

# Veiledende merknader til helseregisterloven § 13 og helseinformasjonssikkerhetsforskriften



Juni 2012

Innledning.....	3
1 Kort oversikt .....	4
1.1 Helseregisterloven § 13 formål og virkeområde.....	4
1.2 Helseinformasjonssikkerhetsforskriften formål og virkeområde.....	4
1.3 Begreper.....	6
2 Helseregisterloven.....	7
2.1 § 13 Tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon.....	7
3 Forskrift 24. juni 2011 nr. 628 om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (helseinformasjonssikkerhetsforskriften)11	
3.1 § 1 Forskriftens formål .....	11
3.2 § 2 Forholdet til personopplysningsloven.....	11
3.3 § 3 Definisjoner .....	12
3.4 § 4 Krav om system for administrering av autorisasjoner for tilgang til helseopplysninger 13	
3.5 § 5 Autorisasjon for tilgang til helseopplysninger for personell som yter eller administrerer helsehjelp.....	14
3.6 § 6 Begrensninger i autorisasjon for tilgang til helseopplysninger.....	16
3.7 § 7 Krav om opplæring .....	17
3.8 § 8 Krav om register over og kontroll av autorisasjoner for tilgang til helseopplysninger 18	
3.9 § 9 Krav om autentisering.....	19
3.10 § 10 Rett til tilgang til helseopplysninger for personell som yter eller administrerer helsehjelp 20	
4.11 § 11 Avtale om lesetilgang på tvers av virksomheter .....	23
4.12 § 12 Særlig avtale om skrivetilgang på tvers av virksomheter .....	25
4.13 § 13 Unntak fra krav om uttrykkelig samtykke .....	26
4.14 § 14 Behandling av den enkelte forespørselen mellom virksomheter .....	27
4.15 § 15 Sperring av helseopplysninger.....	28
4.16 § 16 Krav om dokumentasjon av tilgang.....	30
4.17 § 17 Oppfølging og kontroll av elektronisk tilgang.....	33
4.18 § 18 Dispensasjon.....	33
4.19 § 19 Straff .....	34
4.20 § 20 Ikrafttredelse.....	35

## Innledning

Stortinget vedtok 16. juni 2009 endringer i helseregisterloven og helsepersonelloven. Endringene medførte nye eller endrede bestemmelser i helseregisterloven §§ 6 a, 6 b og 13, med tilhørende forskriftshjemler.

Helseregisterloven § 13 som regulerer tilgang til helseopplysninger, gir nå hjemmel til å fastsette forskrift om tilgang til helseopplysninger på tvers av virksomheter.

Forskrift om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (helseinformasjonssikkerhetsforskriften) ble vedtatt 24. juni 2011. Forskriften er hjemlet i helseregisterloven §§ 13 og 16, helsepersonelloven §§ 45 og 46 og pasient- og brukerrettighetsloven § 5-1.

Denne veilederen gir en overordnet beskrivelse av hvordan helseregisterloven § 13 og helseinformasjonssikkerhetsforskriften er ment å forstås. Veilederen inneholder ingen nye krav eller plikter, men er et bidrag til virksomhetene i arbeidet med å implementere regelverket.

Veilederen er rettet mot:

- Systemleverandører i arbeidet med systemutvikling av behandlingsrettede informasjonssystemer.
- Virksomheter til hjelp i arbeidet med kravspesifikasjon, bestilling av hjelpemidler og elektronisk utstyr, organisering av arbeidsprosesser og rutiner i virksomheten etc.
- IKT- ansvarlige og administratorer ved administrering av autorisasjoner for tilgang til helseopplysninger
- Opplæringspersonell som grunnlag for opplæring og kompetanseoppbygging av ansatte.

Lenke til helseregisterloven og helseinformasjonssikkerhetsforskriften:

<http://www.lovdata.no/all/nl-20010518-024.html>

<http://www.lovdata.no/for/sf/ho/ho-20110624-0628.html>

Veilederen kommer i tillegg til forarbeidene:

[Ot.prp. nr. 51 \(2008–2009\)](#) Om lov om endringer i helseregisterloven og helsepersonelloven (tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av behandlingsrettede helseregistre på tvers av virksomheter)

[Innst. O. nr. 110 \(2008–2009\)](#)

# 1 Kort oversikt

## 1.1 Helseregisterloven § 13 formål og virkeområde

Formålet med endringen av helseregisterloven § 13 er å fjerne regelverksmessige hindre for effektiv og trygg kommunikasjon av helseopplysninger i helsetjenesten, samtidig som pasientens rett til konfidensialitet og vern om personlige integritet ivaretas.

Helseregisterloven skiller mellom tilgang til helseopplysninger og utlevering av helseopplysninger. Helseregisterloven § 13 setter de ytre rammer for hvem som kan gis tilgang til helseopplysninger. Elektronisk tilgang til helseopplysninger som behandles etter helseregisterloven, er begrenset til den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet. Det fremgår av forarbeidene til helseregisterloven § 13 at hensikten med bestemmelsen er å sikre konfidensialitet.

Ved endringen i § 13 åpnes det for at tilgang til helseopplysninger for enkeltpasienter kan gis på tvers av virksomhetsgrenser, under gitte forutsetninger. Tilgang til nødvendige journalopplysninger på tvers av tjenestenivåer vil i enkelte tilfeller være helt avgjørende for å kunne gi pasienten forsvarlig helsehjelp.

Begrensningen i helseregisterloven § 13 gjelder i tillegg til reglene om taushetsplikt i helsepersonelloven, og bestemmelsen gir ikke hjemmelen til å gjøre unntak fra reglene om taushetsplikt. Det følger både av helsepersonelloven §§ 25 og 45 at taushetsbelagte opplysninger bare kan kommuniseres når det er nødvendig for å kunne gi forsvarlig helsehjelp. Dette gjelder så vel kommunikasjon internt i virksomheten som mellom virksomheter. Det er fortsatt reglene om taushetsplikt som regulerer hvilke helseopplysninger det kan gis tilgang til og når tilgang kan gis.

Helseregisterloven § 13 må ses i sammenheng med § 16 som pålegger databehandlingsansvarlig og databehandler å sørge for tilfredsstillende sikring av helseopplysninger. For å sikre økt informasjonssikkerhet ved behandling av helseopplysninger, er det gitt egen forskrift om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (helseinformasjonssikkerhetsforskriften). Forskriften skal gjelde både ved tilgang internt i virksomheter, og ved tilgang på tvers av virksomhetsgrenser.

## 1.2 Helseinformasjonssikkerhetsforskriften formål og virkeområde

Forskriftens formål er å regulere nødvendig tilgang til helseopplysninger og bidra til tilfredsstillende informasjonssikkerhet slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas.

Helsepersonells behov for helseopplysninger ved ytelse av helsehjelp vil avhenge av pasientens sykdomsbilde og eventuelt tidligere sykdomshistorie. Hvor pasienten mottar helsehjelpen vil ofte være uten betydning. Forskriften legger grunnlag for at

helsepersonell kan få tilgang til helseopplysninger i helsehjelpsøyemed, uavhengig av organisatorisk tilknytning. Det er behovet for informasjon om pasienten, for å kunne yte nødvendig helsehjelp, som skal styre helsepersonells tilgang til helseopplysninger.

Helseinformasjonssikkerhetsforskriftens gjelder for alle typer behandlingsrettede helseregistre, ikke bare registre som inneholder opplysninger som inngår i de elektroniske pasientjournalene (ofte kalt EPJ) eller pasientadministrative systemene (PAS). Forskriften dekker også store og små fagsystemer med ulikt innhold og ulik grad av kompleksitet og antall brukere. Informasjonssikkerheten bør være like god, uavhengig av i hvilke systemer helseopplysningene behandles eller befinner seg i.

Forskriften forutsetter at helsepersonell kan gis beslutningsstyrt elektronisk tilgang til helseopplysninger internt i egen virksomhet og på tvers av virksomheter, der formålet er å yte helsehjelp, se § 10. ”Beslutningsstyrt tilgang” innebærer at det må tas en beslutning om å yte helsehjelp før systemet kan gi tilgang til helseopplysninger, og dette skal dokumenteres i systemet. Helsepersonell har bare tilgang til de helseopplysninger som er relevante og nødvendige for helsehjelpen som skal tilbys. Bestemmelsene i forskriften skal legge til rette for at registrering av en beslutning om gjennomføring av et bestemt tiltak automatisk skal kunne resultere i at det blir åpnet for nødvendig tilgang for det helsepersonell som skal gjennomføre tiltaket.

Beslutningsstyrt tilgang krever at informasjonssikkerheten må være like god ved behandling av helseopplysninger på tvers av systemer innen et helseforetak, som ved behandling av opplysningene innenfor samme journalsystem. Videre innebærer det at sikkerheten ved behandling av helseopplysninger på tvers av foretak må være like sikker som behandling av opplysningene innen samme foretak. Tilgang til helseopplysninger på tvers av virksomheter krever derfor at virksomhetene har systemer som kan understøtte dette. Det innebærer at systemene faktisk må være i stand til å gi tilgang kun til journalopplysninger som er relevante og nødvendige for å kunne gi forsvarlig og nødvendig helsehjelp til pasienten.

Forutsatt at to virksomheter oppfyller kravene i forskriften, kan disse inngå avtale om at helsepersonell kan gis tilgang til helseopplysninger uavhengig av virksomhetsgrensene. Departementet gjør oppmerksom på at tilgang til helseopplysninger på tvers av virksomhetsgrenser som hovedregel bare kan avtales for informasjonssystemer som kan oppfylle alle kravene i forskriften. Tilgang til helseopplysninger på tvers av virksomheter skal som hovedregel være basert på samtykke fra pasienten.

Forskriften regulerer ikke tilgang til helseopplysninger for andre formål enn helsehjelp eller administrasjon av slik hjelp. Utlevering av eller tilgang til helseopplysninger til andre formål reguleres av de alminnelige reglene i blant annet helsepersonelloven, helseregisterloven og personopplysningsloven. Forskning, undervisning, kvalitetssikring, kontroll og tilsyn er eksempler på bruk av helseopplysninger til andre formål enn helsehjelp.

## 1.3 Begreper

### **Behandlingsrettet helseregister**

Behandlingsrettet helseregister er definert i helseregisterloven § 2 nr. 7 som journal og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende formål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger.

Definisjonen omfatter helseopplysninger i elektroniske pasientjournalssystemer (EPJ-systemer), pasientadministrative systemer (PAS), røntgeninformasjonssystemer (RIS), medisinske bildearkivsystemer (PACS), laboratoriedatasystemer, små avdelingsvise kliniske systemer og en rekke andre typer fag- og spesialsystemer som benyttes som informasjonssystem og kunnskapsgrunnlag for helsehjelp.

Begrepet helseregister er definert i helseregisterloven § 2 nr. 6 og omfatter registre, fortegnelser, m.v. der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen. Helseregister er et logisk begrep og ikke en datateknisk definisjon. Et behandlingsrettet helseregister kan således bestå av flere datafiler, og det kan fysisk føres flere steder. Flere forskjellige IT-systemer kan benyttes for å bevare og behandle opplysningene i registeret.

### **Databehandlingsansvarlig**

Begrepet databehandlingsansvarlig er definert i helseregisterloven § 2 nr. 8 som den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven.

Helseregisterloven § 6 fastslår at regionale helseforetak og helseforetak, kommune og annen offentlig eller privat virksomhet som tar i bruk behandlingsrettede helseregistre, er databehandlingsansvarlig for opplysningene. Det følger av helseforetaksloven § 9 at utøvende tjeneste skal organiseres som helseforetak. Innenfor den statlige spesialisthelsetjenesten vil derfor helseforetaket være databehandlingsansvarlig for behandlingen av opplysningene innen virksomheten.

Dersom kommunen velger å utføre kommunale helsetjenester innenfor egen organisasjon, vil det være kommunen som er databehandlingsansvarlig for opplysningene.

### **Databehandler**

Begrepet databehandler er definert i helseregisterloven § 2 nr. 9 som den som behandler helseopplysninger på vegne av den databehandlingsansvarlige.

