HØRINGSNOTAT

Forslag til
forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Mai 2010

INNHOLD

1 Høringsnotatets hovedinnhold 4

2 Bakgrunn 6

3 Høringen av forslag til forskrift oktober 2008 7

4 Nærmere om de enkelte bestemmelser i forskriften 11

4.1 Forskriftens formål 11

4.1.1 Forslaget i høringsnotat av oktober 2008 11

4.1.2 Høringsinstansenes synspunkter 11

4.1.3 Departementets vurderinger og forslag 11

4.2 Forskriftens virkeområde 12

4.2.1 Forslaget i høringsnotat av oktober 2008 12

4.2.2 Høringsinstansenes synspunkter 12

4.2.3 Departementets vurderinger og forslag 12

4.3. Definisjoner i forskriften 14

4.3.1 Forslaget i høringsnotatet av oktober 2008 14

4.3.2 Høringsinstansenes synspunkter 14

4.3.3 Departementets vurderinger og forslag 14

4.4 Generelle krav til informasjonssikkerhet 15

4.4.1 Forslagene i høringsnotatet av oktober 2008 15

4.4.2 Høringsinstansenes synspunkter 16

4.4.3 Departementets vurderinger og forslag 17

4.5. Krav til system for utstedelse av autorisasjoner, krav til autentisering og autorisasjon 19

4.5.1 Forslaget i høringsnotat av oktober 2008 19

4.5.2 Høringsinstansenes synspunkter 19

4.5.3 Departementets vurderinger og forslag 21
4.6 Tilgang til helseopplysninger i behandlingsrettet helseregister 24
4.6.1 Forslaget i høringsnotatet av oktober 2008 24
4.6.2 Høringsinstansenes synspunkter 24
4.6.3 Departementets vurderinger og forslag 25
4.7 Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter 27
4.7.1 Forslaget i høringsnotatet av oktober 2008 27
4.7.2 Høringsinstansenes synspunkter 27
4.7.3 Departementets vurderinger og forslag 30
4.8 Sperring av opplysninger 33
4.8.1 Høringsnotatet av oktober 2008 33
4.8.2 Høringsinstansenes synspunkter 33
4.8.3 Departementets vurderinger og forslag 33
4.9 Logging og dokumentasjon av tilgang 34
4.9.1 Forslaget i høringsnotatet av 2008 34
4.9.2 Høringsinstansenes synspunkter 35
4.9.3 Departementets vurderinger og forslag 36
5 Administrative og økonomiske konsekvenser 38
6 Merknader til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre 41
Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre 67

1 Høringsnotatets hovedinnhold

Helse- og omsorgsdepartementet (departementet) sender med dette forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger på høring. Et tidligere forslag til forskrift ble hørt gjennom høringsnotat av oktober 2008 der også forslag til de siste endringene i helseregisterloven § 13 og helsepersonelloven § 45 ble hørt. De nevnte lovendringene i helseregisterloven og helsepersonelloven er nå vedtatt, jf. nedenfor punkt 2. Herværende høringsnotat er en oppfølging av endringene i helseregisterloven § 13.

Dels på bakgrunn av Stortingets behandling av lovforslaget, og dels på bakgrunn av synspunkter fra høringsinstansene i høringen oktober 2008, har departementet utarbeidet et revidert forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger.

Forskriften har regler om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre, det vil si alle informasjons - og journalsystemer som etableres for å kunne gi helsehjelp til pasienter. Eksempler er elektroniske pasientjournalsystemer (EPJ-systemer) og røntgeninformasjonssystemer (RIS). Formålet med forskriften er å bidra til å gi helsepersonell nødvendig tilgang til helseopplysninger slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas. Det gjelder uavhengig av hvem som tilbyr helsehjelpen og hvor den tilbys. Et viktig formål med forskriften er særlig å bidra til god informasjonssikkerhet ved tilgangsstyring og tilgang til helseopplysninger.

Forskriften er delt inn i åtte kapitler. Kapittel 1 inneholder bestemmelser om formål, virkeområde og definisjoner. Kapittel II innholder generelle krav til informasjonssikkerhet. Det omfatter krav om forsvarlige systemer, krav til planlegging, organisering og rutiner, krav om internkontroll og sikkerhetsledelse. De generelle kravene om informasjonssikkerhet utfylles av personopplysningsforskriften. Enkelte regler i forskriften – det gjelder særlig reglene i forskriften kapittel II - følger også av personopplysningsforskriften. Det har vært et dilemma for departementet om i og hvilken grad disse reglene bør inntas i denne forskriften. Departementet har kommet til at de generelle bestemmelsene som er inntatt i forskriften gir så viktige føringer at forskriften ville være mangelfull hvis de ble utelatt.

Kapittel III inneholder krav om system for utstedelse av autorisasjoner og krav til autentisering. Det er pliktbestemmelser rettet mot den databehandlingsansvarlige for det aktuelle behandlingsrettede helseregister. Begrepet autentisering og autorisasjon er definert i kapittel II. Kapittel IV regulerer helsepersonells tilgang til helseopplysninger internt i virksomheten. Det er pliktbestemmelser rettet mot

helsepersonell, personell i pasientadministrasjonen og personell som bistår med elektronisk bearbeiding av opplysningene. Kapittel V inneholder tilleggsbestemmelser for tilgang til helseopplysninger på tvers av virksomheter, og er først og fremst rettet mot den databehandlingsansvarlige for opplysningene. Bestemmelsene er også relevante for helsepersonell som autoriseres for tilgang på tvers av virksomheter.

I forhold til høringsnotatet av oktober 2008 er det gjort flest endringer i reglene om tilgang på tvers av virksomheter. For det første innebærer endringene i helseregisterloven § 13 at det bare kan gis tilgang til helseopplysninger på tvers av virksomheter etter uttrykkelig samtykke fra den registrerte, men det gis adgang til å gjøre unntak fra dette i forskrift. I foreliggende forskrift foreslås at samtykke kan fravikes dersom pasienten på grunn av sin fysiske eller psykiske tilstand ikke er i stand til å gi et uttrykkelig samtykke, og det må antas at pasienten ville ha gitt slikt samtykke dersom han eller hun hadde vært i stand til det. Krav til avtale mellom virksomhetene som gir hverandre tilgang på tvers opprettholdes, men vilkårene for å kunne inngå slik avtale er skjerpet. Foreliggende forslag krever at begge virksomheter har tekniske løsninger som kan avgrense tilgangen til å omfatte strukturert klinisk informasjon relatert til forespørselen. Det kan bare gis tilgang til opplysninger som det på forhånd er vurdert kan deles med andre. Videre kreves at en forespørsel om og tilgang til helseopplysninger i annen virksomhet skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet. Det følger av Stortingets vedtak at forespørselen og tilgang til helseopplysninger kan bare omfatte en person om gangen. Ved behov for gjentatt tilgang til helseopplysninger om samme pasient skal det gjøres en ny forespørsel. Kapittel VI inneholder to bestemmelser om sperring av helseopplysninger. Forslaget i forskriften som ble sendt på høring i oktober 2008 inneholdt ikke slike bestemmelser, men det gikk klart frem av motivene at pasienten i utgangspunktet har rett til å nekte at andre gis tilgang til pasientopplysninger. Hensynet til tydeliggjøring er bakgrunnen for at bestemmelsene nå er inntatt i forskriften.

Kapittel VII har bestemmelser om logging og dokumentasjon av tilgang. Under Stortingets behandling av helseregisterloven ble det i helseregisterloven § 13 sjette ledd fastslått at den registrerte har rett til innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne. Forslaget til forskrift følger dette opp med krav om dokumentasjon av tilgang til opplysninger i behandlingsrettede helseregister og utdypende bestemmelser om innsynsretten.

I arbeidet med forskriften har departementet lagt stor vekt på å få frem et regelverk som er godt balansert mellom hensynet til nødvendigheten av at pasientopplysninger skal være raskt tilgjengelige når det er nødvendig for helsehjelp til pasienten, og

hensynet til pasientens rett til vern om opplysningene. Det er avgjørende viktig for tilliten til helsetjenesten at pasienter kan føle seg trygge på at sensitive opplysninger ikke kommer uvedkommende i hende. Forskriften innebærer at det må gjøres tilpasninger i mange elektroniske systemer for at kravene i forskriften skal etterleves. Virksomhetene må også vurdere om deres organisatoriske og administrative rutiner for å sikre etterlevelse av forskriften er tilfredsstillende. Dette vil kreve en god del arbeid fra virksomhetenes side. Reglene i forskriften må imidlertid også være praktikable og til hjelp for helsepersonell i deres arbeid med å gi helsehjelp til pasienten. Departementet ber spesielt om at høringsinstansene vurderer om forskriften ivaretar denne balansen.

Høringsfrist er 10. september 2010.

2 Bakgrunn

Stortinget vedtok 16. juni i 2009 endringer i helseregisterloven og helsepersonelloven. Det vises til 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) og Innst. O. nr. 110 (2008–2009).

Formålet med lovendringene var å fjerne juridiske hindringer for effektiv kommunikasjon av pasientopplysninger i helsetjenesten samtidig som taushetsplikten og den enkeltes personlige integritet ivaretas.

Lovvedtaket innebar følgende endringer i helseregisterloven:

1. Ny lovhjemmel i helseregisterloven § 6 a om virksomhetsovergripende behandlingsrettede helseregistre. Bestemmelsen innebærer at Kongen i statsråd kan etablere slike registre, samt gi nærmere bestemmelser om blant annet drift og behandling av helseopplysninger i slike registre, i forskrift. Bestemmelsen vil gi rettsgrunnlag for etablering av regionale kjernejournaler. Bestemmelsen gir ikke hjemmelsgrunnlag for en sentral (landsomfattende) kjernejournal.

2. Ny forskriftshjemmel i helseregisterloven § 6 b slik at Kongen i statsråd kan gi forskrift om virksomhetsovergripende behandlingsrettede helseregistre for helsepersonell som arbeider i formalisert arbeidsfelleskap.

3. Endringer i helseregisterloven § 13. Endringene innebærer at Kongen i statsråd kan gi nærmere bestemmelser om tilgang til helseopplysninger, og herunder gjøre unntak fra forbudet i helseregisterloven § 13 første ledd første punktum. Bestemmelsen fastslår at bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller

databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger. Endringene innebærer at tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter kan gis etter uttrykkelig samtykke fra den registrerte, og at det i forskrift kan gjøres unntak fra kravet om at samtykket skal være uttrykkelig. Det er et krav i loven at en forespørsel om og tilgang til helseopplysninger i annen virksomhet bare kan omfatte en pasient om gangen. Videre er det fastslått at den registrerte har rett til innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne.

