NORMEN

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Versjon 5.3

Gjeldende fra 20.07.2018

Utgitt med støtte av:

Direktoratet for e-helse

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

Versjonsnummer
5.3

Vedtatt av styringsgruppen for Normen:
31.05.2018

Gjeldende fra:
20.07.2018

Utgitt med støtte av:
Direktoratet for e-helse

Kontakt:
sikkerhetsnormen@ehelse.no

Publikasjonen kan lastes ned på:
www.normen.no

Forord

For å gi god helsehjelp er det nødvendig å håndtere store mengder opplysninger om enkeltindivider. Disse opplysningene omhandler ofte personlige og sensitive forhold og er avgjørende for helsehjelpens kvalitet. Det er derfor i både virksomhetens og brukernes interesse å få tilgang til og å beskytte opplysningene.

Å behandle opplysninger om pasienter og brukere på en betryggende måte, er avgjørende for å sikre tillit. Helsetjenesten er avhengig av tillit fra både pasienter, brukere, helsepersonell og befolkningen for øvrig. Pasienter og brukere må ha tillit for å våge å gi helsetjenesten sine opplysninger, av og til svært intim og personlig informasjon. Uten disse opplysningene kan vi ikke gi helsehjelp av god kvalitet. Helsepersonell må ha tillit til at opplysningene er korrekte og fullstendige for å kunne gi helsehjelpen. Sektoren trenger tillit for å kunne digitalisere og tilby helsehjelp på nye måter.

Informasjonssikkerhet er en forutsetning for digitalisering. Dette betyr at opplysninger må være korrekte, oppdaterte, fullstendige og tilgjengelige. Teknologien og behandlingen av opplysninger som brukes i helsetjenesten kan bli utsatt for både utilsiktede og tilsiktede hendelser. Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur og ha gode tiltak for å sikre at dette fungerer og samtidig håndtere og lære av tilfeller der den ikke fungerer.

Informasjonssikkerhet og personvern er sentrale begreper når det gjelder beskyttelse av informasjon og teknologi. Personvern handler i hovedsak om å beskytte og ivareta informasjon ut fra hensynet til den enkeltes privatliv og bestemmelsesrett over egne personopplysninger. Dette innebærer bl.a. å sørge for at det ikke lagres flere opplysninger enn nødvendig og at alle har rett til innsyn i sine opplysninger. Informasjonssikkerhet handler om å beskytte informasjon ut fra prinsipper om konfidensialitet, integritet og tilgjengelighet. Etablering av tilstrekkelig teknisk og organisatorisk informasjonssikkerhet er en av de største utfordringene helseforvaltningen og helse- og omsorgstjenesten står overfor ved utviklingen av en digitalisert helse- og omsorgstjeneste.

EUs personvernforordning (EU) 2016/679 av 27. april 2016 implementeres i Norge som lov ved ny personopplysningslov i 2018. Dette fører også til enkelte endringer og tilpasninger i helselovgivningen. Det pågår et tilpasnings- og utviklingsarbeid av Normen. Formålet er å sikre at Normens krav er i overenstemmelse med nytt lovverk, utvide Normens område til å omfatte mer personvern og å oppdatere Normen med nye krav tilpasset den teknologiske utviklingen. Versjon 5.3 av Normen er første steg i dette tilpasnings- og utviklingsarbeidet. I denne versjonen har Normen fått ny struktur, den er gjennomgått for å sikre at det ikke er motstrid mellom Normen og nytt lovverk og enkelte artikler fra forordningen er innarbeidet. Artiklene som er spesielt innarbeidet i v5.3 er

- 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

I neste versjon, 6.0, vil større deler av forordningen innarbeides, bl.a. de registrertes rettigheter.

I versjon 6.0 av Normen vil det bli en tydeligere differensiering av krav mot virksomhetenes størrelse, kompleksitet og andre forhold som påvirker sårbarhet og behov for sikkerhetstiltak.

For nåværende versjon av Normen (5.3) gis følgende leseveiledning til mindre virksomheter (f.eks. fastlegekontor eller en fysioterapeutpraksis):

- **Kapittel 2 Ledelse og ansvar.**
  Kapittel 2.1 og 2.2 leses av alle. Det er et sentralt poeng at den dataansvarlige har ansvar for behandling av personopplysninger i virksomheten. For øvrige kapitler fra 2.3 til 2.7 anbefales det å lese disse i lys av innledningen til kapittel 2.3 om hvordan styringssystemet skal tilpasses virksomheten.
- **Kapittel 3 Risikostyring.**
  Kapitlene til og med 3.3 leses av alle, men merk at omfanget av risikovurderingene må tilpasses virksomheten. Punktene i kapittel 3.4 bør leses som en sjekkliste for å vurdere om en personvernkonsekvensvurdering kan være aktuell. Imidlertid vil nok gjennomføring av en personvernkonsekvensvurdering og evt. forhåndsdrøfting med Datatilsynet som beskrevet i kapittel 3.4 og 3.5 ofte være mindre relevante for små virksomheter.
- **Kapittel 4 Personvern og pasientrettigheter**
  Kapitlet gir en oversikt over aktuelle bestemmelser basert på lovkrav.
- **Kapittel 5 Informasjonssikkerhet**
  Dette er de konkrete kravene til informasjonssikkerhet som stilles i Normen. Alle sikkerhetstiltak skal være egnede, og velges basert på risikovurderinger

31. mai 2018

Innhold

1 Om Normen

1.1 Bakgrunn for Normen

Normen er en bransjenorm utarbeidet og forvaltes av organisasjoner og virksomheter i sektoren med sikte på å bidra til tilfredsstillende informasjonssikkerhet og personvern hos den enkelte virksomhet og i sektoren generelt, samt å bidra til at det etableres mekanismer hvor virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Personvern- og helselovgivningen stiller krav til informasjonssikkerhet og personvern. Disse kravene gjelder uavhengig av Normen, og aktuelle tilsynsmyndigheter (særlig Datatilsynet og Helsetilsynet) kan kontrollere den enkelte virksomhets etterlevelse av det til enhver tid gjeldende regelverk. Personvern- og helselovgivningen stiller også en rekke andre krav til behandling av helse- og personopplysninger enn det som er tema for Normen, f.eks. flere problemstillinger rundt sekundærbruk, spesifikke krav til registre som har egne forskrifter, rettsgrunnlag for behandling av helse- og personopplysninger samt plikt til og krav til journalføring. I tillegg vil også blant annet den kommende sikkerhetsloven vil kunne få betydning.

Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Normens krav er krav som helsetjenesten mener er sentrale for sektorens tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.

Normen er en selvreguleringsmekanisme som kan benyttes av alle aktører i helse- og omsorgssektoren. Overholdelse av kravene i Normen kan brukes for å påvise at virksomhetens forpliktelser etter regelverket overholdes. Gjennom avtale kan aktørene i sektoren forplikte seg til å følge kravene i Normen. Slik avtale gir andre virksomheter grunnlag for å innrette seg i tillit til at vedkommende virksomhet har tilfredsstillende informasjonssikkerhet og personvern.

Normen har krav som dekker de fleste områdene innen informasjonssikkerhet og personvern; mennesker, prosesser og teknologi. Normen har også støttedokumenter i form av veiledningsmateriell. Dette omtales videre i kap. 6.2

1.2 EUs personvernforordning (GDPR)

Personopplysningslovens § 1 gjennomfører EUs personvernforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Personvernforordningen er implementert i norsk lovgivning med grunnlag i Norges forpliktelser etter EØS-avtalen.

I versjon 5.3 av Normen er enkelte artikler fra forordningen innarbeidet. Det vil derfor være ulikt fra kapittel til kapittel hvor stor tilpasning som er gjort. Alle krav i Normen er gjennomgått med tanke på å sikre at det ikke er motstrid mellom Normen og den nye personopplysningsloven.

Tiltak for å sikre personopplysninger, herunder det som i personvernforordningen kalles personopplysningssikkerhet, har stort fokus forordningen. Tiltakene skal være "egnede". Dette betyr at for å finne de riktige tiltakene så må bl.a. både opplysningenes egenart,

informasjonsbehandlingens omfang og egenarten til de som behandler opplysningene tas hensyn til. Tiltakene skal velges basert på risikovurderinger og tiltakene skal være forholdsmessige. Dette kan bety at en liten virksomhet som behandler personopplysninger i lite omfang bør ha andre tiltak enn en større virksomhet som behandler et større omfang av personopplysninger.

1.3 Formål

Formålet med Normen er å bidra til å sikre at en virksomhet som etterlever og innretter seg etter Normen har egnede tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger. 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 og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

Normen skal bidra til at ansatte, pasienter og brukere sikres et godt personvern.

Normen er ment å være et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet og personvern.

Normen skal, innenfor, lovverkets rammer, søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet. Normen skal bidra til å understøtte gode helsetjenester, god pasientsikkerhet, de ansattes personvern, og en aktiv pasientrolle. Med en aktiv pasientrolle menes at pasienten og brukerens rettigheter til egne helseopplysninger ivaretas, men også utviklingen der digitale tjenester etablerer kontakt mellom helsepersonell og innbyggere, pasienter og brukere, og derigjennom bidrar til større delaktighet.

1.4 Målgruppe – hvem Normen gjelder for

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

1.5 Virkeområde – hva Normen regulerer

Normen beskriver og stiller krav til virksomhetenes arbeid med informasjonssikkerhet og personvern for helse- og personopplysninger som behandles i forbindelse med yte, administrere og kvalitetssikre helsehjelp. Normen angir hvilke organisatoriske og tekniske tiltak som anses egnede for å oppnå tilfredsstillende informasjonssikkerhet og personvern for slike behandlinger av helse- og personopplysninger

En virksomhet håndterer i tillegg personopplysninger om egne ansatte. Normens sikkerhetskrav gjelder ikke direkte i denne sammenhengen, men virksomheten skal ivareta de ansattes personvern iht. gjeldende lover og forskrifter og spilleregler i arbeidslivet. Det er spesielt viktig at opplysninger om de ansattes bruk av informasjonssystemene (logging) i hovedsak kun benyttes i sikkerhetsøyemed, 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 regulerer den registrertes innsyn i logger.

Normens krav om ledelse og ansvar, risikovurdering og informasjonssikkerhet er relevante for primær (behandlinger av helse- og personopplysninger som følger av pasientjournalloven) og sekundærbruk (helseregisterloven) av data. Normens krav om personvern og pasientrettigheter gjelder i versjon 5.3 primærbruk, men kan brukes på

sekundærbruk så langt de passer. Neste versjon av Normen vil omfatte sekundærbruk i større grad.

Behandling av helse- og personopplysninger i forskningssammenheng følger helseforskningsloven, men er også underlagt all annen lovgivning på området. Før virksomheten iverksetter et forskningsprosjekt, må Regional komité for medisinsk og helsefaglig forskningsetikk (REK) søkes om forhåndsgodkjennelse.

Normen regulerer virksomhetenes manuelle og elektroniske behandlinger av helse- og personopplysninger, men er særlig innrettet mot de elektroniske behandlingene.

1.6 Normens utvikling og forvaltning

Normen er utarbeidet og forvaltes av en styringsgruppe fra helse- og omsorgstjenesten, se liste på https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/om-normen#styringsgruppe-for-normen

I prinsipielle spørsmål som behandles i styringsgruppa søkes enstemmighet.

Direktoratet for e-helse er sekretariat for styringsgruppens arbeid, med fast deltakelse fra Norsk Helsenett (NHN).

