansvarlig for:

- å sikre at tjenesten ikke skal kunne formidle skadelig kode el.
- egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging
- å ivareta overføringskryptering ende-til-ende

UTGÅTT VERSJON – erstattet av versjon 7.1

5.5.3.2 Krav til meldingskommunikasjon basert på ebXML-rammeverket

Avsender er ansvarlig for:

- rett adressering av elektroniske samhandlingsmeldinger iht. adresseregisteret (NHN.no)
- at meldingen ved behov skal være signert på en slik måte at virksomheten ikke kan benekte å ha sendt den
- avviksrapportering i forbindelse med feilsending
- at melding skal avleveres i avtalt format

Mottaker er ansvarlig for:

- å registrere mottaket ved behov slik at mottaker ikke kan benekte å ha mottatt meldingen
- avviksrapportering i forbindelse med feil, dvs. mottak av melding som ikke er adressert til virksomheten
- at melding skal mottas i avtalt format

Meldingsformidler er ansvarlig for:

- at melding kun skal avleveres til adressaten
- at melding ikke skal endres eller destrueres under transport fra avsender til mottaker
- at melding ikke skal kunne leses av andre enn avsender og mottaker
- at melding skal avleveres innen avtalte tidsfrister fra avsendelse
- avviksrapportering i forbindelse med alle ovenstående punkter

5.5.3.3 Datadeling i sanntid

Samhandling gjennom datadeling tilrettelegger for at innbyggere og aktører i helsesektoren kan ha en mer dynamisk informasjonsdeling. Slik informasjonsdeling kan være at en aktør etterspør eller oppdaterer informasjon hos en annen aktør over et datadelingsgrensesnitt.

Følgende sikkerhetsprinsipper gjelder for datadeling:

- Det må være en sikker brukerautentisering som virksomhetene som tilbyr datadelingsgrensesnitt har tillit til.
- Virksomheten som ber om tilgang, skal kontrollere at brukeren har nødvendige autorisasjoner for det aktuelle datadelingsgrensesnittet.
- Det skal skilles mellom lese- og skriverettigheter til forskjellige informasjonselementer basert på den enkelte brukerautorisasjon.
- Unødvendig mellomlagring skal unngås.
- Det skal være mulig å kunne verifisere legitimiteten til datadelingsgrensesnittet og virksomheten som tilbyr den.
- Felleskomponenter for autentisering av konsument skal benyttes der det er tilgjengelig og hensiktsmessig.
- Felleskomponenter for autentisering av konsument skal benyttes der det er tilgjengelig og hensiktsmessig.

UTKAST VERSJON 7.1 – erstattes av versjon 7.1

5.5.4 E-post og SMS

Virksomheten skal etablere tiltak for å forhindre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten tilgjengeliggjøres ved hjelp av ukryptert e-post og SMS eller andre usikre kanaler.

Om virksomheten bruker ukrypterte kanaler, skal virksomheten

- forsikre seg om ved tekniske og organisatoriske tiltak at e-post ikke inneholder identifiserbare helseopplysninger
- etablere logging for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik.
- vurdere om den samlede informasjonen i SMS og e-post kan medføre brudd på taushetsplikten

5.5.5 Tilkobling til Internett

Teknisk utstyr, f.eks. medisinsk utsyr, eller applikasjoner som kobles til Internett, skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring og rutiner for bruk.

Virksomheten skal etablere

- tekniske tiltak som bidrar til å hindre utilsiktet utlevering og uautorisert tilgang til helse- og personopplysninger
- logging for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik.

5.6 Digital kommunikasjon til den registrerte

Med digital kommunikasjon menes i dette kapittelet meldinger som sendes fra virksomheten til den registrerte i forbindelse med helsehjelp.

Virksomheten skal

- vurdere og beslutte behandlingsgrunnlag
- vurdere egnet løsning og kommunikasjonskanal til formålet
- sørge for at helse- og personopplysninger stilles til rådighet på en slik måte at pasient/bruker ikke er avhengig av å lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen
- sørge for at det er etablert rutiner som ivaretar at meldingen til pasienten ikke er inngripende og krenker personvernet, men samtidig har tilstrekkelig informasjon til pasienten
- gjennomføre tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker. For å sikre korrekt kontaktinformasjon til mottager bør virksomheter som har tilgang til kontakt- og reservasjonsregisteret (digdir.no), benytte dette.

UTGÅTT VERSJON – erstattet av versjon 7.1

5.7 Leverandørforhold

Dataansvarlig har det overordnede ansvaret for å oppfylle lovbestemte krav og krav i Normen. Leverandøren skal tilrettelegge for at dataansvarlig, ved bruk av leverandørens infrastruktur, produkter og tjenester, oppfyller disse kravene. Dette innebærer at leverandøren må implementere nødvendige prosedyrer og sikkerhetstiltak, for å sikre etterlevelse av krav i Normen.

Dataansvarlig skal ha retningslinjer for forvaltning av leverandøravtaler og til enhver tid ha en oppdatert oversikt over disse avtalene. Leverandøravtalene skal regelmessig evalueres og revideres for å sikre at kravene til informasjonssikkerhet ivaretas.

5.7.1 Krav til leverandørers taushetsplikt

En leverandør kan håndtere helse- og personopplysninger enten ved behandling på vegne av den dataansvarlige, ved tjenesteutsetting eller ved at det ytes f.eks. vedlikeholdstjenester som innebærer at leverandørens ansatte kan eksponeres for taushetsbelagt informasjon. Leverandøren skal forsikre at de har rutiner som pålegger alle medarbeidere taushetsplikt om helse- og personopplysninger og annen taushetsbelagt informasjon.

Leverandøren kan selv administrere og oppbevare taushetserklæringer for eget personell, men den dataansvarlige skal sikres innsyn ved behov.

5.7.2 Generelt om avtaler og leverandøroppfølging

Den dataansvarlige har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden. I leveranser av f.eks. tjenester, maskinvare eller nettverk- og informasjonssystemer skal det avtales skriftlig med leverandører hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar. Hvilke av Normens krav som gjennom avtale gjelder for leverandører, er avhengig av hva slags type leveranse det er snakk om, for eksempel:

- databehandling, i form av for eksempel skytjenester eller driftstjenester
- vedlikehold, for eksempel ved fysisk service eller fjernaksess
- leveranse av løsninger og systemer

Avtalene skal inkludere forpliktelser om at partene skal oppfylle relevante krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, samt regulering av sanksjoner ved brudd på denne, relevant lovgivning og avtalen for øvrig.