Lovendringen i helsepersonelloven § 45 innebærer en presisering og utdyping av bestemmelsen. Etter lovendringen lyder bestemmelsen:

"Med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til pasient etter denne lov, gis nødvendige og relevante helseopplysninger i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte. For elektronisk tilgang til helseopplysninger på tvers av virksomheter gjelder helseregisterloven § 13 tredje og fjerde ledd. Det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger.

Helseopplysninger som nevnt i første ledd kan gis av den databehandlingsansvarlige for opplysningene eller det helsepersonell som har dokumentert opplysningene, jf. § 39.

Departementet kan i forskrift gi nærmere bestemmelser til utfylling av første ledd, og kan herunder bestemme at annet helsepersonell kan gis tilgang til journalen også i de tilfeller som faller utenfor første ledd."

Dette høringsnotatet følger opp de ovenfor nevnte endringer i helseregisterloven § 13.

De helsefaglige behov for tilgang til helseopplysninger ble redegjort for i høringsnotatet av oktober 2008 samt den ovennevnte proposisjonen (Ot.prp. nr. 51 (2008–2009). Det redegjøres derfor ikke nærmere for disse her.

3 Høringen av forslag til forskrift oktober 2008

Helse- og omsorgsdepartementet (departementet) sendte forslag til forskrift om informasjonssikkerhet og elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre på høring 20. oktober 2008 – samme høring som forslag til lovendringene i helseregisterloven og helsepersonelloven, jf. ovenfor. Høringsfristen var 12. januar 2009. Høringsnotatet ble sendt til følgende instanser:

Akademikerne
Apotekforeningen
Arbeids- og velferdsdirektoratet (NAV)
Barneombudet

Datatilsynet
De medisinske dekanene
Delta
Den norske advokatforening
Den norske dommerforening
Den norske jordmorforening
Den norske legeforening
Den norske tannlegeforening
Departementene
Direktoratet for nødkommunikasjon
Fagforbundet
Farmasiforbundet
Fellesorganisasjonen
Forbrukerombudet
Funksjonshemmedes fellesorganisasjon (FFO)
Fylkesrådet for funksjonshemmede
Handels- og servicenæringens hovedorganisasjon - HSH
Helsedirektoratet
Helsetilsynet i fylkene
Kompetansesenter for IT i helse- og sosialsktoren AS (KITH)
Kliniske ernæringsfysiologers forening
Kreftforeningen
KS
Landets fylkesmenn
Landets helseforetak
Landets kommuner
Landets pasientombud
Landets regionale helseforetak
Landsforbundet for Utviklingshemmede og Pårørende
Landsforeningen for hjerte- og lungesyke (LHL)
Landsforeningen for private sykehus (PRISY)
Landsforeningen for Pårørende innen Psykiatri
Landsforeningen for trafikkskadde i Norge
Landsorganisasjonen i Norge
Mental Helse Norge
Nasjonalforeningen for folkehelsen
Nasjonalt folkehelseinstitutt
Nasjonalt kompetansesenter for helsetjenestens kommunikasjonsberedskap (KoKom)
Nasjonalt senter for telemedisin
Norges Astma- og Allergiforbund
Norges Blindeforbund
Norges Diabetesforbund
Norges Døveforbund
Norges Farmaceutiske Forening
Norges Fibromyalgiforbund

Norges Handikapforbund
Norges juristforbund
Norges Optikerforbund
Norsk Audiografforbund
Norsk Ergoterapeutforbund
Norsk Forbund for Utviklingshemmede
Norsk Fysioterapeutforbund
Norsk Helsenett AS (Norsk Helsenett SF fra 30.10.09)
Norsk Helsesekretærforbund
Norsk Homeopatisk pasientforening
Norsk Kiropraktorforening
Norsk Manuellterapeutforening
Norsk Pasientforening
Norsk pasientskadeerstatning (NPE)
Norsk psykologforening
Norsk Radiografforbund
Norsk Revmatikerforbund
Norsk senter for elektronisk pasientjournal (NSEP)
Norsk Sykepleierforbund
Norsk Tannpleierforening
Norsk Tjenestemannslag (NTL)
Norske Fotterapeuters Forbund
Norske Kvinners Sanitetsforening
Næringslivets Hovedorganisasjon
Parat helse
Pasientskadenemnda
Privatpraktiserende Fysioterapeuters Forbund
Regjeringsadvokaten
Riksadvokaten
Ryggforeningen i Norge
Røntgeninstituttenes Fellesorganisasjon
Rådet for psykisk helse
Sametinget
Sivilombudsmannen
Spekter
Statens autorisasjonskontor for helsepersonell
Statens helsepersonellnemnd
Statens helsetilsyn
Statens legemiddelverk
Statens råd for funksjonshemmede
Statens seniorråd
Sysselmannen på Svalbard
Universitets- og høyskolerådet
Yrkesorganisasjonenes Sentralforbund

Til sammen 67 høringsinstanser svarte på departementets høringsnotat. Av disse hadde 41 merknader til forskriftsforslaget. Disse høringsinstanser er:

Arbeids-og velferdsdirektoratet
Barneombudet
Bergen kommune
Buskerud fylkeskommune
Datatilsynet
Den norske legeforening
Den norske tannlegeforening
Direktoratet for forvaltning og IKT (Difi)
Frogn kommune
Handels- og servicenæringens hovedorganisasjon (HSH)
Haraldsplass Diakonale Sykehus
Helsedirektoratet
Helse Finnmark
Helse Helse Vest, inkludert uttalelser fra Helse Bergen, Helse Fonna og Helse Stavanger
Helse Midt-Norge
Helse Nord RHF
Helse Sør-Øst, inkluder uttalelse fra Oslo universitetssykehus HF, Ullevål
IKT-Norge
Landsforeningen for hjerte- og lungesyke
Landsorganisasjonen
Leksvik kommune
Lier kommune
Kompetansesenter for IT i helse- og sosialsektoren AS (KITH)
Nasjonalt folkehelseinstitutt
Nasjonalt senter for telemedisin
Norges Handikapforbund
Norsk Optikerforbund
Norsk senter for elektronisk pasientjournal (NSEP)
Norsk Radiografforbund
Norsk Sykepleierforbund
Oslo kommune
Psykologforeningen
Sande kommune
Senter for klinisk dokumentasjon og evaluering
Statens helsetilsyn
Stavanger kommune
Stavanger universitetssykehus
Troms fylkeskommune
Universitets- og høyskolerådet
Universitetssykehuset Nord Norge
Verdal kommune

22 høringsinstanser uttalte at de støtter eller i hovedsak støtter forslaget. Herunder uttalte Stavanger kommune og Norsk senter for elektronisk pasientjournal (NSEP) at kommunikasjon på tvers av virksomheter må bygge på samtykke fra pasienten. De øvrige høringsinstansene har mindre merknader til et eller flere spørsmål forskriften berører, uten at det fremgår klart om de støtter/ikke støtter forslaget.

4 Nærmere om de enkelte bestemmelser i forskriften

4.1 Forskriftens formål

4.1.1 Forslaget i høringsnotat av oktober 2008

I høringsnotatet ble det foreslått at formålet med forskriften skal være å bidra til å gi helsepersonell nødvendig tilgang til helseopplysninger slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte uten å krenke personvernet. For å virkeliggjøre dette skal forskriften sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, kvalitet, integritet og tilgjengelighet.

4.1.2 Høringsinstansenes synspunkter

Ingen høringsinstanser hadde innvendinger mot formålsbestemmelsen. *Kompetansesenter for IT i helse- og sosialsektoren AS (KITH)* foreslo mindre endringer i ordlyden på bestemmelsen, uten at det var ment å innebære noen realitetsendring.

4.1.3 Departementets vurderinger og forslag

Departementet har vurdert ordlyden i forskriften på nytt. Helsetjenesten er helt avhengig av at pasientene har tillitt til at helsetjenesten behandler sensitive pasientopplysninger slik at de ikke kommer i hendene på uvedkommende, samtidig som at opplysningene er tilgjengelig for helsepersonell som har behov for det for å gi helsehjelp til pasienten. Ivaretakelse av dette formålet krever god informasjonssikkerhet. Departementet har derfor vurdert om uttrykket "tilfredsstillende informasjonssikkerhet" i høringsforslaget bør endres til "god informasjonssikkerhet". Det forhold at helseregisterloven § 16 bruker uttrykket "tilfredsstillende informasjonssikkerhet" kan imidlertid tale for at dette begrepet også brukes i forskriften. Et viktig formål med denne forskriften er imidlertid å styrke informasjonssikkerheten, og departementet har kommet til at dette bør synliggjøres i denne forskriften. Departementet forslår derfor at forskriftens formålsbestemmelse bruker uttrykket "god informasjonssikkerhet". Konfidensialitet, integritet, kvalitet og tilgjengelighet er hovedelementer i begrepet informasjonssikkerhet, jf. helseregisterloven § 16. Selv om sporbarhet ikke er uttrykkelig nevnt i bestemmelsen, er også dette et viktig element i informasjonssikkerheten. Sporbarhet er nødvendig for

at man i ettertid kan måle/vurdere om informasjonssikkerheten har vært/er god. Det følger av helseregisterloven § 6 først ledd andre og tredje punktum og bestemmelsene om registrering av hendelser i denne forskriften §§ 31 og 32 at det skal fremgå av registeret hvem som har registrert opplysningene. Dette kan gjøres ved hjelp av digital signatur eller tilsvarende sikker dokumentasjon, og på denne måten er hensynet til sporbarhet ivaretatt.

4.2 Forskriftens virkeområde

4.2.1 Forslaget i høringsnotat av oktober 2008

I høringsnotatet ble det foreslått at forskriften skal gjelde for behandling av helseopplysninger i behandlingsrettede helseregistre som skjer med hjemmel i helseregisterloven § 6 og helsepersonelloven § 46. Begrepet behandlingsrettet helseregister sikter til alle registre som inneholder personidentifiserbar informasjon om pasienter og som benyttes for å yte helsehjelp eller administrere slik hjelp. Eksempler på slike registre er elektroniske pasientjournalsystemer som brukes i pleie- og omsorgstjenesten, av fastleger og helseforetak, pasientadministrative systemer, RIS/PACS, laboratoriedatasystemer, små avdelingsvise kliniske systemer etc.

4.2.2 Høringsinstansenes synspunkter

Ingen høringsinstanser hadde merknader som direkte rettet seg til denne bestemmelsen. *Nasjonalt folkehelseinstitutt* påpeker imidlertid at grenseoppgangen mellom de ulike registertypene ikke alltid er klar. Folkehelseinstituttet viser til at vi har ulike former for helseregistre, blant annet sentrale helseregistre, kvalitetsregistre, forskningsregistre og prosjekter, og behandlingsrettede registre. Instituttet viser til at det sentrale helseregisteret System for vaksinasjonskontroll (SYSVAK), har en fremtredende helsetjenesterelatert funksjon og dermed minner om behandlingsrettede helseregistre. Instituttet tilføyer at SYSVAK er i daglig bruk ved at helsesøstre bruker informasjon fra SYSVAK til å vurdere hvilke vaksiner som skal gis på bakgrunn av de opplysninger som er registrert for det aktuelle barnet.