2 Ledelse og ansvar

Det er et ledelsesansvar å sikre at virksomheten følger krav til personvern og informasjonssikkerhet og at dette ansvaret ivaretas som en del av arbeid med virksomhetsstyring og kvalitetsforbedring. Dette omfatter blant annet å håndtere risiko på en helhetlig måte og sørge for velfungerende styring og kontroll. Personvern og informasjonssikkerhet må håndteres på et tilstrekkelig høyt nivå i organisasjonen.

Sikkerhetstiltak og etterlevelse av de grunnleggende personvernprinsippene skal dokumenteres. Dette er nødvendig for å ivareta kravene til ledelse og kvalitetsforbedring, sikre kravene til internkontroll, sikre og påvise at egnede tekniske og organisatoriske tiltak gjennomføres for at behandlingen av personopplysninger utføres i samsvar med denne forordningen, og at tiltakene kan gjennomgås på nytt og oppdateres ved behov. Videre er det en forutsetning at tiltak dokumenteres for at de kan vises til i protokoll over behandlingen av helse- og personopplysninger.

2.1 Ansvar og organisering av personvern og informasjonssikkerhet

Den som har det overordnede ansvaret for virksomheten skal etablere og opprettholde tilfredsstillende personvern og informasjonssikkerhet. Oppgaver kan utføres av egne ansatte eller overføres til eksterne, f.eks. kan oppgaver delegeres til leverandører. Dette må gjøres i form av skriftlige avtaler. Både virksomheten (dataansvarlig) og leverandøren (databehandler) har ansvar for at personvern og informasjonssikkerhet blir ivaretatt. Hovedansvaret tilligger dataansvarlig.

Arbeidet med informasjonssikkerhet i virksomheten skal organiseres og gjennomføres slik at det kommer klart frem hvem som er ansvarlig på alle nivåer, og hva de er ansvarlig for.

For ansvar vedrørende:

- samarbeid mellom virksomheter om behandlingsrettede helseregistre, se pkt.5.7.5
- tilgang til helseopplysninger mellom virksomheter, se pkt. 5.7.6

Arbeidet med personvern og informasjonssikkerhet må omfatte styring, gjennomføring og kontroll og skal dokumenteres i et styringssystem (internkontroll) som dekker personvern og informasjonssikkerhet (heretter kalt styringssystemet). Både dataansvarlig og databehandler skal ha et styringssystem.

Informasjonssikkerhet og personvern bør i størst mulig grad inngå som en del av det totale styringssystemet i virksomheten. Virksomheter som er omfattet av både Normen 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.

2.2 Dataansvarliges ansvar

Dataansvarlig er den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Dataansvarlig skal etablere og opprettholde tilfredsstillende personvern og informasjonssikkerhet.

Dataansvarlig skal:

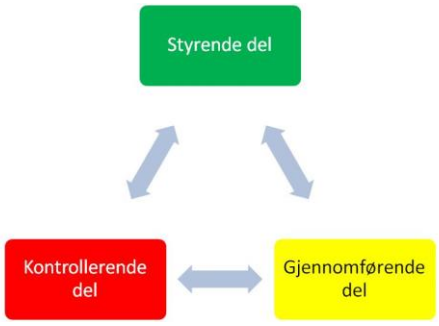
- Etablere styringssystem
- Gjennomføres risikovurderinger og utarbeide personvernkonsekvensvurdering der det er nødvendig
- Etablere egnede tekniske og organisatoriske tiltak
- Sikre de registrertes rett til innsyn og rett til informasjon, og ivareta reglene om retting og sletting av registrerte helse- og personopplysninger
- Etablere prosedyrer for innhenting av samtykke og oppfyllelse av ev. reservasjon mot visse former for behandling av helse- og personopplysninger
- Påse og dokumentere at behandlingene er lovlige
- Varsle ved brudd på personvernet og informasjonssikkerheten

2.3 Styringssystemet

Styringssystem er den del av virksomhetens internkontrollsystem (kvalitetssystem) som omfatter hvordan virksomhetens aktiviteter planlegges, gjennomføres, evalueres og korrigeres. Styringssystemet skal tilpasses virksomhetens størrelse, egenart og aktiviteter og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i.

For mindre virksomheter kan dette bety at ikke alle elementene i punktlisten nedenfor er relevante. Forhold av betydning i vurderingen er om virksomheten er så liten og oversiktlig at ansvarsforhold gir seg selv, eller om det benyttes driftsleverandør som tar seg av teknisk drift med prosedyrer for drift av informasjonssystemene. Dataansvarlig virksomhet er uansett alltid ansvarlig. For fastsettelse av akseptkriterier, kan Normens overordnede krav for etablering av sikkerhetstiltak beskrevet i kapittel 3 legges til grunn. Virksomhetens sikkerhetsmål kan ta utgangspunkt i informasjonssikkerhetsmålene definert kapittel 2.4 nedenfor.

Virksomhetens øverste ledelse skal etablere styringssystemet og gjøre dette kjent i virksomheten. Som eksempel kan styringssystemet struktureres med styrende, gjennomførende og kontrollerende krav og aktiviteter for å rettlede og styre virksomheten når det gjelder personvern og informasjonssikkerhet.



Den styrende delen bør inneholde:

- Informasjonssikkerhetsmål
- Protokoll over behandlinger av helse- og personopplysninger og holde protokollen à jour
- Nivå for akseptabel risiko
- Organisasjons-/ansvarskart ved minimum å:
    - Dokumentere ansvar og oppgaver
    - Beskrive ansvar og oppgaver på alle nivåer
    - Gjøre ansvarsforholdene kjent i organisasjonen
- Sikkerhetsinstruks

Den gjennomførende delen bør inneholde:

- Hvilken type leverandører som skal benyttes og føre oversikt over dem og hvilke oppgaver de utfører
- Avtaler med partnere, databehandlere og leverandører
- Planer for gjennomføring av risikovurderinger og prosedyrer for gjennomføring og oppfølging
- Konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av konfigurasjonen
- Prosedyrer for godkjenning av alle konfigurasjonsendringer i informasjonssystemene
- Prosedyrer for behandlinger av helse- og personopplysninger
- Prosedyrer og regler for bruk av informasjonssystemene som minimum skal ivareta at:
    - Det ikke skal søkes annen informasjon enn den man er autorisert for og har behov for i den aktuelle arbeidssituasjon.
    - Særskilte prosedyrer ved selvautorisering for behandlingsrettede helseregistre skal følges.
    - Enhver uautorisert tilgang til data skal følges opp som avvik.
    - Autentiseringskriteria skal beskyttes, bl.a. ved at passord skal hemmeligholdes.
    - Helse- og personopplysninger som registreres skal være relevante og nødvendige.
    - Registrering skal gjøres snarest mulig etter at informasjonen har fremkommet.
- Prosedyrer for drift av informasjonssystemene
- Dokumentasjon av sikkerhetstiltak – organisatoriske, fysiske og tekniske
- Prosedyrer ved bruk av databehandlere, leverandører av kommunikasjonstjenester, utstyr eller programvare og andre leverandører

Den kontrollerende delen bør inneholde:

- Planer for gjennomføring av sikkerhetsrevisjoner og prosedyre for oppfølging av resultater fra disse sikkerhetsrevisjoner. Sikkerhetsrevisjoner skal gjennomføres jevnlig
- Planer for ledelsens gjennomgang og prosedyre for oppfølging av handlingsplaner besluttet av ledelsen. Ledelsens gjennomgang skal være minimum årlig og dekke bl.a. avvikshendelser og eventuelle korreksjoner i styringssystemet
- Prosedyrer for avvikshåndtering ved bl.a. brudd på prosedyrer

Dokumenter angitt i styringssystemet skal holdes løpende oppdatert og arkiveres fra det tidspunktet dokumentet ble erstattet med en ny gjeldende versjon. Formålet med arkiveringen er blant annet å muliggjøre sporing og korrigering av avvik over tid.

Følgende skal arkiveres i minimum 5 år fra det tidspunkt dokumentet ble tatt ut av bruk:

- Alle dokumenter i styrende, gjennomførende og kontrollerende del ovenfor
- Resultater fra sikkerhetsrevisjoner
- Resultater fra risikovurderinger
- Resultater fra avviksbehandling
- Referat fra ledelsens gjennomgang
- Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregister)
- Avtaler med partnere, databehandlere og leverandører

Følgende skal tas vare på til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem:

- Logger med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene

Dokumentasjon om tiltak knyttet til informasjonssikkerhet skal sikres på tilsvarende måte som helse- og personopplysninger når kjennskap til tiltakene for uvedkommende vil innebære en risiko.

2.4 Informasjonssikkerhetsmål

Sentrale informasjonssikkerhetsmål for helse- og omsorgssektoren er at helse- og personopplysninger skal:

- Være tilgjengelig for rett personell til rett tid i henhold til fastsatte prinsipper for tilgangsstyring etter kap. 5.2.
- Behandles i tråd med reglene om taushetsplikt og være beskyttet slik at uvedkommende ikke får kjennskap til opplysningene. Uvedkommende omfatter også personell som ikke har tjenstlig behov.
- Være fullstendige, oppdaterte og korrekte og et resultat av rettmessige registreringer og kontrollerte aktiviteter.
- Begrenses slik at kun det som er nødvendig av helse- og personopplysninger behandles.

Virksomhetens ledelse skal på bakgrunn av informasjonssikkerhetsmålene ovenfor, og kravene i kap. 3, fastsette nivå for akseptabel risiko. Se mer om dette i kap. 3.

Valgene for å oppnå informasjonssikkerhetsmålene skal dokumenteres. Blant annet er det virksomhetens ansvar å avgjøre om arbeidet skal utføres internt i virksomheten eller om virksomheten skal sette bort hele eller deler av arbeidet til eksterne avtaleparter.

På bakgrunn av dette skal virksomheten etablere egnede tekniske og organisatoriske tiltak. Tiltakene skal settes i verk på bakgrunn av en vurdering av risiko for den registrertes

personvern. I denne vurdering skal det tas hensyn til informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i. Iverksetting av tiltak for vern av personopplysninger skal vurderes for de forskjellige behandlingsaktivitetene.

2.5 Informasjonssikkerhetsinstruks

Øverste ledelse skal sørge for at virksomheten utarbeider og forvalter informasjonssikkerhetsinstruks som sammenfatter de vesentligste kravene til personvern og informasjonssikkerhet i virksomheten. Instruksen skal tilpasses informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i.

Instruksen skal forplikte den ansatte til å følge kravene og oppdateres ved endringer i krav og tiltak.

2.6 Personvernombud

Virksomhetens øverste ledelse skal sørge for at det utpekes personvernombud i all offentlig virksomhet og privat virksomhet når informasjonsbehandlingens omfang krever det. Personvernombudet kan være ansatt eller en ekstern som utfører oppgaver på grunnlag av en tjenesteavtale.

Personvernombudet skal utnevnes på bakgrunn av personlige kvalifikasjoner, særlig god kompetanse på personvernlovgivning og muligheten til å utføre oppgavene. Personvernombudet må ikke ha interessekonflikt med eventuelle andre roller som vedkommende innehar i virksomheten, og skal ikke motta instruksjoner vedrørende hvordan oppgavene skal utføres. Personvernombudet skal ikke beslutte behandlinger av personopplysninger eller metode/verktøy for slike behandlinger.

Personvernombudet skal gis tilstrekkelige ressurser og tilgang på aktuell kompetanse til å utføre sine plikter. Personvernombudet skal rapportere direkte til øverste ledelse i virksomheten.

Databehandler skal også utpeke personvernombud i tråd med reglene ovenfor.