En databehandler er en ekstern person eller virksomhet utenfor den databehandlingsansvarliges virksomhet, f.eks. en ekstern driftsenhet.

## **Helsehjelp**

Begrepet helsehjelp er definert i helsepersonelloven § 3 tredje som enhver handling som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål og som utføres av helsepersonell. Begrepet helsehjelp er vidt, men for at en handling eller et tiltak omfattes av begrepet, er det en forutsetning at handlingen eller tiltaket utføres av helsepersonell eller helsepersonells medhjelper. Helsehjelp kan derfor også være å vurdere helseopplysninger for å avklare hvordan diagnostikk, behandling, pleie etc. skal utføres i det videre forløp, eventuelt vurdere om det ikke skal gis slike tilbud. Helsepersonells råd og veiledning om ytelse av helsehjelp til annet helsepersonell, slik at sist nevnte personell kan yte helsehjelp, er en handling som omfattes av begrepet helsehjelp.

## **Helseopplysninger**

Begrepet helseopplysninger er definert i helseregisterloven § 2 nr. 1 og omfatter 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. Alle pasientopplysninger, det vil si taushetsbelagte opplysninger i henhold til helsepersonelloven, omfattes av gruppen helseopplysninger. Dette inkluderer pseudonyme og aidentifiserte helseopplysninger.

## **Helsepersonell**

Begrepet helsepersonell er definert i helsepersonelloven § 3, og omfatter:

- personell med autorisasjon etter helsepersonelloven § 48 eller lisens etter helsepersonelloven § 49,
- personell i helsetjenesten eller i apotek som utfører helsehjelp,
- elever og studenter som i forbindelse med helsefaglig opplæring utfører helsehjelp.

Vilkårene for tilgang til helseopplysninger i pasientbehandlingsøyemed eller for å tilby annen helsehjelp til en pasient følger av helsepersonelloven §§ 25 og 45. Helsepersonell som kan få tilgang til eller få utlevert helseopplysninger i medhold av helsepersonelloven §§ 25 og 45, kan autoriseres slik at de også kan få elektronisk tilgang til opplysningene for å yte helsehjelp.

## **2 Helseregisterloven**

### **2.1 § 13 Tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon**

*Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt.*

*Kongen i Statsråd kan i forskrift gi nærmere bestemmelser om tilgang til helseopplysninger. Forskriften kan for tilgang til helseopplysninger i behandlingsrettede helseregistre gjøre unntak fra første ledd første punktum.*

*Tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter kan bare gis etter uttrykkelig samtykke fra den registrerte.*

*Kongen i Statsråd kan i forskrift gjøre unntak fra kravet om uttrykkelig samtykke i tredje ledd, jf. § 2 nr. 11.*

*Én forespørsel om og tilgang til helseopplysninger i annen virksomhet kan bare omfatte én pasient om gangen.*

*Den registrerte har rett til innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne.*

### **Merknader til § 13 første ledd**

Bestemmelsen setter rammer for hvem som kan gis tilgang til helseopplysninger. Første ledd fastslår hovedregelen om at det bare er den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, som kan gis tilgang til helseopplysninger som behandles etter loven. Bestemmelsen henger sammen med kravet til konfidensialitet. Dersom andre personer enn nevnt har tilgang til helseopplysninger, har ikke databehandlingsansvarlige eller databehandler oppfylt sine plikter etter loven § 16 om sikring av helseopplysningenes konfidensialitet

**Første ledd andre punktum** presiserer hvilke helseopplysninger det gis tilgang til. Bestemmelsen fastslår at tilgang til helseopplysninger bare kan gis i den grad det er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt. Enhver bruker som får tilgang til helseopplysninger og datasystemer der helseopplysninger behandles, skal være autorisert i samsvar med oppgaver og ansvar. Det betyr at den databehandlingsansvarlige for helseopplysningene og databehandler må sørge for å etablere sikringstiltak som hindrer annen tilgang til opplysningene. Sikringstiltak kan etableres på flere trinn eller nivåer.

Taushetsplikt for helseopplysninger omfatter både en plikt til å tie og en aktiv plikt til å hindre at opplysninger bringes videre til andre eller "lekker ut". Helseregisterloven skiller derfor mellom tilgang til helseopplysninger, jf. § 13, og utlevering av helseopplysninger, jf. § 14. Skillet bygger på den tanke at helsepersonell innen virksomheten skal kunne hente frem nødvendige helseopplysninger fra journalen i henhold til instruks, mens helsepersonell utenifra først må henvende seg til noen innenfor for å kunne få opplysninger fra journalen. Den databehandlingsansvarlige vil på denne måten ha kontroll over opplysningene og sikre at taushetsplikten overholdes.

Det følger av endring i helsepersonelloven § 45 at det innenfor taushetsplikten kan gis tilgang til helseopplysninger på tvers. Det skal følge av journalen at annet helsepersonell er gitt helseopplysninger.

Helsepersonells taushetsplikt gjelder ikke overfor pasienten som opplysningene direkte gjelder, jf. helsepersonelloven § 22. En pasient har tvert imot rett til innsyn i sin journal, jf. helsepersonelloven § 41 og pasientrettighetsloven § 5-1.

Helseregisterloven § 13 første ledd har ikke til hensikt å begrense eller vanskeliggjøre pasienters innsynsrett i egen journal. Bestemmelsen skal forstås slik at den ikke er til



hinder for at en pasient kan få adgang til egne journalopplysninger. Dette betyr imidlertid ikke at pasienten gis rett til direkte tilgang til egne journalopplysninger. Under forutsetning av at pasientens innsynsrett oppfylles, må det være den databehandlingsansvarlige som må vurdere hvordan opplysningene best kan gis, slik at informasjonssikkerheten ivaretas.

### **Merknader til § 13 andre ledd**

Det kan i forskrift gis nærmere bestemmelser om tilgang til helseopplysninger. Forskriften kan gjøre unntak fra hovedregelen om at tilgang kun kan skje internt, og åpner for tilgang til helseopplysninger på tvers av virksomheter. Helseinformasjonssikkerhetsforskriften er gitt med hjemmel i § 13, og hvilke krav som stilles til tilgang på tvers følger av denne.

### **Merknader til § 13 tredje ledd**

Elektronisk tilgang til helseopplysninger på tvers av virksomheter kan bare gis etter uttrykkelig samtykke fra pasienten. Samtykke er i helseregisterloven § 2 nr. 11 definert som en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av helseopplysninger om seg selv.

Pasientens samtykke er bare gyldig dersom pasienten har fått informasjon på forhånd. Dette innebærer at bestemmelsene om informasjonsplikt i helseregisterloven §§ 23 og 24 kommer til anvendelse. Bestemmelsene gjelder ved all behandling av helseopplysninger som skjer ved hjelp av elektroniske hjelpemidler. Det følger av disse at informasjonen til pasienten blant annet skal inneholde:

- navn og adresse på den databehandlingsansvarlige,
- formålet med behandlingen av opplysningene,
- om opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
- om det er frivillig å gi fra seg helseopplysningene,
- annet som gjør den registrerte i stand til å bruke sine rettigheter på en best mulig måte.

Etter helsepersonelloven § 10 er det helsepersonell som har det faglige ansvaret for helsehjelpen, som har plikt til å gi informasjon etter pasientrettighetsloven. Det kan for eksempel være legen som forordner eller utfører tiltak, eller sykepleieren som gir pleie. I helseinstitusjon skal det utpekes en person som skal gi informasjon. Den som er utpekt som ansvarlig for å gi informasjon, har et overordnet ansvar for at pasienten faktisk får informasjon.

Det vil være mest naturlig at det samme personell som informerer pasienten om hans eller hennes helsetilstand og innholdet i helsehjelpen, også informerer om hva slags behandling det gjøres av helseopplysningene om vedkommende. Det presiseres viktigheten av at man i særlig grad forsikrer seg om at pasienten er informert dersom det er aktuelt å gi helsepersonell i andre virksomheter elektronisk tilgang til helseopplysningene. Dette er viktig for å sikre at samtykket blir reelt.

### **Merknader til § 13 fjerde ledd**

Det åpnes for at det i forskrift kan gjøres unntak fra kravet om uttrykkelig samtykke, men denne adgangen skal være snever. I Innst. O nr. 110 (2008–2009) er det inntatt følgende merknader til bestemmelsen:

”Flertallet vil i forbindelse med forslaget til nytt fjerde ledd i helseregisterloven § 13 om hjemmel for forskrift om unntak presisere at helsepersonell ikke uten videre kan legge til grunn at taushet fra pasienten innebærer et stilltiende samtykke. Helsepersonellet må konkret vurdere i hvert enkelt tilfelle om pasienten har fått tilstrekkelig informasjon om behandlingen av opplysningene, og om pasientens atferd tilsier at samtykke foreligger. Dersom pasienten er bevisstløs eller er i en tilstand der han eller hun ikke er i stand til å motta informasjon, må helsepersonell gjøre en konkret vurdering av hva han eller hun antar at pasienten hadde ønsket. I slike tilfeller vil opplysningenes sensitivitet og hvor nødvendige de er for den aktuelle helsehjelpen, være en del av vurderingen.”

### **Merknader til § 13 femte ledd**

En forespørsel om tilgang til helseopplysninger i annen virksomhet kan kun omfatte én pasient om gangen. Ved behov for gjentatt tilgang må det skje en ny forespørsel. Ved behov for oppslag i en annen pasients elektroniske pasientjournal må tilgangsvurderingen gjøres på nytt fra egen virksomhets pasientjournalssystem, basert på tjenestelig behov.

### **Merknader til § 13 sjette ledd**

Sjette ledd fastslår pasientens innsynsrett i logg (hendelsesregister) om hvem som har hatt tilgang til helseopplysninger om ham eller henne. Logging av informasjon om hvem som har hatt tilgang til taushetsbelagte opplysninger om pasienten, er et viktig element for å bedre informasjonssikkerheten. Det er et sentralt element i personvernet at den enkelte skal ha rett til og reell mulighet til å ha kontroll over helseopplysninger om seg selv. Informasjon om hvem som har hatt tilgang til helseopplysninger om en, vil bidra til å øke pasientens kontroll med opplysningene. Innsynsrett og krav til registrering av tilgang følger også av personopplysningsloven og personopplysningsforskriften.

Dette kravet innebærer at systemet må ha funksjonalitet for logging av alle oppslag, både internt og når tilgangen er på tvers. Det er et grunnleggende krav til systemet at det finnes slik funksjonalitet for logging, og at det kan gis innsyn i denne.

Merk at retten til innsyn i logg i behandlingsrettede helseregistre, gjelder all type tilgang. Bestemmelsen gjelder dermed også hvor grunnlaget for tilgangen er annet enn helsehjelp, f. eks hvor det er gitt tilgang til helseopplysninger til forskning eller kvalitetssikring. Også denne type tilgang og bruk av helseopplysninger skal logges slik at pasienten skal kunne få innsyn i all bruk av dennes helseopplysninger.

Loggingen vil inngå som del av dokumentasjonen til registeret, og omfattes av den aktuelle behandlingen av helseopplysninger. Det er derfor ikke nødvendig med egen melding til Datatilsynet for selve loggingen.

Ytterligere krav til hva det skal gis innsyn i, følger av helseinformasjonssikkerhetsforskriften § 16.

### **3 Forskrift 24. juni 2011 nr. 628 om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (helseinformasjonssikkerhetsforskriften)**

#### **3.1 § 1 Forskriftens formål**

*Formålet med forskriften er å regulere nødvendig tilgang til helseopplysninger og å bidra til tilfredsstillende informasjonssikkerhet slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas.*

#### **Merknader til § 1**

Begrepet tilgang til helseopplysninger må forstås med bakgrunn i at helseregisterloven skiller mellom tilgang til helseopplysninger og utlevering av helseopplysninger. Skillet bygger på den tanke at helsepersonell innen virksomheten selv skal kunne hente frem opplysninger fra journalen, mens helsepersonell utenfra først må henvende seg til noen innenfor for å kunne få opplysninger fra journalen.