4.2.3 Departementets vurderinger og forslag

Departementet opprettholder forslaget fra høringsnotatet, men med noen justeringer. Det innebærer at forskriften gjelder behandling av helseopplysninger i behandlingsrettede helseregistre som skjer med hjemmel i helseregisterloven § 6 og helsepersonelloven § 46. Forskriften gir regler om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i disse registrene – når formålet er å yte helsehjelp til pasient. Forskriften regulerer ikke tilgang til helseopplysninger for andre formål enn helsehjelp til pasient, som for eksempel til kvalitetssikring eller forskning.

Dersom en forsker har fått godkjenning fra den regionale komiteen for medisinsk og helsefaglig forskningsetikk til å utføre et forskningsprosjekt som innebærer tilgang til helseopplysninger internt i virksomheten, må den databehandlingsansvarlige konkret vurdere hvordan forskeren kan få tilgang til de opplysninger forskeren har fått tillatelse til å få tilgang til, uten at det samtidig gis tilgang til andre opplysninger. Det samme gjelder ved kvalitetssikringsprosjekter, jf. helsepersonelloven § 26 første ledd. Slike "enkeltstående" tilganger reguleres ikke av denne forskriften.

Utgangspunktet i helseregisterloven er at helseregistre som etableres med hjemmel i helseregisterloven §§ 7 og 8, ikke skal brukes til dokumentasjon av helsehjelp. Dokumentasjon av helsehjelp skal skje i en journal for den enkelte pasient, jf. helsepersonelloven § 39. Dette systemet praktiseres imidlertid ikke uten unntak. SYSVAK er i følge Folkehelseinstituttet i daglig bruk ved at helsesøstre bruker informasjon fra SYSVAK til å vurdere hvilke vaksiner som skal gis på bakgrunn av de opplysninger som er registrert for et aktuelt barn. Slik departementet ser det, bør sikkerheten ved sist nevnte behandling av opplysninger, og pasientens rettigheter i tilknyting til dette, være de samme, uavhengig av hvor opplysningene lagres. Kravene om logging, innsynsrett i logg, autorisasjon og autentisering bør som et utgangspunkt etter departementets vurdering også gjelde ved behandling av opplysninger i disse systemene.

Departementet har på denne bakgrunn vurdert om herværende forskrift også bør gjelde ved behandling av helseopplysninger som skjer med hjemmel i forskrift etter helseregisterloven § 8 dersom formålet med behandlingen av opplysningene er ytelse av helsehjelp til pasient eller å administrere slik hjelp. Departementet er imidlertid i tvil om det passer å anvende forskriftens bestemmelser om tilgangsstyring og tilgang på de sentrale helseregistrene og vil derfor ikke foreslå å utvide forskriftens virkeområde. De sentrale helseregistrene vil likevel ikke være uten bindende regelverk å forholde seg til. Det vises til at direkte personidentifiserende kjennetegn skal lagres kryptert i slike registre (bortsett fra i Nasjonal database for elektroniske resepter), jf. helseregisterloven § 8 tredje ledd siste punktum, og at bestemmelsene om informasjonssikkerhet og internkontroll i personopplysningsforskriften også gjelder for disse registrene.

Under arbeidet med denne forskriften har departementet fått innspill fra Helse Sør Øst RHF om at kvalitetsregistre bør med i forskriften. De opplever at det er stor usikkerhet og uenighet om krav og behov for sikkerhetsnivå for disse. Til dette vil departementet bemerke at det trengs eget hjemmelsgrunnlag - konsesjon fra Datatilsynet eller hjemmel i forskrift – for å etablere kvalitetsregistre. Det vil da være naturlig at man i det vedtak som etablerer det aktuelle kvalitetsregister, også fastsetter eventuelle utdypende regler for informasjonssikkerhet som gjelder for registeret. Et generelt utgangspunkt -

som alltid gjelder – er at reglene om taushetsplikt i helsepersonelloven også gjelder for slike registre. Det innebærer at den databehandlingsansvarlige for det aktuelle registeret har plikt til å hindre at andre får adgang til eller kjennskap til personidentifiserbare opplysninger fra registeret. Dette gjelder med mindre det følger av lov eller i medhold av lov at taushetsplikt ikke er til hinder. Videre vil helseregisterloven § 13 første ledd gjelde for tilgang til opplysningene i registeret, i tillegg til bestemmelsene om informasjonssikkerhet og internkontroll i personopplysningsforskriften, jf. helseregisterloven § 16.

4.3. Definisjoner i forskriften

4.3.1 Forslaget i høringsnotatet av oktober 2008

Høringsnotatet inneholdt 2 definisjoner; autorisasjon og autentisering. Autorisasjon ble definert som: "En person i en bestemt rolle gis bestemte rettigheter til lesing, registrering, redigering, retting, sletting, sperring eller annen behandling av helseopplysninger. Autorisasjon kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra tjenestelige behov og er i henhold til bestemmelser om taushetsplikt." Autentisering ble definert som: "Prosess som gjennomføres for å bekrefte en påstått identitet."

4.3.2 Høringsinstansenes synspunkter

Bare *Helsedirektoratet* hadde konkrete merknader til høringsnotatets forslag til definisjoner. Direktoratet foreslår at man også tar inn en definisjon av "tilgang". Direktoratet viser til definisjonen i Norm for informasjonssikkerhet i helsesektoren som lyder: Med *tilgang* menes i normen at helse- og personopplysninger om en eller flere bestemte pasienter er eller gjøres tilgjengelig for autorisert personell. Beslutning om *tilgang* skal treffes etter en konkret beslutning basert på at det iverksettes tiltak for medisinsk behandling av pasienten.

4.3.3 Departementets vurderinger og forslag

Departementet opprettholder forslaget fra høringsnotatet om at forskriften skal definere begrepene autorisasjon og autentisering. I tillegg foreslår departementet at det tas inn definisjoner av begrepene, "tilgang til helseopplysninger", "direkte tilgang til helseopplysninger" og "sperrede helseopplysninger".

Departementet foreslår at definisjonen av autorisasjon justeres noe i forhold til høringsforslaget. Første setning i høringsforslagets definisjon definerer selve begrepet, mens andre setning i definisjonen setter krav til autorisasjonen. Departementet foreslår at krav til selve autorisasjonen tas inn i et eget kapittel i forskriften, og andre setning i høringsnotatets definisjon foreslås derfor sløyfet.

Autentisering er definert som en prosess som gjennomføres for å bekrefte en påstått identitet. En autentiseringsprosess kan ha ulike sikkerhetsgrader eller

sikkerhetsnivåer. I Norm for informasjonssikkerhet brukes begrepene *autentisering* og *sterk autentisering*. I Datatilsynets veileder 07/01 Internkontroll og informasjonssikkerhet brukes uttrykkene *lav*, *middels* og *høy autentisering,* om de ulike sikkerhetsnivåer. Andre uttrykk som brukes er 1-faktor løsning og 2-faktor løsning. En autentiseringsfaktor er en bit informasjon og en prosess som brukes til å verifisere en persons digitale identitet med tanke på sikkerhet. To-faktor autentisering er et system der to forskjellige metoder blir brukt i autentiseringsprosessen. Å bruke to eller flere faktorer (multi-faktor) i en autentiseringsprosess gir et høyere sikkerhetsnivå.

Helsedirektoratet tar i høringssvaret opp spørsmål om forskriften også bør inneholde en definisjon av begrepet tilgang. Departementet er enig i at det bør tas inn en definisjon av begrepet tilgang i forskriften, fordi dette antagelig vil lette forståelsen av begrepet. Andre setning i direktoratets forslag – *"beslutning om tilgang skal treffes etter en konkret beslutning basert på at det iverksettes tiltak for medisinsk behandling av pasienten*" - oppfatter departementet som et krav om beslutningsstyrt tilgang. Departementet mener at beslutningsstyrt tilgang bør være et krav i forskriften, uavhengig av definisjonen av tilgang til opplysninger.

Et hovedvilkår for å få tilgang til helseopplysninger bør være at tilgang er nødvendig for å yte helsehjelp til pasient eller administrering av slik hjelp. Helsehjelp er et videre begrep og omfatter flere handlinger enn medisinsk behandling. Ordbruken "medisinsk behandling" i normens definisjon vil derfor bli for snever i denne forskriften. Departementet foreslår at regler for tilgangsstyring inntas i et eget kapittel i forskriften. Krav om at tilgangen skal være beslutningsstyrt foreslås inntatt i dette kapittelet. For å skille mellom den "tilgang" man får til helseopplysninger ved utlevering, herunder elektronisk utlevering, av helseopplysninger, har departementet i dette høringsnotatet også inntatt en definisjon av "direkte tilgang til helseopplysninger."

I tillegg til ovennevnte definisjoner foreslår departementet at det tas inn en egen definisjon av "sperrede helseopplysninger". Hensikten med å ta inn en definisjon av "sperrede helseopplysninger" er å synliggjøre pasientens rett til å motsette seg at annet personell gis tilgang til helseopplysninger om ham eller henne, jf. helsepersonelloven §§ 25 og 45.

4.4 Generelle krav til informasjonssikkerhet

4.4.1 Forslagene i høringsnotatet av oktober 2008

Høringsforslaget av oktober 2008 inneholdt seks bestemmelser om generelle krav til informasjonssikkerhet, inntatt i et eget kapittel. Det var krav om forsvarlige systemer, krav til planlegging og organisering, krav til opplæring og kunnskap, krav om

sikkerhetsledelse samt internkontroll. Videre fulgte det av forskriften at personopplysningsforskriften kapittel 2 om informasjonssikkerhet vil gjelde som utfyllende bestemmelser til forskriften.

4.4.2 Høringsinstansenes synspunkter

Ingen høringsinstanser hadde kommentarer til høringsnotatets forslag om krav til forsvarlige systemer, krav om internkontroll eller krav til sikkerhetsledelse.

Tre høringsinstanser hadde merknader til forskriftens krav til planlegging og organisering. Disse er *Helse Bergen HF, Helse Sør-Øst RHF* og *Troms fylkeskommune.* Helse Bergen HF uttaler:

"Her settes det krav om styrende dokumentasjon og rutiner helt ned på laveste nivå (post). Dette er å gå for langt i forhold til den internkontroll som er pålagt foretakene, der det tross alt er en viss frihet i hvordan kontrollen kan utføres. Styrende dokumentasjon må være på overordnet nivå, og det er selvsagt at rutiner må tilpasses der det er behov for det, uten at dette må detaljreguleres."

