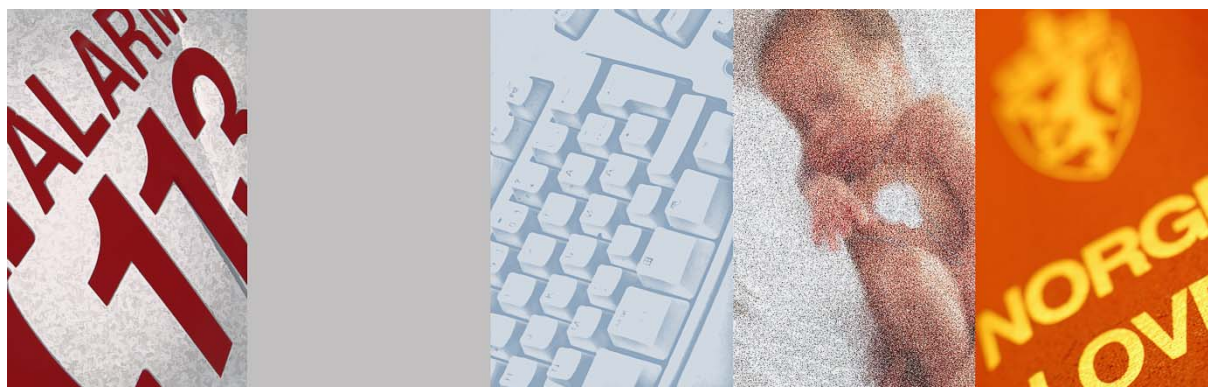


# Norm

## for informasjonssikkerhet

*Helse-, omsorgs- og sosialsektoren*



---

**Utgitt med støtte av:**



Oslo, 2010

## FORORD

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

## FORORD TIL 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 virksomhetsovergrepene *behandlingsrettede helseregistre*
- etablering av virksomhetsovergrepene *behandlingsrettede helseregistre* for helsepersonell med formalisert arbeidsfellesskap

Slike forskrifter er ikke gitt og overnevnte temaer behandles ikke i *Normen*.

*2.juni 2010*

## Innhold

### *DEL I: INNLEDNING*

<b>1</b>	<b>OM NORMEN.....</b>	<b>1</b>
1.0	BAKGRUNN.....	1
1.1	DEFINISJONER .....	1
1.2	LOVGRUNNLAG .....	9
1.3	FORMÅL .....	10
1.4	MÅLGRUPPE – HVEM NORMEN GJELDER FOR.....	10
1.5	VIRKEOMRÅDE – HVA NORMEN REGULERER .....	10
1.6	JURIDISK BINDEDE VED AVTALE .....	11
<b>2</b>	<b>OM FAKTAARK OG VEILEDERE.....</b>	<b>11</b>
2.1	FAKTAARK .....	11
2.2	VEILEDERE .....	12
2.3	FORHOLDET TIL NORMEN .....	12

### *DEL II: ARBEIDET MED INFORMASJONSSIKKERHET*

<b>3</b>	<b>OVERSIKT.....</b>	<b>13</b>
3.1	ANSVAR .....	13
3.2	OVERSIKT OVER OPPGAVER SOM OMFATTES AV DET DAGLIGE ANSVARET FOR INFORMASJONSSIKKERHET 13	
3.3	DOKUMENTASJON .....	14
3.3.1	<i>Styringsdokumenter:</i> .....	14
3.3.2	<i>Gjennomføringsdokumenter:</i> .....	14
3.3.3	<i>Kontrolldokumenter:</i> .....	15
3.3.4	<i>Arkivering</i> .....	15
<b>4</b>	<b>STYRENDE DEL .....</b>	<b>16</b>
4.1	STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET .....	16
4.2	SIKKERHETSMÅL .....	16
4.2.1	<i>Formål</i> .....	16
4.2.2	<i>Overordnede føringer for virksomhetens bruk av informasjonsteknologi</i> .....	16
4.2.3	<i>Sentrale sikkerhetsmål</i> .....	17
4.3	SIKKERHETSSTRATEGI .....	17
4.4	NIVÅ FOR AKSEPTABEL RISIKO .....	17
4.4.1	<i>Konfidensialitet</i> .....	17
4.4.2	<i>Tilgjengelighet</i> .....	17
4.4.3	<i>Integritet</i> .....	18
4.4.4	<i>Kvalitet</i> .....	18
4.5	OVERSIKT OVER BEHANDLINGER AV HELSE- OG PERSONOPPLYSNINGER .....	18
4.6	RISIKOVURDERINGER .....	19
<b>5</b>	<b>GJENNOMFØRENDE DEL .....</b>	<b>20</b>
5.1	ANSVARLIGGJØRING AV ANSATTE – TAUSHETSPLIKT .....	20
5.2	TILGANGSSTYRING .....	20
5.2.1	<i>Autentisering</i> .....	21
5.2.2	<i>Autorisering</i> .....	21
5.2.3	<i>Tilgang</i> .....	22
5.2.4	<i>Utlevering av helse- og personopplysninger til andre enn virksomhetens og forvaltningsorganets eget personell</i> .....	23
5.2.5	<i>Regulering av bruk</i> .....	23
5.2.6	<i>Kontrollerende tiltak</i> .....	23
5.3	BEHANDLING AV HELSE- OG PERSONOPPLYSNINGER .....	24

5.3.1	<i>Prosedyre for bruk av informasjonssystemet</i>	24
5.3.2	<i>Etterkontroll av tilgangsstyring</i>	24
5.3.3	<i>Informasjon og samtykke</i>	24
5.3.4	<i>Den registrertes innsyn i hendelsesregistre</i>	25
5.4	<b>SIKRING AV OMRÅDER OG UTSTYR</b>	25
5.4.1	<i>Nøkler/adgangskort</i>	25
5.4.2	<i>Brukerutstyr (PC og printere - stasjonære)</i>	25
5.4.3	<i>Driftsutstyr (servere og nettverksutstyr)</i>	25
5.4.4	<i>Mobilt utstyr og hjemmekontor</i>	25
5.4.5	<i>Medisinsk teknisk utstyr</i>	26
5.5	<b>ETABLERING OG DRIFT AV INFORMASJONSSYSTEMET</b>	26
5.5.1	<i>Konfigurasjonskontroll</i>	26
5.5.2	<i>Konfidensialitet og integritet</i>	27
5.5.3	<i>Tilgjengelighet</i>	28
5.5.4	<i>Kvalitet</i>	29
5.6	<b>OPPLÆRING OG KOMPETANSE</b>	29
5.7	<b>DATAKOMMUNIKASJON</b>	29
5.7.1	<i>Tilkoblingsikkerhet</i>	29
5.7.2	<i>Meldingsformidling og e-post som inneholder sensitive personopplysninger</i>	30
5.7.3	<i>E-post som ikke inneholder sensitive personopplysninger</i>	30
5.7.4	<i>Tilkobling til Internett</i>	31
5.7.5	<i>Kommunikasjon med pasienter/brukere</i>	31
5.8	<b>AVTALER</b>	31
5.8.1	<i>Leverandør av kommunikasjonstjenester</i>	32
5.8.2	<i>Databehandler</i>	32
5.8.3	<i>Leverandører</i>	33
5.8.4	<i>Sikkerhetsleverandører</i>	33
<b>6</b>	<b>KONTROLLERENDE DEL</b>	<b>34</b>
6.1	<b>SIKKERHETSREVISJON</b>	34
6.2	<b>RISIKOVURDERING</b>	34
6.3	<b>AVVIKSHÅNDTERING</b>	34
6.4	<b>LEDELSENS GJENNOMGANG</b>	35
6.5	<b>KONTROLL AV TILGANGER</b>	36
	<b>LOV- OG FORSKRIFTSREGISTER:</b>	<b>37</b>

## ***DEL I: INNLEDNING***

### **1 OM NORMEN**

#### **1.0 Bakgrunn**

*Normen* er utarbeidet av organisasjoner (se forordet) i *sektoren* med sikte på å bidra til tilfredsstillende informasjonssikkerhet hos den enkelte *virksomhet* og i *sektoren* generelt, samt å bidra til å etablere 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. 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. Regelverket stiller også en rekke andre krav til *behandling av helse- og personopplysninger* enn det som er tema for *Normen*.