Virksomheten skal gjennom avtaler forsikre seg om at leverandøren har et styringssystem for informasjonssikkerhet og personvern som inkluderer blant annet sikkerhetsrevisjon og avviksbehandling. Virksomheten skal påse at leverandører og andre som utfører arbeid som kan påvirke sikkerheten i nettverk- og informasjonssystemer, utfører arbeidet på en måte som gjør at virksomhetens krav til informasjonssikkerhet overholdes.

Virksomheten skal gjøre sikkerhetstiltakene gjeldende overfor leverandører som kan påvirke nettverk- og informasjonssystemer, i den grad det er nødvendig for å opprettholde et egnet sikkerhetsnivå.

UTGÅTT VERSJON – erstattet av versjon 7.1

5.7.3 Tjenesteutsetting

Ved tjenesteutsetting (utkontraktering) av IKT-funksjoner eller andre funksjoner av betydning for informasjonssikkerhet eller personvern skal avtalen som minimum omfatte følgende punkter knyttet til informasjonssikkerhet og personvern:

- dokumentert risikovurdering som viser at den tjenesteutsettende virksomhetens akseptkriterier samt Normens sikkerhetsnivå er etablert. Ved tjenesteutsetting av IKT-tjenester til andre land bør forhold ved vertslandet vurderes fordi de kan påvirke risikovurderingen.
- hvilke oppgaver av sikkerhetsmessig betydning som er omfattet, og ansvarsforholdene for disse
- beskrivelse av leverandørens løsning og grensesnitt mot virksomheten i form av konfigurasjonskart

Avtalen skal sikre at virksomheten også gis rett til å revidere leverandørens aktiviteter som er knyttet til avtalen. Revisjonene kan gjennomføres av en avtalt tredjepart.

Virksomheten skal sørge for å ha en god plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av tjenesteleveransen. Ved terminering av kontrakten skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid.

5.7.4 Databehandler

Databehandler skal bare behandle helse- og personopplysninger, samt annen taushetsbelagt informasjon etter instruks fra dataansvarlig. Hvordan databehandler kan behandle data på vegne av dataansvarlig, skal reguleres i avtale.

Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre nødvendige sikkerhetstiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven. Tilstrekkelige garantier betyr at databehandleren oppfyller kravene i lov og forskrift samt de kravene fra Normen som er relevante for det aktuelle avtaleforholdet.

5.7.4.1 Databehandlers underleverandører

Databehandleren skal ikke engasjere underleverandører uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den dataansvarlige. Dersom det er innhentet en generell, skriftlig tillatelse, skal databehandleren underrette den dataansvarlige om eventuelle planer for endring av underleverandører. Den dataansvarlige skal kunne motsette seg slike endringer.

Databehandleren er ansvarlig for at sine underleverandører oppfyller sine forpliktelser.

Underleverandør og andre som utfører arbeid for eller på vegne av virksomheten, og som kan få tilgang til virksomhetens nettverk- og informasjonssystemer har et selvstendig ansvar for å overholde nødvendige krav til informasjonssikkerhet og for ivaretakelse av de registrertes personvern. Det skal fremkomme av avtalen med leverandøren at underleverandører har samme plikter som databehandler etter databehandleravtalen. Dette

UTKAST VERSJON – erstatter 7.1 versjon 7.1

skal reguleres i avtale mellom databehandler og underleverandør. Avtalen skal kunne gjøres tilgjengelig for dataansvarlig.

5.7.4.2 Innhold i databehandleravtale

En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av et annet avtaleverk. Databehandleravtalen skal være skriftlig.

Innholdet i databehandleravtale er regulert i personvernforordning artikkel 28 Databehandler (www.lovdata.no). Se mer om bruk av databehandler i Normens faktaark for bruk av databehandler (faktaark 10)

Databehandlerens selvstendige ansvar for informasjonssikkerhet og for ivaretakelse av de registrertes personvern skal presiseres.

Det skal fremgå av avtalen at databehandler forplikter seg til å oppfylle lovbestemte krav, samt de kravene fra Normen som er relevante for det aktuelle avtaleforholdet.

5.7.4.3 Databehandlers oversikt over behandlinger

Databehandler skal føre en oversikt (protokoll) over alle kategorier av behandlingsaktiviteter som utføres på vegne av en dataansvarlig.

Se mer i Normens faktaark 13

Dataansvarlig skal sørge for at databehandler mottar nødvendig informasjon for at databehandler kan føre en slik oversikt.

5.7.4.4 Databehandlers andre plikter

Dersom databehandler behandler helse- og personopplysninger fra flere virksomheter, skal databehandler ved hjelp av tekniske tiltak, som ikke kan overstyres av dataansvarliges brukere, ivareta at det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering.

Databehandler skal uten ugrunnet opphold melde til dataansvarlig at avvik har oppstått. Databehandler skal bidra til at dataansvarlig kan overholde fristen for eventuell melding til Datatilsynet innen 72 timer.

5.7.5 Vedlikehold, fjernaksess eller fysisk service

Virksomheten skal, i tillegg til øvrige krav i Normen, gjennom avtale sørge for at

- leverandørens utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett, eller medbrakt utstyr som knyttes til virksomhetens utstyr, ikke har skadelig programvare som inneholder virus e.l., og at utstyret er sikret mot adgang fra uvedkommende
- all tilgang og fysisk adgang skal være autorisert av virksomheten. Tilgangen skal logges og adgangen skal kontrolleres.
- tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes når leverandøren utfører arbeid på virksomhetens utstyr/programvare

UTGÅTT VERSJON – erstattet av versjon 7.1

5.7.6 Systemleverandører

Virksomheter i helse- og omsorgssektoren som tar i bruk informasjonssystemer som behandler helse- og personopplysninger, skal stille krav om innebygd personvern i løsningene.