Også Helse Sør-Øst RHF viser til forskriftens bestemmelse om at det skal utarbeides informasjonssikkerhetsplaner, styrende dokumenter og rutiner for behandling av helseopplysninger. Videre vises til merknaden til bestemmelsen der det fremgår at dersom en stor avdeling er inndelt i flere poster, kreves for eksempel at den enkelte post skal ha sine egne skrevne rutiner med avdelingsplanen som overbygging. Helseforetaket mener dette er lite hensiktmessig, da nødvendige rutiner alltid vil måtte utarbeides etter behov, og uten at dette detaljreguleres nærmere.

Troms fylkeskommune viser til forskriftens krav om overordnet strategi, informasjonssikkerhetsplaner og planverk. Fylkeskommunen mener dette er ordbruk som kanskje ikke er kompatibel med en liten enmannsbedrift. Kommunen uttaler at forslaget til forskrift har tatt utgangspunkt i dagens sykehussektor, men at helsesektoren og helsepersonell er et langt videre begrep enn sykehussektoren. Fylkeskommunen ønsker primært at deler av forskriften ikke gjennomføres eller utsettes. Subsidiært foreslår kommunen følgende tekst: *Virksomheter som tar i bruk behandlingsrettede helseregistre skal utarbeide en strategi og målsetting for informasjonssikkerheten i virksomheten som skal være tilpasset virksomhetens art, aktiviteter og størrelse.*

Bare Troms fylkeskommune har kommentert forskriftens krav om opplæring og kunnskap. Fylkeskommunen mener det bør være en selvfølge at helsepersonell har en selvstendig plikt til å holde seg orientert om gjeldende lovverk innenfor helsesektoren. Videre uttales at dersom man ønsker sterkere kontroll med at helsepersonell virkelig innehar disse kunnskapene, bør man innføre en autorisasjonsprøve som må være bestått før helsepersonell får sin autorisasjon.

To høringsinstanser har merknader til forskriftens forhold til personopplysningsforskriften. *Kompetansesenter for IT i helse- og sosialsektoren AS* (KITH) viser til at personopplysningsforskriften i sin helhet gjelder for helseregistre, selv om enkelte bestemmelser ikke er relevante. KITH finner det derfor uheldig at det i forskriften refereres til kapittel 2 i personopplysningsloven, da dette lett kan misforstås dit hen at resten av forskriften ikke gjelder.

Helsedirektoratet påpeker at forskriften omhandler forhold som langt på vei allerede er påpekt andre steder i regelverket og i Norm for informasjonssikkerhet. Direktoratet mener at det i utgangspunket er unødvendig å gjenta disse bestemmelsene i forskrift, men direktoratet ser samtidig behovet for å samle bestemmelsene i en forskrift for på den måten å sikre tilfredsstillende informasjonssikkerhet ved behandling av helse- og personopplysninger i EPJ-systemene. Direktoratet mener at forskriften hovedsakelig bør konsentreres om tilgang til helseopplysninger i EPJ-systemer på tvers av virksomheter.

Helse Sør-Øst RHF mener at selv om personopplysningsforskriften på flere områder samsvarer med normen for informasjonssikkerhet i helsesektoren, synes det hensiktmessig at flere av kravene i normen formaliseres i den nye forskriften. Helseforetaket ser det som særlig viktig at kravene som gjelder risikovurderinger og kontinuitet blir formalisert i forskriften.

4.4.3 Departementets vurderinger og forslag

Departementet er enig med Helsedirektoratet i at forskriften først og fremst bør konsentrere seg om tilgang til helseopplysninger og tilgangsstyring. For å synliggjøre dette mener departementet at forskriftens navn bør være *forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.* Departementet mener det er viktig at forskriften inneholder et eget kapittel med generelle krav til informasjonssikkerhet for behandling av helseopplysninger, selv om noen av bestemmelsene kan sies å følge av personopplysningsforskriften.

God informasjonssikkerhet krever organisatoriske så vel som tekniske og fysiske tiltak. Organisatoriske tiltak omfatter klare ansvarslinjer, gode rutiner hos alle som bruker systemet/behandler helseopplysninger, risikovurderinger, dokumentasjon av informasjonssystemene m.v. God informasjonssikkerhet kan ikke alene ivaretas eller måles ut fra de tekniske funksjonalitetskrav et elektronisk system har.

De ulike virksomhetene i helsetjenesten er ikke noen homogen gruppe. De kan være meget forskjellige, både i størrelse, innhold og kompleksitet: Oslo universitetssykehus HF består i dag av flere sykehus, blant andre Ullevål, Rikshospitalet og Aker, der

Ullevål alene har ca 9 500 ansatte. På den annen side kan en tannlege- eller legevirksomhet, fysioterapeutvirksomhet, psykologvirksomhet kanskje ha to eller tre ansatte. Det sier seg selv at de organisatoriske tiltakene som må til for å sikre god informasjonssikkerhet – og særlig tilgangsstyring - i disse virksomhetene vil kreve svært ulik tilnærming. Departementet er ut fra dette enig med Troms fylkeskommune i at informasjonssikkerhetstiltakene må være tilpasset virksomhetens art, aktiviteter og størrelse.

Kravene til planlegging, organisering og rutiner i forslaget til forskrift gir rom for dette, selv om kravene er noe mer detaljerte og spisset mot helsetjenesten, enn personopplysningsforskriften. Det samme gjelder bestemmelsen om internkontroll. En viktig hensikt med internkontroll er å sikre at krav fastsatt i lov og forskrift overholdes. Plikten til internkontroll skal sikre at kravene i denne forskriften overholdes. Det er etter departementets vurdering ikke tilstrekkelig at ovennevnte krav tas inn som merknader til personopplysningsforskriften eller er omhandlet i Norm for informasjonssikkerhet, blant annet fordi merknadene og normen ikke er direkte rettslig bindende.

Departementet er enig med Helse-Sør Øst RHF i at nødvendige rutiner alltid må utarbeides ved behov, og uten at dette detaljreguleres nærmere. Det er blant annet på denne bakgrunn at forskriften kun setter krav om at det skal foreligge rutiner, men det er virksomheten selv som må utarbeide innholdet i rutinene. Man kan imidlertid ikke la være ha rutiner, og det må gjelde for alle nivåer i virksomheten. Ledelsen i virksomheten må kunne vise til hvordan regelverket er implementert i egen virksomhet – der den faktiske behandlingen av helseopplysningene finner sted. Det er ikke nok å ha et overordnet regelverk og forutsette at det etterleves nedover i virksomheten. Den databehandlingsansvarlige må kunne dokumentere at forskriftens krav er implementert på alle nivåer i virksomheten.

Departementet er også enig med Troms fylkeskommune i at helsepersonell har en selvstendig plikt til å holde seg orientert om gjeldende lovverk. Ikke desto mindre finner departementet det nødvendig å innta et krav om opplæring i denne forskriften. De ulike virksomhetene innen helsetjenesten er som nevnt meget forskjellige, og sårbarhet – og risikovurderingene forbundet med behandling av helseopplysninger vil trolig også være ulike. Det er derfor helt nødvendig at helsepersonell ved ansettelse gis opplæring i hvordan god informasjonssikkerhet gjennomføres innen akkurat denne virksomheten, der vedkommende har sin arbeidsplass.

4.5. Krav til system for utstedelse av autorisasjoner, krav til autentisering og autorisasjon

4.5.1 Forslaget i høringsnotat av oktober 2008

I høringsnotatet ble det i forskriften § 11 foreslått en plikt for den databehandlingsansvarlige til å etablere nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av tilgangsrettigheter til helseopplysninger som behandles i virksomhetens behandlingsrettede helseregistre. Det ble stilt krav om at tilgangsstyringen skal bygge på konkrete risikovurderinger for urettmessig tilegnelse av helseopplysninger. Videre fremgikk at tilgangsstyringen skal bidra til å sikre at informasjonssikkerheten, herunder bestemmelsene om taushetsplikt og pasientens rett til konfidensialitet blir ivaretatt.

I de etterfølgende bestemmelser §§ 12 til 14 ble det gitt særskilte regler for autorisasjon for:

- ytelse av helsehjelp eller administrasjon av slik hjelp (§ 12)
- besvarelse av henvendelser (§ 13)
- kontrollkommisjonen innen det psykiske helsevern (§ 14)
- andre formål (§ 15)

Det ble foreslått krav om at det enkelte helsepersonells tjenstlige behov for tilgang til helseopplysninger skulle vurderes og om nødvendig oppdateres jevnlig, samt plikt for den databehandlingsansvarlige til å føre et register over autorisasjoner. Videre ble det fastsatt minstekrav til innhold i et slikt register.

Forskriften fastslo videre at enhver som gis elektronisk tilgang til helseopplysninger skal kunne identifiseres som en bestemt person i en bestemt rolle (autentiseres), og at ingen skal gis mulighet til å kunne få tilgang til helseopplysninger i et behandlingsrettet helseregister før nødvendig opplæring i informasjonssikkerhet er gitt.

4.5.2 Høringsinstansenes synspunkter

Åtte høringsinstanser har kommentert en eller flere av bestemmelsene. Det er *Legeforeningen*, *Kompetansesenter for IT i helse- og sosialsektoren AS (KITH)*, *IKT-Norge*, *Helse Bergen HF*, *Helse Sør-Øst RHF* og *Ullevål sykehus, Fornyings- og administrasjonsdepartementet og Datatilsynet*. Noen av disse – som høringsuttalelsene fra Fornyings- og administrasjonsdepartementet, KITH og IKT-Norge er omtalt i punkt 4.6.2 nedenfor.

Legeforeningen viser til at forskriften § 11 stiller overordnede krav til at det etableres nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av tilgangsrettigheter, samt at forskriften § 12 fastslår at helsepersonell som har behov

for det for å kunne gi forsvarlig helsehjelp, kan gis tilgang. Foreningen bemerker at ingen av bestemmelsene beskriver hva som konkret kreves for å få tilgang. Legeforeningen savner en mer konkret regulering av disse mekanismene, i alle fall en mer utfyllende redegjørelse i merknadene til forskriften. Legeforeningen uttaler også at de er svært kritiske til de øvrige bestemmelsene (dvs. §§ 13, 14 og 15, se punkt 4.5 1 foran). Foreningen uttaler: "Hva som ligger i å besvare henvendelser er ikke definert i forskriften, men i merknaden fremkommer at det er ment å omfatte henvendelser hvis besvarelse ikke anses som helsehjelp til pasienten, for eksempel personell i informasjonsskranken som skal informere om hvor en pasient ligger. Denne bestemmelsen er åpenbart i strid med helsepersonellovens regler for innsyn i helseopplysninger, og gir således i strid med departementets egne intensjoner tilgang ut over det som følger av taushetspliktsreglene. Vi antar for øvrig at de fleste sykehus har administrative systemer som har opplysninger som ikke faller inn under taushetspliktsreglene, og som ikke- autorisert personell kan hente denne type opplysninger fra."