*Normen* er utviklet med basis i personopplysningslovens regler om bransjevisse adferdsnormer (jf. personopplysningsloven § 42 tredje ledd nr. 6). Disse reglene bygger i sin tur på EU-direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Direktivet er implementert i norsk lovgivning med grunnlag i Norges forpliktelser etter EØS-avtalen.

*Normen* stiller krav som detaljerer og supplerer gjeldende regelverk. Oppfylles disse kravene, er det *sektorens* oppfatning at dagens regelverk vedrørende tilfredsstillende informasjonssikkerhet oppfylles. *Normen*, og de kravene *Normen* inneholder, blir juridisk bindende ved avtale i den grad innholdet ikke allerede fremgår av lov eller forskrift, se pkt. 1.6. Slik avtale gir andre *virksomheter* grunnlag for å innrette seg i tillit til at vedkommende *virksomhet* har tilfredsstillende informasjonssikkerhet.

Det understrekes for øvrig at opplæring og bevisstgjøring av de ansatte er av vesentlig betydning for å sikre forsvarlig håndtering av *helse- og personopplysninger* i det daglige arbeidet.

#### **1.1 Definisjoner**

Register over lover og forskrifter som det refereres til i *Normen* finnes på side 37.

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 sikkerhetsbarriere. 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, integritet* eller *kvalitet* 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 ”**aktualisere/aktualisert/aktualisering**” menes i *Normen* den konkrete utnyttelsen av en tildelt *autorisasjon*, hvor formålet spesifikt skal angis. Se også *tilgang*.

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.). Opplysninger om en person regnes som anonymisert dersom identifiseringen krever uforholdsmessig stor arbeidsinnsats eller uforholdsmessige store kostnader.

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

Med ”**autorisere/autorisert/autorisasjon**” menes i *Normen* at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, 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 ”**autorisasjonsregister**” menes i *Normen* et register over utstedte *autorisasjoner* som føres av den *databelhandlingsansvarlige*.

Med ”**avidentifisert**” 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 nr. 2). For å regnes som *avidentifiserte*, skal dataene være bearbeidet slik at de uten løpenummer fremstår som anonyme.

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.

-B-

Med ”**behandling**” menes i *Normen* enhver formålsbestemt bruk av *helse- og personopplysninger*, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. helseregisterloven § 2 nr. 5 og personopplysningsloven § 2 nr. 2).

Med ”**behandlingsrettet helseregister**” menes i *Normen* journal- og informasjonssystem eller annet *helseregister* som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte *pasient* og som utføres av helsepersonell, samt administrasjon av slike handlinger, jf. helseregisterloven § 2 nr. 7. Se også *elektronisk pasientjournal (EPJ)* og *tjenestedokumentasjon*.

-D-

Med ”**databelandler**” menes den som *behandler helse- og personopplysninger* på vegne av den *databelhandlingsansvarlige*, jf. helseregisterloven § 2 nr. 9 og personopplysningsloven § 2 nr. 5). Det presiseres at en *databelandler* er en ekstern person eller *virksomhet* utenfor den *databelhandlingsansvarliges virksomhet*. Det vil si at den *databelhandlingsansvarliges* egne medarbeidere ikke er dennes *databelhandlere*.

Med ”**databelhandlingsansvarlig**” menes den som bestemmer formålet med *behandlingen* og hvilke hjelpemidler som skal brukes, hvis ikke *databelhandlingsansvaret* er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 nr. 8 og personopplysningsloven § 2 nr. 4 (her benyttes begrepet ”*behandlingsansvarlig*”). Det presiseres at det er *virksomheten* som er *databelhandlingsansvarlig* for *behandling av helse- og personopplysninger*. Ansvaret skal ivaretas av den daglige ledelsen av *virksomheten*, og *virksomheten* er pliktsubjekt.

-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 pasientjournalssystem (EPJ-system)**” menes i *Normen* elektroniske systemer med nødvendig funksjonalitet for å registrere, søke frem, presentere, kommunisere, redigere, 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 barnevernssystem. Opplysninger i ulike *fagsystemer* kan både utgjøre *elektronisk pasientjournal (EPJ)* og annen *tjenestedokumentasjon*.

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.

## -H-

”*helse- og personopplysninger*” benyttes i *Normen* som en fellesbetegnelse for *helseopplysninger* og/eller *personopplysninger* innenfor *Normens* virkeområde slik det er definert i pkt. 1.5 nedenfor.

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

Med ”*helseopplysninger*” menes i *Normen* taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson, jf. helseregisterloven § 2 nr. 1.

Med ”*helseregister*” menes i *Normen* registre, fortegnelser, m.v. der *helseopplysninger* er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen, jf. helseregisterloven § 2 nr 6.

Med ”*hendelsesregister*” menes i *Normen* et logisk *register* der hendelser i informasjonssystemet er nedtegnet, se neste definisjon.

Med ”*hendelsesregistrering*” menes i *Normen* registrering av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentakelse av sikkerhetsbrudd.

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

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

## -K-

Med ”**koblingsnøkkel**” menes i *Normen* en personentydig kode som refererer til de identifiserte opplysningene som gjør det mulig å identifisere et enkeltindivid i en *avidentifisert* fil.

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.

Med ”**kvalitet**” menes i *Normen* at *helse- og personopplysninger* må være korrekte, oppdaterte, relevante og tilstrekkelige som grunnlag for å yte helsehjelp.

## -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.

## -M-

Med ”**meldeplikt**” menes i *Normen* plikten den enkelte *databelhandlingsansvarlige* har til å melde om *behandling* av *helse- og personopplysninger* til Datatilsynet. *Meldeplikten* følger av [helseregisterloven § 29](#) og [personopplysningsloven § 31](#).

## -N-

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

Med ”**Norsk Helsenet**” menes i *Normen* Norsk Helsenet SF.

Med ”**nødrettstilgang**” menes i *Normen* en *tilgang* hvor prinsippene for tilgangsstyring ikke blir fulgt, fordi det for å avverge fare eller skade er behov for øyeblikkelig *tilgang* til *helse- og personopplysninger*, og dette ut fra de foreliggende omstendigheter må vurderes som rettmessig.

## -P-

Med ”**pasient**” menes i *Normen* en person som henvender seg til helsetjenesten med anmodning om helsehjelp, eller som helsetjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle jf. pasientrettighetsloven § 1-3, bokstav a.

Med ”**pasient/bruker**” menes i *Normen* *pasient* eller person som er i kontakt med sosialtjenesten som klient eller tjenestemottaker.

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

Med ”**personopplysninger**” menes i *Normen* opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1).

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

Med ”**pseudonymisering**” menes i *Normen* prosessen der identiteten til *helse- og personopplysninger* skjules, men likevel slik at helseopplysningene er individualisert og det lar seg gjøre å følge hver person gjennom behandling av helse- og personopplysninger uten at identiteten røpes (jf. helseregisterloven § 2 nr. 4).