Personvernombudet skal bistå dataansvarlig, databehandler og de ansatte i arbeidet med personvern og informasjonssikkerhet slik at nivå for akseptabel risiko blir ivaretatt.

2.7 Ledelsens gjennomgang

Virksomhetens øverste ledelse skal selv evaluere virksomhetens aktiviteter og følge opp at informasjonssikkerheten ivaretas ved minimum årlig gjennomgang. Plikten omfatter bl.a. gjennomgang av avvik, herunder uønskede hendelser, slik at lignende forhold kan forebygges.

Ledelsens gjennomgang må sees i sammenheng med økonomi- og virksomhetsplanleggingen da beslutningene kan få økonomiske konsekvenser.

Formål med gjennomgangen er en kontroll av status på sikkerhetsnivået og om dette er i samsvar med virksomhetens informasjonssikkerhetsmål. På bakgrunn av risiko og aktualitet bør følgende punkter inngå:

- Formålene med behandling av helse- og personopplysninger og protokoll over behandlingen av helse- og personopplysninger

- Ansvarsforhold og organisering mht. personvern og informasjonssikkerhet
- Resultat fra sikkerhetsrevisjoner
- Resultat fra risikovurderinger og personvernkonsekvensvurdering der det er nødvendig
- Resultater fra avviksbehandling. Virksomhetens ledelse skal regelmessig følge opp at tiltak på grunnlag av avvik fastlegges, planlegges og gjennomføres
- Oppfølging av leverandører ift hvilke tekniske løsninger som benyttes
- Kontroll og oppfølging av inngåtte avtaler (se kap. 5.7)
- Nivå for akseptabel risiko
- Eventuelt beslutte oppdatering av informasjonssikkerhetsmål

Dersom gjennomgangen avdekker at virkelig situasjon ikke når opp til fastsatt nivå for akseptabel risiko skal det vedtas tiltaksplaner for å oppnå fastsatt nivå for akseptabel risiko, med plassering av ansvar.

3 Risikostyring

Det er et ledelsesansvar å sørge for velfungerende risikostyring og kontroll. Dette innebærer å etablere oversikt over informasjonstyper som behandles i virksomheten, hvilken risiko det medfører for både virksomheten og de registrerte og hvilke tiltak som skal gjennomføres.

Både den dataansvarlige og databehandleren skal gjennomføre forholdsmessige tekniske og organisatoriske tiltak. Dette inkluderer å sikre konfidensialitet, integritet, tilgjengelighet og robusthet i informasjonssystemene. Det skal tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres.

For mindre virksomheter innebærer dette at arbeidet med risikostyring skal ta hensyn til bl.a. virksomhetens størrelse og organisering. Hvis f.eks. virksomheten selv utfører IKT-driftsoppgaver, vil virksomhetens egen risikovurdering bli mer omfattende enn om en driftsleverandør står for disse oppgavene. Dataansvarlig virksomhet er uansett alltid ansvarlig.

For å hindre utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert tilgjengeliggjøring av eller tilgang til personopplysninger skal følgende overordnede krav som minimum legges til grunn for etablering av sikkerhetstiltak:

Konfidensialitet
Konfidensialitet skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysningene. Dette innebærer blant annet at:

- Personer utenfor virksomheten skal ikke kunne få uautorisert tilgang til helse- og personopplysninger.
- Personer i virksomheten skal gis tilgang i henhold til fastsatte prinsipper for tilgangsstyring i henhold til krav i kap. 5.2.
- Det skal registreres i logger i behandlingsrettede helseregistre (inkl. elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang.

Integritet

- Det skal registreres i behandlingsrettede helseregistre (inkl. elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting. På denne måten sikres sporbarhet til opprinnelse.
- Sikkerhetstiltak skal iverksettes slik at personer eller teknologi, i eller utenfor virksomheten, ikke skal kunne endre helse- og personopplysninger uten autorisasjon.
- Helse- og personopplysninger skal være korrekte og knyttes til rett identifisert person.
- Helse- og personopplysninger skal føres i henhold til relevant kodeverk.
- Helse- og personopplysninger skal være fullstendige og ajourført i forhold til behandlingen av opplysningene.

Tilgjengelighet

- Innenfor rammen av taushetsplikten skal helse- og personopplysninger være tilgjengelig når man har tjenstlige behov.
- Selvautorisering kan etableres som en mulighet for autoriserte brukere til å gi seg selv tilgang uten å følge fastsatte prinsipper for å få tilgang til helse- og

personopplysninger i henhold til kap. 5.2. I så tilfelle må det utarbeides egne prosedyrer for dette. Begrunnelsen for selvautorisering skal dokumenteres.

- Misbruk av selvautorisering skal følges opp som avvik.
- Se kap. 5.9 om klassifisering av informasjonssystemenes kritikalitet og fastsettelse av akseptabel risiko for tilgjengelighet for hver aktuell klassifisering.

Robusthet

- Det skal finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting av personopplysningssikkerheten og informasjonssikkerheten for øvrig

På bakgrunn av disse overordnede kravene og virksomhetens informasjonssikkerhetsmål, se kap. 2.4, må virksomheten selv fastsette nivå for akseptabel risiko som skal gjelde i egen virksomhet

3.1 Protokoll over behandlinger av helse- og personopplysninger

En samlet og oppdatert oversikt over alle behandlinger av helse- og personopplysninger i virksomheten, er et viktig styringsdokument for informasjonssikkerhet, og et praktisk redskap i det gjennomførende arbeidet. Oversikten vil også gi bidrag til den generelle internkontrollen i virksomheten. Den vil bidra til å dokumentere etterlevelsen av lovverket. Oversikten kan f.eks. utarbeides som en database med oversikt over de behandlinger av helse- og personopplysninger som til enhver tid gjennomføres virksomheten. Denne kan omfatte IT-systemer, databaser, prosjekter (forskningsprosjekter osv.), medisinsk utstyr og manuelle registre mv.

Virksomheter som behandler helseopplysninger må ha en slik oversikt over behandlingsaktiviteter. Denne oversikten kalles i personvernforordningen "Protokoll over behandlinger av helse- og personopplysninger"

Protokollen skal minimum inneholde følgende opplysninger:'

- Navnet på og kontaktopplysninger til den dataansvarlige og eventuelt felles dataansvarlig
- Databehandlere og databehandleravtaler
- Navnet på og kontaktopplysninger til personvernombud
- Formålene med behandlingen
- Behandlingsgrunnlag
- Kategorier av registrerte (eksempelvis pasienter – barn og voksen, klient, bruker av tjenesten, ansatt, helsepersonell, bruker av informasjonssystem)
- Kategorier av personopplysninger (eksempelvis ansattopplysninger, helseopplysninger)
- Hvorvidt det behandler personopplysninger av særlige kategorier
- Mottakere av personopplysninger (eksempelvis NAV, HELFO, reseptregisteret, forsikringsselskap, o.l.)
- Eventuell overføring til utlandet og bekreftelse på at mottaker følger regulatoriske krav
- Planlagt lagringstid

- Beskrivelse av tekniske og organisatoriske sikkerhetstiltak, jf. styringssystemet
- Om det er utarbeidet personvernkonsekvensvurdering

Protokollen skal være skriftlig, og kan være elektronisk.

3.2 Oversikt over IKT-utstyr

Virksomheten skal ha oversikt over alt IKT-utstyr. Denne oversikten skal inkludere stasjonære og bærbare datamaskiner, mobiltelefoner og annet kommunikasjonsutstyr, servere, nettverksutstyr (rutere, svitsjer, brannmurer, osv.), skrivere, lagringsnettverk, apper, IP-telefoner mv.

I større virksomheter bør følgende tiltak gjennomføres:

- Utarbeide oversikt over maskin- og programvare som vedlikeholdes med automatiske verktøy
- Inventarsystemet for programvare bør spore versjon av det underliggende operativsystemet samt programmer som er installert på det

3.3 Risikovurdering

Risikovurderinger har betydning både i det styrende, det gjennomførende og det kontrollerende informasjonssikkerhetsarbeidet.

Før behandling av helse- og personopplysninger igangsettes skal det gjennomføres risikovurderinger for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. I tillegg skal virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten

Dataansvarlig og databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som står i forhold til risikoen. Ved vurdering av hvilke tiltak som skal iverksettes, skal det tas hensyn til informasjonsbehandlingens art og sammenhengen den utføres i, omfang, formål, den tekniske utviklingen og gjennomføringskostnadene for tiltakene.

Formålet med risikovurderingen er å avdekke om dataansvarlig og databehandler har iverksatt tilstrekkelige tiltak slik at egnet sikkerhetsnivå oppnås, eller om ytterligere tiltak må iverksettes.

En viktig del av oppgaven er kartlegging av opplysningene som må sikres, og å kartlegge miljøet opplysningene befinner seg i. Her vil protokollen over behandlinger av helse- og personopplysninger være et utgangspunkt, se kapittel 4.1. Risikovurderingen skal i tillegg identifisere behov for risikoreduserende tiltak ved å sammenligne avdekket risiko med nivå for akseptabel risiko. Nivå for akseptabel risiko bygger på informasjonssikkerhetsmålene.

Risikobegrepet rommer to størrelser: sannsynlighet for at noe skal skje, og hvilke konsekvenser denne hendelsen kan få. Når vi snakker om sikkerhetsrisiko for informasjonssystemer, vil de hendelsene som på denne måten vurderes være knyttet til de

tre aspektene man vanligvis forbinder med informasjonssikkerhet. Dette er konfidensialitet, integritet og tilgjengelighet.

Risikovurderingen starter med utgangspunkt i nivå for akseptabel risiko og består av følgende trinn:

1. Forberedelser med planlegging og organisering
2. Kartlegging og vurdering av behandlingene av personopplysninger
3. Identifisere uønskede hendelser
4. Konsekvensvurderinger
5. Sannsynlighetsvurderinger
6. Risikoberegning og vurdering
7. Tiltak som iverksettes

Risikovurdering skal som minimum gjennomføres før:

- det iverksettes behandling av helse- og personopplysninger
- etablering av nye informasjonsbehandlingssystemer eller registre som inneholder helse- og personopplysninger
- det iverksettes organisatoriske endringer som kan påvirke informasjonsbehandlingen
- det iverksettes tekniske endringer i utstyr og/eller programvare som kan påvirke informasjonsbehandlingen
- det iverksettes andre endringer med betydning for informasjonssikkerheten
- det iverksettes tilgang til helseopplysninger mellom virksomheter

Risikovurderingen skal dokumenteres. Konklusjonene fra vurderingen skal sammenlignes med fastlagt nivå for akseptabel risiko. Er risikoen høyere enn fastsatt nivå for akseptabel risiko skal det iverksettes tiltak (nye/endrede) for å oppnå akseptabel risiko. Dersom tekniske tiltak for å oppnå akseptabel risiko ikke innføres umiddelbart, kan det i en overgangsperiode benyttes administrative tiltak, f.eks. i form av prosedyrer.

Virksomhetens ledelse skal også jevnlig gjennomføre risikovurderinger for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser.

3.4 Personvernkonsekvensvurdering

Dersom det er sannsynlig at en type behandling av helse- og personopplysninger vil medføre en høy risiko for personvernet, skal den dataansvarlige foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha. En vurdering av personvernkonsekvenser skal gjøres før behandlingen av personopplysninger starter. Dersom det skal utvikles et nytt system, må vurderingen gjøres så tidlig som mulig i utviklingsprosessen og i hvert fall som en del av kravsettingen.