Etter forskriften kan tilgang til helseopplysninger kun gis for å yte helsehjelp. Helsehjelp er definert i helsepersonelloven § 3 tredje ledd, som enhver handling som har forebyggende, diagnostiske, behandlende, helsebevarende eller rehabiliterende mål og som utføres av helsepersonell. Begrepet helsehjelp er et vidt begrep og omfatter også råd og veiledning helsepersonell gir kollegaer - dersom hensikten er at kollegaen skal yte helsehjelp. Videre er det å gjennomgå en pasients journal for å vurdere om pasienten har behov for helsehjelp, å anse som helsehjelp. Dette gjelder både der helsepersonell vurderer hva slags helsehjelp pasienten bør tilbys og der helsepersonell vurderer om pasienten har behov for helsehjelp.

Kravet til at helsehjelpen skal være forsvarlig er en rettslig standard og består av tre hovedelementer. Tjenestene må holde tilfredsstillende kvalitet, ytes i tide og i tilstrekkelig omfang. Kravet om at helsehjelpen skal være effektiv må ses i lys av helsepersonelloven § 6 som fastslår at helsepersonell skal sørge for at helsehjelpen ikke påfører pasienter, helseinstitusjon, trygden eller andre unødvendig tidstap eller utgift.

Forskriften skal bidra til tilfredsstillende informasjonssikkerhet ved tilgang til helseopplysninger, og er en presisering av kravene som følger av helseregisterloven § 16. Det er helt sentralt at hensynet til pasientens personvern ivaretas når det gis tilgang til helseopplysninger, enten det skjer internt eller eksternt.

#### **3.2 § 2 Forholdet til personopplysningsloven**

*Personopplysningsloven gjelder med de særlige regler om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre som er gitt i denne forskriften, jf. helseregisterloven § 2 nr. 7.*

## **Merknader til § 2**

Det følger av bestemmelsen at reglene i forskriften gjelder i tillegg til bestemmelsene i personopplysningsloven med tilhørende forskrift 15. desember nr. 1265 om behandling av personopplysninger (personopplysningsforskriften). Særlig relevante er reglene om informasjonssikkerhet i personopplysningsforskriften kapittel 2 og reglene om internkontroll i kapittel 3.

Dette innebærer at kravene som følger av forskriften supplerer kravene som følger av personopplysningslov og personopplysningsforskrift.

## **3.3 § 3 Definisjoner**

*I forskriften menes med*

- 1. autorisasjon for tilgang til helseopplysninger: bestemte rettigheter til å lese, registrere, redigere, rette, slette, sperre eller på annen måte behandle helseopplysninger*
- 2. strukturerte helseopplysninger: helseopplysninger som er inndelt slik at helsepersonellens tilgang kan begrenses til de opplysningene som vurderes som relevante og nødvendige for å yte helsehjelp til den enkelte pasient.*

### **Merknader til § 3 nr. 1**

Helsepersonells autorisasjon for tilgang til elektroniske helseopplysninger skal angi hvilke rettigheter vedkommende har til å behandle opplysningene. Autorisasjonen skal utformes slik at reglene om taushetsplikt kan etterleves.

Innholdet i autorisasjonen må ta utgangspunkt i hvilken rolle vedkommende helsepersonell har i virksomheten. En beslutning om innholdet i, og omfanget av, en autorisasjon skal bygge på helsefaglig kunnskap og vurderinger. Det er forbudt å lese, søke etter eller på annen måte tilegne seg helseopplysninger uten at det er begrunnet i ytelse av helsehjelp, administrasjon av slik hjelp, eller har særskilt hjemmel i lov eller forskrift, jf. helseregisterloven § 13a og helsepersonelloven § 21a.

Autorisasjonen må også inneholde informasjon om hvorvidt den som er autorisert kan registrere beslutninger om helsehjelp, som innebærer at også annet helsepersonell kan gis tilgang til helseopplysninger i den konkrete pasientens journal.

Det presiseres at autorisasjon er en nødvendig forutsetning for tilgang til helseopplysninger ved beslutningsstyrt tilgang, men det er ikke en tilstrekkelig forutsetning. Lovlig rett til tilgangen utløses ikke før det er registrert en beslutning som innebærer at helsepersonell skal yte helsehjelp til den angjeldende pasienten.

### **Merknader til § 3 nr. 2**

Med strukturerte helseopplysninger menes helseopplysninger som er inndelt slik at helsepersonells tilgang kan begrenses til de opplysningene/opplysningssett som vurderes som relevante og nødvendige for å yte helsehjelp til den enkelte pasient. Forskriften bruker uttrykket ”vurderes som relevante og nødvendige” fordi det i forkant av en slik vurdering ikke vil være mulig å vite akkurat hvilke opplysninger som vil være relevante

og nødvendige. I noen tilfeller kan alle journalopplysninger være nødvendige for å vurdere hva slags helsehjelp en pasient bør tilbys, i andre tilfelle vil det være begrenset til kunnskap om bestemte sykdommer eller journalnotater.

Mange sykehus benytter en strukturering basert på en utvidet/tilpasset ”Norgesjournal”, hvor det innenfor den enkelte kategori kan inngå en rekke forskjellige dokumenttyper, sammen med informasjon (metadata) som tidspunkt og forfatter. Forskriften bygger på det utgangspunkt at denne struktureringen gir de nødvendige tekniske muligheter til å begrense tilgangen til det som er relevant og nødvendig. Det er en forutsetning at strukturen kan gjenspeiles i autorisasjonen og i praktisk funksjonalitet.

En organisering av informasjon om enkeltpasienter som er lik på tvers av alle pasientjournaler, slik at helsepersonell vet hvilke typer informasjon som finnes hvor, vil gjøre det lettere for helsepersonell å finne frem til relevant og nødvendig informasjon. En oversiktlig strukturering vil gi bedre sikkerhet, spare tid og bidra til bedre personvern.

Definisjonen omhandler ikke hvem det er som skal vurdere hvilke helsepersonell som skal foreta vurderingen av hvilke opplysninger som er relevante og nødvendige. Som oftest vil det være det helsepersonellet som skal vurdere hvilken helsehjelp pasienten eventuelt skal tilbys, som også må vurdere hva som er relevant og nødvendig. Dersom pasienten er ukjent for vedkommende helsepersonell kan det være formålstjenlig å samarbeide med helsepersonell som tidligere har gitt helsehjelp til pasienten i en slik vurdering.

### **3.4 § 4 Krav om system for administrering av autorisasjoner for tilgang til helseopplysninger**

*Den databehandlingsansvarlige skal etablere nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av autorisasjoner for tilgang til helseopplysninger.*

#### **Merknader til § 4**

Bestemmelsen gjelder alle autorisasjoner som gis for tilgang til helseopplysninger i den databehandlingsansvarliges virksomhet. Kravet om system for administrasjon av autorisasjoner og tilgangskontroll gjelder både når formålet med tilgangen til opplysningene er å yte forsvarlig helsehjelp, og når det gis tilgang til helseopplysninger i henhold til annet rettsgrunnlag.

Det følger av bestemmelsen at prosessen med tildeling av autorisasjon for tilgang til helseopplysninger består av to ledd, en organisatorisk del og en teknisk del.

Den organisatoriske delen innebærer å bestemme innholdet i autorisasjonen, det vil si hvilke rettigheter og plikter et bestemt helsepersonell skal ha for behandling av helseopplysninger. Andre organisatoriske tiltak er å sikre at databehandlingsansvarlig og databehandler har tilstrekkelig kompetanse, innarbeiding av rutiner og holdninger i virksomheten osv.

Nødvendig organisering av system for tildeling og administrasjon av autorisasjoner forutsetter at det er etablert rutiner for utarbeiding av stillingsbeskrivelser eller arbeidsbeskrivelser, som faktisk tydeliggjør og formaliserer de ulike roller i virksomheten.

Den tekniske delen består i å gjennomføre tiltak/handlinger slik at funksjonen autorisasjon implementeres i systemet i tråd med spesifikasjonen. Kontroll for å sikre autorisert bruk kan gjennomføres ved ulike sikringstiltak. Fysisk sikring omhandler sikring av systemets omgivelser ved lås, varslingssystemer etc. Teknisk sikring gjelder tilgangskontroller ved bruk av passord eller lignende.

Det skal settes tekniske skranke for de muligheter helsepersonell har til å logge inn i et IT-system og behandle helseopplysninger. Grunnlaget for å vurdere hvilke tekniske sperrer autorisasjonen skal sette er blant annet rolle og arbeidssted internt i virksomheten, virksomhetens organisasjon og rutiner. Det å ha teknisk mulighet til å lese journalopplysninger er ikke det samme som å ha autorisasjon til lese i journalen. Lovlig tilgang til helseopplysninger krever at reglene om taushetsplikt etterleves. Regler om helsepersonells taushetsplikt følger av helsepersonelloven kapittel 5, og for tilgang til helseopplysninger i journal og journalopplysninger vil reglene i helsepersonelloven §§ 25 og 45 være relevante.

Det skal foretas risikovurderinger av sannsynligheten for at en urettmessig tilegnelse av helseopplysninger kan skje, og eventuelle konsekvenser hvis det skjer. Det er en ledelsesoppgave å vurdere hvilken risiko som er akseptabel. Gjennomføring av risikovurderinger forutsetter god kjennskap til virksomhetens organisering og rutiner.

Kontroll av tildelte autorisasjoner må skje jevnlig, og endres i tråd med endringer i ansvars- og ansettelsesforhold, jf. § 6 fjerde ledd.

### **3.5 § 5 Autorisasjon for tilgang til helseopplysninger for personell som yter eller administrerer helsehjelp**

*Den databehandlingsansvarlige kan gi helsepersonell autorisasjon for tilgang til helseopplysninger for å kunne yte forsvarlig helsehjelp til en pasient.*

*Helsepersonells medhjelper, jf. helsepersonelloven § 5, kan gis autorisasjon for tilgang til helseopplysninger når det er nødvendig for å utføre medhjelperens oppgaver overfor pasienten. Personell som administrerer helsehjelp, jf. helsepersonelloven § 26 andre ledd, kan gis tilgang til helseopplysninger når det er nødvendig for å administrere helsehjelp til en pasient.*

*En autorisasjon skal knyttes til en entydig identifisert person i en bestemt rolle.*

#### **Merknader til § 5 første ledd**

Bestemmelsen gjelder autorisasjoner for tilgang til helseopplysninger der formålet med tilgangen er å yte forsvarlig helsehjelp til en pasient. Autorisasjon kan gis til helsepersonell, men også i noen tilfeller til helsepersonells medhjelper og administrativt personell.

Autorisasjon for tilgang til helseopplysninger fordi det anses nødvendig for å kunne fatte beslutning om helsehjelp, kan bare gis til personell som i kraft av sin rolle kan ta en slik beslutning. Bestemmelsen forutsetter et helsepersonell kan ha ulike autorisasjoner for ulike roller.

Bestemmelsen setter ikke maksimumskrav til antall registrerte helsepersonell som kan gis tilgang, eller mengde informasjon det kan gis tilgang til. Ivaretagelse av tilfredsstillende

informasjonssikkerhet krever imidlertid at den databehandlingsansvarlige har et gjennomtenkt forhold til dette spørsmålet ved tildeling av autorisasjoner for tilgang til helseopplysninger, og at innholdet i autorisasjonene vurderes ut ifra vedkommende helsepersonells rolle og oppgave i virksomheten. Dette må også ses i sammenheng med § 6 hvor tilgangen skal begrenses i omfang til det som er nødvendig.

### **Merknader til § 5 andre ledd**

Helsepersonells medhjelper er nærmere omtalt i helsepersonelloven § 5. Bestemmelsen fastslår at helsepersonell i sin virksomhet kan overlate bestemte oppgaver til annet personell hvis det er forsvarlig ut fra oppgavens art, personellets kvalifikasjoner og den oppfølging som gis.

Helsepersonells medhjelper som gis tilgang til helseopplysninger i et behandlingsrettet helseregister, vil som regel også være utdannet helsepersonell. Det kan for eksempel være en anestesisykepleier som utfører oppgaver på instruksjon fra en anestesilege eller en radiograf som utfører oppgaver på instruksjon fra en radiolog. Anestesisykepleieren eller radiografen vil i slike tilfeller dels kunne yte helsehjelp i kraft av sin egen formelle rolle, dels være medhjelper for lege med instruksjonsmyndighet.