For at virksomhetene skal kunne ivareta sitt ansvar som dataansvarlig, skal informasjonssystemene ha funksjonalitet som oppfyller lovbestemte krav og relevante krav i Normen[3].

Se også Normens krav mappet mot krav i anskaffelser, krav i ISO 27001 og kontroller i ISO27002 (vedlegg til Normen)

Kommentert [GJ3]: Lenke til oppdatert mapping

5.7.7 Leverandøroppfølging

Informasjonssikkerhet og personvern knyttet til anskaffelser og leverandøroppfølging skal inngå i virksomhetens styringssystem for informasjonssikkerhet og personvern. Alle faser i leverandørstyring, fra anskaffelse til avtalen er avsluttet, skal omfattes.

Virksomheten skal sikre

- klarhet i ansvar og roller
- at kompetanseressurser innen informasjonssikkerhet og personvern deltar i anskaffelser og leverandørstyring
- at virksomhetens ledelse (og styret hvis dette er relevant) som hovedregel involveres i beslutninger som gjelder bruk av private leverandører og tjenesteutsetting av et visst omfang

Kravstilling og nødvendige sikkerhetstiltak ved bruk av leverandører skal bygge på en dekkende risikovurdering. Risikovurderingen skal alltid omfatte scenarioer som omfatter leverandørens autoriserte og ev. uautoriserte tilgang til helse- og personopplysninger og annen taushetsbelagt informasjon.

Virksomheten skal sikre at relevante sikkerhetskrav inngår i alle anskaffelser. Virksomheten skal sørge for at den har tilstrekkelig bestillerkompetanse tilgjengelig.

5.7.8 Overføring av opplysninger til utlandet

Virksomheter som overfører personopplysninger til utlandet, skal passe på at beskyttelsesnivået i personopplysningsloven ikke undergraves ved overføringen.

Alle landene innenfor EU/EØS-området har innført personvernforordningen og slik sikret at personopplysninger behandles forsvarlig. Europakommisjonen har i tillegg anerkjent at noen tredjeland[4] har et tilstrekkelig nivå for vern av personopplysninger. Derfor kan personopplysninger fritt overføres til disse statene. Dette forutsetter at

UTGÅTT VERSJON - erstattet av versjon 7.1

[3] Se vedlegg «Oversikt over Normens krav»
[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

personopplysningslovens øvrige vilkår er oppfylt. Se kapittel 5.7.5, særlig kravene til risikovurdering, og landrisikovurdering.

Se også Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection (commission.europa.eu).

Dersom det skal benyttes leverandører eller tjenester etablert utenfor EU/EØS, kan det gjelde spesielle krav. Disse kravene skal sikre at opplysningene er underlagt samme beskyttelsesnivå som i EU/EØS-området. Når virksomheten overfører personopplysninger til stater utenfor EU/EØS-området, såkalte «tredjeland», skal den bruke et av overføringsgrunnlagene i forordningen.

Se også Overføring av personopplysninger ut av EØS (www.datatilsynet.no)

Ved overføring av opplysninger til land utenfor EU/EØS skal virksomheten sikre at den har tilstrekkelig kompetanse (f.eks. juridisk kompetanse) tilgjengelig for å gjennomføre dette i tråd med relevante krav.

5.7.9 Skytjenester

Bruk av skytjenester ved behandling av helse- og personopplysninger krever at den dataansvarlige gjennomfører dekkende risikovurderinger, og ellers følger kravene til avtaler og leverandøroppfølging i Normen.

Noen særlig viktige momenter er at

- ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset leveransemodellen som benyttes
- dataansvarlig har oversikt over hvor data behandles geografisk, slik at kravene i kapittel 5.7.8 kan ivaretas
- dataansvarlig skal påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid med lovbestemte krav og Normens krav
- dataansvarlig har sørget for å ha en god plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten

5.8 Håndtering av informasjonssikkerhetsbrudd

5.8.1 Avvikshåndtering

Uønskede hendelser (for eksempel brudd på rutiner, personvernet, informasjonssikkerheten eller nettverk- og informasjonssystemer) skal behandles som avvik. Avvik skal behandles for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.

Virksomheten skal ha rutiner for å oppdage og håndtere avvik. Avviksbehandlingen skal være dokumentert.

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

UTGÅTT VERSJON - erstattet av versjon 7.1

Ved alvorlige eller gjentatte avvik skal det gjennomføres ny risikovurdering.

Avviksmeldinger som inneholder personopplysninger eller informasjon med betydning for informasjonssikkerheten, skal sikres.

I Normen omtales rapportering av avvik på personvern og informasjonssikkerhet til Datatilsynet, Statens helsetilsyn og Nasjonal sikkerhetsmyndighet.

5.8.2 Brudd på personopplysningssikkerhet

Brudd på personopplysningssikkerheten er avvik som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

5.8.2.1 Melding til Datatilsynet

Dersom avviket er et brudd på personopplysningssikkerheten skal avviket rapporteres til Datatilsynet innen 72 timer, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og rettigheter.

For detaljert regler, unntak fra meldeplikten og metode for å melde, se https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

5.8.2.2 Underretting til den registrerte

Dersom det er sannsynlig at avviket har eller vil føre til høy risiko for den registrerte, skal virksomheten underrette vedkommende.

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

Virksomheten bør så langt det er mulig, ta direkte kontakt med den registrerte.

5.8.3 Varsel til 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

UTKAST/HØRINGSVERSJON – erstattet av versjon 7.1

Ved slike hendelser skal virksomheten
- følge opp og informere pasienter og pårørende
- gjennomgå hendelsen
- identifisere og følge opp risikoreduserende tiltak

For detaljerte regler og metode for å melde, se https://www.helsetilsynet.no/tilsyn/varsel-om-alvorlige-hendelser/oversikt/

5.8.4 Varsel til Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet fungerer som det nasjonale kontaktpunktet for sikkerhet i nettverk og informasjonssystemer. Virksomheter som leverer samfunnskritiske og digitale tjenester, skal varsle Nasjonal sikkerhetsmyndighet innen 24 timer om avvik som følge av enhver negativ virkning på sikkerheten i nettverks- og informasjonssystemer. Varselet skal inneholde følgende informasjon:

- navn og kontaktinformasjon til tilbyderen
- den berørte tjenesten
- beskrivelse av hendelsen, inkludert mulige årsaker og konsekvenser
- antall berørte brukere
- hendelsens påvirkning i andre land

Nødvendig dokumentasjon og informasjon skal gjøres tilgjengelig for tilsynsmyndigheten. Informasjonen i varselet skal oppdateres innen 72 timer.