Til utkastets §§ 14 og 15 uttaler Legeforeningen:

"At det skal gis direkte tilgang til EPJ til personer som ikke omfattes av helsepersonelloven, slik det legges opp til i § 14 og § 15 er en nyvinning som vi ikke kan se at departementet har begrunnet tilstrekkelig i sitt høringsnotat. Den som etter helsepersonelloven eller annen lovgivning har rett på opplysninger fra journal vil være tilstrekkelig hjulpet ved at opplysningene blir utlevert av den som har ansvaret for journalen. Vi kan verken se behovet for, eller nødvendigheten av, at det skal gis direkte tilgang i slike tilfeller. Dette bidrar til ytterligere fare for spredning av personopplysinger, og her må personvernhensynet åpenbart veie tyngre enn hensynet til at det vil være praktisk for tilsynet eller andre å få direkte tilgang. Retten til opplysninger vil i de aller fleste tilfeller være begrenset til relevante og nødvendige opplysninger, og det kan ikke være slik at det er den som ønsker opplysninger som skal lete seg gjennom journalen for å finne det man er ute etter. Særlig mener vi § 15 gir en alt for vid hjemmel til tilgang."

Helse Bergen HF uttaler at de er positive til at det blir foreslått avgrenset tilgang for kontrollkommisjonen. Helse Bergen mener imidlertid at personell med støttefunksjoner bør håndteres annerledes enn tilsynsmyndigheter og eventuelle andre eksterne. Det samme gjør KITH. KITH foreslår at det tas inn følgende bestemmelse som dekker disse gruppene": *Personell som har en støttefunksjon i forbindelse med ytelse eller administrering av helsehjelp, kan bare gis elektronisk tilgang til de helseopplysninger som er nødvendig for å kunne ivareta denne støttefunksjonen.*

Helse Bergen HF, Helse Sør-Øst RHF og Ullevål universitetssykehus har alle kommentarer til høringsnotatets merknader til forskriftens krav om at tildelte tilgangsrettigheter jevnlig skal vurderes og om nødvendig oppdateres jevnlig, samt merknaden om at fravær på eksempelvis 4 ukers ferie, skal medføre en midlertidig sperring av brukerkonto.

Helse Bergen HF uttaler at det ikke er praktisk mulig å sperre tilgangen til personell på fire ukers ferie i et foretak med over 8 000 ansatte. Det samme uttaler Ullevål universitetssykehus. Universitetssykehuset ser samtidig at det er viktig at tilganger/autorisasjoner jevnlig skal kontrolleres. Sykehuset mener at kravet må settes mer generelt, slik at det kan være mulig å få dette praktisk gjennomført.

Helse Sør-Øst RHF mener det er lite hensiktsmessig å stenge tilgangen i forbindelse med avvikling av ferie av mer ordinær karakter og at dette i tillegg vil bli vanskelig å administrere. Helseforetaket mener at dette bør det være innenfor ledelsens og systemansvarliges ansvarsområde å vurdere.

Datatilsynet mener at kravet til autentisering bør styrkes til 2-faktor autentisering, og at dette også bør gjelde for tilgang internt i virksomheten. Datatilsynet viser til helsepersonellovens § 21b og Helsetilsynets foreløpige praktisering av denne, og uttaler at med dagens krav til autentisering vil forbudet mot snoking fort miste realitet.

Fornyings- og administrasjonsdepartementet uttaler at de oppfatter forskriftsutkastet § 17 som en klargjøring av at felleskontoer ikke vil gi grunnlag for tilgang til helseopplysninger, og poengterer viktigheten av at denne bestemmelsen etterleves.

4.5.3 Departementets vurderinger og forslag

Høringsnotatets forslag til regler om tilgang til helseopplysninger i behandlingsrettede helseregistre (forskriften kapittel III) fastslo krav til utstedelse av autorisasjoner og helsepersonells bruk av den tildelte autorisasjonen - i felles bestemmelser. Departementet har kommet til at en slik systematikk kan gjøre regelverket vanskelig å forholde seg til og lett kan misforstås. I forslaget til forskrift som nå sendes på høring har departementet tatt inn krav som pålegges den databehandlingsansvarlige ved den/de som utsteder autorisasjoner i kapittel III i forskriften, mens krav og forutsetninger for bruk av en tildelt autorisasjon er inntatt i forskriften kapittel IV.

Ingen av høringsinstansene har, slik departementet oppfatter det, uttalt seg negativt til høringsnotatets krav om system for utstedelse av autorisasjoner og krav om autorisasjon og autentisering. Høringsinstanser har heller ikke hatt innvendinger til at den enkelte autorisasjon må bygge på konkrete risikovurderinger for urettmessig behandling av helseopplysninger. Disse kravene følges derfor opp i dette forskriftsforslaget. I tillegg foreslås at autorisasjonen skal være tidsbegrenset, uten at det oppstilles noe krav om maksimum varighet. Varigheten til en autorisasjon må vurderes konkret og ut i fra formålet med autorisasjonen. Departementet kan være enig i at det i mange tilfelle vil være lite hensiktsmessig å stenge muligheten for tilgang i forbindelse med avvikling av ferie eller andre fraværsgrunner som opptrer mer eller mindre regelmessig og ikke er av langvarig karakter. Hensikten med kravet om

tidsbegrensning er at virksomheten skal ha et bevisst forhold til spørsmålet ved tildeling av autorisasjon. For en fast ansatt med faste gjøremål i en stabil virksomhet som ikke gjennomgår organisatoriske endringer, er det ikke noe i veien for at en autorisasjon kan ha en varighet på 1 til 2 år. Skjer det endringer i ansettelsesforhold eller endringer i organisasjonen må imidlertid innholdet i autorisasjonen vurderes på nytt.

For helsepersonell som skal ta i bruk en autorisasjon er det viktig at autorisasjonen støtter opp om og så langt som mulig bidrar til at tilgangsmulighetene i størst mulig grad samsvarer med hva helsepersonell har tjenstlig behov for. Tilgangsstyringssystemet må derfor konfigureres slik at risikoen for at helsepersonell kan få tilgang til helseopplysninger om pasienter de ikke er involvert i helsehjelpen til, blir minst mulig. For å bidra til dette foreslår departementet at den databehandlingsansvarlige skal vurdere og konfigurere tilgangen med hensyn til antall registrerte det gis tilgang til, mengde informasjon om den enkelte det gis tilgang til og varigheten av tilgangen. Det vises til forskriftsforslaget § 10 andre punktum. Som nevnt innledningsvis i høringsnotatet er det viktig at reglene i forskriften er praktikable. Departementet ber derfor om høringsinstansenes syn på om kravene i forskriftsforslaget § 10 andre punktum er tilstrekkelig fleksible til at helsepersonell kan få tilgang til nødvendige og relevante opplysninger når det er tjenstlig behov for det for å yte forsvarlig helsehjelp til pasienten.

Både høringsnotatet av oktober 2008 og dette høringsnotatet har en bestemmelse om at ingen kan gjøre bruk av en tildelt autorisasjon i videre omfang enn det som følger av reglene om taushetsplikt. Det er en plikt som pålegges alle tjenesteytere som gis autorisasjon. Dette følger allerede av loven, men det er viktig å synliggjøre dette kravet også i denne forskriften.

Departementet er litt usikker på hva Legeforeningen mener når de uttaler - til forskriftens forslag om besvarelse av henvendelser - at de antar at de fleste sykehus har administrative systemer som har opplysninger som ikke faller inn under taushetsplikten, og som ikke autorisert personell kan hente slike opplysninger fra. Departementet legger til grunn at opplysninger om og hvor en bestemt pasient eventuelt er innlagt på sykehus, er taushetsbelagte opplysninger, som det vil kreves autorisasjon for å få tilgang til, jf. blant annet helsepersonelloven § 26 tredje ledd. Hensikten med bestemmelsen er å fastslå at tilgangen i disse tilfeller skal begrenses til kun de opplysninger som er nødvendig for å svare på henvendelsen – det vil si at det skal være mulig bare å få tilgang til opplysninger om en pasient er innlagt, og eventuelt hvor vedkommende er innlagt. På bakgrunn av høringsuttalelsene har departementet gruppert autorisasjonene noe annerledes i dette forskriftsforslaget, enn i høringsnotatet av oktober 2008. Departementet har inndelt autorisasjonen i følgende grupper:

- Autorisasjon for ytelse av helsehjelp, jf. helsepersonelloven §§ 25 første ledd og 45 første ledd
- Autorisasjon for administrering av helsehjelp, jf. helsepersonelloven § 26 andre ledd
- Autorisasjon for ytelse av nødvendige støttefunksjoner, jf. helsepersonelloven § 25 andre ledd

Det forhold at helseopplysninger er underlagt taushetsplikt innebærer at det bare kan gis tilgang til helseopplysninger når det er fastsatt i lov eller i medhold av lov. Inndelingen av autorisasjonene har derfor tatt utgangspunkt i helsepersonellovens regler om taushetsplikt og opplysningsrett/opplysningsplikt. En forutsetning for at noen kan få direkte elektronisk tilgang til helseopplysninger er at man først er autorisert til det. Autorisasjonen fastslår rammen for tilgangsmulighetene.

Høringsnotatets bestemmelser om autorisasjon for andre formål er tatt ut av forskriften. Departementet er enig med Legeforeningen i at en egen autorisasjonsbestemmelse for andre formål (for eksempel kvalitetssikring og forskning) kan favne for vidt. Departementet mener at tilgang til helseopplysninger til andre formål enn helsehjelp til pasient primært bør skje ved at opplysningene utleveres, og bare unntaksvis ved at det gis direkte tilgang til opplysningene med grunnlag i en enkeltstående autorisasjon til akkurat dette formålet. Direkte tilgang til helseopplysninger til for eksempel forskning eller kvalitetssikring forutsetter bruk av funksjoner som kan trekke ut ulike "bestillinger" av strukturerte og forhåndsdefinerte opplysninger. Departementet antar at implementering av slike funksjoner ligger noe frem i tid. Forskriften vil imidlertid kunne videreutvikles etter hvert som funksjonaliteten i EPJ-systemene endres.