En personvernkonsekvensvurdering skal gjennomføres når det medfører høy risiko for personvernet:

- ved bruk av ny teknologi
- dersom behandlingens art, omfang, formål og sammenhengen den utføres i tilsier det
- [Henvisning til kommende liste fra Datatilsynet]

Personvernkonsekvensvurdering skal spesielt gjennomføres når behandlingen er:

- behandling i stor skala av helseopplysninger i eller av personopplysninger om straffedommer og straffbare forhold
- en systematisk og omfattende vurdering av personlige aspekter ved personer basert på automatisert behandling (profilering), som danner grunnlag for avgjørelser som har rettsvirkning eller påvirker den registrerte i betydelig grad

Dersom behandlingen av helse- og personopplysninger er regulert av gjeldende rett og det allerede er utført en vurdering av personvernkonsekvenser som en del av en generell konsekvensvurdering i forbindelse med vedtakelsen av det aktuelle regelverket, kan kravet om vurdering av personvernkonsekvenser falle bort.

Personvernkonsekvensvurdering skal minst inneholde:

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

Dersom man har flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer kan man gjøre en felles vurdering for disse.

Ved behov, for eksempel dersom risikoen endres, bør det foretas en gjennomgang av hvorvidt behandlingen gjennomføres i samsvar med personvernkonsekvensvurderingen. Om virksomheten har personvernombud skal ombudet rådføres ved gjennomføring av vurderingen.

Det skal planlegges tiltak som reduserer risikoen for personvernet. Dersom behandlingen av helse- og personopplysninger vil medføre en høy risiko, som ikke kan reduseres ved hjelp av rimelige midler, skal den dataansvarlige rådføre seg med Datatilsynet før behandlingen starter.

3.4.1 Ytterligere vurderingskriterier

Følgende ni kriterier kan benyttes for å avgjøre om en behandling vil kreve en vurdering av personvernkonsekvenser. Hvis dataansvarlig svarer ja på to eller flere av spørsmålene om den planlagte behandlingen av helse- og personopplysninger, må det gjennomføres en vurdering av personvernkonsekvenser:

1. Er behandlingen en evaluering eller poengvurdering?
2. Omfatter den automatiserte avgjørelser?
3. Innebærer den systematisk overvåking?
4. Involverer den sensitive personopplysninger?
5. Dreier det seg om en behandling av personopplysninger i stor skala?
6. Vil to eller flere datasett sammenstilles?
7. Omfatter den personopplysninger om registrerte med særskilt beskyttelsesbehov?
8. Tar den i bruk ny teknologi eller brukes eksisterende teknologi til nye formål?
9. Vil konteksten for behandlingen begrense muligheten de registrerte har til å utøve sine rettigheter?

Dersom en behandling oppfyller færre enn to kriterier, kan det hende det ikke er behov for en konsekvensvurdering.

3.5 Forhåndsdrøfting med Datatilsynet

Den dataansvarlige skal rådføre seg med Datatilsynet dersom:

- personvernkonsekvensvurderingen tilsier at behandlinger av helse- og personopplysninger vil medføre en høy risiko, også etter planlagte tiltak
- personvernkonsekvensvurderingen tilsier at behandlinger av helse- og personopplysninger vil medføre en høy risiko uansett tiltak

Den dataansvarlige skal framlegge det følgende for Datatilsynet:

- Ansvarsfordelingen mellom dataansvarlig, felles dataansvarlige og databehandlere, dersom dette er relevant
- Formålene med den planlagte behandlingen og hvordan den skal gjennomføres
- Tiltakene og garantiene som er fastsatt for å verne de registrertes personvern
- Kontaktopplysninger til personvernombudet, dersom dette er relevant
- Personvernkonsekvensvurderingen
- All annen informasjon som Datatilsynet ber om

Dersom Datatilsynet mener at behandlingen strider mot personvernlovgivningen skal tilsynet gi skriftlige råd til den dataansvarlige. Dette gjelder særlig dersom den dataansvarlige ikke i tilstrekkelig grad har identifisert eller redusert risikoen.

4 Personvern og pasientrettigheter

I versjon 5.3 av Normen er enkelte artikler fra forordningen innarbeidet, se forordet. Forordningens regler om de registrertes rettigheter og de tilhørende pasientrettigheter er ikke innarbeidet i denne versjonen. Dette arbeidet vil fortsette i kommende versjoner av Normen. Det vil si at dette kapittelet er ikke uttømmende på personvern og pasientrettigheter generelt, men omtaler enkelte temaer.

4.1 Taushetsplikt

For å sikre konfidensialitet for helse- og personopplysninger skal virksomhetens leder sikre at alt personell som gis tilgang har taushetsplikt, og at de er bevisst taushetspliktens innhold og omfang, for alle helse- og personopplysninger samt for annen informasjon med betydning for informasjonssikkerheten. Det skal som minimum:

- Beskrives konsekvenser ved brudd på taushetsplikten.
- Beskrives konsekvenser ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for (ulovlig tilegnelse).
- Beskrives konsekvenser ved å endre/forsøk på å endre opplysninger man ikke har autorisasjon til å endre.

Brudd på taushetsplikten og/eller ulovlig tilegnelse skal som konsekvens minimum medføre en advarsel for den som begår bruddet, og bruddet skal behandles iht. avviksprosedyre. Ved alvorlige eller gjentatte brudd på taushetsplikten må konsekvenser for ansettelsesforholdet vurderes.

Brudd på taushetsplikten og/eller ulovlig tilegnelse er forbudt og varsling av tilsynsmyndighetene og anmeldelse må vurderes.

4.2 Den registrertes rettigheter

Det skal etableres prosedyrer og gjennomføres tiltak for å sikre at:

- Pasienten/brukeren får informasjon om virksomhetens behandling av helse- og personopplysninger, og sine rettigheter til innsyn i, retting, sletting og sperring av registrerte opplysninger om seg selv
- Det innhentes skriftlig samtykke fra pasienten/brukeren i alle tilfelle hvor dette er nødvendig, herunder når tilgangen til den aktuelle behandlingen av helse- og personopplysninger ikke er fastsatt i lov eller har et annet gyldig grunnlag
- Pasienten/brukeren sikres innsyn i egne helse- og personopplysninger
- Pasientens/brukerens rettigheter til retting/sletting av helse- og personopplysninger ivaretas
- Pasientens rett til sperring av hele eller deler av egen pasientjournal ivaretas

Dersom den registrerte sender en anmodning elektronisk, skal informasjonen om mulig gis elektronisk, med mindre den registrerte ber om noe annet.

Ved tilgang til helseopplysninger mellom virksomheter skal dataansvarlig informere pasienten/brukeren om bruk av tilgang til helseopplysninger mellom virksomheter. Informasjonen skal tilpasses pasientens/brukerens forutsetninger og tilstand, og kan unnlates dersom det er klart utilrådelig. Informasjonen skal blant annet inneholde

- hvilke virksomheter som gis tilgang
- hvilke helse- og personopplysninger tilgangen omfatter
- at pasienten/brukeren kan motsette seg at det gis tilgang

4.2.1 Innsyn i personopplysninger og logger

Pasienten og brukeren har rett til innsyn i egne opplysninger i behandlingsrettet helseregister (inklusiv EPJ / fagsystem) og har rett til en enkel og kortfattet forklaring av faguttrykk eller lignende. Pasienten og brukeren kan nektes innsyn i opplysninger i journalen etter særlige regler.

Det skal etableres prosedyrer for å sikre at den registrertes rettigheter for innsyn i logger blir ivaretatt. Prosedyrene skal som et minimum sikre at den registrerte får informasjon om:

- Person og organisatorisk tilhørighet til den som har behandlet helseopplysningene
- Hvilke behandlinger av helse- og personopplysninger som er utført
- Når behandlingene av helse- og personopplysninger er gjort

Ved bruk av tilgang til helseopplysninger mellom virksomheter skal den registrerte i tillegg få informasjon om:

- person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene
- hvorfor helseopplysningene er hentet frem
- hvilke tidsperioder vedkommende har hentet frem helseopplysningene

4.3 Utlevering av helse- og personopplysninger

4.3.1 Til andre enn virksomhetens og forvaltningsorganets eget personell

Når det er nødvendig for å kunne yte forsvarlig helsehjelp, kan helse- og personopplysninger overføres, utlevering eller gis til annet helsepersonell enn virksomhetens eget personell. Dette skal skje i samsvar med lovbestemte regler om taushetsplikt. Behandlingen av forespørsel om overføring eller utlevering av helse- og personopplysninger skal skje i samsvar med prosedyrer som ivaretar kravene til konfidensialitet, integritet og tilgjengelighet. Det skal alltid fremgå av journalen når helse- og personopplysninger er gitt til annet personell enn virksomhetens eget personell.

Utlevering av helse- og personopplysninger fra et forvaltningsorgan til et annet forvaltningsorgan kan bare skje når dette er nødvendig for å fremme omsorgstjenesten eller for å forebygge vesentlig fare for tap av liv og helse eller dersom det foreligger annet grunnlag i lov. Dette skal skje i samsvar med lovbestemte regler om taushetsplikt. Behandlingen av forespørsel om overføring eller utlevering av helse- og personopplysninger

skal skje i samsvar med prosedyrer som ivaretar kravene til konfidensialitet, integritet og tilgjengelighet.

Utlevering av helse- og personopplysninger fra en virksomhet til en annen virksomhet (begge innenfor helse- og omsorgstjenesten) kan skje dersom ett av følgende vilkår er oppfylt:

- den registrerte samtykker i utleveringen
- det er fastsatt i lov at det er adgang til slik utlevering
- utlevering er nødvendig for å beskytte en persons vitale interesser, og den registrerte ikke er i stand til å samtykke
- det utelukkende utlevering opplysninger som den registrerte selv frivillig har gjort alminnelig kjent

Pasienten eller brukeren kan motsette seg at helseopplysninger i et behandlingsrettet helseregister (elektronisk pasientjournal (EPJ), felles journal og nasjonale behandlingsrettede helseregistre) gjøres tilgjengelige for helsepersonell og at helseopplysninger registreres eller behandles på andre måter i nasjonal Kjernejournal.

4.3.2 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 opplysningene til virksomhetens ledelse. Tilgjengeliggjøring skal begrenes til opplysninger som er nødvendig og relevant for formålet. Helseopplysningene skal så langt som mulig behandles uten at den registrertes navn og fødselsnummer fremgår. Dersom det likevel er nødvendig å videreformidle personidentifiserbare opplysninger, kan pasienten/brukeren motsette seg tilgjengeliggjøring.

Helsepersonell plikter å tilgjengeliggjøre pasientens fødselsnummer og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data til virksomhetsinterne pasientadministrative system (jf. helsepersonelloven § 26).

4.3.3 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 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.

5 Informasjonssikkerhet

Dette kapitlet beskriver sentrale sikkerhetstiltak som skal gjennomføres av virksomheter som behandler helse- og personopplysninger. Dette omfatter både dataansvarlige og databehandlere. Alle sikkerhetstiltak skal være egnede, og velges basert på risikovurderinger. Det kan dermed være nødvendig å gjennomføre mer omfattende tiltak enn det som er beskrevet her.

5.1 Ansatte, kompetanse og holdningsskapende arbeid

5.1.1 Vilkår og betingelser

Ved ansettelse må det settes vilkår og betingelser for den enkelte ansatte om hvordan personopplysninger skal behandles i virksomheten og hvilke overordnede krav som stilles. Dette kan inkluderes i arbeidsavtalen mellom arbeidsgiver og arbeidstager eller avtales skriftlig på annet hensiktsmessig vis.