Innen en måned etter at varselet er sendt, skal virksomheten levere en hendelsesrapport til varslingsmottakeren. Rapporten skal inneholde oppdatert informasjon om de nevnte forholdene og hvilke tiltak som er iverksatt for å håndtere hendelsen.

Varslingsmottakeren kan kreve statusoppdateringer og nødvendig informasjon for å utføre sine oppgaver.

For definisjoner av nettverks- og informasjonssystemer og sikkerhet i nettverks- og informasjonssystemer, se kapittel 6 Vedlegg og 6.2 Vedlegg i Normen.

UTGÅTT VERSJON – erstattet av versjon 1

5.9 Beredskap

Virksomheten skal etablere og iverksette nødvendige sikkerhetstiltak for å kunne opprettholde kontinuitet og motstandsdyktighet ved en hendelse. Dette inkluderer evnen til å forebygge, detektere, håndtere og gjenopprette normaltilstand etter fysiske eller tekniske hendelser som kan påvirke informasjonssikkerheten og personopplysningssikkerheten.

Manglende tilgjengelighet til nettverk- og informasjonssystemene, tjenester og produkter kan medføre skader både for virksomheten, virksomhetens autoriserte brukere,

pasienten/brukeren ved ytelse av helsehjelpen, og den registrerte. Virksomheten skal sørge for at nødvendige helse- og personopplysninger er tilgjengelige.

Virksomheten skal utarbeide, vedlikeholde og dokumentere beredskapsplaner for ulike hendelser og varsling. Det skal gjennomføres jevnlige øvelser for å teste planverket og utvikle kompetansen til å håndtere hendelser. Beredskapsplanene skal utarbeides med basis i de nasjonale beredskapsprinsippene (https://www.regjeringen.no) og beskrive organisering og ledelse av beredskap, samt hvilke beredskapstiltak som skal iverksettes ved ulike hendelser. Målet er å minimere konsekvensene av slike hendelser og sikre stabil drift av nettverk og informasjonssystemer og tjenester. Dersom det er relevant, bør øvelser gjennomføres i samarbeid med underleverandører eller andre som utfører arbeid for eller på vegne av virksomheten.

Ved etablering av beredskapsplaner skal virksomheten kartlegge konsekvensen av bortfall av hele eller deler av virksomheten. Dette skal vurderes både for virksomheten selv, leverandører, underleverandører og for autoriserte brukere. Systemer skal klassifiseres etter prioritering basert på konsekvensene av tjenestestopp, fra kritisk til akseptabelt. Klassifiseringen skal inkludere kartlegging av avhengigheter og fastsettelse av akseptabel risiko for tilgjengelighet

Det skal også kartlegges og dokumenteres hvilke andre informasjonssystemer og hvilken infrastruktur de klassifiserte informasjonssystemene er avhengige av. Disse skal ha samme klassifisering og sikkerhetsnivå som for de klassifiserte informasjonssystemene.
For hver klassifisering skal ledelsen beslutte akseptabel risiko for tilgjengelighet, inkludert fastsettelse av maksimal avbruddstid.

Med utgangspunkt i klassifiseringen skal virksomheten etablere beredskapsplaner for alternativ drift uten bruk av informasjonssystemene og alternativ drift med delvis støtte fra informasjonssystemene. Beredskapsplanene skal øves på, testes, revideres og oppdateres minst en gang i året.

UTGÅTT VERSJON – erstattet av versjon 7.1

6 Vedlegg

6.1 "Oversikt over Normens krav"

Vedlegget "Oversikt over Normens krav" inneholder alle kravene med "skal" i Normen, noe som gjør det enklere å vurdere om virksomhetene følger Normen. I tillegg inkluderer vedlegget en oversikt over relevante lovkrav og er sammenstilt med de internasjonale standardene ISO 27001:2023 og ISO 27002:2022.

Virksomhetene kan benytte oversikten i sitt arbeid med å etablere styringssystemer for informasjonssikkerhet og personvern, samt etablere og vedlikeholde internkontroll og informasjonssikkerhetstiltak for å sikre at de er i samsvar med relevante lovkrav.

6.2 Definisjoner

Det kan ikke utledes rettigheter eller plikter av definisjonene alene. De må leses i den sammenheng de benyttes i Normen.

-A-

Med «**administratorrettighet**» menes i Normen øverste tilgangsnivå til system, server, database og sikkerhetsbarrierer. Tilgangsnivået har som oftest rettigheter til å utføre alle operasjoner.

Med **«akseptabel risiko»** menes i Normen hvor stor risiko virksomheten kan akseptere for at det inntreffer en hendelse som kan forårsake brudd på kravene til konfidensialitet, integritet og tilgjengelighet/robusthet i et konkret tilfelle. Risikoens størrelse avhenger av hvor stor sannsynlighet det er for at hendelsen skal inntreffe, og av konsekvensen av en slik hendelse. Hver enkelt virksomhet må vurdere konkret hvordan akseptabel risiko for vedkommende virksomhet skal oppnås, ved hjelp av akseptkriterier for risiko.

Med **«akseptkriterier for risiko»** menes i Normen ledelsens føringer for når en risiko er akseptabel. Akseptkriterier beskriver hvordan risiko skal aksepteres, og kan bestå av beslutningsprosesser, hvem som kan akseptere risiko av ulik størrelse innenfor gitte rammer, eller nivåer som beskriver hvor stor risiko som er akseptabel.

Med «**annen informasjon med betydning for informasjonssikkerheten**» menes i Normen informasjon der uautorisert tilgang eller andre sikkerhetsbrudd vil medføre en risiko for virksomheten, f.eks. konfigurasjonsfiler, resultat av risikovurderinger, beredskapsplaner, passordfiler, nettverkskart mv.

Med «**anonymisert**» menes i Normen helse- og personopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson (jf. helseregisterloven § 2 nr. 3).