Et annet eksempel er personell ved et sykehus som registrerer journalnotat etter diktafonopptak eller skanner journaldokumenter som foreligger i papirform. I slike tilfeller skal det ikke gis autorisasjon for tilgang til andre dokumenter enn de som blir registrert og de opplysninger som er nødvendig for å registrere dokumentene på riktig sted i journalen slik at medhjelperrollen kan utføres.

Helsepersonelloven § 26 andre ledd fastsetter rammer for hvilke opplysninger en autorisasjon til personell i pasientadministrasjonen kan gi tilgang til. Opplysninger det kan gis tilgang til er pasientens personnummer (fødselsnummer) og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data. Personell i pasientadministrasjonen kan ikke gis autorisasjon for tilgang til flere opplysninger enn de her nevnte.

### **Merknader til § 5 tredje ledd**

Det er et krav at autorisasjonen skal knyttes til en entydig identifisert person i en bestemt rolle. Utstedelse av en autorisasjon skal gjøres på basis av to forhold:

- 1) Personens identitet og
- 2) Den rollen personen har i virksomheten.

Et bestemt helsepersonell kan ha ulike roller i en virksomhet - i ulike tidsrom og ut fra ulike oppgaver vedkommende skal utføre. For eksempel kan det være slik at en lege i rollen "ansvarlig tilstedevakt" må ha tilgang til flere pasienters journaler enn en lege som ikke har slik vakt, men har et mer avgrenset ansvarsområde.

Det er personens rolle som er bestemmende for innholdet/omfanget av autorisasjonen, og ikke hvem personen er eller hvilken faggruppe han eller hun tilhører. Men det vil naturlig nok være slik at de fleste roller vil kreve formell kompetanse og mange roller vil derfor bare kunne tildeles helsepersonell som har denne kompetansen, for eksempel sykepleiere eller leger.

Autorisasjonssystemet må gi mulighet til å opprette roller som kan knyttes til de autorisasjoner som er nødvendige for at personell som tildeles rollen, skal kunne få tilgang til nødvendige og relevante opplysninger. Det vil si helseopplysninger som vurderes som relevante og nødvendige i forhold til de oppgaver som tilligger rollen. En rolle må kunne begrenses til kun å gjelde en avgrenset del av virksomheten, for eksempel medisinsk avdeling på et bestemt sykehus innen et helseforetak.

Det betyr at et helsepersonell (en identitet) kan ha ulike autorisasjoner, av ulikt omfang, til ulike formål og av ulik varighet. Rollen og autorisasjonen må knyttes til en identifisert person, og det innebærer også at vedkommende må kunne identifiseres i systemet. Dette henger også sammen med kravet til autentisering, se § 9.

Helsepersonell som skal treffe beslutning om ytelse av helsehjelp må selv ha tilgang til de opplysningene som er nødvendig for å treffe beslutningen. Det skal følge av autorisasjonen om helsepersonell har myndighet til å treffe slik beslutning, jf. § 5.

### **3.6 § 6 Begrensninger i autorisasjon for tilgang til helseopplysninger**

*Autorisasjon for tilgang til å lese, registrere, redigere, rette, slette, sperre eller på annen måte behandle helseopplysninger kan bare gis i det omfang som er nødvendig for at den enkelte kan ivareta sine arbeidsoppgaver.*

*Det kan bare gis autorisasjon for tilgang til helseopplysninger i ekstern virksomhet når autorisasjonen for dette er registrert i virksomhetens egne systemer.*

*En autorisasjon for tilgang til helseopplysninger skal tidsbegrenses.*

*Den enkeltes behov for tilgang skal vurderes og endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold.*

#### **Merknader til § 6 første ledd**

Det følger av bestemmelsen at en autorisasjon skal gis det innhold som er nødvendig for at helsepersonell skal kunne ivareta sine oppgaver og sitt ansvar ovenfor pasienten på en forsvarlig måte. En autorisasjon skal ikke gis større omfang enn nødvendig. Behovet den enkelte har for opplysninger, vil variere med hvilken tjeneste vedkommende utfører i forhold til pasienten. Tilgangsstyringen må ta høyde for dette, slik at det bare er nødvendige og relevante opplysninger det gis tilgang til.

En autorisasjon må - i tillegg til å kunne differensiere hvilke opplysninger det gis tilgang til - også kunne differensiere i forhold til oppgaver som skal utføres; skal helsepersonellet bare kunne lese opplysningene eller skal han eller hun også kunne skrive, kopiere, rette eller slette opplysninger; skal autorisasjonen også omfatte myndighet til å ta beslutning om helsehjelp etc. En konkret autorisasjon må kunne omfatte en eller flere av de elementer en autorisasjon kan bestå i. Eksempler:

- En autorisasjon til personell som i kraft av sin rolle i virksomheten har myndighet til å skrive i eller gjøre anmerkninger i journalen, må ha en autorisasjon som omfatter skrivetilgang.



- En autorisasjon til personell som i kraft av sin rolle bare har rett til å lese i journalen, må få en autorisasjon som bare omfatter lesetilgang.
- Helsepersonell som i kraft av sin rolle har myndighet til å treffe beslutning om å tilby helsehjelp, må få en autorisasjon som omfatter myndighet til å treffe en slik beslutning, og de rettigheter og plikter som følger av beslutningen.

#### **Merknader til § 6 andre ledd**

Bestemmelsen tydeliggjør skillet mellom intern og ekstern tilgang. Hensikten med bestemmelsen er å sikre at det gjøres en eksplisitt vurdering av om helsepersonell som har et tjenstlig behov for elektronisk tilgang til helseopplysninger i egen virksomhet, også skal kunne forespørre informasjon i ekstern virksomhet. Forutsetningene for tilgang til helseopplysninger på tvers av virksomhetene, er at det i eget system er en eksplisitt mulighet til å autorisere en bruker for ”rett til å forespørre informasjon i ekstern virksomhet”. Det er nødvendig for å forhindre at alle brukere som har et tjenstlig behov for tilgang i egen virksomhet, automatisk kan forespørre informasjon i ekstern virksomhet. I den eksterne virksomheten skal det tilsvarende være et system for å autorisere de brukere som kan logge seg på virksomhetens behandlingsrettede helseregistre.

#### **Merknader til § 6 tredje ledd**

Bestemmelsen forutsetter at den databehandlingsansvarlige med utgangspunkt i egen organisasjon og risikovurdering gjør en konkret vurdering av autorisasjonens varighet. Varigheten må også ses i sammenheng med vedkommendes roller og ansvarsområder.

#### **Merknader til § 6 fjerde ledd**

Endringer i organisering av virksomheten eller endringer i oppgave og ansvarsforhold, vil kreve ny vurdering av om en utstedt autorisasjon er hensiktsmessig eller om den bør endres. Dette henger sammen med kravet i § 5 om at tilgang skal knyttes til en bestemt rolle, og at systemet for administrering må dokumentere dette, jf. § 4.

### **3.7 § 7 Krav om opplæring**

*Den databehandlingsansvarlige skal sørge for at alle som gis autorisasjon for tilgang til helseopplysninger, får nødvendig opplæring og informasjon om bruken av autorisasjonen, begrensningene og mulighetene. Opplæringen skal som hovedregel gis før autorisasjonen utstedes, men i spesielle tilfelle kan den gis så snart som mulig etterpå.*

#### **Merknader til § 7**

Det følger allerede av personopplysningsforskriften § 2-8 at medarbeidere skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.

I tillegg til generell brukeropplæring som skal gis til alle som skal gis autorisasjon, krever bestemmelsen at den enkelte gis tilpasset opplæring i egen bruk og behandling av helseopplysninger, med utgangspunktet i vedkommendes rolle i virksomheten. Det bør

legges opp til at opplæring og kompetanseoppbygging skal vedvare, utdypes og videreføres etter hvert som en får erfaring med bruk av systemet.

Opplæringen bør i tillegg til bruk av informasjonssystemet basert på autorisasjonen, også bidra til at helsepersonell har kunnskap og adferd som sikrer ivaretagelse av informasjonssikkerhet, personvern og taushetsplikt.

Det kan ikke gis dispensasjon fra kravet om opplæring.

### **3.8 § 8 Krav om register over og kontroll av autorisasjoner for tilgang til helseopplysninger**

*Den databehandlingsansvarlige skal oppbevare oversikt over utstedte autorisasjoner for tilgang til helseopplysninger og begrunnelsene for dem. Oversikten skal gi informasjon om hvem som er tildelt autorisasjon, til hvilken rolle autorisasjonen er tildelt, formålet med den, tidspunktet for når den ble gitt, varigheten av autorisasjonen og om autorisasjonen er tilbakekalt.*

#### **Merknader til § 8**

Bestemmelsen forutsetter at databehandlingsansvarlig har rutiner for å oppdatere og vedlikeholde informasjon om utstedte autorisasjoner, og at denne oppbevares. I dokumentasjonen skal det fremkomme hvem som er tildelt autorisasjon, til hvilken rolle autorisasjonen er tildelt, formålet med den, tidspunktet for når den ble gitt, varigheten av autorisasjonen og om autorisasjonen er tilbakekalt. Dette må ses i sammenheng med § 4 som stiller krav til organisatoriske og tekniske tiltak for å administrere autorisasjoner, og øvrige krav i forskriften til innhold og omfang av autorisasjoner og knytningen til bestemte personer og roller.

Dokumentasjonen er også nødvendig for å kunne logge og spore hvem som har hatt tilgang til hvilke opplysninger, og for å kunne gi pasienten tilfredsstillende innsyn i hendelseslogger, jf. § 16.

Forskriften stiller ikke krav til hvor eller hvordan informasjonen oppbevares, og det vil være opp til virksomheten å vurdere hvor det er mest hensiktsmessig med slik dokumentasjon. Det kan være mulig å la denne dokumentasjonen fremgå av brukeradministrasjonen i eksisterende systemer. Forutsetningen er at virksomheten har oversikt over utstedte autorisasjoner, og har rutiner for administrasjon som gir nødvendig oversikt og mulighet for endringer ved behov.

Hvis dokumentasjonen er inntatt i et helseregister, er det naturlig at oppbevaringstiden følger registeret. Som utgangspunkt vil arkivlov med forskrifter komme til anvendelse for offentlige virksomheter. Ved etablering av Norsk helsearkiv vil krav til bevaring og avlevering også gjøres gjeldende overfor nærmere bestemte private virksomheter.

Generelt forutsetter sletting (kassasjon) av arkivmateriale at det enten er hjemlet i arkivloven eller at det innhentes godkjenning fra Riksarkivaren.

### 3.9 § 9 Krav om autentisering

*Den som gis elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister, skal autentisere seg ved bruk av personlig kvalifisert sertifikat eller en annen tilsvarende sikker autentiseringsløsning. Ved bruk av annen tilsvarende autentiseringsløsning må en risikovurdering vise at denne har tilstrekkelig sikkerhet.*

#### **Merknader til § 9**

Når det gis tilgang til helseopplysninger er det viktig at det er stor grad av sikkerhet for at personen som gis tilgang faktisk er den han eller hun utgir seg for å være. I helsepersonelloven § 21a og helseregisterloven § 13a er det nedfelt et forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger. Helsepersonellet kan være gjenstand for reaksjoner, herunder straff, ved brudd på bestemmelsene. Det må derfor være en sikker knytning mellom tilgang og vedkommende person.

Etter helseregisterloven § 13 og forskriften § 16 har også pasienten rett til innsyn i logg (hendelsesregister) fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne. Det er derfor nødvendig at det i systemet automatisk logges hvem som gjør hva, slik at pasientens innsynsrett kan ivaretas.

Bestemmelsen må ses i sammenheng med helseregisterloven § 6 første ledd:

”Behandlingsrettede helseregistre kan føres elektronisk. Det skal fremgå av registeret hvem som har registrert opplysningene. Dette kan gjøres ved hjelp av elektronisk signatur eller tilsvarende sikker dokumentasjon.”