Som et minimum må slike vilkår/betingelser inkludere:

- Sikkerhetsinstruksen
- Taushetserklæring
- Virksomhetens sanksjonsmuligheter ved brudd

5.1.2 Opplæring og kompetanse

Virksomheten skal iverksette tiltak som ivaretar at:

- alle som gis tilgang til og/eller drifter informasjonssystemene og tilhørende informasjon skal ha tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta informasjonssikkerheten.
- alle som har tilgang til helse- og personopplysninger behandler disse etter gjeldende regelverk, Normen og virksomhetens rutiner

Kompetansebygging må skje kontinuerlig og være tilpasset de ulike roller og brukergrupper. Særskilte opplæringstiltak må vurderes for nyansatte og ved endringer i informasjonssystemene eller i behandlingen av helse- og personopplysninger.

5.1.3 Opphør av ansettelse

Når et ansettelsesforhold opphører må det sikres at den som har vært ansatt leverer tilbake til arbeidsgiver alle medier (herunder digitalt, papir, osv.) som kan inneholde personopplysninger som denne har fått tilgang til i egenskap av å være ansatt i helse- og omsorgssektoren.

Taushetsplikten gjelder også etter at ansettelsesforholdet er opphørt.

5.2 Tilgangsstyring

Dette berører hvordan man foretar:

- Autorisering som er tildeling av rettigheter til å kunne lese, registrere, rette, slette og/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.
- Regulering av privat bruk av virksomhetens informasjonssystemer.
- Kontrollerende tiltak.

Innenfor rammen av taushetsplikten skal den dataansvarlige sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte.

Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten.

Tilgangsstyring skal etableres for alle behandlingsrettede helseregistre (inkl. elektronisk pasientjournal (EPJ)) og fagsystemer.

Tilgjengeliggjøring av helse- og personopplysninger til annet helsepersonell enn virksomhetens eget personell er regulert i kap. 4.3.

Bare autorisert personell kan få tilgang til helse- og personopplysninger.

Tilgang til behandlingsrettede helseregistre (inklusiv EPJ / fagsystem) skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes 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 de som har tjenstlig behov.

Ved tilgang til helseopplysninger mellom virksomheter skal begge virksomhetene ha tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger som minst ivaretar at:

- helseopplysningene ikke gjøres tilgjengelige dersom pasienten/brukeren har motsatt seg eller motsetter seg det
- det kun gis tilgang til helseopplysninger som er relevante og nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til pasienten/brukeren
- helsepersonellet er autorisert for slik tilgang, og har autentisert seg ved bruk av sikker autentiseringsløsning

5.2.1 Autorisering

Dataansvarlig er ansvarlig for at autorisasjoner tildeles, administreres og kontrolleres.

Ved tildeling av autorisasjon skal lovbestemt taushetsplikt vurderes og ivaretas.

Dataansvarlig skal delegere myndighet for å tildele autorisasjon til den enkelte enhets ansvarlige leder. I dette ligger at ansvarlig leder, innen eget ansvarsområde, skal vurdere og godkjenne det enkelte personells behov for å kunne få tilgang til helse- og personopplysninger. Tildelt autorisasjon skal sikre at den enkelte kan få tilgang til nødvendige helse- og personopplysninger i samsvar med personellets ansvar og oppgaver, så langt lovbestemt taushetsplikt ikke er til hinder for det.

Benyttes roller i virksomheten, skal autorisering skje for hver rolle uavhengig av personellets øvrige roller.

Det skal etableres prosedyre for tildeling og administrasjon av tilgangsrettigheter:

- Autorisasjon for å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov. Autorisasjonen skal tildeles i henhold til betryggende prosedyrer. Lovbestemt taushetsplikt skal vurderes og overholdes. Også tekniske tiltak skal iverksettes for å ivareta krav til konfidensialitet ved aktivt å hindre uvedkommende i å få tilgang og for å sikre dokumentasjon av denne tildelte autorisasjon. Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.
- Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger. Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes.
- Autorisasjon for andre tjenester gis etter tjenstlig behov, f.eks. autorisasjon til bruk av e-post, bruk av Internett e.l.

Følgende tiltak skal iverksettes for å hindre at personer uten autorisasjon får tilgang til helse- og personopplysninger:

- Tekniske og organisatoriske tiltak skal iverksettes slik at personer ikke skal kunne få tilgang til helse- og personopplysninger de ikke er autorisert for.
- Dersom det er åpnet for selvautorisering, skal tekniske tiltak etableres på en slik måte at helsepersonell kan få tilgang til nødvendige helse- og personopplysninger. Slik tilgang skal grunngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))
- Misbruk av selvautorisering skal følges opp som avvik.
- Tekniske tiltak skal iverksettes slik at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har endret og hva som er endret.
- Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger. All tildeling av autorisasjon skal registreres i et autorisasjonsregister.

5.2.1.1 Autorisasjonsregister

Dataansvarlig skal sørge for at det oppettes et autorisasjonsregister. Registeret skal som minimum inneholde:

- informasjon om hvem som er tildelt autorisasjon
- til hvilken rolle autorisasjonen er tildelt (om rolle 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)

5.2.1.2 Nasjonal kjernejournal

Dataansvarlig for nasjonal kjernejournal kan delegere myndighet for å tildele autorisasjon til den enkelte virksomhet som skal ta i bruk kjernejournal. Tilgang skal da skje gjennom autorisasjonsløsning i egen virksomhet. For kjernejournal skal autorisasjonen være tidsbegrenset. Den enkelte virksomhet er ansvarlig for at det opprettes et autorisasjonsregister i samsvar med det som er beskrevet ovenfor. Retningslinjer for autorisasjon og tilgangsstyring i kjernejournalen er nærmere beskrevet i egne retningslinjer for nasjonal kjernejournal.

5.2.1.3 Tilgang mellom virksomheter

Ved tilgang til helseopplysninger mellom virksomheter skal helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet:

- beskrive rettigheter og plikter som følger av autorisasjonen
- være i samsvar med regler om taushetsplikt
- dokumenteres i virksomhetens autorisasjonsregister
- tidsbegrenses
- alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold

Ved tilgang til helseopplysninger mellom virksomheter kan pasienten/brukeren kreve at tilgang til egne helseopplysninger sperres for helsepersonell fra andre virksomheter enn der opplysningene er nedtegnet. Med sperring menes en teknisk løsning der journalopplysninger gjøres utilgjengelige for enkeltpersoner, grupper av helsepersonell eller helsepersonell i andre virksomheter enn der journalnotatene er registrert.

5.2.2 Autentisering

Autentisering skal som minimum ivareta følgende:

- Ved tilgang til behandlingsrettede helseregistre (inkl. elektronisk pasientjournal (EPJ)) og fagsystemer skal ulike ansettelsesforhold identifiseres. Det skal benyttes tilfredsstillende autentisering i henhold til gjennomført risikovurdering.
- Flere personer skal ikke benytte samme autentiseringskriteria.

- Tildeling av autentiseringskriteria (som brukernavn og passord) skal gjennomføres på en betryggende måte.
- Ved tilgang til helseopplysninger mellom virksomheter skal det benyttes sikker autentiseringsløsning.
- Tilgang fra hjemmekontor og/eller mobilt utstyr skal sikres ved autentisering som ikke innebære økt risiko utover det som gjelder for stasjonært utstyr. En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet. Dette gjelder også for avdelingskontor som kommuniserer ved hjelp av linjer man ikke har fysisk kontroll over.

Benyttes roller skal ulike roller identifiseres og ved behov gis ulike autentiseringskriteria.

5.2.3 Kontroll av tilgangsrettigheter

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 informasjonsområdet som blir berørt av bruddet.

Virksomhetens ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister (inkl elektronisk pasientjournal (EPJ)) eller i et fagsystem. Se kapittel 5.4.4. Logging.

Dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang, skal virksomhetens ledelse varsles. Forøvrig skal hendelsen behandles iht. etablerte prosedyrer for avviksbehandling, særlig med henblikk på å få avklart om eksisterende tilgangskontroll er god nok.

Dersom kontrollen viser at det har skjedd en urettmessig tilgang, skal Datatilsynet informeres. Videre skal virksomhetens ledelse vurdere om pasienten/brukeren skal informeres.

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 prosedyrer for avviksbehandling.

5.3 Fysisk sikkerhet og håndtering av utstyr

5.3.1 Nøkler/adgangskort

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

5.3.2 Brukerutstyr (PC og printere - stasjonære)

Sikkerhetstiltak skal hindre at personer som ikke er autoriserte får tilgang til helse- og personopplysninger – enten ved adgangsregulert kontroll av lokaler med utstyr, eller ved at utstyret sikres mot misbruk og skjermer, utskrifter mv. skjermes mot uautorisert innsyn.

5.3.3 Driftsutstyr (servere og nettverksutstyr)

Sikkerhetstiltak skal hindre at annet enn autorisert personell får adgang til slikt utstyr. Alle lagringsmedia, dvs. disker, minnepinne, CD, mv., skal merkes, og alle helse- og personopplysninger skal slettes når lagringsmediet tas ut av bruk. Plikt til arkivering av opplysningene må uansett overholdes.

5.3.4 Mobilt utstyr og hjemmekontor

For slikt utstyr kan man ikke sikre lokaler, utstyret må derfor sikres. Det skal gjennomføres risikovurdering av de løsninger som benyttes. Det skal etableres administrative prosedyrer for bruk av mobilt utstyr og hjemmekontor.

Sikkerhetstiltak skal hindre at personer som ikke er autoriserte får tilgang til helse- og personopplysninger ved at:

- Tekniske tiltak iverksettes slik at det kun kan kommuniseres med predefinert utstyr. Autentisering skal ikke innebære økt risiko utover det som gjelder for stasjonært utstyr. En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet.
- Helse- og personopplysninger skal bare lagres lokalt når dette er nødvendig ut fra tjenstlig behov og skal alltid lagres kryptert.
- All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer sikres ved kryptering iht. «NSM Cryptographic Requirements Version 3.1»[1].

5.3.5 Kryptering

Tekniske tiltak skal iverksettes slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres.

5.3.6 Medisinsk utstyr

Lagringsenhet for elektromedisinsk utstyr som behandler helse- og personopplysninger skal plasseres i avlåst rom eller i bemannet område.

[1] https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf

Medisinsk utstyr som behandler helse- og personopplysninger skal inkluderes i virksomhetens arbeid med informasjonssikkerhet, herunder i risikovurderinger, tilgangsstyring og prosedyrer 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 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.

- Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt.

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

- Risikovurdering som viser at nivå for akseptabel risiko oppfylles
- 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

Konfigurasjonskontroll skal reguleres gjennom avtale ved:

- Bruk av databehandler.
- Bruk av fjernaksess for vedlikehold og oppdateringer.

5.4.2 Endringsstyring

Alle endringer i organisasjonen, informasjonssystemene og systemer som har innvirkning på informasjonssikkerheten skal forankres på relevant ledernivå.

Virksomheten skal utarbeide prosedyrer for endringsledelse som skal ta opp i seg følgende tema:

- Identifisering av vesentlige endringer
- Planlegging og testing av endringer
- Vurdering av potensielle konsekvenser, for eksempel ved å gjennomføre en risikovurdering
- Godkjennelsesprosedyre for endringer
- Kommunikasjon av plan til aktuelle personer/roller
- Reserveprosedyrer om endringen må avbrytes, feiler eller at uønskede hendelser oppstår
- Endringslogg med relevante opplysninger

5.4.3 Sikkerhetskopiering

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

- Sikkerhetskopier skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret.
- Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte og kan tilbakeføres.