Med «**autentisering**» menes i Normen prosessen som gjennomføres for å bekrefte en påstått identitet.

UTKAST VERSJON - erstattet av versjon 7.1

Med «**autorisasjonsregister**» menes i Normen et register over utstedte autorisasjoner som føres av den dataansvarlige.

Med «**avvik**» menes i Normen enhver håndtering av helse- og personopplysninger som ikke utføres i henhold til gjeldende regelverk, retningslinjer eller rutiner, samt andre sikkerhetsbrudd. Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

-B-

Med «**behandling**» menes i Normen enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, tilgjengeliggjøring ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Med «**behandlingens art**» menes i Normen virksomhetens spesifikke type behandlinger.

Med «**behandlingsgrunnlag**» menes i Normen et rettslig grunnlag for å behandle personopplysninger. Dette kan for eksempel være samtykke eller hjemmel i lov. Hva som er et gyldig behandlingsgrunnlag, fremgår av personvernforordningens artikkel 6 og 9.

Med «**behandlingsrettet helseregister**» menes i Normen pasientjournal og informasjonssystem eller annet register, fortegnelse eller lignende, der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen, og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner, jf. pasientjournalloven § 2 d).

Med «**bruker**» menes i Normen en person som anmoder om eller mottar tjenester omfattet av helse- og omsorgstjenesteloven som ikke er helsehjelp, jf. pasient- og brukerrettighetsloven § 1-3 bokstav f.

-D-

Med «**dataansvarlig**» menes i Normen 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. Hvis ikke dataansvaret er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 e), pasientjournalloven § 2 e) og personvernforordningen Artikkel 4) (her benyttes begrepet «behandlingsansvarlig»). Det presiseres at det er virksomheten som er dataansvarlig for behandling av helse- og personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten, og virksomheten er pliktsubjekt.

Med «**databehandler**» menes **i** Normen en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den dataansvarlige. Det presiseres at en databehandler er en ekstern person eller virksomhet utenfor den dataansvarliges virksomhet. Det vil si at den dataansvarliges egne medarbeidere ikke er dennes databehandlere.

UTKAST TT VERSJON – erstattet av versjon 7.1

-E-

Med «**egnet sikkerhetsnivå»** menes det sikkerhetsnivå som oppnås ved gjennomføring av egnede sikringstiltak (tekniske, organisatoriske, fysiske og personellmessige). Hvilke tiltak som anses egnede vil bero på risikoen, og det skal tas hensyn til den tekniske utvikling, gjennomføringskostnader, behandlingens art, omfang, formål og sammenhengen behandlingen utføres i. Egnet sikkerhetsnivå må ivareta konfidensialitet, integritet, tilgjengelighet og robusthet i informasjonssystemene på en balansert måte, der det legges stor vekt på risikoen for pasient/bruker og ytelse av forsvarlig helsehjelp.

-F-

Med **"felleskomponent"** menes åpne, gjenbrukbare løsninger som dekker typiske behov på digitaliseringsfeltet, slik som innlogging, autentisering, registre, osv.

-H-

Med «**helsehjelp**» menes i Normen handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende, rehabiliterende eller pleie- og omsorgsformål, og som utføres av helsepersonell.
Med «**helse- og personopplysninger**» menes i Normen en fellesbetegnelse for helseopplysninger eller personopplysninger innenfor Normens virkeområde.

Med «**helseopplysninger**» menes i Normen personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om helsetilstand, jf. personvernforordningen artikkel 4 nr. 15.

Med «**helseregister**» menes i Normen registre, fortegnelser, mv. der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen, jf. helseregisterloven § 2 d).

Med **hendelser** menes enhver hendelse med negativ virkning på sikkerheten i nettverk- og informasjonssystemer.

Med «**herunder elektronisk**» menes i Normen at data (for eksempel dokumenter, logger, diagrammer mv.) som er lagret i en datamaskin, også omfattes av sammenhengen.

Med «**hjemmekontor**» menes i Normen behandling av helse- og personopplysninger på PC som virksomheten har stilt til disposisjon, fra f.eks. hjem, hytte, hotellrom eller lignende. Bruk av PC som virksomheten ikke har stilt til disposisjon (for eksempel PC på internettkafé, hotell-PC, flyplass-PC), er ikke definert som hjemmekontor.

-I-

UTGÅTT VERSJON - erstattet av versjon 7.1

Med «**informasjonssystemer**» menes i Normen et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon. Eksempler på informasjonssystemer i helse- og omsorgstjenesten er: saks- og dokumentasjonssystem, arkivsystem, behandlingsrettet helseregister, e-post, sikkerhetssystemer, nettverksoperativsystemer, databasesystemer, lagringssystemer, backupsystemer, infrastruktur, medisinske støttesystemer, medisinsk utstyr og laboratoriesystemer.

Med «**infrastruktur**» menes i Normen den tekniske løsningen (komponenter og basis-programvare) som benyttes til innhenting, lagring, behandling, presentasjon og overføring av helse- og personopplysninger (f.eks. stasjonære og bærbare datamaskiner, mobiltelefoner, servere, nettverksutstyr (brannmurer og rutere), skrivere, lagringsnettverk, apper mv.).

Med «**integritet**» menes i Normen at helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting.

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.

-K-

Med «**kommune**» menes i Normen en juridisk enhet som kommune og fylkeskommune.

Med «**konfidensialitet**» menes i Normen at helse- og personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene.

Med «**konfigurasjon**» menes i Normen informasjonssystemets utforming inklusive både teknisk utstyr og programvare.

Med «**konfigurasjonsendring**» menes i Normen en endring av informasjonssystemets utforming som følge av installasjon, oppgradering eller fjerning av utstyr eller programvare.

-L-

Med «**leverandør**» menes i Normen juridisk enhet som yter tekniske eller administrative tjenester til virksomheten. Eksempler er EPJ-leverandør, røntgenleverandør, leverandør av løsning for SMS-meldinger, IKT-leverandør mv.

Med «**logg**» menes i Normen et logisk register der hendelser i informasjonssystemet er nedtegnet, se neste definisjon.