## -R-

Med ”**register**” menes i *Normen* en logisk sammenstilling av opplysninger. En database eller et regneark er en teknisk løsning for et *register*.

Med ”**registrert/den registrerte**” menes i *Normen* den som opplysninger kan knyttes til, jf. personopplysningsloven § 2 nr. 6. Eksempler og begreper som brukes om *den registrerte* er søker, *pasient/bruker* og tjenestemottaker. En ansatt kan være omfattet av begrepet.

## -S-

Med ”**sektor/sektoren**” menes i *Normen* helse-, omsorgs-, og sosialsektoren eller en eller deler av de nevnte.

Med ”**sensitive personopplysninger**” 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,

jf. personopplysningsloven § 2 nr. 8).

Med ”**sikkerhetsnivå 4**” menes i *Normen* to-faktor *autentisering* hvor en faktor er dynamisk basert på kvalifiserte sertifikater og ellers tilfredsstillende kravene til sikkerhetsnivå 4 i

”Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor”.

-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 § 15, sosialtjenesteloven § 8-8 og forvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften § 2-9. *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 på sikkerhetsnivå 4* 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 ”**tilstedeværelsesregister**” menes i *Normen* et *register* som viser faktisk tilstedeværelse av personell, for eksempel *hendelsesregister* fra adgangskontroll (nøkkelkort), timeregistreringssystem og stemplingsur. *Tilstedeværelsesregisteret* kan også inneholde informasjon om bruk av mobilt utstyr og *hjemmekontor*.

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

Med ”**tjenstlig behov**” menes i *Normen* at personer med nærmere bestemte arbeidsoppgaver, trenger nødvendige *helse- og personopplysninger* for å yte helsehjelp, omsorgs- eller sosialtjeneste 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 ”**tjenstedokumentasjon**” menes i *Normen* dokumentasjon for planlegging, kartlegging, oppfølging og informasjonsutveksling som vedrører tjenstemottakerens søknad, praktiske og medisinske problemer, behov, ressurser, tiltak i form av helsehjelp, hjelpemidler, mm. Sammen med *elektronisk pasientjournal (EPJ)* vil *tjenstedokumentasjonen* utgjøre dokumentasjonsplikten etter helsepersonelloven mv. Det er ingen lovfestet dokumentasjonsplikt etter sosialtjenesteloven.

-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 § 13a og helsepersonelloven § 21a.

-V-

Med ”*virksomhet*” menes i *Normen* juridisk enhet som helseforetak, *kommune*, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse m.v.

## 1.2 Lovgrunnlag

*Normen* er først og fremst basert på personvern- og helselovgivningens krav til å etablere tilfredsstillende informasjonssikkerhet for systemer inneholdende *helse- og personopplysninger*, jf. personopplysningsloven § 13, helseregisterloven § 16 og personopplysningsforskriften kapittel 2.

Etterleves *Normen* vil den gi bidrag til *virksomhetens* internkontrollsystem vedrørende *helse- og personopplysninger*, jf. helseregisterloven § 17, personopplysningsloven § 14 og personopplysningsforskriften kap. 3. Den generelle internkontrollplikten omfatter mer, og skal sørge for at den *databehandlingsansvarlige* er i stand til å ivareta alle forpliktelser som *behandling av helse- og personopplysninger* medfører, se forskrift om internkontroll i sosial- og helsetjenesten. *Normen* dekker ikke denne internkontrollplikten i sin helhet.

*Normen* er i samsvar med bestemmelser som for *helse- og personopplysninger*:

- Pålegger *taushetsplikt* og regulerer informasjonsrett, se helsepersonelloven kapittel 5 og § 45, forskrift om pasientjournal, helseregisterloven §§ 11 til 15, pasientrettighetsloven § 5-3, spesialisthelsetjenesteloven §§ 6-1 og 6-4, kommunehelsetjenesteloven § 6-6, sosialtjenesteloven § 8-8, psykisk helsevernloven § 1-6, forvaltningsloven §§ 13 flg. og offentleglova.
- Pålegger *virksomhetene* å etablere systemer som sikrer at *taushetsplikt* mv. kan ivaretas, se spesialisthelsetjenesteloven § 3-2, tannhelsetjenesteloven § 1-3a, lov om statlig tilsyn med helsetjenesten § 3, og kommunehelsetjenesteloven § 1-3a.
- Pålegger selvstendig opplysningsplikt, se helsepersonelloven kapittel 6, kommunehelsetjenesteloven § 6-6a, smittevernloven kapittel 2, spesialisthelsetjenesteloven §§ 3-3, 3-13 og 3-15, helseregisterloven § 9, og psykisk helsevernloven § 3-10.
- Pålegger opplysningsplikt, se tannhelsetjenesteloven §§ 1-5 og 6-2, kommunehelsetjenesteloven §§ 3-4 og 6-3, spesialisthelsetjenesteloven § 6-2, forskrift med hjemmel i psykisk helsevernloven om kontrollkommisjonens virksomhet § 1-8, pasientrettighetsloven § 8-5, helseregisterloven §§ 10 og 31, og offentleglova.
- Pålegger *meldeplikt*, se helseregisterloven § 29 og personopplysningsloven § 31.
- Pålegger dokumentasjonsplikt og/eller gir regler for saksgang, kommunikasjonsformer mv., se helsepersonelloven kap. 8, psykisk helsevernloven §§ 1-8, 2-2, 4-4, 4-6, 4-7, 4-8, 4-9 og kapittel 3, pasientrettighetsloven § 3-6, helseregisterloven kapittel 5 og arkivloven.
- Gir innsynsrettigheter, se helsepersonelloven § 41, pasientrettighetsloven kapittel 5, spesialisthelsetjenesteloven § 3-11 og helseregisterloven kapittel 3 og 4.
- Setter forbud mot urettmessig tilegnelse av *helse- og personopplysninger*, jf. helseregisterloven § 13a og helsepersonelloven § 21a.
- Gir rammer for informasjonssikkerhet ved medisinsk og helsefaglig forskning, se helseforskningsloven.

Ved eventuell motstrid mellom *Normen* og til enhver tid gjeldende lover eller forskrifter, vil lov og forskrift alltid gå foran *Normen*.

### **1.3 Formål**

Formålet med *Normen* er:

1. at en *virksomhet* som etterlever og innretter seg etter *Normen* har tilfredsstillende informasjonssikkerhet for sin *behandling av helse- og personopplysninger*, og
2. at 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 tilfredsstillende informasjonssikkerhet for sin *behandling av helse- og personopplysninger*.

### **1.4 Målgruppe – hvem Normen gjelder for**

*Normen* gjelder for enhver *virksomhet* i sektoren som ved avtale har forpliktet seg til å følge *Normen*, herunder legevirksomheter, helseforetak, Arbeids- og velferdsforvaltningen (NAV), tannklinikker, sykehus, apotek, apotekkjeder, *kommuner*, fylkeskommuner, frittstående laboratorier, røntgeninstitutter, psykologpraksis, fysioterapiinstitutter, bandasjistvirksomheter, rehabiliteringsinstitusjoner, o.a., samt de nevnte *virksomheters leverandører* og andre i den grad de *behandler helse- og personopplysninger* og de 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 for *helse- og personopplysninger* som *behandles* i forbindelse med pasientbehandling, herunder medregnet også pasientadministrasjon og utlevering av legemidler. Herunder angir *Normen* hvilke tiltak som anses nødvendig for å oppnå tilfredsstillende informasjonssikkerhet 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 (*hendelsesregistrering*) 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. personopplysningsloven §18).