5.4.4 Logging

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

- Det skal etableres prosedyrer for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke.
- Det skal etableres prosedyrer for ved behov å kunne sammenholde loggene med autorisasjonsregister.
- Dersom brudd avdekkes skal personalmessige reaksjoner iverksettes.
- Dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, dvs. det er gjentatt tilgang av flere personer som ikke er autorisert, skal nødvendige tekniske tiltak iverksettes.
- Loggene og autorisasjonsregister skal sikres mot endring og sletting av uautorisert personell.

For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logg over følgende:

- Autorisert bruk av informasjonssystemene skal registreres.
- Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet.
- Nettverksoperativsystemer skal registrere alle forsøk på uautorisert bruk.
- Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk.
- Bruk av selvautorisering til behandlingsrettet helseregister skal registreres.
- Loggene skal sikres mot endring og sletting av uautorisert personell.

Følgende skal som minimum registreres i loggene:

- entydig identifikator for den autoriserte brukeren
- rollen den autoriserte brukeren har ved tilgangen
- virksomhetstilhørighet
- organisatorisk tilhørighet til den som er autorisert
- type opplysninger det er gitt tilgang til
- hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer
- grunnlaget for tilgangen
- tidspunkt og varighet for tilgangen

Ved bruk av tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende logges hos virksomhetene:

- person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene
- hvorfor helseopplysningene er hentet frem
- hvilke tidsperioder vedkommende har hentet frem helseopplysningene

Alle logger skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister.

5.4.5 Styring og håndtering av tekniske sårbarheter

Styring og håndtering av tekniske sårbarheter skal følge prosedyrene for endingsstyring. Virksomheten skal ha prosedyrer for å skaffe seg informasjon om tekniske sårbarheter i 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 prosedyrer og operative tiltak som ivaretar:

- Ansvaret for: overvåkning, risikovurdering, korrigering og koordinering
- Hvordan virksomheten skal reagere og varsle om sårbarheter
- Prioritering og etablering av tidslinje for korrigering
- Alle korrigeringer bør testes før de implementeres

5.4.6 Sikkerhetsrevisjon av informasjonssystemer

Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner. Det skal foreligge en godkjent plan for sikkerhetsrevisjoner.

Sikkerhetsrevisjonen skal som minimum omfatte vurderinger av:

- Plassering av ansvar og organisering av sikkerhetsarbeidet
- Kvalitet på sikkerhetsmål og sikkerhetsstrategi
- Overholdelse av prosedyrer for bruk av informasjonssystemer og helse- og personopplysninger
- Resultat av opplæring
- Forvaltning og bruk av helse- og personopplysninger
- Tilgang til helse- og personopplysninger og tiltak mot uautorisert innsyn
- Testing, analysering og vurdering av hvor effektive de tekniske og organisatoriske sikkerhetstiltak er
- Ivaretakelse av informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og leverandører

Resultatene og konklusjonene fra sikkerhetsrevisjonene skal dokumenteres. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemene som ikke er forutsatt, skal dette behandles som avvik.

5.5 Kommunikasjonssikkerhet

5.5.1 Styring av nettverkssikkerhet

Nettverkssikkerhet er et sentralt tiltak for å sikre behandling av helse- og personopplysninger.

Virksomheten skal tydelig definere hvilke krav som gjelder for nettverkssikkerheten, og tiltakene som iverksettes skal være basert på en risikovurdering.

5.5.2 Sikring av nettjenester

Ved tilkobling til nett utenfor virksomheten skal det etableres tekniske tiltak som ivaretar at:

- Kun eksplisitt angitt tillatt trafikk kan passere, annet stoppes
- Minst to uavhengige, tekniske tiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne få uautorisert tilgang til og/eller kunne endre eller slette helse- og personopplysninger.
- Trafikk kan ikke passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra virksomhetens systemer.
- Logging iverksettes for å kontrollere at regler ikke brytes; ved brudd stenges kanalen inntil ny sikker løsning finnes.

5.5.3 Meldingsformidling

Det må 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 er ansvarlig for:

- Egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging.
- Tjenesten skal ikke kunne formidle program som inneholder virus e.l.
- Sikker overføringskryptering ende-til-ende.
- Rett adressering.
- Ved behov skal meldingen eller e-posten være signert på en slik måte at virksomheten ikke kan benekte å ha sendt den.
- Avviksrapportering i forbindelse med feilsending.
- Melding eller e-post avleveres i avtalt format.

Mottaker er ansvarlig for:

- Egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging.
- Ivareta overføringskryptering ende-til-ende.
- Ved behov skal mottaket registreres slik at mottaker ikke kan benekte å ha mottatt meldingen eller e-posten.

- Avviksrapportering i forbindelse med feil, dvs. mottak av melding eller e-post som ikke er adressert til virksomheten.
- Melding eller e-post mottas i avtalt format.

Meldingsformidler er ansvarlig for:

- Melding eller e-post kun avleveres til adressaten.
- Melding eller e-post skal ikke endres eller destrueres under transport fra avsender til mottaker.
- Melding eller e-post skal ikke kunne leses av andre enn avsender og mottaker.
- Melding eller e-post skal avleveres innen avtalte tidsfrister fra avsendelse.
- Avviksrapportering i forbindelse med alle ovenstående punkter.

5.5.4 E-post, SMS og sosialmedier

Virksomheten skal iverksette tiltak for å forhindre at helseopplysninger tilgjengeliggjøres ved hjelp av e-post, SMS eller andre ukrypterte kanaler.

- Virksomheten skal forsikre seg om ved tekniske tiltak og organisatoriske tiltak at e-post ikke inneholder identifiserbare helseopplysninger.
- Logging skal iverksettes for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik og personalmessige konsekvenser skal vurderes.

5.5.5 Tilkobling til Internett

Virksomheten skal iverksette tiltak:

- Tekniske tiltak som sikrer at Internett-tjenesten er logisk atskilt fra der helse- og personopplysninger behandles.
- Logging iverksettes for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik og personalmessige konsekvenser skal vurderes.

5.6 Digital kommunikasjon med pasienter/bruker

Ved digital kommunikasjon med pasienten er virksomheten ansvarlig for at:

- Samtykke fra pasienten/brukeren er innhentet til å formidle helse- og personopplysninger elektronisk. Samtykke skal innhentes i tråd med regler for samtykke. Samtykke fra pasienten/brukeren er etter denne Normen det eneste grunnlaget for datakommunikasjon med pasienter/brukere. Samtykket kan trekkes tilbake når som helst.
- Dersom pasient/bruker har oppgitt digital kontaktinformasjon kan dette anses som et samtykke til at virksomheten kan sende timepåminnelse per SMS. Videre skal virksomheten påse at det gjennomføres tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker i SMS-løsning for påminnelse om timeavtale og annet administrativt innhold. Det skal legges til rette for at pasient/bruker kan melde fra til virksomheten om at de ikke ønsker å motta slike meldinger. Den samlede informasjonen i meldingen må vurderes ut fra om innholdet totalt sett kan medføre brudd på taushetsplikten.

- Det gjennomføres tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker. Den samlede informasjonen i meldingen må vurderes ut fra om innholdet totalt sett kan medføre brudd på taushetsplikten.
- Pasienten/brukeren entydig identifiseres.
- Tekniske tiltak iverksettes slik at all kommunikasjon krypteres.
- Det ikke skal kunne kommuniseres samtidig med andre parter enn den angitte pasient/brukeren.
- Helse- og personopplysninger ikke stilles til rådighet på en slik måte at pasient/bruker er avhengig av å lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen.

5.7 Leverandørforhold og avtaler

I dette punktet omtales kun de avtalemessige forhold som angår informasjonssikkerhet. Det gjøres oppmerksom på at kravene i kapittel 5.7 (med unntak av 5.7.2 Databehandler) vil gjennomgå en fullstendig revidering i neste versjon av Normen, og kravene bør derfor leses som veiledende krav.

Under er listet eksempler på kommunikasjonsparter hvor det utveksles identifiserbare helse- og personopplysninger, og/eller parter som har/får adgang til utstyr og/eller programvare hvor slike opplysninger behandles. Det skal inngås skriftlige avtaler med disse, dersom ikke annet er angitt. Avtalene skal inkludere forpliktelser om at partene skal oppfylle de krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet, samt regulering av sanksjoner ved brudd på Normen og avtalen for øvrig.

- Leverandør av kommunikasjonstjenester, f.eks. Norsk Helsenett.
    - For virksomheter innen sektoren som ved tilknytningsavtale med Norsk Helsenett har forpliktet seg til å tilfredsstille kravene i dette dokument, er ingen særskilt avtale om informasjonssikkerhet nødvendig for kommunikasjon via helsenettet.
- Databehandlere, som utfører behandling av helse- og personopplysninger på vegne av virksomheten.
- Leverandører av utstyr og/eller programvare som må ha adgang for vedlikehold, feilretting, oppdatering, ved hjelp av online tilkobling og/eller fysisk oppmøte.
- Sikkerhetsleverandører.
- Forutsatt at kravene under kap. 5.6 oppfylles, kreves det ikke særskilt avtale med hver enkelt pasient/bruker.
- Studenter og stipendiater som ikke er underlagt dataansvarliges instruksjonsmyndighet

5.7.1 Leverandør av kommunikasjonstjenester

Leverandøren har selvstendig ansvar for:

- at alle tilknyttede virksomheter tilfredsstiller kravene i dette dokument, eller å legge inn tekniske tiltak som hindrer tilknyttede virksomheter, som ikke tilfredsstiller kravene, i å utsette øvrige tilknyttede virksomheters helse- og personopplysninger for risiko.

- at kun virksomheter og/eller tjenester som har avtale med leverandøren får adgang til leverandørens kommunikasjonsnett.
- at kommunikasjonspakker, dvs. meldinger, e-post, online kommunikasjon o.l., kun overføres til oppgitt autentisert adressat.
- tilstrekkelig kapasitet og alternative kommunikasjonslinjer slik at kommunikasjonspakkene er tilgjengelige for mottaker ved behov (meldinger leveres innen oppgitte tidsfrister, online kommunikasjon skjer uten brudd, mv.).
- at det er etablert tekniske tiltak som sikrer at kommunikasjonspakkerikke blir endret, skadet, ødelagt og/eller forsvinner i overføringen.
- at det er etablert tekniske tiltak og organisatoriske tiltak som hindrer at andre kan foreta angrep via leverandørens kommunikasjonsnett.

5.7.2 Databehandler

Databehandler har et selvstendig ansvar for informasjonssikkerhet og for ivaretakelse av den registrertes personvern.

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

5.7.2.1 Valg av databehandler

Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven.

Tilstrekkelige garantier betyr at databehandleren oppfyller kravene i lov og forskrift samt Normens kapittel 3 og 4, og de kravene fra Normen som er relevante for det aktuelle avtaleforhold.

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 kan motsette seg slike endringer.

For databehandleravtaler utenfor EU/EØS vil særlige vilkår gjelde. Informasjon om dette finnes hos Datatilsynet.

5.7.2.2 Databehandlers underleverandører

Databehandleren er ansvarlig for at hans underleverandører oppfyller sine forpliktelser.

Underleverandør har selvstendig ansvar for informasjonssikkerhet og for ivaretakelse av de registrertes personvern. Underleverandører har samme plikter som databehandler etter databehandleravtalen. Dette skal reguleres i avtale mellom Databehandler og Underleverandør.

5.7.2.3 Innhold i databehandleravtale

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

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

Det skal fremgå av avtalen at databehandler forplikter seg til å oppfylle kravene i Normen.