Bestemmelsene pålegger ikke den databehandlingsansvarlige noen plikt til å gi autorisasjon for direkte tilgang til helseopplysninger. Den databehandlingsansvarlige kan således velge å bestemme at opplysningene skal *utleveres – manuelt eller elektronisk* - til vedkommende i stedet for at vedkommende skal gis autorisasjon til *direkte* tilgang. Departementet har vurdert om den databehandlingsansvarlige bør ha en plikt til å gi helsepersonell direkte tilgang til opplysningene. Departementet har kommet til det må være opp til den databehandlingsansvarlige for behandlingen av opplysningene å bestemme på hvilken måte helsepersonell skal få tilgang til nødvendige og relevante helseopplysninger. Det foreslås derfor i forskriften at autorisasjon *kan* gis. Dette for ikke å frata den databehandlingsansvarlige rett til å treffe beslutning om noe annet, dersom det skulle være behov for det. Som eksempel kan anføres at en ansatt har misbrukt sin autorisasjon.

4.6 Tilgang til helseopplysninger i behandlingsrettet helseregister

4.6.1 Forslaget i høringsnotatet av oktober 2008

Bestemmelsene om elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre var i høringsnotatet av oktober 2008 integrert i bestemmelsene om autorisasjon. Høringsnotatet av oktober 2008 hadde derfor ikke et eget kapittel i forskriften som særskilt regulerte helsepersonells bruk av autorisasjonen og forutsetninger for bruken.

4.6.2 Høringsinstansenes synspunkter

Høringsinstansenes kommentarer til bestemmelsene om krav/vilkår for autorisasjon kan også sees på som synspunkter på den videre bruk og forutsetninger for autorisasjonen. Det gjelder for eksempel merknaden fra *Legeforeningen* nevnt under punkt 4.5.2 om at foreningen savnet en mer konkret regulering av tilgangsmekanismene, og i alle fall en mer utfyllende redegjørelse i merknadene til forskriften. Det samme gjelder høringsuttalelsene fra *Fornyings- og administrasjonsdepartementet, Kompetansesenter for IT i helse- og sosialsektoren* og *IKT-Norge* som omtales nedenfor.

Kompetansesenter for IT i helse- og sosialsektoren AS (KITH) hadde ingen merknader til selve forskriftsteksten (§ 12), men mener at det som sto skrevet om beslutningsstyrt tilgang i merknadene bygger på en misforståelse av hva beslutningsstyrt tilgang er. KITH uttaler:

"Beslutningsstyrt tilgang er *påbygning* til den tradisjonelle rollebaserte tilgang. I tradisjonell rollebasert tilgangsstyring assosieres tilgangsrettigheter til roller. En slik rolle kan da tildeles en eller flere brukere som derigjennom blir autorisert for tilgang til en delmengde av de opplysninger som finnes. Når brukeren først er autorisert utløses retten til å lese de opplysninger som er omfattet av autorisasjonen ved at brukeren logger på det aktuelle systemet. Disse rettighetene er statiske og uavhengig av om brukeren har noe tjenestelig behov for opplysninger om den enkelte pasient. Tilgangen kan kun endres gjennom at autorisasjonen endres.

Benyttes beslutningsstyrt tilgang derimot, gir autorisasjonen brukeren får gjennom rollen kun en potensiell rett til å lese de opplysninger som er omfattet av autorisasjonen. Den faktiske retten utløses først ved at noen som er autorisert for det, tar en beslutning som innebærer at brukeren blir involvert i helsehjelp til en bestemt pasient. Den tilgangen som brukeren da får, begrenses til de typer opplysninger som er omfattet av brukerens autorisasjon. Når det tiltaket som beslutningen gjaldt er gjennomført opphører tilgangen. Beslutningsstyrt tilgang er altså i sin natur en tilgang som gis implisitt som følge av en beslutning relatert til helsehjelp, å snakke om eksplisitt beslutningsstyrt tilgang gir altså ikke mening."

IKT-Norge har også merknader til høringsnotatets omtale av beslutningsstyrt tilgang og viser til følgende omtale i merknadene til § 12: "Med beslutningsstyrt tilgang menes at tilgang skal baseres på en eksplisitt beslutning fra vedkommende helsepersonell som søker tilgang. For tilgang til helseopplysninger i annen avdeling/post enn vedkommende har sitt arbeid, skal det normalt kreves eksplisitt beslutning som vilkår for tilgang." IKT-Norge mener at dette er en svært uheldig begrensning som vil være svært vanskelig å følge opp i praksis. IKT-Norge viser til at i en klinikksituasjon hvor det gås vakter vil det være ulike behov fra vakt til vakt for tilgang til pasientens journaler, og at det på natten ofte er en vakt som har ansvaret for mange avdelinger og poster. IKT-Norge mener dette blir i motstrid til helsepersonelloven § 45, som fastslår at helsepersonell som yter helsehjelp skal gis tilgang til helseopplysninger, men mindre pasienten motsetter seg det.

Helse Bergen HF har kommentarer til i merknadene der det uttales at det ikke skal innhentes opplysninger om tidligere behandlet pasient av egen interesse. Helse Bergen stiller spørsmål ved uttrykket "egen interesse". Helseforetaket mener at det er normalt og ønskelig å kvalitetssikre egen behandling av pasienten i ettertid, og at dette må kunne gjøres innen rimelig tid etter at pasienten er ferdigbehandlet uten at det blir "kriminalisert". Foretaket uttaler videre at det er viktig at helsepersonell også lærer av egen erfaring og at dette også kommer andre pasienter til gode.

4.6.3 Departementets vurderinger og forslag

Departementet foreslår at det tas inn et eget kapittel IV i forskriften om tilgang til helseopplysninger i behandlingsrettet helseregister. Materielt sett foreslås det ingen endringer i forhold til høringsnotat av oktober 2008, men oppbyggingen av reglene og strukturen er endret, se punkt 4.5.3 foran.

Bestemmelsene i kapittel IV gjelder i utgangspunktet både ved tilgang internt i virksomheten og ved tilgang på tvers. Bestemmelsene i forskriften kapittel V er tilleggskrav ved tilgang på tvers.

Departementet har merket seg kommentaren fra KITH vedrørende høringsnotatets språkbruk "rollebasert og eksplisitt beslutningsstyrt tilgang" Bakgrunnen for at departementet uttrykte seg slik i høringsnotatet var å synliggjøre at også beslutningsstyrt tilgang – som KITH fremhever er en påbygning til alminnelig tradisjonell tilgang – kan åpne for ganske vide tilgangsmuligheter. Det vises til KITHs uttalelse " Den faktiske retten utløses først ved at noen som er autorisert for det, tar en beslutning som innebærer at brukeren blir involvert i helsehjelp til en bestemt pasient." Slik departementet forstår det refererer ikke "brukeren" i nevnte setning seg nødvendigvis til en eller flere bestemt navngitt personell, men til roller – som for eksempel kan has av samtlige personell på den eller de avdelinger en pasient skal motta tjenester fra. Innføring av beslutningsstyrt tilgang vil således i seg selv ikke hindre at helsepersonell

kan få tilgang til helseopplysninger han eller hun strengt tatt ikke har behov for. Det avgjørende vil være hvordan den enkelte virksomheten internt tilrettelegger og organiserer den beslutningsstyrte tilgangen. En nøye gjennomtenkt tilrettelegging og organisering av den rollebaserte beslutningsstyrte tilgangen - basert på risikovurderinger, vil være helt avgjørende for ivaretakelse av god informasjonssikkerhet. Dette gjelder særlig de store virksomheter. I mindre virksomheter - hvor bare en eller to har tilgang til journalsystemet – må dette kunne gjøres ganske enkelt. Det vises før øvrig til punkt 4.5.3 om krav om tilgangsstyring.

Departementet mener at det ikke er nødvendig med et absolutt krav om 2-faktor autentisering internt i virksomheten, jf. Datatilsynets uttalelse nevnt under punkt 5.4.2. Dette gjelder særlig med tanke på de mindre virksomhetene. Dette hindrer selvfølgelig ikke at virksomhetene, og da særlig de store helseforetakene, legger opp til å innføre 2-faktor autentisering på sikt. (To-faktor autentisering er et system der to forskjellige metoder blir brukt i autentiseringsprosessen.)

Departementet ser det som svært viktig - som Helse Bergen HF påpeker – at helsepersonell normalt kvalitetssikrer egen behandling av pasienten. Videre er det viktig at helsepersonell lærer av egen erfaring.

Departementet er av den oppfatning at oppfølging eller kvalitetssikring alt etter omstendighetene også bør kunne skje etter at en pasient er utskrevet fra sykehuset. I noen tilfeller kan det være slik at sykehuset tar kontakt med pasienten i en viss tid etter utskrivelsen og/eller at det er avtalt at pasienten kan henvende seg direkte til sykehuset, dersom det skulle være behov for det. Departementet mener at tilgang til pasientens helseopplysninger i slike tilfeller også kan skje med grunnlag i at det skal gis helsehjelp til pasienten.

Et annet eksempel kan være at virksomheten har bestemt at visse typer tiltak alltid skal gjennomgås i ettertid. Det vil i utgangspunktet ikke anses å være en del av helsehjelpen til pasienten. Helsepersonelloven § 26 første ledd vil kunne gi rettsgrunnlag for kvalitetssikring i et slikt tilfelle.

Bruk av helsepersonelloven § 26 første ledd forutsetter at virksomhetens ledelse har besluttet at intern kvalitetssikring skal skje. Det kan for eksempel være ønskelig at innleggende lege kvalitetssikrer sine egne vurderinger ved innleggelsene. Helsepersonell kan imidlertid ikke uten videre gå inn i en pasients journal for kvalitetssikringsformål - uten at det er forankret i en beslutning fra virksomhetens ledelse.

4.7 Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

4.7.1 Forslaget i høringsnotatet av oktober 2008

Det ble i høringsnotatet av oktober 2008 foreslått tre særskilte bestemmelser om tilgang til helseopplysninger på tvers av virksomheter.

I forskriftsforslaget § 19 ble det fastslått at helsepersonell kan gis lesetilgang til helseopplyninger i ekstern virksomhet dersom virksomhetene på forhånd hadde inngått avtale om det. Det ble presisert i forskriften at avtale om lesetilgang bare kunne inngås for tilfeller der formålet med tilgangen er pasientbehandling eller annen type helsehjelp til pasienten. Videre ble det presisert at det skal fremgå av avtalen hvilke personell i hvilke roller som gis lesetilgang samt hvilke forutsetninger som skal gjelde. Det ble også presisert at det ikke kan inngås avtale om nødrettstilgang.

Forskriftsforslaget § 20 åpnet for at avtalen også kunne åpne for å nedtegne anmerkninger dersom det er nødvendig for å oppfylle formålet med lesetilgangen, som nevnt i § 19.

I forskriftsforslaget § 18 ble fastslått at avtale, jf. ovenfor, bare kan inngås dersom gjennomføring av den ikke svekker informasjonssikkerheten ved behandling av helseopplysninger ved noen av virksomhetene.