*Normen* regulerer den registrertes innsyn i *hendelsesregistre*.

*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 forhåndsgodkjenning.

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

*Normen* angir det nivå som da gjeldende versjon av *Normen* ble utferdiget, ble ansett nødvendig for å oppnå tilfredsstillende informasjonssikkerhet. Dette nivået kan likevel overprøves av Datatilsynet i det enkelte tilfellet.

## **1.6 Juridisk bindende ved avtale**

*Normen* er juridisk bindende for *virksomheter*, deres *leverandører* og andre som gjennom avtale med Norsk Helsenett SF, hverandre eller andre har forpliktet seg til å følge *Normen* i den grad *Normens* innhold ikke allerede er fastsatt i lov eller forskrift.

Alle *virksomheter* som er eller vil knytte seg til *helsenettet*, må avtalerettslig forplikte seg til å følge *Normen*. Tilknytningsavtalen med Norsk Helsenett SF innebærer at *virksomhetens* forpliktelser vedrørende sikkerhet hos andre *virksomheter*, jf. personopplysningsforskriften § 2-15, er ivarettatt ved kommunikasjon via *helsenettet*. Brudd på *Normen* kan gi sanksjoner i henhold til tilknytningsavtalen, herunder utestengelse fra *helsenettet*.

Det kan også inngås andre avtaler hvor partene forplikter seg til å følge *Normen*. Avtalepartene kan da gjensidig legge til grunn at den annen part har tilfredsstillende informasjonssikkerhet for den *behandling* av *helse- og personopplysninger* som er omfattet av den enkelte avtale. Konsekvenser ved brudd på *Normen* må reguleres i avtalene. Den enkelte avtales virkeområde vil være avgjørende for om andre *virksomheter* også kan legge avtalen til grunn for egen kommunikasjon med en eller begge avtalepartene.

*Normen* gjelder for både helse-, omsorgs- og sosialsektoren. Sanksjonene ved regelbrudd vil imidlertid kunne være ulike for de forskjellige sektorene.

Uten avtaler som nevnt, er *Normen*, i den grad den ikke omtaler lov eller forskrift, et veiledende dokument om hva som anbefales for å etablere tilfredsstillende informasjonssikkerhet.

## **2 OM FAKTAARK OG VEILEDERE**

I tilknytning til *Normen* utarbeides et sett med faktaark og veiledere (støttedokumenter). *Sektoren* er selv ansvarlig for å utarbeide dokumentene. Før dokumentene kan tas i bruk av *sektoren* skal de kvalitetssikres juridisk av Helsedirektoratet. Støttedokumentene finnes på [www.normen.no](http://www.normen.no).

### **2.1 Faktaark**

Faktaarkene beskriver nærmere hvordan *virksomhetene* kan oppfylle enkelte sentrale krav i *Normen* og gir praktisk veiledning til dette. *Virksomhetene* må selv holde seg oppdaterte i forhold til nye og endrede faktaark.

## **2.2 Veiledere**

Det er utarbeidet en rekke veiledere i tilknytning til informasjonssikkerhet i *sektoren*.

## **2.3 Forholdet til Normen**

Eksisterende og fremtidige støttedokumenter er kun å anse som veiledende dokumenter. Dette gjelder selv om det inngås avtale om at *Normen* skal være juridisk bindende.

Ved motstrid mellom *Normen* og støttedokumenter har *Normen* forrang.

## **DEL II: ARBEIDET MED INFORMASJONSSIKKERHET**

### **3 OVERSIKT**

#### **3.1 Ansvar**

Det er *virksomheten* ved ledelsen som har ansvar for å etablere og opprettholde tilfredsstillende informasjonssikkerhet. Dette er blant forpliktelsene til *databehandlingsansvarlig*. Det skal angis i melding/konsesjonssøknad til Datatilsynet hvilken stilling som har det daglige ansvaret for oppfyllelse av *virksomhetens* plikter, herunder for informasjonssikkerheten. Det daglige ansvaret tilligger som oftest daglig leder i *virksomheten*. Den som har det daglige ansvaret for informasjonssikkerheten, kan overføre oppgaver til egne ansatte. Oppgaver kan også overføres til eksterne, f.eks. kan man delegerer oppgaver til *leverandører*. Dette må gjøres i form av skriftlige avtaler. Uansett om oppgaver er delegert eller ikke, ligger det juridiske ansvaret hos *databehandlingsansvarlig*.

Arbeidet med informasjonssikkerhet må omfatte styring, gjennomføring og kontroll. Kapitlene 4 til 6 i Del II er bygget opp etter denne strukturen med en styrende del, en gjennomførende del og en kontrollerende del.

#### **3.2 Oversikt over oppgaver som omfattes av det daglige ansvaret for informasjonssikkerhet**

Den som har det daglige ansvaret skal fastlegge hvordan 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. Videre er *virksomhetens* leder ansvarlig for at bestemmelsene i personopplysningsforskriften kap. 2 og 3 følges, herunder følgende:

*Personopplysningsforskriftens kapittel 2:*

- Dokumentere hvilke *helse- og personopplysninger* som *behandles*.
- Etablere sikkerhetsmål for *virksomhetens* *behandlinger* av *helse- og personopplysninger*, dokumentere disse og gjøre disse kjent i *virksomheten*.
- Fastslå formål med *behandling* av *helse- og personopplysninger* og utarbeide sikkerhetsstrategi, dokumentere disse og gjøre disse kjent i *virksomheten*.
- Legge overordnede føringer for bruk av informasjonsteknologi, dokumentere disse og gjøre disse kjent i *virksomheten*.
- *Konfigurere* informasjonssystemene slik at tilfredsstillende informasjonssikkerhet oppnås og dokumentere *konfigurasjonen*.
- Etablere nivå for *akseptabel risiko*.
- Besørge risikovurderinger gjennomført.
- Definere ansvaret for informasjonssikkerhet ved minimum å:
  - Dokumentere ansvar og oppgaver i et organisasjonskart.
  - Beskrive ansvar og oppgaver på alle nivåer.
  - Gjøre ansvarsforholdene kjent i organisasjonen.
- Etablere styringssystem for informasjonssikkerhet som bl.a. skal omfatte:

- Prosedyrer for *behandlinger* av *helse- og personopplysninger*.
- Prosedyrer for bruk av informasjonssystemene.
- Prosedyrer for bruk av papirutskrifter.
- Dokumentasjon av sikkerhetstiltak – organisatoriske, fysiske og tekniske.
- Prosedyrer for avvikshåndtering.
- Prosedyrer ved bruk av *databehandlere, leverandører* av kommunikasjonstjenester, utstyr eller programvare og andre *leverandører*.
- Prosedyrer for godkjenning av alle *konfigurasjonsendringer* i informasjonssystemene.
- Følge opp at sikkerheten ivaretas i *virksomheten* ved jevnlig sikkerhetsrevisjoner og minimum årlig ledelsesgjennomgang av bl.a. avvikshendelser, samt vedta eventuelle korreksjoner i styringssystemet m.m.

*Personopplysningsforskriftens kapittel 3:*

- Ivareta reglene om *pasientenes/brukernes* rett til informasjon om og innsyn i, samt reglene om retting og sletting av registrerte *helse- og personopplysninger*.
- Etablere prosedyrer for innhenting av *samtykke* og oppfyllelse av evt. reservasjon mot visse former for *behandling* av *helse- og personopplysninger*.
- Besørge melding eller konsesjonssøknad til Datatilsynet.
- I tillegg har *virksomhetens* leder ansvar for at de *behandlinger* *virksomheten* foretar er lovlige.