Det presiseres at forskriften stiller krav ikke bare til at det logges hvem som har *registrert* opplysninger, men at all tilgang og oppslag skal logges.

Det skal alltid fremkomme og unikt kunne identifiseres hvilken person som har utført hvilke handlinger i helseregisteret, fortrinnsvis ved bruk av helsepersonellnummer (HPR-nummer). Dette kan for eksempel gjelde i situasjoner hvor ekstern bruker gjør påtegninger på røntgenbilder.

Det er derfor et krav at all tilgang til helseopplysninger kan knyttes til identifisert helsepersonell, og at autentiseringen skal baseres på personlig kvalifisert sertifikat eller annen tilsvarende sikker autentiseringsløsning. Med ”personlig kvalifisert sertifikat” forstås sertifikat som oppfyller Kravspesifikasjon for PKI i offentlig sektor. Etter Kravspesifikasjonen inkluderer dette sertifikater som kun er beregnet på autentisering eller kryptering, og dermed ikke er merket med ”kvalifisert”.

Bestemmelsen oppstiller ”annen tilsvarende sikker autentiseringsløsning” som alternativ til personlig kvalifisert sertifikat. Dette innebærer at det må foretas en risikovurdering av om annen sikkerhetsløsning, enn personlig kvalifisert sertifikat, kan anses som tilfredsstillende sikkerhet. Kravet til autentiseringsløsning i § 9 skal bidra til å sikre at vedkommende som gis tilgang til helseopplysningene faktisk er den vedkommende utgir seg for, og at tilgang kan logges og knyttes til en identifisert person.

Det må tas utgangspunkt i de krav forskriften setter til sikkerhet når det vurderes hva som er ”tilsvarende”. Spørsmålet om annen løsning har tilfredsstillende sikkerhet må vurderes konkret, og kan være forskjellig fra virksomhet til virksomhet. Sentralt i vurderingen vil blant annet være hvor ”transparent” virksomheten her, hvor stor den er, den databehandlingsansvarliges mulighet for kontroll osv. Den databehandlingsansvarliges mulighet for kontroll kan i mange tilfeller være større dersom det bare gis tilgang internt, enn om det åpnes for tilgang utenfra. Det må derfor også vurderes hvilke sikkerhetstiltak som er etablert. Særlig viktig vil sikkerheten i infrastrukturen som benyttes for tilgang til helseopplysninger være. Foregår tilgangen i en infrastruktur hvor øvrige sikkerhetstiltak skjermes tilgang for uvedkommende, kan det være akseptabelt med en annen autentisering enn personlig kvalifisert sertifikat så lenge kravet om knytning til enkeltperson ivaretas.

Det kan i risikovurderingen også tas i betraktning hvilke mekanismer virksomheten har for sikker tildeling av autentiseringsløsning. Hvis tildeling av autentiseringsløsning skjer på en slik måte at virksomheten har kontroll over knytning mellom autentiseringsløsning og person, f.eks. ved personlig oppmøte og identitetskontroll ved utdeling av brukernavn og passord, kan dette anses som tilsvarende sikkerhet. Det kan også tenkes at det kan være mulig å bruke allerede eksisterende autentiseringsløsninger i virksomheten, dersom dette gir tilstrekkelig sikkerhet.

Det understrekes at valg av annen autentiseringsløsning må gjøres på bakgrunn av en konkret risikovurdering som skal dokumenteres.

### **3.10 § 10 Rett til tilgang til helseopplysninger for personell som yter eller administrerer helsehjelp**

*Den som er autorisert for tilgang til helseopplysninger etter § 5, har bare rett til å behandle helseopplysninger som er nødvendige og relevante for å kunne yte eller administrere helsehjelp.*

*Retten til tilgang til helseopplysninger skal følge av en konkret beslutning om å yte helsehjelp til pasienten og være tilpasset pasientens behov for helsehjelp. Beslutningen skal dokumenteres.*

*Kravet om at retten til tilgang til helseopplysninger skal følge av en konkret beslutning om å yte helsehjelp til en pasient, kan fravikes dersom det på annen måte kan sikres at det ikke gis tilgang til flere opplysninger enn det som er nødvendig og relevant ut fra formålet med tilgangen.*

*Retten til tilgang til helseopplysninger varer så lenge det er nødvendig for å yte eller administrere helsehjelpen.*

#### **Merknader til § 10 første ledd**

Det er kun hvor helsepersonell er autorisert for tilgang til helseopplysninger, at vedkommende kan gis rett til tilgang til disse opplysningene. At det foreligger autorisasjon er således ikke nok, men det er en forutsetning for etterfølgende rett til

tilgang. Autorisasjonen gis for en tidsperiode, mens retten avgjøres fra gang til gang. Retten til tilgang kan kun gis til de helseopplysninger som er nødvendige og relevante for å yte den aktuelle helsehjelpen.

Kravet om at det bare kan gis tilgang til nødvendige og relevante opplysninger for å kunne gi helsehjelp til pasienten, må anses som et funksjonskrav. Dette innebærer krav om at journalen må struktureres slik at denne funksjonen kan oppfylles. Strukturerte journaler muliggjør også organisering av informasjon i elektroniske pasientjournalssystemer, slik at brukere raskt kan finne frem til relevante opplysninger.

Bestemmelsen krever at systemene som benyttes må kunne gi en differensiert mulighet for tilgangsstyring slik at en ved korrekt bruk av systemet kan hindre at helsepersonell får tilgang til andre opplysninger enn det som de etter gjeldende regelverk skal ha tilgang til. Det enkelte systemets funksjoner og muligheter må gjenspeiles/utnyttes i den praktiske tilgangsstyringen.

Dersom utstyret eller de tekniske hjelpemidlene som brukes ikke har tilstrekkelig differensiert teknisk tilgangsstyring, må den databehandlingsansvarlige avhjelpe dette ved andre tiltak slik at pasientens rett til konfidensialitet og forskriftens formål for øvrig, etterleves. For eksempel kan helsepersonell gis en mer begrenset autorisasjon, i tillegg til at virksomheten organiseres slik at det er tilrettelagt for hyppige vurderinger av tilgangsrettigheter, og at virksomheten raskt kan gjøre endringer/tilpasninger i disse. Det samme gjelder i forhold til personell i pasientadministrasjonen. Med bakgrunn i foretatte risikovurderinger er det databehandlingsansvarligs ansvar å avpasse de tekniske og organisatoriske tiltakene til hverandre, slik at kravene til informasjonssikkerheten i virksomheten etterleves og at målene for virksomheten nås.

### **Merknader til § 10 andre ledd**

Det understrekes at hovedregelen om beslutningsstyrt tilgang til helseopplysninger som utgangspunkt også gjelder ved intern tilgangsstyring; beslutningsstyrt tilgangsstyring er således ikke bare en forutsetning for tilgang til helseopplysninger på tvers av virksomheter.

Bestemmelsen krever at virksomheten bygger opp og organiserer sitt autorisasjonssystem slik at det støtter opp om beslutningsstyrt tilgang tilpasset den type helsehjelp virksomheten yter.

Bestemmelsen har som utgangspunkt at det ligger beslutninger til grunn for all helsehjelp, og at tilgang til helseopplysninger automatisk skal følge av en slik beslutning. Det kan være eksplisitte beslutninger som for eksempel en kommunes vedtak om å tilby en søker sykehjemsplass, eller mer implisitte beslutninger, som når en allmennlege mottar en pasient som har bestilt time. Når beslutningen om helsehjelp registreres i pasientens elektronisk journal, åpner dette for at helsepersonell som forventes å skulle delta i gjennomføringen av helsehjelpen (behandlingsforløpet) kan få tilgang til relevante helseopplysninger. Hvilke opplysninger det da gis tilgang til skal følge av helsepersonellens autorisasjon og en vurdering av hva slags helsehjelp pasienten vil kunne ha behov for. I tillegg til at slik tilgangsstyring sikrer at tilgangsmuligheten i størst mulig grad begrenses til helsepersonell som skal yte helsehjelp til pasienten, sikrer den også at

registreringen i journalen av tilgangen automatisk kan knyttes opp mot den beslutning om helsehjelp som legitimerer tilgangen.

På sykehus vil det ved mottak av og journalføring av opplysninger om innkommet pasient vurderes et planlagt eller forventet behandlingsforløp for pasienten. Vurdert behandlingsforløp gjør det klart hvor helsehjelpen skal tilbys og hvilke helsepersonell man forventer vil kunne bli delaktig i ytelse av helsehjelpen. Det kan være medisinsk avdeling, hjerte-medisinsk avdeling, kirurgisk avdeling, ortopedisk avdeling etc. Videre kan det være klart eller sannsynlig at pasienten vil motta helsehjelp fra anestesivdeling, operasjonsavdeling, radiologisk avdeling eller andre fagspesialiserte avdelinger. Også etter at en pasient er tatt under behandling for eksempel på et sykehus, tas det en rekke beslutninger. Enkelte av disse beslutningene kan resultere i at også annet helsepersonell blir involvert i helsehjelpen, og disse må da få tilgang til nødvendige opplysninger.

For å kunne treffe en forsvarlig beslutning om ytelse av helsehjelp, må det helsepersonell som skal treffe beslutningen selv ha tilgang til relevante helseopplysningene. Det skal følge av autorisasjonen dersom helsepersonell har myndighet til på eget initiativ å tilegne seg de opplysninger fra en pasients journal som er nødvendige for å treffe slik beslutning.

Det følger også av prinsippet om beslutningsstyrt tilgang at helsepersonell som har myndighet til å treffe beslutning om helsehjelp og som kan involvere annet helsepersonell, også må ha myndighet til å gi dette helsepersonellet tilgang til de helseopplysninger som er nødvendige for å kunne yte forsvarlig helsehjelp. For eksempel, en anestesilege på kirurgisk avdelingen som mener det er nødvendig med tilsyn av indremedisiner før en anestesi, må kunne åpne for tilgang til aktuelle helseopplysninger for aktuelt personell i indremedisinsk avdeling.

Bestemmelsen innebærer at dersom det ikke er tatt noen beslutning om at en bestemt pasient skal gis helsehjelp, vil helsepersonell heller ikke ha lovlig tilgang til registrerte opplysninger om pasienten. Beslutningen om helsehjelp skal dokumenteres i pasientens journal.

Selv om en har beslutningsstyrt tilgang kan det likevel være slik at en autorisasjon for tilgang til helseopplysninger gir en noe videre teknisk mulighet for tilgang til elektronisk lagrede helseopplysninger enn hva overholdelse av taushetsplikten strengt tatt innebærer. Begrunnelsen for dette er at kravet til informasjonssikkerhet også setter krav til opplysningenes tilgjengelighet. Videre er det slik at helsepersonell ikke på forhånd helt eksakt kan avgrense hvilke opplysninger som er nødvendige for å kunne vurdere eller yte helsehjelp. Mange ganger kan det være nærmest umulig eller i hvert fall meget vanskelig å avgrense tilgangen til kun de opplysninger som er nødvendige for helsehjelpen. Videre vil det være vanskelig å vurdere helt eksakt hvilke helsepersonell som skal yte helsehjelp til en bestemt pasient. Det er først og fremst i pasientens interesse at nødvendige og relevante helseopplysninger er til stede for helsepersonell – som grunnlag for helsefaglige vurderinger – i samspelet mellom helsepersonell og pasient.

Det er ikke til å unngå at helsepersonell i enkelte tilfeller kan få tilgang til helseopplysninger de strengt tatt ikke har behov for. I tillegg til tekniske sperrer for tilgang til helseopplysninger, må den databehandlingsansvarlige også sørge for andre tiltak, herunder organisatoriske og administrative tiltak, for at hensynet til pasientenes

konfidensialitet skal ivaretas. Den databehandlingsansvarlige må også påse at helsepersonell har kunnskap og en adferd, som gjør at opplysningenes konfidensialitet og pasientenes integritet ivaretas.

Se også forskriften § 7 om krav til opplæring og § 16 om krav til dokumentasjon av tilgang.

#### **Merknader til § 10 tredje ledd**

Bestemmelsen kan særlig være relevant ved tilgang til spesialiserte fagsystemer hvor kun et begrenset antall personell (internt i virksomheten) vil være autorisert for tilgang. Tredje ledd kan som hovedregel ikke brukes som rettsgrunnlag for tilgang til opplysninger på tvers av virksomheter.