Med «**logging**» menes i Normen registrering av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

-M-

Med «**mottaker**» menes i Normen en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som personopplysninger tilgjengeliggjøres til, enten det dreier seg om en tredjepart eller ikke. Offentlige myndigheter som kan motta personopplysninger innenfor rammen av en særskilt undersøkelse i samsvar med

UTGÅTT VERSJON – erstattet av versjon 7.1

unionsretten eller medlemsstatenes nasjonale rett, skal imidlertid ikke anses som mottakere; nevnte offentlige myndigheters behandling av slike opplysninger skal være i samsvar med gjeldende regler for vern av personopplysninger i henhold til formålet med behandlingen.

-N-

Med **nettverks- og informasjonssystemer** menes:

- elektronisk kommunikasjonsnett som nevnt i ekomloven § 1-5 nr. 2
- en enhet eller en gruppe av sammenkoblede eller beslektede enheter som behandler digitale data automatisk ved hjelp av et program
- digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a eller b for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes.

Med «**Norsk Helsenett**» menes i Normen Norsk Helsenett SF.

Med **Norm/Normen**» menes dette dokumentet. Andre dokumenter i tilknytning til Normen, for eksempel faktaark og veiledninger, er ikke omfattet av begrepet.

-O-

Med «**organisatoriske tiltak**» menes i Normen ikke-tekniske tiltak. Eksempler på slike tiltak er rutiner, opplæring og endringer av organisasjon og funksjoner for å ivareta oppgaver.

-P-

Med «**pasient**» menes i Normen en person som henvender seg til helse- og omsorgstjenesten med anmodning om helsehjelp, eller som helse- og omsorgstjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle, jf. pasient- og brukerrettighetsloven § 1-3 bokstav a.

Med «**pasientsikkerhet**» menes i Normen vern mot unødig skade som følge av helsetjenestens ytelser eller mangel på ytelser.

Med «**personopplysninger**» menes i Normen enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Med «**personopplysningssikkerhet**» menes i Normen vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade ved bruk av tekniske, organisatoriske, fysiske og personellmessige tiltak.

Med «**personvernkonsekvensvurdering**» menes i Normen en systematisk prosess som identifiserer og evaluerer potensielle personvernkonsekvenser fra alle interessenters synsvinkel i et prosjekt, initiativ, foreslått system eller en prosess.

UTKAST VERSJON – erstattet av versjon 7.1

Med «**personvernombud**» menes i Normen en formelt oppnevnt kontakt for personvern og informasjonssikkerhet internt mot dataansvarlig (virksomhetens ledelse) og ansatte og eksternt mot Datatilsynet og den registrerte (pasienter, inkluderte i studier og egne ansatte).

Med «**protokoll over behandlingsaktiviteter**» menes oversikt over behandlingsaktiviteter etter reglene i personvernforordningens art. 30.

-R-

Med «**register**» menes i Normen enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag. En database eller et regneark er en teknisk løsning for et register.

Med «**registrert / den registrerte**» menes i Normen det individet som opplysninger kan knyttes til. Eksempler og begreper som brukes om den registrerte, er søker, pasient/bruker, deltager i forskningsprosjekt, pårørende og tjenestemottaker. En ansatt kan være omfattet av begrepet.

Med **«robusthet»** menes i Normen organisasjonen og informasjonssystemers evne til å gjenopprette normaltilstand etter f.eks. en fysisk eller teknisk hendelse. Dette oppnås gjennom egnede tekniske, organisatoriske, fysiske og personellmessige tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting av personopplysningssikkerheten og informasjonssikkerheten for øvrig.

-S-

Med «**samtykke**» menes i Normen enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende.

Med «**sektor/sektoren**» menes i Normen helse- og omsorgstjenesten eller en eller deler av de nevnte.

Med «**selvautorisering**» menes i Normen en autorisasjon gitt til helsepersonell for å kunne få tilgang til helse- og personopplysninger de vanligvis ikke har tjenstlig behov for.

Med «**sensitive personopplysninger / særlige kategorier**» menes i Normen opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
c) helseforhold (helseopplysninger)
d) seksuelle forhold
e) medlemskap i fagforeninger

Med «**sikker autentiseringsløsning**» menes i Normen en autentiseringsløsning som for eksempel er basert på personlig kvalifisert sertifikat, eller annen autentiseringsløsning som gjennom en risikovurdering viser at den har tilstrekkelig sikkerhet.

UTGÅTT VERSJON – erstattet av versjon 7.0

Med **sikkerheten i nettverks- og informasjonssystemer** menes evnen nettverk- eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede, overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nettverks- og informasjonssystemer.

-T-

Med «**taushetsplikt**» menes i Normen lovpålagt eller avtalt plikt til å hindre at andre får adgang eller kjennskap til helse- og personopplysninger, jf. helsepersonelloven § 21, helseregisterloven § 17, pasientjournalloven § 15, helse- og omsorgstjenesteloven § 12-1, spesialisthelsetjenesteloven § 6-1 og forvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten. Taushetsplikt innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

Med «**tekniske tiltak**» menes i Normen tiltak av teknisk karakter som ikke kan påvirkes eller omgås av medarbeidere, og ikke er begrenset av handlinger som den enkelte forutsettes å utføre. Eksempler på slike tiltak kan være autentisering ved personlig kvalifisert sertifikat eller konfigurering av en brannmur slik at den kun tillater bestemt trafikk, eller en meldingstjeneste som er laget slik at alle meldinger automatisk blir kryptert.

Med «**tilgang**» menes i Normen at helse- og personopplysninger om en eller flere bestemte pasienter/brukere er eller gjøres tilgjengelig for autorisert personell. Beslutning om tilgang til behandlingsrettede helseregistre skal treffes etter en konkret vurdering basert på at det ytes helsehjelp til pasienten. Tilgang til fagsystemer i forbindelse med ytelser til pasient/bruker skal etableres basert på tjenstlig behov. Tilgang i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra tjenstlig behov.

Med «**tilgjengelighet**» menes i Normen at helse- og personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Med «**tjenstlig behov**» menes i Normen at personer med nærmere bestemte arbeidsoppgaver trenger nødvendige helse- og personopplysninger for å yte helsehjelp, omsorgstjeneste eller utføre administrasjon i forbindelse med dette. Dersom pasienten har sperret hele eller deler av helse- og personopplysningene, kreves særskilt hjemmel for tilgang til disse.