### **3.3 Dokumentasjon**

Nedenfor er gitt en samlet oversikt over nødvendig dokumentasjon, og regler for lagring av historiske dokumenter. I den utstrekning samme dokument er nevnt flere steder er det samme dokument som benyttes i flere sammenhenger.

Dokumentasjon om tiltak knyttet til informasjonssikkerhet skal sikres på tilsvarende måte som *helse- og personopplysninger*.

#### **3.3.1 Styringsdokumenter:**

- Formålene med *behandlingene* av *helse- og personopplysninger*
- Oversikt over *behandlinger* av *helse- og personopplysninger*
- Overordnede føringer for bruk av informasjonsteknologi
- Sikkerhetsmål
- Nivå for *akseptabel risiko*
- Sikkerhetsstrategi
- Organisasjons-/ansvarskart

#### **3.3.2 Gjennomføringsdokumenter:**

- Formålene med *behandlingene* av *helse- og personopplysninger*
- Oversikt over *behandlinger* av *helse- og personopplysninger*
- Oversikt over partnere, *databehandlere* og *leverandører*

- Avtaler med partnere, *databehandlere* og *leverandører*
- Konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av *konfigurasjonen*
- Prosedyrer for *behandlinger* av *helse- og personopplysninger*
- Prosedyrer for bruk av informasjonssystemene
- Dokumentasjon av sikkerhetstiltak – organisatoriske, fysiske og tekniske

### 3.3.3 Kontrolldokumenter:

- Planer for gjennomføring av risikovurderinger og prosedyre for oppfølging av resultater fra disse vurderinger
- Planer for gjennomføring av sikkerhetsrevisjoner og prosedyre for oppfølging av resultater fra disse revisjoner
- Planer for ledelsens gjennomgang og prosedyre for oppfølging av handlingsplaner besluttet av ledelsen
- Prosedyrer for avvikshåndtering

### 3.3.4 Arkivering

Dokumenter angitt i 3.3.1 – 3.3.3 skal holdes løpende oppdatert og arkiveres fra det tidspunktet dokumentet ble erstattet med en ny gjeldende utgave. Formålet med denne arkivering er blant annet å muliggjøre sporing og korrigerende av *avvik* over tid. *Virksomhetens* ledelse skal arkivere følgende dokumentasjon med betydning for informasjonssikkerheten:

*5 års lagring minimum fra det tidspunkt dokumentet ble tatt ut av bruk:*

- Alle dokumenter angitt i 3.3.1 – 3.3.3
- 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*

*2 års lagring minimum:*

- *Hendelsesregistre* med sikkerhetsmessig betydning, herunder registrering av *autorisert* bruk og forsøk på *uautorisert* bruk av informasjonssystemene. Dersom oppføringer i *hendelsesregistre* kan knyttes til enkeltpersoner, skal *hendelsesregistrene* slettes når de sikkerhetsmessige formål er oppfylt, men først etter 2 år
- *Tilstedeværelsesregister* som er relevante ift kontroll mot *autorisasjonsregistre* og *hendelsesregistre*

Denne bestemmelsen regulerer ikke arkivering av *helse- og personopplysninger* som sådanne, men vil likevel omfatte de *personopplysninger* som inngår i *hendelsesregistre*.

## 4 STYRENDE DEL

### 4.1 Styringssystem for informasjonssikkerhet

*Virksomhetens* ledelse skal etablere et styringssystem for informasjonssikkerhet som en del av *virksomhetens* internkontrollsystem. Dette styringssystemet angir aktiviteter for å rettlede og styre *virksomheten* når det gjelder informasjonssikkerhet og skal som minimum omfatte de forhold og den dokumentasjonen som er omhandlet i pkt. 3.2 og 3.3 ovenfor.

I det følgende er det gitt en nærmere beskrivelse av sentrale elementer i styringssystemet.

### 4.2 Sikkerhetsmål

Det skal fastsettes sikkerhetsmål for *virksomheten*. Sikkerhetsmålene skal beskrive:

- Formålet med *behandling* av *helse- og personopplysninger*
- Overordnede føringer for *virksomhetens* bruk av informasjonsteknologi

#### 4.2.1 Formål

Det skal fastslås hva som er formålene med *behandlingene* av *helse- og personopplysninger* i *virksomheten*. Utgangspunktet er følgende:

Formålet med hver *behandling* av *helse- og personopplysninger* i *sektoren* er å yte forsvarlig helsehjelp og/eller yte sosialtjenester.

For helsesektoren innebærer dette blant annet handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte *pasient* og som utføres av helsepersonell, videre å sette *virksomheten* i stand til effektivt å forvalte helsetjenester iht. helselovgivningens bestemmelser, drive undervisning og forskning, og foreta rapportering iht. myndighetenes krav.

I omsorgs- og sosialsektoren innebærer dette at *pasienten/brukeren* skal få et tilpasset tilbud gjennom blant annet saksbehandling, vedtaksbehandling og tjenesteplanlegging. Videre skal *virksomheten* være i stand til effektivt å kunne fakturere, administrere tjenesten, utarbeide statistikk og styringsdata m.v.

#### 4.2.2 Overordnede føringer for virksomhetens bruk av informasjonsteknologi

Sammen med formålene med *behandlingene* av *helse- og personopplysninger* i *virksomheten* skal overordnede føringer for *virksomhetens* bruk av informasjonsteknologi beskrives i sikkerhetsmål. De overordnede føringene for bruk av informasjonsteknologi beskriver hvordan informasjonsteknologi er tatt i bruk og integrert i *virksomhetens* drift.

### 4.2.3 Sentrale sikkerhetsmål

Sentrale sikkerhetsmål er at *helse- og personopplysninger* skal:

- Være tilgjengelig for rett personell til rett tid i henhold til fastsatte prinsipper for tilgangsstyring etter pkt. 5.2 nedenfor.
- 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 målene over, og kravene i pkt. 4.4, fastsette nivå for *akseptabel risiko*.

## 4.3 Sikkerhetsstrategi

De strategiske valg for å oppnå sikkerhetsmålene skal nedfelles i en sikkerhetsstrategi. 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.

## 4.4 Nivå for akseptabel risiko

De overordnede krav for *virksomhetens* behandling av *helse- og personopplysninger* som skal legges til grunn for etablering av sikkerhetstiltak, omfatter følgende:

### 4.4.1 Konfidensialitet

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

- Personer utenfor *virksomheten* uansett ressurser og kunnskap 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 pkt. 5.2 nedenfor.
- Det skal registreres i *hendelsesregistre* i *behandlingsrettede helseregistre* (inkl *elektronisk pasientjournal (EPJ)*) og *fagsystem* hvem som har hatt *tilgang*.

### 4.4.2 Tilgjengelighet

- For de som har *tilgang*, hvor *taushetsplikten* er vurdert og ivaretatt, skal *helse- og personopplysninger* være tilgjengelige når det er *tjenstlig behov* for dem.
- *Nødrettstilgang* 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 pkt. 5.2.3 nedenfor. I så tilfelle må det utarbeides egne prosedyrer for dette. Begrunnelsen for *nødrettstilgang* skal dokumenteres og hvert enkelt tilfelle skal følges opp som et *avvik*.

- Se pkt. 5.5.3 om klassifisering av informasjonssystemenes kritikalitet og fastsettelse av *akseptabel risiko* for *tilgjengelighet* for hver aktuelle klassifisering.