#### **Merknader til § 10 fjerde ledd**

Bestemmelsen krever at virksomheten vurderer om varigheten av de ulike helsepersonells tilgang til ulike typer helseopplysninger skal differensieres. En slik vurdering kan for eksempel gjøres ut fra hvilken rolle det aktuelle helsepersonellet har i forhold til beslutning om og gjennomføring av hjelpen. Mens enkelte ikke vil ha behov for tilgang til helseopplysninger etter at en pasienten er utskrevet fra et sykehus, vil andre fortsatt ha behov for tilgang, for eksempel for å kunne vurdere de siste analyseresultater og skrive epikrise. Tidsrommet omfatter også tiden det tar å dokumentere/registrere opplysningene.

Retten til tilgang må være innenfor varigheten til autorisasjonen.

### **4.11 § 11 Avtale om lesetilgang på tvers av virksomheter**

*Den databehandlingsansvarlige kan inngå avtale med annen virksomhet om lesetilgang til strukturerte helseopplysninger i behandlingsrettet register som virksomheten er ansvarlig for, dersom:*

- a) formålet med tilgangen er å yte helsehjelp til pasient*
- b) begge virksomheter har tekniske løsninger som kan avgrense tilgangen til å omfatte strukturerte helseopplysninger knyttet til en navngitt pasient*
- c) gjennomføringen ikke svekker informasjonssikkerheten ved behandling av helseopplysninger ved noen av virksomhetene*
- d) begge parter i avtalen kjenner den andre partens sikkerhetsmål og sikkerhetsstrategi*

*Avtalen skal angi*

- a) typer helsehjelp avtalen gjelder*
- b) de tekniske løsningene som skal benyttes ved tilgangen*
- c) eventuelt andre vilkår for tilgangen.*

## **Merknader til § 11 første ledd**

Virksomheter som gis tilgang til hverandres behandlingsrettede helseregistre må på forhånd ha inngått en særskilt avtale om tilgang på tvers av virksomhetene. Utgangspunktet er at tilgang kun gjelder lesetilgang. All lesetilgang fra eksternt helsepersonell skal logges og identifiseres.

Det presiseres at kravet om avtale ikke kommer i stedet for andre sikkerhetskrav, men i tillegg. Avtalen må holde seg innenfor lovens og forskriftens rammer.

Det er en forutsetning at slik avtale bare inngås der det er behov for det. Dette vil særlig gjelde i tilfeller der det er utstrakt samarbeid om behandling av pasienter på tvers av virksomhetsgrensene. Avtale om tilgang til helseopplysninger på tvers av virksomhetsgrenser kan bare avtales for informasjonssystemer som kan oppfylle alle kravene i forskriften.

Det legges til grunn at meldingsutveksling og eventuell annen form for utlevering av helseopplysninger fortsatt skal benyttes der dette anses mest formålstjenelig og sikkert. Dette vil også være gjeldende i de tilfeller der pasienten ikke samtykker til tilgang til helseopplysninger på tvers.

For helseinstitusjoner som har et meget fast og formelt samarbeid om oppgavedeling innenfor en bestemt gren av medisinen kan det være mest formålstjenelig å inngå avtale om tilgang på tvers. For andre helseinstitusjoner kan det være mest formålstjenelig å basere seg på meldingsutveksling. Når det gjelder kommunikasjon mellom fastleger og helseforetak antas at det i mange tilfeller kan være mest hensiktsmessig å kommunisere via utveksling (epikriser og henvisninger) av meldinger. Det samme gjelder mellom fastlege og pleie- og omsorgstjenesten. Det er første og fremst der meldingsutveksling ikke er godt nok, at avtale om tilgang på tvers av virksomhetsgrenser bør inngås.

For eksempel kan avtale på tvers mellom primær- og spesialisthelsetjeneste være hensiktsmessig, ved samhandling mellom en kommunes legevakt og sykehus; det gjelder særlig der kommunens legevakt er lokalisert på sykehuset. Et annet eksempel er ved teamsamarbeid mellom primærhelsetjenesten og spesialisthelsetjenesten for oppfølging av pasienter med nærmere bestemte lidelser. Her kan det være hensiktsmessig at sykehusansatte har direkte lesetilgang til pasientopplysninger i journal i primærhelsetjenesten – og/eller at en ansatt i kommunen har lesetilgang til opplysninger i pasientens journal i spesialisthelsetjenesten.

**Første ledd bokstav a** presiserer at bestemmelsen bare gjelder der formålet med tilgangen er helsehjelp. Tilgang til journalopplysninger på tvers skal bare kunne gis når det er behov for det, til dem som deltar i behandlingen, for å kunne tilby pasienten forsvarlig helsehjelp. Det innebærer at det ikke kan gis tilgang på tvers av virksomhetsgrenser etter denne bestemmelsen dersom formålet er kvalitetssikring, undervisning eller forskning.

**Første ledd bokstav b** stiller krav om at begge virksomheter har systemer med nødvendig tilgangsstyring. Tilgangsstyringen må bidra til at det bare er nødvendige og relevante opplysninger det gis tilgang til, innenfor rammene av de strukturerte og standardiserte opplysningene. Dette innebærer at databehandlingsansvarlige som har journalsystemer som ikke kan oppfylle en slik funksjon, ikke kan inngå avtale med annen virksomhet om tilgang på tvers.

Forespørselen om tilgang må kunne knyttes til en navngitt pasient, og dette henger sammen med forskriften § 14 og helseregisterloven § 13 som presiserer at en forespørsel



om tilgang bare kan gjelde én pasient om gangen. Dette stiller tilsvarende krav til systemene om at det er mulig å gi tilgang kun til enkeltpasienter.

Det innebærer ikke at det må inngås ny avtale hver gang det er behov for tilgang på tvers av virksomheter. Avtalen skal ikke inneholde personidentifiserbare data og må formuleres på generelt nivå.

**Første ledd bokstav c og d** forutsetter at den databehandlingsansvarlige som åpner for tilgang til helseopplysninger fra ekstern virksomhet, før avtale inngås, har mulighet til å sjekke at virksomheten den inngår avtale med kan oppfylle kravet til tilfredsstillende informasjonssikkerhet. Det er en forutsetning at avtaler om tilgang på tvers av virksomheter, ikke på noen måte vil svekke informasjonssikkerheten til helseopplysninger.

Gjennomføring av kravet i bokstavene c og d innebærer at den databehandlingsansvarlige som gir tilgang til opplysningene må ha kunnskap om tilgangsstyringen og andre forhold som kan påvirke informasjonssikkerheten i den virksomheten som gis tilgang. Tilgang på tvers av virksomhetsgrenser kan i utgangspunktet bare avtales for informasjonssystemer som kan oppfylle alle forskriftens bestemmelser. Kunnskap om den eksterne virksomhetens sikkerhetsmål og sikkerhetsstrategi vil være premisser i vurderingen av om det vil være hensiktsmessig å inngå avtale om tilgang på tvers og eventuelt i hvilket omfang.

#### **Merknader til § 11 andre ledd**

Det må følge av avtalen hvilke type helsehjelp den gjelder. Behovet for og virkeområdet for avtalen skal være fundert på konkrete behovs- og nødvendighetsvurderinger. At det generelt kan oppstå en situasjon der det kan være "kjekt å ha" tilgang til opplysninger på tvers av virksomheten er ikke nok.

Det må også fremgå av avtalen hvilke forutsetninger som ligger til grunn for avtalen, blant annet hvilke tekniske løsninger som skal benyttes av partene ved slik tilgang. Dette inkluderer informasjon om tilgangsstyring og informasjonssikkerhet, som er forutsetninger som må være til stede etter første ledd.

Den databehandlingsansvarlige må også kunne sette vilkår for behandlingen av opplysningene i den virksomheten som gis tilgang. Databehandlingsansvarlig kan ikke fraskrive seg dette ansvaret ved avtale. Begge parter vil ha ansvar for informasjonssikkerheten, og det bør også fremgå av avtalen at den virksomheten som får tilgang skal etablere internkontroll for å sikre at helseregisterloven, helseinformasjonssikkerhetsforskriften og avtalen overholdes. Både den databehandlingsansvarlige og den som gis tilgang vil kunne bli holdt ansvarlig ved overtredelse av avtalen og nevnte regelverk.

#### **4.12 § 12 Særlig avtale om skrive-tilgang på tvers av virksomheter**

*Dersom det er nødvendig for helsehjelpen pasienten tilbys og for å utføre formålet med lesetilgang etter § 11, kan avtalen for særskilte områder gi helsepersonell i en*

*bestemt rolle adgang til å registrere opplysninger i det behandlingsrettede helseregisteret det er gitt tilgang til.*

### **Merknader til § 12**

Det kan under gitte forutsetninger avtales skrivetilgang på tvers, i tillegg til lesetilgang. Bestemmelsen har et virkeområde begrenset til samarbeid der det er nødvendig for helsehjelpen som pasienten tilbys at helsepersonell i en bestemt rolle gis adgang til å registrere opplysninger. Bestemmelsen gir imidlertid ikke hjemmel for å erstatte registrering av nødvendige og relevante opplysninger i pasientens journal i egen virksomhet, med registrering i det helseregistret det er gitt tilgang til. All skrivetilgang fra eksternt helsepersonell skal logges og identifiseres.

Et eksempel på hvor bestemmelsen vil kunne anvendes, er innenfor radiologien: En pasient er innlagt på et sykehus for å ta MR, CT eller annen type røntgen undersøkelse, og legen på sykehuset trenger hjelp til å tolke funnene av en spesialist i annen virksomhet. Legen i den eksterne virksomheten (som tolker bildet) vil i enkelte tilfelle kunne ha behov for å gjøre en anmerkning på bildet for å synliggjøre hvor på bildet funn ligger. Dersom det gjøres en tolkning av bildet, må det også registreres/fremgå hvem det er som har gjort denne tolkningen.

### **4.13 § 13 Unntak fra krav om uttrykkelig samtykke**

*Kravet etter helseregisterloven § 13 tredje ledd om uttrykkelig samtykke for tilgang til helseopplysninger på tvers av virksomheter, kan fravikes dersom pasienten på grunn av sin fysiske eller psykiske tilstand ikke er i stand til å gi et slikt samtykke, og det må antas at pasienten ville ha gitt uttrykkelig samtykke dersom han eller hun hadde vært i stand til det. Det skal fremgå av registeret at uttrykkelig samtykke ikke er gitt og begrunnelsen for det.*

### **Merknader til § 13**

Bestemmelsen gir bare unntak fra kravet til uttrykkelig samtykke etter helseregisterloven § 13, jf. helseregisterloven § 2 nr. 11. Helseregisterloven § 13 åpner ikke for unntak fra samtykkekrav som følger av pasientrettighetsloven<sup>1</sup>.

Dersom pasienten er bevisstløs eller er i en tilstand der vedkommende ikke er i stand til å motta informasjon, må helsepersonell gjøre en konkret vurdering av hva hun antar at pasienten hadde ønsket. I slike tilfeller vil opplysningenes sensitivitet og hvor nødvendige de er for den aktuelle helsehjelpen, være en del av vurderingen.

Det skal i registeret gis en kort omtale av hvilken tilstand pasienten er i, som begrunner hvorfor han eller hun ikke er i stand til samtykke.

---

<sup>1</sup> Det følger av pasientrettighetsloven § 4-1 at helsehjelp bare kan gis med pasientens samtykke. Samtykke kan gis uttrykkelig eller stilltiende. Stilltiende samtykke anses å foreligge dersom det ut fra pasientens handlemåte og omstendighetene for øvrig er sannsynlig at hun eller han godtar helsehjelpen, jf. pasrl. § 4-2.

Det presiseres at helsepersonell ikke uten videre kan legge til grunn at taushet fra pasienten innebærer et stilltiende samtykke. Helsepersonellet må konkret vurdere i hvert enkelt tilfelle om pasienten har fått tilstrekkelig informasjon om behandlingen av opplysningene, og om pasientens adferd tilsier at samtykke foreligger.