Med «**tredjepart**» menes i Normen enhver annen fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ enn den registrerte, den dataansvarlige, databehandleren og de personer som under den dataansvarlige eller databehandlerens direkte myndighet har fullmakt til å behandle personopplysninger.

UTKASTVERSJON - Komitéutkast Versjon 7.1

-U-

Med «**underleverandør**» menes i Normen en virksomhet som inngår en kontrakt om å utføre hele eller deler av forpliktelsene til en databehandlers avtale.

-V-

Med «**virksomhet**» menes i Normen juridisk enhet som helseforetak, helseforvaltning, kommune, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse mv., eller databehandler/leverandør som ved avtale er forpliktet til å følge Normen.

6.3 Støttedokumenter

I tilknytning til Normen er det utarbeidet en rekke støttedokumenter i form av faktaark, veiledere og maler. Dette materiellet dekker de fleste områder innen informasjonssikkerhet og personvern.

Støttedokumentene er ikke bindende, men er kun å anse som veiledende dokumenter. Ved motstrid mellom Normen og støttedokumenter har Normen forrang.

6.3.1 Faktaark

Faktaarkene beskriver nærmere hvordan virksomhetene kan oppfylle enkelte sentrale krav i Normen og gir praktisk veiledning til dette. Faktaarkene er tematiske med et omfang på 1–4 sider.

6.3.2 Veiledere

Veiledere er støttedokumenter med et omfang på 30–50 sider som går i dybden i et tematisk fagområde eller en delsektor.

6.3.3 Maler

I tilknytning til faktaark og veiledere er det utarbeidet maler i form av dokumentmaler og sjekklister som gir brukeren en redigerbar versjon til bruk i egen virksomhet.

6.4 Referanser

Alle lover og forskrifter: https://lovdata.no/

Datatilsynet: https://www.datatilsynet.no/

Den amerikanske standardiseringsorganisasjonen, NIST:
https://www.nist.gov/topics/cybersecurity

Det europeiske personvernrådet (European Data Protection Board – EDPB):
https://edpb.europa.eu/

Digitaliseringsdirektoratets hjemmeside om informasjonssikkerhet:
https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet

UTGÅTT VERSJON – erstattet av versjon 7.1

European Union
Hjemmeside for NIS2-direktivet (Direktiv (EU) 2022/2555)
Directive - 2022/2555 - EN - EUR-Lex

Hjemmeside for Norm for informasjonssikkerhet helse- og omsorgstjenesten:
https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

Helsedirektoratets rundskriv og veiledere:
https://www.helsedirektoratet.no/lov-og-forskrift/rundskriv-veiledere-til-lov-og-forskrift-og-lovfortolkninger

Kravspesifikasjon for PKI i offentlig sektor:
(https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/)

NSMs anbefaling til kryptoløsninger: kortliste-krav-til-krypto

NSM-veileder i kryptokrav:
https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/

NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.1:
https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor:
https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/

Referansekatalogen for e-helse. E-helsestandarder og andre kravdokumenter som er obligatoriske med hjemmel i forskrift, eller anbefalt av offentlig myndighet:
https://ehelse.no/standarder-kodeverk-og-referansekatalog/referansekatalogen

The European Union Agency for Network and Information Security (ENISA):
https://www.enisa.europa.eu/

GATT VERSJON – erstatt

6.5 Normens historikk

1. UTGAVE
Stadig mer av arbeidet i helsesektoren er basert på elektronisk behandling av pasientenes opplysninger. Likeledes foregår en stadig større andel av kommunikasjonen mellom virksomhetene elektronisk.

Den økende elektroniske behandlingen av opplysninger gir muligheter, men skaper også utfordringer for informasjonssikkerheten hos virksomhetene. Elektronisk behandling medfører blant annet at opplysningene enklere og raskere kan gjøres tilgjengelig både internt i en virksomhet og eksternt utenfor virksomheten. Dette er en fordel, forutsatt at opplysningene kun gjøres tilgjengelig for rett vedkommende til rett tid. Det kan imidlertid oppstå utilsiktede konsekvenser for opplysningenes konfidensialitet, og særskilte tiltak må etableres for å sikre at uvedkommende ikke får tilgang til opplysninger som er lagret

elektronisk. Det er behov for mekanismer som gir tillit til at alle aspekter ved informasjonssikkerhet er tilfredsstillende ivaretatt hos de aktuelle virksomhetene.

Dette er bakgrunnen for Sosial- og helsedirektoratets initiativ til at helsesektoren utarbeider sin egen norm for informasjonssikkerhet. Normen er utarbeidet av representanter for sektoren, herunder fra Den norske legeforening, representanter for de regionale helseforetakene, Norsk Sykepleierforbund, Norges Apotekerforening og Kommunenes Sentralforbund. I tillegg har Datatilsynet, Helsetilsynet, Rikstrygdeverket og Sosial- og helsedirektoratet deltatt i arbeidet.

Formålet med normen er å bidra til tilfredsstillende informasjonssikkerhet i helsesektoren. Normen er også ment å være et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet. I tillegg til tilfredsstillende informasjonssikkerhet stiller helseregisterloven, personopplysningsloven og øvrig regelverk en rekke andre krav til behandling av pasienters opplysninger. Disse kravene er ikke omhandlet i denne normen.
28. juni 2006.

2. UTGAVE
Styringsgruppen for Normen besluttet sommeren 2008 å innarbeide endringer i Normen som følge av lov- og forskriftsendringer og ønske om økt elektronisk samhandling mellom aktørene i sektoren. Nytt er også at Norsk Helsenett, private laboratorier, Den norske tannlegeforening, Den offentlige tannhelsetjenesten og Norges Farmaceutiske Forening deltar i styringsgruppen for Normen. I tillegg er Helse- og omsorgsdepartementet og Direktoratet for forvaltning og IKT (Difi) observatører i arbeidet.

Helsetilsynet har, etter eget ønske, trådt ut av styringsgruppen.