#### 4.4.3 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*.

#### 4.4.4 Kvalitet

- *Helse- og personopplysninger* skal henføres til rett identifisert person.
- *Helse- og personopplysninger* skal føres i henhold til kodeverket.
- *Helse- og personopplysninger* skal være fullstendige og ajourført i forhold til *behandlingen* av opplysningene.

På bakgrunn av disse overordnede kravene og *virksomhetens* sikkerhetsmål, se pkt. 4.2, må *virksomheten* selv fastsette nivå for *akseptabel risiko* som skal gjelde i egen *virksomhet*.

### 4.5 Oversikt 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*. Oversikten kan f.eks. utarbeides som en database med oversikt over de systemer og registre for *behandling* av *helse- og personopplysninger* som til enhver tid er i bruk i *virksomheten*. Dette kan omfatte IT-systemer, databaser, prosjekter (forskningsprosjekter etc.), medisinsk teknisk utstyr og manuelle registre mv.

På et overordnet nivå skal oversikten inneholde følgende opplysninger:

- Kategorier av *helse- og personopplysninger*
- Formålet med *behandlingene*
- Juridisk hjemmelsgrunnlag for *behandlingene*
- Angivelse av system/register/utstyr, og om det er elektronisk eller manuelt
- Grunnlaget for *behandlingene*
- Om opplysningene er sensitive eller ikke-sensitive. *Helseopplysninger* er alltid sensitive *personopplysninger*
- Konesjonsplikt/*meldeplikt*/hjemmel for unntak
- Evt. partnere, *databehandlere* eller *leverandører*
- Internt ansvarlig for det enkelte system/register/utstyr

På et mer detaljert nivå kan oversikten inneholde nærmere opplysninger og kommentarer relatert til punktene ovenfor, samt informasjon om hvilke sikkerhetstiltak som er iverksatt for det enkelte system, *register* eller utstyr og dato for siste gjennomførte risikovurdering.

#### **4.6 Risikovurderinger**

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, se pkt. 6.2.

Risikovurdering tar utgangspunkt i kravet om forholdsmessig sikring av opplysninger. Formålet med vurderingen er å avdekke om *databelhandlingsansvarlig* har iverksatt tilstrekkelige tiltak slik at dette blir oppnådd, eller om ytterligere tiltak må iverksettes. Vurderingen vil gjøres i lys av og skal tuftes på de sikkerhetsmål og sikkerhetsstrategier som er fastlagt.

En viktig del av oppgaven er kartlegging av de opplysninger som må sikres, og å kartlegge det miljø opplysningene befinner seg i. Her vil oversikten over *behandlinger av helse- og personopplysninger* være et utgangspunkt, se pkt. 4.5. 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 fastlagte sikkerhetsmål og sikkerhetsstrategi, se pkt. 4.4.

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 fire aspektene man vanligvis forbinder med informasjonssikkerhet. Dette er *konfidensialitet, integritet, tilgjengelighet og kvalitet*.

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
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

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 teknologiske tiltak for å oppnå *akseptabel risiko* ikke innføres umiddelbart, kan det i en overgangsperiode benyttes administrative tiltak, f.eks. i form av prosedyrer.

## 5 GJENNOMFØRENDE DEL

### 5.1 Ansvarliggjøring av ansatte – 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 en straffbar handling og anmeldelse må vurderes.

### 5.2 Tilgangsstyring

Dette berører hvordan man foretar:

- *Autentisering* som sikrer identifisering av *autorisert* bruker.
- *Autorisering* som er tildeling av rettigheter til å kunne lese, registrere, redigere, rette, slette og/eller sperre *helse- og personopplysninger*.

- Tilgjengeliggjøring av *helse- og personopplysninger* om bestemte *pasienter/brukere* for *autorisert* personell.
- Utlevering av *helse- og personopplysninger* til annet personell enn *virksomhetens* eget personell.
- Regulering av privat bruk av *virksomhetens* informasjonssystemer.
- Kontrollerende tiltak.

*Autorisering og tilgang* er kun aktuelt for personell:

- som er underlagt egen *virksomhets* instruksjonsmyndighet (f.eks. egne ansatte)
- som arbeider under instruksjonsmyndighet av *virksomhetens* eventuelle *databehandlere*

*Autorisasjon* kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet i *tjenstlige behov* og er i henhold til bestemmelser om *taushetsplikt*. Det er kun slikt personell som kan gis *tilgang* til *helse- og personopplysninger*.

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

Utlevering av *helse- og personopplysninger* til annet helsepersonell enn *virksomhetens* eget personell er regulert i pkt. 5.2.4.

### 5.2.1 Autentisering

En spesiell utfordring i *sektoren* er at en og samme person kan ha ulike roller. *Autorisering* skal skje selvstendig for hver enkelt rolle og *autentisering* må sikre identifisering i korrekt rolle i hvert enkelt tilfelle.

- Ulike roller skal identifiseres og ved behov gis ulike autentiseringskriteria.
- Ved *tilgang* til *behandlingsrettede helseregistre* (inkl *elektronisk pasientjournal (EPJ)*) og *fagsystemer* skal ulike ansettelsesforhold identifiseres og gis ulike autentiseringskriteria. 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 bruk av mobilt utstyr, *hjemmekontor* og trådløs kommunikasjon skal *autentiseringen* ikke innebære større risiko enn for stasjonært utstyr og *autentisering* på sikkerhetsnivå 4 må benyttes.

### 5.2.2 Autorisering

*Databehandlingsansvarlig* er ansvarlig for at *autorisasjoner* tildeles, administreres og kontrolleres.

Ved tildeling av *autorisasjon* skal lovbestemt *taushetsplikt* vurderes og ivaretas.

*Databehandlingsansvarlig* 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
- formålet med *autorisasjonen*
- tidspunkt for når *autorisasjonen* ble gitt og eventuelt tilbakekalt
- informasjon om hvilken *virksomhet* den *autoriserte* er knyttet til

*Databehandlingsansvarlig* skal delegere ansvar og myndighet for å tildele *autorisasjon* til den enkelte enhets ansvarlige leder. I dette ligger at ansvarlig leder har, innen eget ansvarsområde, ansvaret for å 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 personelletts ansvar og oppgaver, så langt lovbestemt *taushetsplikt* ikke er til hinder for det.

For personer som har ulike roller i *virksomheten*, skal *autorisering* skje for hver rolle uavhengig av vedkommendes øvrige roller.

Det skal etableres prosedyre for tildeling og administrasjon av tilgangsrettigheter:

- *Autorisasjon* for å lese, registrere, redigere, 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.

### 5.2.3 Tilgang

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

*Tilgang* til *behandlingsrettede helseregistre* 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*. Dette gjelder også for *tilgang* i ordinære akuttsituasjoner, som ikke er å regne som *nødrettstilgang*. Det skal alltid fremgå av journalen at slik *tilgang* er gitt der reglene om *taushetsplikt* krever det.

*Tilgang* til *fagsystemer* skal gis på bakgrunn av beslutninger om *tjenstlig behov*. *Virksomheten* skal sikre at *taushetspliktreglene* overholdes.

#### 5.2.4 Utlevering av helse- og personopplysninger til andre enn virksomhetens og forvaltningsorganets eget personell

Når det er nødvendig for å kunne yte forsvarlig helsehjelp, kan *helse- og personopplysninger* overføres, utleveres 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, kvalitet 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 sosialtjenesten 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, kvalitet og tilgjengelighet*.