#### **4.14 § 14 Behandling av den enkelte forespørselen mellom virksomheter**

*En forespørsel om og tilgang til helseopplysninger i annen virksomhet skal som hovedregel gå gjennom autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet.*

*I tilfeller hvor det er avtalt mellom virksomhetene, kan forespørselen gå igjennom autorisasjons- og autentiseringsmekanismer ved virksomheten hvor de etterspurte opplysningene finnes.*

*Forespørselen om og tilgangen til helseopplysninger kan bare omfatte en person om gangen.*

*Behandlingen av forespørselen kan automatiseres dersom pasienten overfor virksomheten som gir tilgang til opplysningene, har avgitt en frivillig, uttrykkelig og informert erklæring om å godta at andre virksomheter kan gis tilgang til opplysningene. Tilgangen kan være så lenge det er nødvendig for å yte helsehjelp til pasienten.*

*Når pasienten ikke har samtykket skal forespørselen behandles manuelt.*

*Forespørselen om tilgang og resultatet av behandlingen av forespørselen, skal registreres.*

#### **Merknader til § 14 første ledd**

Helsepersonell som ønsker tilgang til helseopplysninger i ekstern virksomhet må begynne prosessen med først å bli autorisert og autentisert for tilgang til opplysninger i egen virksomhet. Tilgang til opplysninger i den eksterne virksomheten kan bare gis der det tjenstlige behovet er identifisert og dokumentert i egen virksomhet, og autorisasjonen må derfor gis av egen virksomhet. Det samme gjelder autentiseringen for helsepersonell, som vil være egen virksomhets ansvar.

Hovedregelen er at autentiseringen til annen virksomhets system, skal gå via egne interne systemer. Dette krever imidlertid samhandling mellom de to virksomhetenes systemer. Der hvor virksomhetene etter en risikovurdering finner det hensiktsmessig, kan det også benyttes fellestjenester for validering og federering som f. eks ID-porten.

#### **Merknader til § 14 andre ledd**

Bestemmelsen åpner for at forespørselen kan skje via autorisasjons- og autentiseringsmekanismer i regi av den virksomhet hvor de etterspurte opplysningene finnes.

Det kan for eksempel være aktuell når helsepersonell fra spesialisthelsetjenesten yter helsehjelp til en pasient i et kommunalt sykehjem eller et (inter)kommunalt distriktsmedisinsk senter.

Et annet eksempel er tilfeller der spesialist fra et spesialistsykehus tilbringer noen dager på et annet sykehus (som tilhører en annen virksomhet) for å undersøke/behandle pasienter i sykehusets nærområde. Vedkommende helsepersonell kan da bli autorisert for tilgang til den andre virksomhetens system.

#### **Merknader til § 14 tredje ledd**

Forespørsel til ekstern virksomhet om tilgang til en pasients helseopplysninger, kan ikke omfatte mer enn én pasient om gangen. Ved behov for gjentatt tilgang må det skje en ny forespørsel. Ved behov for oppslag i en annen pasients helseopplysninger må tilgangsvurderingen gjøres på nytt fra egen virksomhets system, basert på tjenestelig behov.

#### **Merknader til § 14 fjerde ledd**

Bestemmelsen fastsetter vilkår for at behandlingen av forespørselen kan skje automatisk. Automatisert behandling krever at pasientens samtykke må være registrert i journalen til pasienten i den virksomheten som gir tilgang til opplysningen, i tillegg til at pasienten må samtykke ved selve tidspunktet når tilgangen skjer.

Det følger av andre punktum at tilgangen kan være så lenge det er nødvendig å yte helsehjelp til pasienten. Ordet helsehjelp referer til behandlingsforløpet for den aktuelle sykdommen eller lidelsen pasienten mottar helsehjelp for.

#### **Merknader til § 14 femte ledd**

Dersom pasienten ikke har avgitt samtykke i den virksomheten som gir tilgang til opplysningene, skal forespørselen til den andre virksomheten skje manuelt, eksempelvis ved telefonoppringning. Dersom pasienten heller ikke gir samtykke til den eksterne virksomheten, skal opplysningene utleveres i henhold til ordinære rutiner.

I tilfeller hvor pasienten ikke er i stand til å gi et uttrykkelig samtykke, må det vurderes konkret hvorvidt pasienten ville ha gitt slikt samtykke, jf. 13. I så fall må virksomheten vurdere om situasjonen tilsier at det kan gis tilgang, eller om de etterspurte opplysningene heller bør utleveres på en annen hensiktsmessig måte.

### **4.15 § 15 Sperring av helseopplysninger**

*Dersom pasienten har motsatt seg at andre får tilgang til helseopplysninger, jf. pasientrettighetsloven § 5-3 og helsepersonelloven § 25 og § 45, skal opplysningene sperres.*

*Pasienten kan bestemme om sperringen bare skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for dem pasienten selv bestemmer, eller om de bare skal være tilgjengelige etter samtykke.*

*Det skal fremgå av journalen om registrerte opplysninger er sperret.*

*Det kan gis tilgang til sperrede opplysninger dersom tungtveiende grunner taler for det, jf. pasientrettighetsloven § 5-3.*

### **Merknader til § 15 første ledd**

Pasienten har etter pasientrettighetsloven § 5-3 en rett til å motsette seg utlevering av journal eller opplysninger i journal. Pasienten har en tilsvarende rett til å motsette seg at andre får tilgang til helseopplysninger, og de skal i tilfelle sperres for tilgang.

Selv om alle helseopplysninger regnes som sensitive opplysninger, vil det ofte være slik at noen helseopplysninger fremstår som mer sensitive enn andre. Opplysninger om tidligere psykisk sykdom, visse smittsomme sykdommer, særskilt ømtålige spørsmål etc., kan pasienten føle belastende dersom opplysningene blir delt med annet helsepersonell. Det er derfor viktig at helsepersonell ved registrering av opplysninger har et bevisst forhold til hvilke opplysninger som etter journalføringen kan være tilgjengelig for annet helsepersonell, og samtaler med pasienten om det.

Det presiseres at pasientens rett til sperring av helseopplysninger skal være reell. Den gjelder generelt, både ved tilgang internt i virksomheten og ved tilgang på tvers.

### **Merknader til § 15 andre ledd**

Bestemmelsen legger til rette for at pasienten selv kan ha kontroll med hvilke opplysninger annet helsepersonell kan få tilgang til. Pasienten kan bestemme om sperringen bare skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for dem pasienten selv bestemmer eller om de bare skal være tilgjengelige etter samtykke.

Hvis en pasient vil at tilgang til helseopplysninger om henne bare skal gis til personell i mottakelsesavdelingen, og for øvrig bare etter samtykke, må tilgangsstyringen ha funksjonalitet som sikrer at dette ivaretas.

Dersom et fagsystem ikke har funksjonalitet for sperring av helseopplysninger, må virksomheten søke om dispensasjon fra dette kravet. Det at et fagsystem ikke har funksjonalitet for sperring innebærer imidlertid ikke at pasientopplysningene ikke skal vernes. Helsepersonelloven §§ 25 og 45 og pasient- og brukerrettighetsloven § 5-3 om pasientens rett til å motsette seg at annet helsepersonell får tilgang til opplysningene, vil fortsatt gjelde.

### **Merknader til § 15 tredje ledd**

Det skal fremgå av journalen at det er registrert opplysninger som er sperret. Dette skal gjøres uten hensyn til type opplysninger, fordi det i forkant kan være vanskelig å vurdere om og eventuelt hvor viktige disse opplysningene er for helsehjelpstilbudet til pasienten.

Ofte kan det være uproblematisk for helsepersonell i en konkret behandlingssituasjon å vite at det finnes sperrede opplysninger, fordi personellet kan spørre pasienten om hvilke opplysninger det gjelder, og ut fra det vurdere om det er behovet for dem. Pasienten kan da selv gi aktuelt helsepersonell den nødvendige informasjon eller samtykke til at helsepersonell gis tilgang til de sperrede opplysningene. Hvis pasienten ikke er i stand til å informere om opplysningene eller ikke er i stand til å samtykke, kan helsepersonell bare få tilgang til opplysningene etter pasientrettighetsloven § 5-3.

### **Merknader til § 15 fjerde ledd**

Pasientens rett til å reservere seg mot at annet helsepersonell gis tilgang til helseopplysninger er ikke absolutt. I enkelte tilfelle vil det kunne være av stor betydning at helsepersonell får kjennskap til tidligere sykdomshistorie eller medisinsk/kirurgisk behandling. En forutsetning for at helsepersonell skal få tilgang til opplysninger pasienten har motsatt seg at det gis tilgang til, er dersom ”tungtveiende grunner taler for det”.

En akutt situasjon hvor det kreves at pasienten øyeblikkelig legges i narkose i forkant av operasjon/kirurgisk inngrep kan være eksempel på en slik situasjon. Det må være det helsepersonellet som har ansvaret for pasienten i akutt situasjonen, og som på selvstendig grunnlag kan treffe beslutning om helsehjelp, som må vurdere om han eller hun må ha tilgang til de sperrede opplysningene. Herunder må beslutningstakeren vurdere om og i hvilken grad andre tjenesteytere som er involvert i behandlingen av pasienten skal få kjennskap til opplysningene.

### **4.16 § 16 Krav om dokumentasjon av tilgang**

*All tilgang til opplysninger i et behandlingsrettet helseregister skal dokumenteres automatisk i registeret. Dokumentasjonen skal inneholde informasjon om*

- a) navn, rolle og organisatorisk tilhørighet til den som har fått tilgang*
- b) grunnlaget for tilgangen*
- c) tidspunktet vedkommende har hatt tilgang til opplysningene.*

*Dokumentasjonen skal inngå som en del av registeret og pasienten har rett til innsyn i dokumentasjonen, jf. pasientrettighetsloven § 5-1 og helseregisterloven § 13 sjette ledd.*

*Pasienten har rett til utskrift av dokumentasjonen. Informasjonen i utskriften skal kunne sorteres etter pasientens ønske.*

*Forespørsler om innsyn og utskrift skal besvares uten ugrunnet opphold og senest 30 dager etter at henvendelsen kom inn. Det kan ikke tas vederlag for utskrifter med mindre særlige forhold tilsier det.*

### **Merknader til § 16 første ledd**

Bestemmelsen er en spesialbestemmelse for behandlingsrettede helseregistre og gjelder i tillegg til de mer generelle bestemmelsene i personopplysningsforskriften § 2-14 om registrering av uautorisert bruk av informasjonssystem og § 2-16 om registrering av autorisert og forsøk på uautorisert bruk.

All tilgang skal registreres automatisk i systemet, dvs. hendelseslogg. Dette kravet følger også av helseregisterloven § 13 sjette ledd, og av helsepersonelloven § 45 hvor det skal registreres i journal dersom annet helsepersonell er gitt helseopplysningene. Logging av informasjon om hvem som har hatt tilgang til taushetsbelagte opplysninger, er et viktig tiltak for å bedre informasjonssikkerheten. Det er et sentralt element i personvernet at den enkelte skal ha rett til og reell mulighet til å ha kontroll over helseopplysninger om seg

selv. Informasjon om hvem som har hatt tilgang til helseopplysninger om en via innsyn i logg, vil bidra til å øke pasientens kontroll med opplysningene og gjøre personvernet mer betryggende. All tilgang skal logges.

Logging er et supplement til god tilgangsstyring, og kommer ikke i stedet for andre sikkerhetstiltak eller tilgangsstyring.

Det understrekes at kravet om dokumentasjon gjelder alle tilfeller der det gis tilgang til helseopplysninger i et behandlingsrettet helseregister, ikke bare der formålet er helsehjelp til pasient. Det innebærer at behandlingsrettede helseregistre må ha funksjonalitet for logging, og at det også skal logges tilgang som gis på annet grunnlag enn etter denne forskriften, f. eks til forskning eller kvalitetsstyring. Pasientens rett til å få innsyn i hvem som har hatt tilgang til hennes helseopplysninger, gjelder således all type tilgang.