Databehandleravtalen skal beskrive:

- Databehandlers oppgaver
- Hensikten med behandlingen av helse- og personopplysninger
- Varigheten av behandlingen
- Behandlingens formål og art
- Typen personopplysninger
- Kategorier av registrerte
- Dataansvarliges rettigheter og plikter

Databehandleravtalen skal regulere:

- Konkrete sikkerhetstiltak
- Databehandler skal på eget initiativ treffe alle tiltak som er nødvendig for å sikre god informasjonssikkerhet, herunder å følge kravene i Normen
- Databehandler skal bare kunne overføre personopplysningene til utlandet etter instruks fra den dataansvarlige
- Databehandler skal bare autorisere personer som er underlagt taushetsplikt for behandling av helse- og personopplysninger
- Krav til bruk av underleverandører (annen databehandler)
- Dataansvarlig skal sikres innsynsrett for å forsikre seg om at kravene etterleves.

Databehandleravtalen skal regulere at databehandler har plikt til å bistå med/i:

- tekniske og organisatoriske tiltak for å utøve den registrertes rettigheter
- relevante tekniske og organisatoriske tiltak for å sikre god informasjonssikkerhet
- å melde brudd på personvernet til Datatilsynet
- å varsle den registrerte om brudd på personvernet
- dokumentasjon av allerede gjennomført relevant personvernkonsekvensvurdering eller gjennomføring av personvernkonsekvensvurdering
- forhåndsdrøftinger med Datatilsynet
- slette eller tilbakelevere personopplysningene etter instruks
- gjøre tilgjengelig all informasjon som viser at pliktene etter databehandleravtalen er ivaretatt
- å bidra i sikkerhetsrevisjoner
- å bidra i inspeksjoner
- endring av instrukser fra den dataansvarlige er som er i strid med lovverket

En databehandler som også er en leverandør av et system eller en tjeneste som krever en personvernkonsekvensvurdering skal fremlegge dette eller bistå med å utarbeide dette.

5.7.2.4 Databehandlers oversikt over behandlinger

Databehandler skal føre en oversikt over alle kategorier av behandlingsaktiviteter som utføres på vegne av en dataansvarlig. Oversikten skal inneholde:

- Navnet på og kontaktopplysningene til databehandleren
- Navnet på dataansvarlig som databehandleren opptrer på vegne av
- Dataansvarliges personvernombud
- Kategoriene av behandling utført på vegne av hver dataansvarlig
- Overføring av personopplysninger til utlandet
- Beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene

Oversikten skal være skriftlig og kan være digital.

5.7.2.5 Databehandlers øvrige plikter

Dersom databehandler behandler helse- og personopplysninger fra flere virksomheter skal databehandler ved hjelp av tekniske tiltak som ikke kan overstyres av brukerne ivareta at:

- det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering.
- ingen andre enn databehandleren, de som arbeider under databehandlerens instruksjonsmyndighet og virksomhetene selv har tilgang til virksomhetens opplysninger.

Databehandler skal uten ugrunnet opphold melde avvik på personopplysningssikkerhet til dataansvarlig.

5.7.3 Leverandører

Virksomheten skal for å ivareta konfidensialitet, integritet og tilgjengelighet for helse- og personopplysninger forsikre seg om at:

- leverandørens personale har undertegnet taushetserklæring som innebærer en absolutt taushetsplikt med henblikk på alle helse- og personopplysninger.
- leverandøren etterlever Normen med tanke på dataansvarliges plikter vedrørende sikkerhetsrevisjoner og avviksbehandling.
- leverandørens utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett eller medbrakt utstyr som knyttes til virksomhetens utstyr, ikke har ondsinnet programvare som inneholder virus e.l. og at utstyret er sikret mot adgang fra uvedkommende.
- leverandøren kun skal få adgang etter særskilt tillatelse fra virksomheten i hvert enkelt tilfelle, og kun adgang til de enheter hvor det er behov.
- all adgang skal skje under overvåking fra virksomhetens personale.
- tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes når leverandøren utfører arbeid på virksomhetens utstyr/programvare, slik at virksomhetens oppgavebehandling ivaretas.

5.7.4 Sikkerhetsleverandører

Den dataansvarlige skal etablere nødvendige sikkerhetstiltak. Et alternativ til egen etablering av sikkerhetstiltak kan være å få utført sikkerhetsoppgaver hos en leverandør hvor fordeling av oppgaver mellom virksomheten og leverandøren til sammen skal tilfredsstille kravene i

Normen. En sikkerhetsleverandør kan for eksempel utføre oppgavene i kap. 5.7.2 eller andre deler av Normen.

Med sikkerhetsleverandøren skal det inngås avtale om gjennomføring av konkrete sikkerhetsoppgaver hvor følgende avtalefestes:

- Hvilke sikkerhetsoppgaver som er omfattet og ansvarsforholdene for disse.
- Beskrivelse av leverandørens løsning i form av konfigurasjonskart.
- Dokumentert risikovurdering som viser at virksomhetens nivå for akseptabel risiko samt Normens sikkerhetsnivå er etablert.

Sikkerhetsleverandøren skal etterleve kravene i kap. 5.7.2.

5.7.5 Samarbeid mellom virksomheter om behandlingsrettede helseregistre

To eller flere virksomheter kan samarbeide om felles journal som skal erstatte virksomhetenes interne journal. Virksomhetene skal da inngå skriftlig avtale om:

- hva samarbeidet omfatter
- hvordan pasientens eller brukerens rettigheter skal ivaretas
- hvordan helseopplysningene skal behandles og sikres, også ved endringer i eller opphør av samarbeidet
- databehandlingsansvaret

Den eller de virksomhetene som har den faktiske kontrollen med og ansvaret for databehandlingen er dataansvarlig(e). Dersom alle virksomhetene er dataansvarlige, kan det utpekes en representant som fungerer som kontaktpunkt for henvendelser fra pasienter og/eller brukere.

Når en kommune og en eller flere private tjenesteytere som yter tjenester på vegne av kommunen tar i bruk felles journal for å oppfylle journalføringsplikten skal kommunen være dataansvarlig, fordi kommunen bestemmer formålet med og bruken av felles journal.

Samarbeid om felles journal åpner for mulighet for bruk av et behandlingsrettet helseregister når to eller flere virksomheter samarbeider om å yte helse- og/eller omsorgstjenester, tilsvarende til tidligere virksomhetsovergripende pasientjournal i formalisert arbeidsfellesskap. Forskrift om virksomhetsovergripende pasientjournal i formalisert arbeidsfellesskap er nå opphevd, men virksomheter som har inngått avtale i henhold til forskriften kan fortsette dette samarbeidet.

5.7.6 Tilgang til helseopplysninger mellom virksomheter

Det kan etableres tilgang til helseopplysninger mellom virksomheter. Med tilgang menes at helsepersonell i en virksomhet gis adgang til direkte elektronisk å hente frem helseopplysninger om pasienter/brukere registrert ved en annen virksomhet.

Reglene for tilgangen mellom virksomheter som omtales her gjelder ikke for tilgang til helseopplysninger mellom virksomheter som samarbeider om et felles behandlingsrettet helseregister, jf. kapittel 5.7.5.

Forskrift om tilgang til helseopplysninger mellom virksomheter fastsetter at virksomhetene skal inngå avtale om tilgang til helseopplysninger mellom virksomheter.

Avtalen skal være skriftlig og minst angi:

- hva avtalen gjelder
- hvilke behovs- og risikovurderinger som ligger til grunn for avtalen
- hvilke behandlingsrettede helseregistre, deler av registre eller typer av opplysninger avtalen omfatter
- rutiner og fordeling av oppgaver for å ivareta kravene i forskriften

Før det åpnes for tilgang til helseopplysninger mellom virksomheter skal begge virksomhetene gjennomføre risikovurdering for å påse at pasienten/brukerens personvern ivaretas. Risikovurderingene skal minst omfatte risiko for brudd på taushetsplikten og svekket informasjonssikkerhet.

5.8 Håndtering av informasjonssikkerhetsbrudd

5.8.1 Avvikshåndtering

Virksomhetens ledelse, eller det organ ledelsen bemyndiger, skal behandle avvik med det formål å gjenopprette normal tilstand, fjerne årsaken til avviket og å hindre gjentagelse.

Avvikshåndteringen iverksettes ved sikkerhetsbrudd og/eller når behandling av helse- og personopplysninger er utført i strid med gjeldende regelverk, retningslinjer eller prosedyrer. Avvikshåndtering kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige prosedyrer.

- Hver enkelt medarbeider er ansvarlig for å rapportere oppdagede avvik på fastsatt skjema til nærmeste leder, eller annen utpekt person/organ.
- For hvert rapportert avvik skal det foretas en innsamling av fakta om hendelsesforløpet og foretas en vurdering som grunnlag for iverksettelse av korrigerende tiltak.
- Det skal foreslås tiltak og eventuelle alternative tiltak med beskrivelse av plan for gjennomføring for å gjenopprette normal tilstand og forhindre gjentagelse.
- Tiltak og plan på det nivå som er gjennomførbart skal vedtas. Tiltaket skal være slik at det hindrer eller reduserer sannsynligheten for gjentagelse.
- Tiltaket iverksettes iht. plan med rapportering til virksomhetens ledelse, eller det organ ledelsen bemyndiger.
- Det sendes statusrapport til virksomhetens ledelse eller det organ ledelsen bemyndiger, som dokumenterer resultatet av avvikshåndteringen.
- Ved gjentatte avvik skal det gjennomføres ny risikovurdering.

Systemer for avvikshåndtering må kunne håndtere meldinger om avvik selv om de verken har ført til – eller potensielt kunne ført til – skade for en identifisert pasient

Ved brudd på personvernet, som har medført konsekvenser for den registrerte, skal den dataansvarlige melde avviket til Datatilsynet innen 72 timer etter å ha fått kjennskap til det.

Meldes avviket senere, skal årsaken til forsinkelsen oppgis. Det er ikke nødvendig å melde avvik som ikke har medført noen konsekvenser for den registrerte.

Meldingen til Datatilsynet skal inneholde:

- beskrivelse av bruddet på personopplysningssikkerheten inklusive
    - kategorier av registrerte som er berørt
    - omtrentlig antall registrerte som er berørt
    - hvilke typer personopplysninger bruddet omfatter
    - omtrentlig antall registrerte som er berørt
- navnet på og kontaktopplysningene til personvernombudet eller annen kontakt der mer informasjon kan innhentes
- beskrivelse av de sannsynlige konsekvensene av avviket
- beskrivelse av tiltak den dataansvarlige har iverksatt eller foreslår å iverksette for å håndtere og redusere eventuelle skadevirkninger av avviket

Melding til Datatilsynet kan gis trinnvis om det ikke er mulig å gi all informasjon samtidig.

5.8.2 Underretting til den registrerte

Den registrerte skal varsles om avviket har medført sletting, endring eller uautorisert tilgjengeliggjøring/tilgang helse- og personopplysningene.

Varselet skal inneholde:

- Beskrivelse av bruddet på alminnelig språk
- Kontaktopplysningene til personvernombudet eller en annen rolle som kan gi nærmere informasjon
- Beskrivelse av konsekvensene av avviket.
- Beskrivelse av gjennomførte eller planlagte tiltak for å håndtere og redusere skadevirkninger.