4.7.2 Høringsinstansenes synspunkter

Forskriftens bestemmelse om lesetilgang på tvers av virksomheter er den bestemmelsen som har foranlediget de fleste kommentarer.

Forskriftens bestemmelser om begrenset anmerkningstilgang/skrivetilgang (forskriften § 20) har ikke blitt kommentert i like stort omfang, og tilslutningen til bestemmelsen synes å være noe mer forbeholden enn tilslutningen til bestemmelsen om lesetilgang: *Helse Stavanger HF* mener man må være varsom med å åpne for skrivetilgang på tvers, og at dette må avtales særskilt. *Helse Fonna HF* mener bestemmelsen om skrivetilgang på tvers av virksomheter er helt uproblematisk.

Sande kommune uttaler at de opplever at begrepet virksomhet i denne sammenheng er svakt definert i forhold til den kommunale organisering av tjenester. Kommunen mener det bør klarere defineres hvilke typer virksomheter som er å forstå som interne, og hvilke som er eksterne, samt at kravene til sikkerhet ved tildeling av rett til deling av definerte deler av helseregistre innenfor klare tidsvinduer blir tydeligere definert.

Helse Stavanger HF uttaler at de i hovedtrekk slutter seg til forslag til endringer som kan åpne for journaltilgang (lesetilgang) på tvers av virksomhetsgrenser, og legger til at dette i de fleste praktiske tilfelle vil gjelde mellom 2 virksomheter.

Helse Bergen HF uttaler at de er enig i at man ikke kan avtale bruk av nødrett. Helseforetaket tilføyer at det imidlertid ikke må bli slik at det sperres for bruk av nødrett. Helseforetaket viser til at i det tette samarbeidet som er mellom Haukeland universitetssykehus og Haraldsplass diakonale sykehus, så er det nettopp i kritiske akuttsituasjoner at det har vært behov for tilgang til journal mellom sykehusene. Helseforetaket uttaler at ved god og praktisk løsning av "tilgang på tvers" vil bruk av nødrett trolig være lite aktuell. For de tilfellene dette likevel må brukes, så vil det da være mulig å følge dette opp gjennom avvikshåndtering.

Helse Fonna HF uttaler at for dem er § 19 i forslaget til forskrift den viktigste biten i hele høringsnotatet. Helseforetaket mener at utformingen av denne paragrafen er uklar, og stiller spørsmål om hvorfor nødrett ikke skal brukes.

Nasjonalt senter for telemedisin uttaler at avtalebasert lesetilgang på tvers av virksomheter utvilsomt kan fylle et behov. Senteret legger til at det her er særlige utfordringer knyttet til Distriktsmedisinske sentra som (også) utfører spesialisthelsetjenester.

Norges teknisk-naturvitenskapelige universitet anser også forslaget om lesetilgang på tvers av virksomheter som den viktigste bestemmelsen i forskriften - det gjelder for praktisk klinisk virksomhet, etablering av behandlingskjeder og samarbeid mellom spesialisthelsetjenesten og kommunehelsetjenesten.

Kompetansesenter for IT i helse- og sosialsektoren AS (KITH) påpeker to forhold ved utformingen av § 19. For det første gjelder det selve avtalen og hva den skal inneholde. KITH tror det er urealistisk å kreve at navnene på de som skal kunne gis tilgang er angitt i selve avtalen. KITH viser til at bemanningen langt fra er statisk og uttaler at det knapt vil være mulig å gjennomføre en revisjon av en slik avtale hver gang en lege slutter eller en ny lege begynner. KITH mener derfor det bør være tilstrekkelig at det avtales hvordan en skal informere hverandre om hvilket personell som til enhver tid er omfattet av avtalen. KITH mener det bør åpnes for at avtalen kan omfatte mer enn to virksomheter, ettersom det i mange tilfeller trolig vil være slik at flere virksomheter har et gjensidig behov for tilgang.

Det andre gjelder tilgang når det foreligger en nødrettssituasjon. KITH kan ikke se noe saklig grunn for at tilgang skal nektes dersom det foreligger en situasjon hvor den som søker tilgang kan påberope seg nødrettsbestemmelsen i straffeloven § 47. KITH uttaler at de undres på om det virkelig er mulig gjennom en bestemmelse i en forskrift å sette straffeloven § 47 til side eller søke å hindre at den kan komme til anvendelse.

Helse Sør-Øst og *IKT-Norge* stiller også spørsmål ved hensiktsmessigheten av nødrettsbestemmelsen.

Helsedirektoratet uttaler at direkte tilgang til informasjon i egne systemer for personell utenfor virksomheten gir en rekke nye utfordringer med hensyn til informasjonssikkerhet (hvordan), tilgangsstyring (hvem og hva) og i forhold til journalføring. Direktoratet er enig i at det bør åpnes for tilgang til helseopplysninger i EPJ-system på tvers av virksomheter. Direktoratet mener imidlertid at det er upraktisk og lite gjennomførbart at slik tilgang skal måtte "avtales" mellom virksomhetene. Direktoratet mener avtaleverket blir for stort og uoversiktlig. Direktoratet uttaler at dersom det skal inngås avtaler mellom alle virksomheter/juridiske enheter betyr dette inngåelse av millionvis av avtaler.

Direktoratet mener at dette kan gjøres på en enklere og like sikker måte ved at noen gis myndighet til å fastsette nærmere minstekrav for tilgang til helseopplysninger på tvers av virksomheter. Direktoratet viser til at de har under arbeid en rapport om minstekrav som må være til stede for at det skal kunne åpnes for tilgang til virksomhetsinterne helseopplysninger på tvers av virksomheter, og at denne vil bli oversendt HOD i løpet av januar 2009. Direktoratet uttaler videre at det må tilrettelegges for at virksomhetene kan stole på at de øvrige virksomhetene oppfyller minstekravene, og mener dette kan gjøres via en tiltrodd tredjepart. Ett eksempel er Norm for informasjonssikkerhet i helsesektoren. Direktoratet viser til at virksomhetene ikke har inngått avtale med hverandre, men i stedet har sluttet seg til ett sett av minstekrav (Normen) ved inngåelse av avtale med Norsk Helsenett.

Oslo kommune ser positivt på forskriften § 19 som åpner for lesetilgang på tvers av virksomheter. Kommunen uttaler:

”I pleie- og omsorgstjenesten har Oslo kommune konkurranseutsatt driften av om lag 1/3 av sykehjemmene og innført brukervalg i hjemmetjenesten. Dette innebærer at deler av den helsehjelpen kommunen har ansvar for å yte, blir utført av medarbeidere som er ansatt i private virksomheter (kommersielle og ideelle). Dette er helsehjelp som inngår som del av det samlede kommunale helsetilbudet, som er finansiert av kommunen og som inngår i IPLOS rapporteringen til SSB. Skal de private utførerne kunne yte forsvarlig helsehjelp, må de ha tilgang til de opplysningene som er registrert i kommunens pleie- og omsorgssystem om de pasientene de yter hjelp til.”

Norsk Sykepleierforbund uttaler at direkte tilgang til pasientjournaler mellom virksomheter krever mye av teknologien og ikke minst av den databehandlingsansvarlige. Forbundet påpeker at det må sikres at uvedkommende ikke får tilgang til opplysninger de ikke skal ha. Forbundet viser til pasientens rett til å bestemme at enkelte ikke skal ha tilgang til journalen, eller at visse informasjonselementer i journalen skal unntas for innsyn. Forbundet mener det bør beskrives hvordan dette kan løses i praksis, slik at pasientens tillit til systemet blir ivaretatt.

Norsk senter for elektronisk pasientjournal (NSEP v/ NTNU) viser til at ved tilgang på tvers, vil tilgang til informasjonsmengde og type kunne bli en helt annen og være individuell. Videre uttales at det kan være opplysninger der som ikke er relevante og nødvendige for formålet som blir oppgitt. NSEP mener tilgang på tvers er mest aktuelt for situasjoner med planlagte tjenester og der virksomheter og helsepersonell samarbeider tett om pasienter på en slik måte at kommunikasjon med for eksempel henvisning og epikriser ikke strekker til. Videre uttales at tilgang på tvers ved funksjonsfordeling mellom sykehus og samarbeid om pasienter med store og kompliserte behov i pleie- og omsorgstjenesten, for eksempel palliativ behandling hjemme, vil være mest aktuell. NSEP viser videre til at erfaring med tilgang på tvers er at det blir lite brukt i akuttsituasjoner.

NSEP mener at en avtale om lesetilgang mellom virksomheter ikke bare skal omhandle de sikkerhetsmessige forholdene, men også være spesifisert i forhold til hvilke formål dette skal gjelde, som for eksempel som et ledd i en avtalt planlagt arbeidsfordeling i et standardisert pasientforløp (behandlingslinje) som det kan vises til. NSEP mener det ikke vil være praktisk gjennomførbart å knytte avtalen til navngitt helsepersonell og roller og ser heller ikke noen gevinst i det. NSEP mener at det som er viktigst er at når tilgang opprettes skal det være for navngitt pasient og avgrenset til dennes journal, og det skal være gitt eksplisitt samtykke.

Vedrørende bestemmelsen om begrenset skrivetilgang uttalar *Apotekene Vest*: "Vi er i utgangspunktet skeptisk til mulighet for å skrive i journaler "fra utsiden", bl.a. pga. eierskap til opplysningene, og ansvarsfordeling mellom partene ved eventuelle feil. Det finnes imidlertid situasjoner der det vil være en stor fordel at flere instanser kan skrive i samme journal, for eksempel for pasienter med omfattende hjelpbehov både fra primær- og sekundær-, samt eventuelt også sosialtjenesten. Forskrifter eller retningslinjer kan støtte opp under god og sikker gjennomføring også ved slike fellesjournaler. "

4.7.3 Departementets vurderinger og forslag

Departementet mener at tilleggskravene for direkte tilgang til helseopplysninger på tvers av virksomhetsgrenser bør komme tydeligere frem, enn det gjorde i høringsnotatet av oktober 2008. Bakgrunnen for dette er dels uttalelser i Ot.prp. nr. 51 (2008–2009) og Stortingets behandling av denne, jf. Innst. nr. 110 (2008–2009), og dels synspunkter fra høringsinstansene.