Oppstillingen i første ledd over informasjon som skal dokumenteres automatisk, er å betrakte som et minimumskrav til et hendelsesregister. For å kunne oppfylle kravene om oppfølging og kontroll av elektronisk tilgang i forskriften § 17, kan det være nødvendig å inkludere annen informasjon i hendelsesregisteret, for eksempel mer detaljert knytning mellom hendelsene og opplysningene. Dette kan for eksempel være tidsstempeling i systemet, knyttet til innlogging og senere hendelser som lesing eller redigering. Virksomhetene bør søke å finne fram til løsninger som er best mulig egnet til å avdekke uautorisert tilgang til helseopplysninger.

**Første ledd bokstav a** stiller krav om at personer som har fått tilgang til pasientens helseopplysninger, skal identifiseres med navn, rolle og organisatorisk tilhørighet. Kravet om dokumentasjon må ses i sammenheng med bestemmelsene i forskriften om autorisasjon for tilgang for helsepersonell med entydig knytning til identitet og rolle, og kravet til autentisering.

**Første ledd bokstav b** sier at grunnlaget for tilgangen skal dokumenteres, og dette omfatter både rettslig grunnlag og faktisk grunnlag. Ved ytelse av helsehjelp må registreringen inkludere tilstrekkelige opplysninger slik at det er mulig å kontrollere i ettertid om tilgangen var berettiget.

Reglene om taushetsplikt i helsepersonelloven og helseregisterloven skal følges. Det betyr at helseopplysningene kun skal brukes til å yte helsehjelp, administrasjon av helsehjelp eller der hvor bruken ellers har hjemmel i lov eller forskrift. Det skal fremkomme av dokumentasjonen hvilken hjemmel som er grunnlaget for tilgangen. Ved beslutningsstyrt tilgang skal beslutningen om helsehjelp som legitimerer tilgangen, fremkomme av dokumentasjonen av grunnlaget for tilgangen.

Eksempler på rettslig grunnlag som skal dokumenteres i registeret:

- Helsepersonelloven § 25 eller § 45 for utlevering og tilgang på tvers,
- Helsepersonelloven § 25 andre ledd dersom servicepersonell er gitt tilgang til helseopplysninger
- Helsepersonelloven § 29 og helseforskningsloven § 35 hvor det er gitt tilgang til helseopplysninger til forskning

- Helsepersonelloven § 29 b hvor departementet har bestemt bruk av helseopplysninger til kvalitetssikring, administrasjon, styring eller planlegging av helse- og omsorgstjenesten
- Helsepersonelloven § 26 første ledd når helseopplysninger er gitt til virksomhetens ledelse for internkontroll og kvalitetssikring

**Første ledd bokstav c** krever at det dokumenteres hvilket tidspunkt vedkommende har hatt tilgang til opplysningene.

Mens det for enkelte beslutninger om helsehjelp vil være tilstrekkelig at den som skal gjennomføre beslutningen tilegner seg nødvendige opplysninger fra journalen en gang, vil det ved andre tilfeller være behov for tilgang over noe lengre tid, for eksempel så lenge pasienten er innlagt på et sykehus. For at dokumentasjonen av tilgangen skal bli mer oversiktlig for pasienten, kan tidspunktet vedkommende har hatt tilgang til opplysningene i slike tilfeller erstattes med det tidsrom vedkommende har hatt tilgang til opplysningene. Med tidsrom menes her det tidspunkt vedkommende helsepersonell første gang åpnet journalen på grunnlag av en beslutning om helsehjelp, og det tidspunkt vedkommende siste gang åpnet journalen på grunnlag av den samme beslutningen.

#### **Merknader til § 16 andre ledd**

Dokumentasjonen av hvem som er gitt tilgang skal bevares i journalen så lenge den eksisterer, og skal følge journalen når den avleveres til arkivdepot i samsvar med arkivloven.

Dette kravet bør ses i sammenheng med § 8 om register over autorisasjoner for tilgang.

#### **Merknader til § 16 tredje ledd**

Det følger av bestemmelsen at pasienten har rett til utskrift av dokumentasjonen. Bestemmelsen gjelder alle pasienter som er registrert i et behandlingsrettet helseregister hos den databehandlingsansvarlige. Det er ikke noe krav om at en er pasient når en ber om dokumentasjon av tilgang. Dokumentasjonen av tilgangen skal gi en kortfattet oversikt over hvem som har hatt tilgang til journalen, når de har hatt tilgang samt hvorfor de har hatt tilgang.

Det følger av andre punktum at informasjonen i utskriften skal kunne sorteres etter pasientens ønske. Aktuelle grupperinger kan være de parameterne som fremgår av loven og forskriften, det vil si hvilke helseopplysninger det er gitt tilgang, rettsgrunnlag og formål, helsepersonellkategorier, roller, tidsintervall etc.

#### **Merknader til § 16 fjerde ledd**

Krav om innsyn og utskrift skal besvares uten ugrunnet opphold, og det er en maksimal frist på 30 dager. Det skal ikke tas vederlag for slik utskrift med mindre særlige forhold tilsier det.



Eksempel på særlige forhold er at en person hyppig ber om utskrift. Et eventuelt vederlag skal ikke overstige de faktiske kostnadene ved å etterkomme kravet, se også helseregisterloven § 22 og offentleglova § 8.

Dersom en pasient ber om utskrift kun en gang eller to ganger under/etter et sykehusopphold kan det ikke tas betaling for dette. Det kan heller ikke tas betaling for innsyn til personer som tidligere har vært innlagt på sykehuset.

#### **4.17 § 17 Oppfølging og kontroll av elektronisk tilgang**

*Den databehandlingsansvarlige skal jevnlig kontrollere hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister. Dersom kontrollen viser at noen kan ha tilegnet seg helseopplysninger urettmessig, skal Datatilsynet og Statens helsetilsyn informeres, jf. personopplysningsforskriften § 2-6. Pasienten opplysningene er knyttet til skal også informeres.*

##### **Merknader til § 17**

Bestemmelsen forutsetter at virksomheten har en plan for når og hvor ofte, og eventuelt på hvilke vilkår slik kontroll skal foretas. Planen bør bygge på konkrete risikovurderinger, og vil blant annet være avhengig av hvordan tilgangsstyringssystemet er innrettet. Kontroll som nevnt bør alltid foretas dersom det foreligger mistanke om at noen ulovlig har tilegnet seg helseopplysninger.

Kravet må ses i sammenheng med internkontroll.

Urettmessig tilgang til helseopplysninger som oppdages ved kontroll, skal meldes til Statens helsetilsyn og Datatilsynet. Samtidig skal pasienten dette gjelder informeres.

Logging og kontroll av autorisert og uautorisert tilgang er kontrolltiltak overfor de ansatte i henhold til arbeidsmiljøloven kapittel 9, og databehandlingsansvarlig må informere de ansatte og drøfte med tillitsvalgte etter arbeidsmiljøloven § 9-2.

#### **4.18 § 18 Dispensasjon**

*Departementet kan etter søknad for nærmere angitte systemer dispensere fra ett eller flere krav i forskriften. En dispensasjon skal være tidsbegrenset.*

##### **Merknader til § 18**

Det presiseres at dispensasjonshjemmelen ikke gir anledning til å sette alle krav i forskriften til side, og det kan ikke gis dispensasjon fra forskriften som sådan. Dispensasjonshjemmelen er ikke begrunnet i et ønske om å implementere tekniske systemer og løsninger i ulike behandlingsrettede helseregistre før disse systemene kan tilfredsstillende de fastsatte sikkerhetskravene. Dispensasjon skal derfor bare gis unntaksvis for en tidsbegrenset periode.

Bestemmelsen fastslår at dispensasjon bare kan gis for ”nærmere angitte systemer”, for eksempel et radiologisystem (RIS) eller et laboratoriesystem. Kravet til ”nærmere angitt system” skal forstås strengt. Dette kravet innebærer at alle virksomheter må ha oversikt

over alle behandlingsrettede informasjonssystemer de har tatt i bruk, og vurdere informasjonssikkerhet, tilgang og tilgangsstyringen til systemene opp mot forskriftens krav. Dersom enkelte fagsystemer ikke oppfyller ett eller flere krav i forskriften når den trer i kraft, må søknad om dispensasjon konkretiseres og knyttes til de enkelte systemer som ikke oppfyller kravene.

Ansvar for å sikre at de behandlingsrettede informasjonssystemer oppfyller regelverkets krav og adgangen til å søke om dispensasjon, er lagt til databehandlingsansvarlig.

I en eventuell søknad om dispensasjon må det tydelig fremgå hvilken bestemmelse eller bestemmelser i forskriften det søkes om dispensasjon fra. Det kan ikke søkes om dispensasjon fra alle bestemmelsene i forskriften. En dispensasjon skal også være tidsbegrenset, og det bør fremkomme av søknaden hvilken tidsperiode det søkes for.

Det presiseres at det ikke kan søkes om dispensasjon fra alle bestemmelsene i forskriften. Dette gjelder blant annet kravet i § 7 om opplæring, da opplæring og kompetanseoppbygging er helt avgjørende for tilfredsstillende informasjonssikkerhet. Opplæring kan heller ikke regnes som et system.

Dersom et fagsystem ikke har funksjonalitet for sperring av helseopplysninger, må det søke om dispensasjon fra dette kravet. En eventuell dispensasjon innebærer imidlertid ikke at personopplysninger ikke skal vernes. Helsepersonelloven §§ 25 og 45 om pasientens rett til å motsette seg at annet helsepersonell får tilgang til opplysningene og pasient- og brukerrettighetsloven § 5-3, kommer uansett til anvendelse. Det er ikke anledning til å dispensere fra disse kravene.

Helseregisterloven §§ 15 og 16 fastsetter de overordnede premissene for kravene til informasjonssikkerheten ved all behandling av helseopplysninger, og vil være styrende ved vurdering av dispensasjon. Eventuelle dispensasjonssøknader må alltid vurderes i lys av hva som kan anses å være "tilfredsstillende informasjonssikkerhet" med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet. Det kan ikke gis dispensasjon fra de generelle kravene til informasjonssikkerhet som følger av helseregisterlov, personopplysningslov og personopplysningsforskrift.

Helseregisterloven §§ 15 og 16 vil også begrense omfanget av dispensasjon fra forskriften § 6 første ledd om at autorisasjon for tilgang til å lese, registrere, redigere, slette, sperre eller på annen måte behandle helseopplysninger kan bare gis i det omfang som er nødvendig for at den enkelte kan ivareta sine arbeidsoppgaver.

Dispensasjon gis etter en konkret vurdering, hvor det vil bli tatt hensyn til de store forskjeller i sektorens bruk av tekniske løsninger, kompleksiteten i det tekniske utstyret og de nyanskaffelser som må gjøres for ytterligere å bedre informasjonssikkerheten.

#### **4.19 § 19 Straff**

*Den som forsettlig eller grovt uaktsomt overtrer bestemmelsene i forskriften § 6 og § 10 straffes med bøter eller fengsel inntil ett år eller begge deler.*

#### **Merknader til § 19**

Bestemmelsen er en straffesanksjonsbestemmelse ved forsettlig eller grov uaktsom overtredelse av forskriften §§ 6 og 10, som begrenser tilgang til helseopplysninger til det

som er nødvendig for å yte helsehjelp i en aktuell situasjon. Overtredelse av § 6 og 10 reguleres av denne bestemmelsen, og kommer i stedet for straff etter helseregisterloven § 34 første ledd.

Straff for annen forsettlig eller grov uaktsom overtredelse, reguleres av helseregisterloven § 34.

I tillegg kan tilsynsmyndighetene ilegge pålegg, tvangsmulkt og erstatning etter helseregisterloven §§ 32, 33 og 35. Statens helsetilsyn og Datatilsynet er tilsynsmyndigheter for forskriften.

## **4.20 § 20 Ikrafttredelse**

*Forskriften gjelder fra den tid Kongen fastsetter.*

### **Merknader til § 20**

Forskriften trer tidligst i kraft fra 1. januar 2013.

Det forutsettes at virksomhetene vil oppfylle kravene i forskriften fra den trer i kraft. Dersom kravene ikke kan oppfylles, må det søkes om dispensasjon etter forskriften § 18.