Utlevering av *helse- og personopplysninger* fra en *virksomhet* til en annen *virksomhet* (begge innenfor omsorgs- eller sosialtjenesten) 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
- utleveringen er nødvendig for å beskytte en persons vitale interesser, og *den registrerte* ikke er i stand til å samtykke
- det utelukkende utleveres opplysninger som *den registrerte* selv frivillig har gjort alminnelig kjent
- utleveringen er nødvendig for at *virksomheten* kan gjennomføre sine arbeidsrettslige plikter eller rettigheter

#### 5.2.5 Regulering av bruk

Datasystemene skal bare brukes til pålagte oppgaver. Bruk av datasystemene for privat brev/dokumentskrivning, utveksling av privat e-post m.m. kan kun:

- *Autoriseres* i den grad dette ikke utsetter *helse- og personopplysninger* for risiko.

#### 5.2.6 Kontrollerende tiltak

Det skal i størst mulig utstrekning benyttes *tekniske tiltak* for å oppfylle kravene ovenfor. All *autorisert* bruk og forsøk på *uautorisert* bruk av informasjonssystemene skal registreres og *registeret* skal lagres i minimum 2 år. *Hendelsesregistrene* skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd.

- Det skal etableres prosedyrer for å analysere *hendelsesregistrene* slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke.

- Det skal etableres prosedyrer for ved behov å kunne sammenholde *hendelsesregistrene* med *autorisasjonsregister* og *tilstedeværelsesregister*.
- 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.
- *Hendelsesregistrene*, *autorisasjonsregister* og *tilstedeværelsesregister* skal sikres mot endring og sletting av uautorisert personell.

### 5.3 Behandling av helse- og personopplysninger

*Virksomhetens* ledelse skal påse at det utarbeides og iverksettes prosedyrer for *behandling* av *helse- og personopplysninger*. Brudd på prosedyrer skal behandles som *avvik*. Følgende prosedyrer skal som minimum foreligge:

#### 5.3.1 Prosedyre for bruk av informasjonssystemet

Regler for bruk av informasjonssystemet skal nedfelles i prosedyre 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 *nødrettstilgang* for *behandlingsrettede helseregistre* skal følges. Hvert enkelt tilfelle skal følges opp som et *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.

#### 5.3.2 Etterkontroll av tilgangsstyring

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 (gjørne i forbindelse med sikkerhetsrevisjon).
- Ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet.

#### 5.3.3 Informasjon og samtykke

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 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. Samtykke innhentes i tråd med alminnelige regler for samtykke.
- *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.

#### **5.3.4 Den registrertes innsyn i hendelsesregistre**

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

- Hvem som har hatt *tilgang*.
- Hvor ofte *tilgangen* er benyttet.

Tilsvarende prosedyrer skal etableres for *fagsystem*.

### **5.4 Sikring av områder og utstyr**

#### **5.4.1 Nøkler/adgangskort**

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

#### **5.4.2 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. skjerms mot uautorisert innsyn.

#### **5.4.3 Driftsutstyr (servere og nettverksutstyr)**

Sikkerhetstiltak skal hindre at annet enn *autorisert* personell får adgang til slikt utstyr.

#### **5.4.4 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* på sikkerhetsnivå 4 må benyttes for bruk av slikt utstyr.
- *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. Datatilsynets til enhver tid gjeldende anbefalinger.

#### 5.4.5 Medisinsk teknisk utstyr

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

Medisinsk teknisk 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.

### 5.5 Etablering og drift av informasjonssystemet

Dette omhandler de tiltak som må iverksettes for at *helse- og personopplysninger* skal være sikret mot at personer som ikke er *autoriserte* får *tilgang* og at opplysningene er tilgjengelige ved behov. Med informasjonssystemet menes det samlede utstyr og programvare som behandler eller kan behandle *helse- og personopplysninger*.

#### 5.5.1 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.

## 5.5.2 Konfidensialitet og integritet

Dette omhandler de *tekniske tiltak* og organisatoriske tiltak som skal iverksettes for å hindre at personer uten *autorisasjon* får *tilgang* til *helse- og personopplysninger*.

- Minst to uavhengige *tekniske tiltak* skal iverksettes slik at personer utenfor *virksomheten* uansett ressurser og kunnskap ikke skal kunne få uautorisert *tilgang* til og/eller kunne endre eller slette *helse- og personopplysninger*.
- *Tekniske tiltak* 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 *nødrettstilgang*, skal *tekniske tiltak* etableres på en slik måte at helsepersonell i nødrettssituasjoner, kan få *tilgang* til nødvendige *helse- og personopplysninger*. Slik *tilgang* skal grunngis og registreres i *behandlingsrettede helseregistre* (inkl *elektronisk pasientjournal (EPJ)*) og hvert enkelt tilfelle skal følges opp som et *avvik*.
- *Tekniske tiltak* skal iverksettes slik at personer i eller utenfor *virksomheten* uansett ressurser og kunnskap 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.
- To uavhengige *tekniske tiltak* skal iverksettes slik at uautorisert programvare ikke skal kunne endre *helse- og personopplysninger*.
- Systemet som administrerer *autorisasjon* skal skille mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre *helse- og personopplysninger*. All tildeling av *autorisasjon* skal registreres i et *autorisasjonsregister*.
- Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av *helse- og personopplysninger*.
- *Tilgang* fra *hjemmekontor* og/eller mobilt utstyr skal sikres ved *autentisering* på sikkerhetsnivå 4. Dette gjelder også for avdelingskontor som kommuniserer ved hjelp av linjer man ikke har fysisk kontroll over.
- Alle lagringsmedia, dvs. disketter, 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.

For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres *hendelsesregistre* 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 *nødrettstilgang* til *behandlingsrettet helseregister* skal registreres.
- *Hendelsesregistrene* skal sikres mot endring og sletting av uautorisert personell.

Følgende skal som minimum registreres i *hendelsesregistre*:

- entydig identifikator for den *autoriserte* brukeren
- rollen den *autoriserte* brukeren har ved *tilgangen*

- virksomhetstilhørighet
- organisatorisk tilhørighet til den som er *autorisert*
- hvilke type opplysninger det er gitt *tilgang* til
- grunnlaget for *tilgangen*
- tidspunkt og varighet for *tilgangen*

Alle *hendelsesregistre* skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med *autorisasjonsregister* og *tilstedeværelsesregister*.

### 5.5.3 Tilgjengelighet

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 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.

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

#### **5.5.4 Kvalitet**

*Virksomheten* må fastsette prosedyrer for å ivareta kravene til *kvalitet*.

### **5.6 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.

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*.

### **5.7 Datakommunikasjon**

Når det benyttes datakommunikasjon skal hver enkelt *virksomhet* enten selv ivareta de påfølgende krav, eller sørge for at de som utfører oppgaven / leverer tjenesten ivaretar kravene.

All kommunikasjon med virksomheter/tjenester utenfor *virksomheten* bør fortrinnsvis foregå ved hjelp av en kanal, dvs. én netjtjenesteleverandør. Dersom det benyttes flere netjtjenesteleverandører mot systemer hvor det behandles *helse- og personopplysninger* må alle tilfredsstille kravene.

#### **5.7.1 Tilkoblingssikkerhet**

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

- Kun eksplisitt angitt tillatt trafikk kan passere, annet stoppes.
- Trafikk kan ikke passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra *virksomhetens* systemer.
- *Hendelsesregistrering* iverksettes for å kontrollere at regler ikke brytes; ved brudd stenges kanalen inntil ny sikker løsning finnes.

### 5.7.2 Meldingsformidling og e-post som inneholder *sensitive personopplysninger*

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 utlevering 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 utlevering 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.