Det er ikke nødvendig å varsle den registrerte dersom:

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

5.9 IKT-beredskap

Manglende tilgjengelighet til helse- og personopplysninger kan medføre skader både for virksomheten og for virksomhetens brukere. Virksomheten må derfor sørge for at nødvendige helse- og personopplysninger er tilgjengelige også ved stopp i hele eller deler av det elektroniske informasjonssystemet.

For å kunne etablere nødvendige prosedyrer for å ivareta tilgjengelighet ved stopp må virksomheten foreta en kartlegging av de enkelte informasjonssystemer med henblikk på kritikalitet. Kritikaliteten må vurderes både for virksomheten som sådan og for dens brukere. De systemer med tilhørende helse- og personopplysninger som virksomheten benytter, skal klassifiseres:

- Systemer hvor stopp av tjeneste kan være kritiske, for eksempel
    - livstruende for pasient
    - kritisk for virksomhetens drift
- Systemer hvor stopp av tjeneste får alvorlige konsekvenser, f.eks. kan medføre
    - feilbehandling av pasient
    - betydelig merarbeid for personell
    - tapt effektivitet
    - tapte inntekter for virksomheten
- Systemer hvor stopp av tjeneste kan føre til svekkelse av pasientens tillit.
- Systemer hvor lengre stopp kan aksepteres.
- Systemer som ikke prioriteres.

Det skal også kartlegges hvilke andre systemer de klassifiserte systemene er avhengige av. Disse skal ha samme klassifisering og nivå for akseptabel risiko som de kritiske systemene. For hver aktuell klassifisering skal ledelsen fastsette nivå for akseptabel risiko for tilgjengelighet, som et minimum en maksimal avbruddstid.

Med utgangspunkt i klassifiseringen av informasjonssystemene skal virksomheten etablere nødprosedyrer:

- Alternativ drift uten bruk av informasjonssystemene.
- Alternativ drift med delvis støtte fra informasjonssystemene.

Disse prosedyrene skal minimum testes årlig.

Virksomhetens ledelse skal, iht. klassifiseringen ovenfor, vurdere å etablere alternativ løsning som sikrer kontinuitet av informasjonssystemene ved uforutsett driftsstans.

6 Vedlegg

6.1 Definisjoner

Ord og uttrykk som er definert nedenfor er skrevet med kursiv i Normen. 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 ”**advarsel**” menes i Normen en skriftlig reaksjon fra virksomheten overfor en ansatt som har brutt prosedyrer e.l. Det skal klart fremgå at det dreier seg om en advarsel, årsaken til advarselen og hva som kan bli konsekvensene av nye brudd på prosedyrer e.l.

Med ”**akseptabel risiko**” menes i Normen hvor stor risiko sektoren kan akseptere for at det inntreffer en hendelse som kan forårsake brudd på konfidensialitet, tilgjengelighet eller integritet for helse- og personopplysninger. Risikoens størrelse avhenger av hvor stor sannsynlighet det er for at hendelsen skal inntreffe og av konsekvensen av en slik hendelse. Normen beskriver et nivå for akseptabel risiko i sektoren. Hver enkelt virksomhet må foreta en konkret vurdering av hvordan akseptabel risiko for vedkommende virksomhet skal oppnås.

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.

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

Med ”**autorisere/autorisert/autorisasjon**” menes i Normen at en person ~~i en bestemt rolle~~ kan gis eller er gitt bestemte rettigheter til lesing, registrering, retting, sletting og/eller sperring av helse- og personopplysninger. Autorisasjon kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra tjenstlig behov og er i henhold til bestemmelser om taushetsplikt.

Med ”**avvik**” menes i Normen enhver håndtering av helse- og personopplysninger som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, 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 av 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). Se også elektronisk pasientjournal (EPJ) og tjenestedokumentasjon.

Med ”**biometriske opplysninger**” menes i Normen personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger.

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.

-E-

Med ”**elektronisk pasientjournal (EPJ)**” menes i Normen elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp, se også helsepersonelloven § 40 første ledd og forskrift om pasientjournal § 3 a). Dette inkluderer både somatisk og psykiatrisk journal o.a., hver for seg eller samlet. Se også behandlingsrettet helseregister.

Med ”**elektronisk pasientjournalsystem (EPJ-system)**” menes i Normen elektroniske systemer med nødvendig funksjonalitet for å registrere, søke frem, presentere, kommunisere, rette og slette opplysninger i elektronisk pasientjournal (EPJ). Dette inkluderer både radiologisystemer, systemer for somatisk og psykiatrisk journal, pasientadministrative systemer og andre systemer som inneholder helseopplysninger.

-F-

Med ”**fagsystem**” menes i Normen en applikasjon eller et IT-system som behandler helse- og personopplysninger. Begrepet systemløsning brukes også om et fagsystem. Eksempler på fagsystem er: pleie- og omsorgssystem (PLO), legekontorsystem og barnevernsystem. Opplysninger i ulike fagsystemer kan både utgjøre elektronisk pasientjournal (EPJ) og annen tjenestedokumentasjon.

Med **"felles journal"** menes i Normen samarbeid mellom to eller flere virksomheter om behandlingsrettet helseregister som skal erstatte virksomhetens interne journal, jf. pasientjournalloven § 9.

Med ”**forvaltningsorgan**” menes i Normen et hvert organ for stat eller kommune. Privat rettssubjekt regnes som forvaltningsorgan i saker hvor det treffer enkeltvedtak eller utferdiger forskrift, jf. forvaltningsloven § 1.

-G-

Med ”**genetiske opplysninger**” menes i Normen personopplysninger om en fysisk persons nedarvede eller ervervede genetiske egenskaper som gir unik informasjon om den aktuelle fysiske personens fysiologi eller helse, og som særlig er framkommet etter analysering av en biologisk prøve fra den aktuelle fysiske personen.

-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 og/eller personopplysninger innenfor Normens virkeområde.

Med ”**helsenettet**” menes i Normen nettverket som tilbys av Norsk Helsenett SF.

Med ”**helseopplysninger**” menes i Normen personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes 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 ”**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-

Med "**indirekte identifiserbare helseopplysninger**" 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, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet (jf. helseregisterloven § 2 b). For å regnes som indirekte identifiserbare helseopplysninger, skal dataene være bearbeidet slik at de uten løpenummer fremstår som anonyme.

Med "**integritet**" menes i Normen at helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting og være korrekte, oppdaterte, relevante og tilstrekkelige som grunnlag for å yte helsehjelp.

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 "**kategorier av behandlinger**", se behandlingens art

Med "**kategorier av registrerte**" menes i Normen at personer er kategorisert i grupper og undergrupper. For eksempel personer etter: pasient, bruker, beskjeftigelse, dødsårsak, funksjonshemming, nasjonalitet, årstall, føde- eller oppvekststed mv.

Med "**kjernejournal**" menes i Normen et elektronisk sentralt virksomhetsovergripende behandlingsrettet helseregister som samler et begrenset sett relevante helseopplysninger som er nødvendig for å yte forsvarlig helsehjelp i ett register, jf. pasientjournalloven § 13 og forskrift om nasjonal kjernejournal (kjernejournalforskriften).

Med "**koblingsnøkkel**" menes i Normen en personentydig kode som refererer til de identifiserte opplysningene som gjør det mulig å identifisere et enkeltindivid i en fil med indirekte identifiserbare helseopplysninger.

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 "**lagringsenhet**" menes i Normen gjenstand til å lagre helse- og personopplysninger elektronisk.

Med "**leverandør**" menes i Normen juridisk enhet som yter tekniske og/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 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 ”**Norsk Helsenett**” menes i Normen Norsk Helsenett SF.

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

-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.

”**Pasientopplysninger**”, se helse- og personopplysninger**.**

Med ”**personlig kvalifisert sertifikat**” menes i Normen to-faktor autentisering hvor en faktor er dynamisk basert på kvalifiserte sertifikater og ellers tilfredsstiller kravene til sikkerhetsnivå 4 i ”Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor”.

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 fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Med ”**personopplysningssikkerhet**” menes i Normen tekniske og organisatoriske tiltak som er iverksatt for å sikre individets personvern rettigheter.

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 prosess.

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.

Med "**pseudonymisering**" menes i Normen behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person.

-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 og tjenestemottaker. En ansatt kan være omfattet av begrepet.

-S-

Med "**samtykke**" menes i Normen fra den registrerte 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 "**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.

-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 tilgjengelige 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 iverksettes 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 ”**tjenestedokumentasjon**” menes i Normen dokumentasjon for planlegging, kartlegging, oppfølging og informasjonsutveksling som vedrører tjenestemottakerens søknad, praktiske og medisinske problemer, behov, ressurser, tiltak i form av helsehjelp, hjelpemidler, mm. Sammen med elektronisk pasientjournal (EPJ) vil tjenestedokumentasjonen utgjøre dokumentasjonsplikten etter helsepersonelloven mv.

Med ”**tjenstlig behov**” menes i Normen at personer med nærmere bestemte arbeidsoppgaver, trenger nødvendige helse- og personopplysninger for å yte helsehjelp, omsorgstjeneste og/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.

-U-

Med ”**ulovlig tilegnelse**” menes i Normen å bryte forbudet mot å lese, søke eller på annen måte tilegne seg, bruke eller besitte helseopplysninger, uten at det er begrunnet i helsehjelpen til pasienten, administrasjon av slik hjelp eller særskilt hjemmel i lov eller forskrift, jf. helseregisterloven § 18, pasientjournalloven § 16 og helsepersonelloven § 21a.

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.

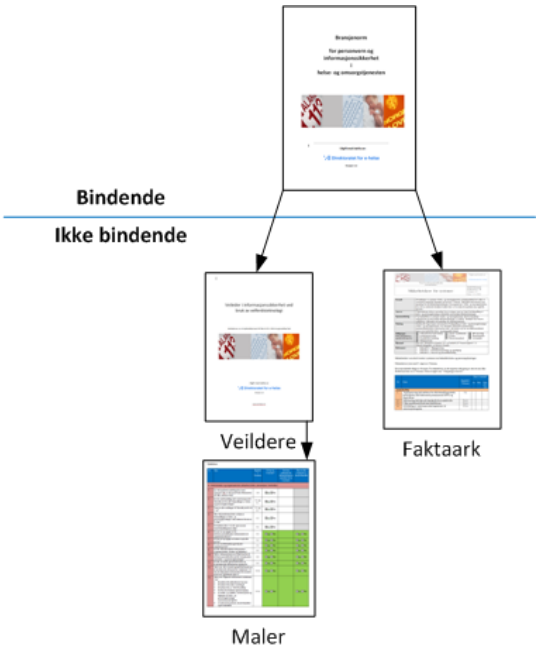
Med "**virksomhetsovergripende pasientjournal**" menes i Normen behandlingsrettet helseregister hvor helsepersonell, og personell som yter helse- og omsorgstjenester etter helse- og omsorgstjenesteloven, nedtegner eller registrerer opplysninger om pasient og bruker, jf. helsepersonelloven § 39 og § 40.

6.2 Støttedokumenter

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

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

Figuren nedenfor viser dette prinsippet:



6.2.1 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.

6.2.2 Veiledere

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

6.2.3 Maler

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

6.3 Referanser

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

NSM sin anbefaling til kryptoløsninger: kortliste-krav-til-krypto

NSM veileder i krypto krav:
https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf

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

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

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

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

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

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

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

EU kommisjonens artikkel 29 gruppe:
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

6.4 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 iverksettes 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 virksomheter.

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 lægeforening, representanter for de regionale helseforetak, 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 overnevnte 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 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.

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.

Besøksadresse
Direktoratet for e-helse
Verkstedveien 1
0277 Oslo

Kontakt
sikkerhetsnormen@ehelse.no