Styringsgruppen besluttet høsten 2009 å utvide Normens virkeområde. Normen gjelder nå både helse-, omsorgs- og sosialsektoren.

Samtidig ble det vedtatt at problemstillinger knyttet til de ansattes personvern skal inkluderes i Normen så langt det passer.

I juni 2009 vedtok Stortinget endringer i helseregisterloven. Dette åpner for å gi forskrifter om
- tilgang til helseopplysninger på tvers av virksomheter
- etablering av virksomhetsovergripende behandlingsrettede helseregistre
- etablering av virksomhetsovergripende behandlingsrettede helseregistre for helsepersonell med formalisert arbeidsfellesskap

Slike forskrifter er ikke gitt, og ovennevnte temaer behandles ikke i Normen.
2. juni 2010.

2. UTGAVE, VERSJON 2.1
Styringsgruppen for Normen besluttet 29. november 2012 å endre kravet til sikkerhetsnivå 4, slik at det er mulig med alternative løsninger under forutsetning av at risikovurdering dokumenterer og bekrefter at alternativ løsning har tilstrekkelig sikkerhet.

3. UTGAVE
Styringsgruppen for Normen besluttet 5. desember 2013 å innarbeide endringer som følge av forskrift om virksomhetsovergripende pasientjournal i formalisert arbeidsfellesskap. I tillegg er ansvaret for autorisasjonsregister i kjernejournal presisert, regler for tilgjengeliggjøring av helseopplysninger til kvalitetssikring og læring innarbeidet, og det er referert til dokumentet «Kravspesifikasjon for PKI i offentlig sektor» for minimumskrav til krypteringsstyrke.

UTGÅTT VERSJON – erstattet av versjon 7.1

4. UTGAVE
Styringsgruppen for Normen besluttet 5. juni 2014 å innarbeide endringer som følge av at sosialtjenesteloven fra 1991 (LOV-1991-12-13-81) er opphevet. Virkeområdet for Normen er samtidig endret til helse- og omsorgstjenesten. I tillegg er det tydeliggjort at Normen gjelder for tjenester i Arbeids- og velferdsetaten som er tilknyttet Helsenettet og for de kommunale tjenester i lokalt NAV-kontor som er tilknyttet Helsenettet.

5. UTGAVE
Styringsgruppen for Normen besluttet 12. februar 2015 å innarbeide endringer som følge av ny helseregisterlov, pasientjournalloven og forskrift om tilgang til helseopplysninger mellom virksomheter.

5. UTGAVE, VERSJON 5.1
Styringsgruppen for Normen besluttet 4. juni 2015 å endre ordlyden for sikring av dokumentasjon av tiltak (kapittel 3.3) som følge av krav i offentleglova.

5. UTGAVE, VERSJON 5.2
Styringsgruppen for Normen besluttet 9. juni 2016 å tydeliggjøre teksten iht. lovverk for felles journal. Videre er enkelte formuleringer endret for å gi en bedre forståelse av kravene.

5. UTGAVE, VERSJON 5.3
Styringsgruppen for Normen besluttet 31. mai 2018 flere endringer som var første skritt på veien i et større revisjons- og utviklingsarbeid av Normen.

EUs personvernforordning (EU) 2016/679 av 27. april 2016 implementeres i Norge som lov ved ny personopplysningslov i 2018. Dette førte også til enkelte endringer og tilpasninger i helselovgivningen.

Formålet med versjon 5.3 var å sikre at Normens krav var i overenstemmelse med nytt lovverk, utvide Normens område til å omfatte mer personvern og oppdatere Normen med nye krav tilpasset den teknologiske utviklingen. Normen fikk ny struktur, den var gjennomgått for å sikre at det ikke er motstrid mellom Normen og nytt lovverk, og enkelte artikler fra forordningen var spesielt innarbeidet:

- Art 30 - Protokoller over behandlingsaktiviteter
- Art 32 - Sikkerhet ved behandlingen
- Art 33 og 34 - Melding og underretning om avvik
- Art 35 - Personvernkonsekvensvurdering
- Art. 24 og 28- Databehandlingsansvarlig og databehandler
- Art. 37 og 38- Personvernombud

6. UTGAVE, VERSJON 6.0
Styringsgruppen for Normen vedtok 4. februar 2020 en større revisjon av Normen. Denne versjonen av Normen er resultatet av et langvarig revisjons- og utviklingsarbeid. Hovedmålene har vært å sikre at Normens krav er dekkende for nye krav i personvernforordningen og samtidig teknologinøytral og tilpasset nåtidens teknologi. Det har også vært et viktig mål å forenkle fremstillingene og gjøre Normen mer leser- og brukervennlig. Det er blant annet tatt inn nye krav, tekst er slettet og krav er presisert eller endret. Normens virkeområde er endret, og kravet til forholdsmessighet kommer tydeligere frem. Det er gjort en gjennomgang og forenkling av teksten, samtidig som noe tekst er tatt ut og flyttet til veiledningsmateriellet. Versjon 6.0 var gjenstand for en bred høring.

UTGAVE, VERSJON 6.1 Styringsgruppen for Normen besluttet 21. november 2022 endringer i Normens omtale av risiko. Normen gikk over til å benytte akseptkriterier for risiko i

Gått ut av bruk – erstattet av versjon 7.1

stedet for nivåer for akseptabel risiko. Videre besluttet styringsgruppen at Normen skulle benytte begrepet «skadelig» i stedet for «ondsinnet» programvare. Definisjonen på «personlig kvalifisert sertifikat» ble tatt ut. Samtidig ble det gjennomført en gjennomgang av hele dokumentet og utdaterte referanser ble oppdatert.

7. UTGAVE, VERSJON 7.0

Oppdatering for å innta krav som er gjort gjeldende ved at digitalsikkerhetsloven og digitalsikkerhetsforskriften er satt i kraft. Kapittel som Nødrutiner er endret til beredskap, og tatt inn krav til digital beredskap. Versjon 7.0 av Normen ble godkjent av styringsgruppen via epost-godkjenning 25.09.2025.

UTGÅTT VERSJON – erstattet av versjon 7.1

NORMEN

Besøksadresse
Helsedirektoratet
Vitaminveien 4,
0483 Oslo

Kontakt
normen@helsedir.no