### 5.7.3 E-post som ikke inneholder sensitive personopplysninger

*Virksomheten* skal iverksette tiltak for å forhindre at *sensitive personopplysninger* utleveres ved hjelp av e-post.

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

## 5.7.4 Tilkobling til Internett

Virksomheten skal iverksette tiltak:

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

## 5.7.5 Kommunikasjon med *pasienter/brukere*

Virksomheten er ansvarlig for at:

- Samtykke fra *pasienten/brukeren* er innhentet til å formidle *helse- og personopplysninger* elektronisk. Samtykke skal innhentes i tråd med alminnelige regler for samtykke. Samtykke fra *pasienten/brukeren* er etter denne *Normen* det eneste grunnlaget for datakommunikasjon med *pasienter/brukere*.
- *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* skal 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.

## 5.8 Avtaler

I dette punktet omtales kun de avtalemessige forhold som angår informasjonssikkerhet.

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 tilfredsstillere kravene i dette dokument, er ingen særskilt avtale om informasjonssikkerhet nødvendig for kommunikasjon via *helsenettet*, se pkt. 1.6. Denne avtalen oppfyller de krav til avtaler som er pålagt etter personopplysningsforskriften § 2-15.
- *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 pkt. 5.7.5 oppfylles, kreves det ikke særskilt avtale med hver enkelt *pasient/bruker*.
- Studenter og stipendiater som ikke er underlagt *databelhandlingsansvarliges* instruksjonsmyndighet.

### 5.8.1 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 kommunikasjonspakker ikke 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.

### 5.8.2 Databehandler

*Databehandler* har et selvstendig ansvar for informasjonssikkerhet etter [helseregisterloven § 16](#) og [personopplysningsloven § 13](#). I avtalen må sikkerhetsforhold reguleres konkret.

*Databehandlerens* selvstendige plikt til å etterleve [helseregisterloven § 16](#) og [personopplysningsforskriften kap. 2](#) må presiseres. I tillegg skal det stilles kriterier for *akseptabel risiko* hos *databehandleren*, samt at *databelhandlingsansvarlig* skal sikres innsynsrett for å forsikre seg om at kravene etterleveres. Utover dette skal det fremgå av avtalen at *databehandler* tilfredsstiller kravene i Normen. *Databehandler* skal ikke behandle *helse- og personopplysninger* på annen måte enn det som er avtalt med *databelhandlingsansvarlig*.

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 opplysningene.

### 5.8.3 Leverandører

*Virksomheten* skal for å ivareta *konfidensialitet, integritet, tilgjengelighet* og *kvalitet* 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 *databehandlingsansvarliges* 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.

### 5.8.4 Sikkerhetsleverandører

Personopplysningsforskriften kap. 2 fastslår som hovedregel at den *databehandlingsansvarlige* selv skal etablere nødvendige sikkerhetstiltak. Et alternativ til egen etablering av sikkerhetstiltak kan være å få utført sikkerhetsoppgaver hos underleverandør hvor fordeling av oppgaver mellom *virksomheten* og underleverandøren til sammen skal tilfredsstillere kravene i *Normen*. En sikkerhetsleverandør kan for eksempel utføre oppgavene i pkt. 5.7 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 pkt. 5.8.3.

## 6 KONTROLLERENDE DEL

*Virksomhetens* ledelse skal følge opp at sikkerheten ivaretas i *virksomheten*, se også pkt. 5.2.6. Det skal gjennomføres fem typer oppfølging, i tillegg til den daglige oppfølging:

- Sikkerhetsrevisjoner
- Risikovurderinger i *virksomhetens* enheter
- Avvikshåndtering
- Ledelsens gjennomgang
- Kontroll av hvem som har hatt elektronisk *tilgang* til *helse- og personopplysninger* i et *behandlingsrettet helseregister* (inkl *elektronisk pasientjournal (EPJ)*) eller *fagsystem*.

### 6.1 Sikkerhetsrevisjon

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

Revisjonen 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
- Effekten av etablerte sikkerhetstiltak
- Ivaretagelse av informasjonssikkerhet hos kommunikasjonspartnere, *databelandlere* og *leverandører*

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

### 6.2 Risikovurdering

*Virksomhetens* ledelse skal også jevnlig gjennomføre risikovurderinger for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser. Det vises til pkt. 4.6.

### 6.3 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 gjentakelse.

Avviksbehandlingen iverksettes ved sikkerhetsbrudd og/eller når *behandling av helse- og personopplysninger* er utført i strid med gjeldende regelverk, retningslinjer eller prosedyrer. Avviksbehandling 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 rapporterte *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 avviksbehandlingen.
- Ved gjentatte *avvik* skal det gjennomføres ny risikovurdering.

Dersom det har blitt foretatt en uautorisert utlevering av *helse- og personopplysninger* skal Datatilsynet varsles.

#### **6.4 Ledelsens gjennomgang**

*Virksomhetens* ledelse skal selv følge opp at informasjonssikkerheten ivaretas ved minimum årlig gjennomgang. 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* mål og strategi. Følgende skal som minimum gjennomgås:

- Resultat fra sikkerhetsrevisjoner.
- Resultat fra risikovurderinger.
- Resultater fra avviksbehandling. *Virksomhetens* ledelse skal regelmessig følge opp at tiltak på grunnlag av *avvik* fastlegges, planlegges og gjennomføres.
- Ansvarsforhold og organisering mht. sikkerhet.
- Formål med *behandling av helse- og personopplysninger* og oversikt over *helse- og personopplysninger* som *behandles* i *virksomheten*.
- *Konfigurasjonskart* over informasjonssystemene.
- Sikkerhetsmål, nivå for *akseptabel risiko* og strategier for informasjonssikkerhet.
- Kontroll og oppfølging av inngåtte avtaler (ref pkt 5.8).

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

Gjennomgangen skal danne grunnlag for eventuelle endringer av sikkerhetsmål og/eller sikkerhetsstrategi.

## **6.5 Kontroll av tilganger**

*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*.

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 kan *virksomhetens* ledelse vurdere om *pasienten/brukeren* skal informeres.

## **LOV- OG FORSKRIFTSREGISTER:**

Arkivloven (lov 4. desember 1992 nr. 126)

Forskrift om internkontroll i sosial- og helsetjenesten (forskrift 20. desember 2002 nr. 1731)

Forskrift om kontrollkomisjonens virksomhet (forskrift 21. desember 2000 nr. 1408)

Forskrift om pasientjournal (forskrift 21. desember 2000 nr. 1385)

Forvaltningsloven (lov 10. februar 1967 nr. 00)

Helseforskningsloven (lov 20. juni 2008 nr. 44)

Helsepersonelloven (lov 2. juli 1999 nr. 64)

Helseregisterloven (lov 18. mai 2001 nr. 24)

Kommunehelsetjenesteloven (lov 19. november 1982 nr. 66)

Offentleglova (lov 19. mai 2006 nr.16)

Pasientrettighetsloven (lov 2. juli 1999 nr. 63)

Personopplysningsforskriften (forskrift 15. desember 2000 nr. 1256)

Personopplysningsloven (lov 14. april 2000 nr. 31)

Psykisk helsevernloven (lov 2. juli 1999 nr. 62)

Smittevernloven (lov 5. august 1994 nr. 55)

Sosialtjenesteloven (lov 13. desember 1991 nr. 81)

Spesialisthelsetjenesteloven (lov 2. juli 1999 nr. 61)

Statlig tilsyn med helsetjenesten (lov 30. mars 1984 nr. 15)

Tannhelsetjenesteloven (lov 3. juni 1983 nr. 54)