I dette høringsforslaget er det derfor inntatt flere og mer presise krav enn i det tidligere utkastet. Departementet foreslår at forskriften også setter krav til forespørselen om å få direkte tilgang til helseopplysninger i annen virksomhet og de tekniske forutsetninger for dette. Det foreslås presisert at forespørselen skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet. Forespørselen samt beslutningen om å etterkomme den, eller ikke, skal registreres. Ved behov for gjentatt tilgang til

helseopplysninger om samme pasient skal det gjøres en ny forespørsel. Disse kravene er for øvrig også foreslått i Helsedirektoratets rapport med forslag til minstekrav til EPJ-systemer. Videre foreslås at direkte tilgang til helseopplysninger bare kan omfatte strukturerte helseopplysninger som er relevante og nødvendige for å nå formålet med behandlingen av opplysningene. Departementet mener også at det bør gå klart frem av forskriften at tilgang til helseopplysninger i ekstern virksomhet bare kan omfatte opplysninger som det på forhånd er vurdert at det kan gis tilgang til. For sammenhengens skyld foreslås at helseregisterloven § 13 femte ledd - en forespørsel om og tilgang til helseopplysninger i annen virksomhet kan bare omfatte en person om gangen – gjentas i forskriften.

I motsetning til høringsnotatet av oktober 2008 legger herværende forskrift til grunn at direkte tilgang til helseopplysninger på tvers av virksomheter bare kan gis etter samtykke fra den registrerte. Det vises til helseregisterloven 13 tredje ledd. Departementet foreslår at det gjøres unntak fra dette kravet der pasienten på grunn av sin fysiske eller psykiske tilstand, ikke er i stand til å samtykke.

Begrepet virksomhet i uttrykket "tilgang til helseopplysninger i behandlingsrettede helseregistre" refererer til den virksomhet, eventuelt person, som er databehandlingsansvarlig for behandlingen av helseopplysningene. Departementet viser til helseregisterloven § 13 første ledd første punktum som fastslår at bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger, og videre til helseregisterloven § 13 andre ledd andre punktum som fastslår at det i forskrift kan gjøres unntak fra dette utgangspunktet. Denne forskriften er et slikt unntak.

Innenfor den statlige spesialisthelsetjenesten referer virksomhetsbegrepet seg til det aktuelle helseforetak som yter spesialisthelsetjenester. En virksomhet kan også være en enkeltmannsbedrift, for eksempel innen tannhelse, psykiatri, annen spesialisert helsetjeneste eller det kan være private sykehus, som Diakonhjemmet Sykehus AS og Lovisenberg Diakonale Sykehus.

Innen kommunehelsetjenesten vil den enkelte kommune være ansvarlig virksomhet i forhold til de helsetjenester den selv yter – og således også databehandlingsansvarlig for behandlingen av helseopplysningene. Dersom kommunen inngår avtale eller kjøper helsetjenester av en privat virksomhet – vil den private virksomheten være databehandlingsansvarlig.

Avtaleinstituttet kommer ikke i stedet for andre sikkerhetskrav, men i tillegg, jf. Ot.prp. nr. 51 (2008–2009). Det fremgår av proposisjonen at det kun er der det er behov for

tilgang på tvers – i pasientbehandlingsøyemed - at det kan inngås avtaler om direkte tilgang. Meldingsutveksling og annen form for utlevering av helseopplysninger skal benyttes der dette anses mest formålstjenlig, i det hensyn til pasienten og til sikker informasjonsutveksling skal ivaretas på best mulig måte.

Departementet antar – som også Norsk senter for elektronisk pasientjournal uttaler i sin høringsuttalelse – at direkte tilgang på tvers av virksomheter vil være mest aktuelt for situasjoner med planlagte tjenester og der virksomheter og helsepersonell samarbeider meget tett om pasienten. Departementet er enig med KITH og NSEP at det kan synes uhensiktsmessig at avtalen skal knytte tilgangen til bestemt navngitt personell. Dette kravet er derfor tatt ut i dette forskriftsforslaget. Det bør imidlertid fremgå av avtalen hvilke formål avtalen skal dekke, jf. høringsuttalelsen fra NSEP. Kravet til formålsfastsettelse i avtalen innebærer slik departementet ser det at avtalen må inngås mellom to virksomheter. Det er ikke noe i veien for at en virksomhet inngår flere avtaler.

Som i høringsnotatet av oktober 2008 legger departementet til grunn av det ikke kan inngås avtale om nødrettstilgang. Departementet har imidlertid tatt ut denne begrensningen i forskriftsforslaget – fordi den kan skape rettslig uklarhet om hva nødrett er. Bakgrunnen for at bestemmelsen ble foreslått i forskriften av oktober 2008 er omtalen av nødrettstilgang i Norm for informasjonssikkerhet punkt 4.4.2. Det fremgår der at nødrettstilgang kan etableres som en mulighet for autoriserte brukere til å gi seg selv direkte elektronisk tilgang uten å følge fastsatte prinsipper for å få tilgang til helse- og personopplysninger.

Nødrett er regulert i straffeloven § 47 som lyder: Ingen kan straffes for Handling, som han har foretaget for at redde nogens Person eller Gods fra en paa anden Maade uavvendelig Fare, naar Omstændighederne berettigede ham til at anse denne som særdeles betydelig i Forhold til den Skade, som ved hans Handling kunde forvoldes. Denne bestemmelsen vil selvfølgelig gjelde helt uavhengig av forskriften her.

Departementet opprettholder forslaget om begrenset skrivetilgang i journaler på tvers av virksomhetsgrenser. Anmerkningen som nedskrives skal signeres ved bruk av kvalifisert sertifikat. Forutsetningen for å tillate skrivetilgang for særskilte tilfeller er at dette klart er avtalt mellom virksomhetene. Departementet mener at en slik nedskreven anmerkning som er signert ved bruk av personlig sertifikat vil oppfylle helsepersonells journalføringsplikt. Det er imidlertid ikke noe i veien for at den samme anmerkningen registreres internt i den virksomheten som nedtegner anmerkningen. Det som er viktig er at det er avtalt mellom virksomhetene hvordan dette skal gjøres, og at dette fremgår av avtalen.

Departementet har også vurdert om det bør være tillatt å kopiere data fra en virksomhet til en annen, men har kommet til at det ikke bør åpnes for å kopiere data fra en virksomhet til en annen. Er det behov for å overføre opplysninger fra en journal til en annen, bør dette skje med utgangspunkt i en forespørsel om utlevering som vurderes på vanlig måte. Dermed vil både forespørselen og den eventuelle utleveringen bli sporbar både hos utleverer og mottaker. Departementet vil imidlertid ikke utelukke at direkte kopiering kan være en mulighet i fremtiden. En annen sak er at helsepersonell som har hatt direkte elektronisk lesetilgang til annen virksomhets journal kan referere til denne kunnskap/informasjon som grunnlag for egne overveielser/vurderinger av hva slags helsehjelp pasienten skal tilbys, og deretter registrere disse i journalen.

4.8 Sperring av opplysninger

4.8.1 Høringsnotatet av oktober 2008

Forslaget i forskriften som ble sendt på høring oktober 2008 inneholdt ingen særskilte bestemmelser om sperring. Under beskrivelsen av gjeldende rett ble det imidlertid klart uttalt at pasienten har rett til å nekte utlevering av journalopplysninger (også kalt sperring av journal) mellom helsepersonell.

4.8.2 Høringsinstansenes synspunkter

Kompetansesenter for IT i helse- og sosialsektoren AS (KITH) foreslår at det tas inn et eget kapittel i forskriften om sperrede opplysninger.

4.8.3 Departementets vurderinger og forslag

En pasient har som hovedregel rett til å motsette seg at taushetsbelagte opplysninger gis til samarbeidende personell, når dette er nødvendig for å kunne gi forsvarlig helsehjelp, jf. helsepersonelloven § 25. Videre følger det av helsepersonelloven § 45 at helsepersonell som skal yte eller yter helsehjelp til pasient skal gis helseopplysninger med mindre pasienten motsetter seg det. For direkte elektronisk tilgang til helseopplysninger får reservasjonsretten kun praktisk betydning for kommunikasjon internt i virksomheten. For direkte elektronisk kommunikasjon på tvers av virksomheter kreves som hovedregel samtykke fra pasienten. Dette følger av helsepersonelloven § 45 andre punktum, som henviser til helseregisterloven § 13 tredje og fjerde ledd.

En forutsetning for at pasientens rett til å motsette seg kommunikasjon av opplysninger kan oppfylles, er at det elektroniske systemet kan sperre de aktuelle opplysningene for innsyn fra andre. Departementet foreslår derfor at det tas inn en bestemmelse i forskriften om at pasienten kan kreve at helseopplysninger som kan knyttes til vedkommende sperres. Fra pasientens ståsted vil en slik bestemmelse kunne bedre

tilliten til helsetjenesten. Fra helsepersonellets ståsted vil det være at stor betydning at det elektroniske systemet utformes slik at det støtter etterlevelse av regelverket.

Pasientens rett til å motsette seg kommunikasjon av opplysninger gjelder ikke uten unntak. Det følger av pasientrettighetsloven § 5-3 annet punktum at utlevering likevel kan skje dersom tungveiende grunner taler for det. I merknadene til pasientrettighetsloven, Ot.prp. nr. 12 (1998–1999) uttales: "I praksis vil «tungtveiende grunner» være situasjoner hvor overføring av opplysninger anses nødvendig for å hindre fare for liv eller alvorlig helseskade, for eksempel etter utskrivning fra sykehus hvor primærhelsetjenesten får etterfølgende behandlingsansvar. Det vises forøvrig til § 45 i forslag til ny helsepersonellov og merknadene til denne."

I merknadene til helsepersonelloven § 45 uttales: "Imidlertid kan det tenkes tilfeller hvor journalen bør utlånes eller overføres selv om pasienten motsetter seg dette. For eksempel i forbindelse med tvangsinnleggelser av psykiatriske pasienter, vil pasienten kunne tenkes å motsette seg utlevering av journalopplysninger. Det vil kunne være av stor betydning at behandlende personell får kjennskap til tidligere sykdomshistorie eller behandling. I slike tilfeller vil man kunne bygge på rettsstridsreservasjonen i § 23 og det vil således kunne åpnes for at journalen kan overføres eller lånes ut til tross for at pasienten har motsatt seg det dersom det er av særlig stor betydning for helsehjelpen. Dette må i så fall besluttes av det helsepersonell som har ansvaret for helsehjelpen."

Departementet mener ovenstående formuleringer om utlevering også må kunne legges til grunn ved spørsmål om elektronisk tilgang til sperrede opplysninger.

4.9 Logging og dokumentasjon av tilgang

4.9.1 Forslaget i høringsnotatet av 2008

I høringsnotatet ble det foreslått at den databehandlingsansvarlige skal sørge for at det lagres hendelsesregistre (logger) over uautoriserte forsøk på pålogging til helseopplysninger og over autoriserte pålogginger til helseopplysninger - for å avdekke uautorisert tilgang til opplysninger i behandlingsrettede helseregistre, eller forsøk på slik tilgang. I merknadene til bestemmelsen ble det uttalt at for å nå dette målet, må virksomheten ha flere logger eller hendelsesregistre.

Forslaget inneholdt også minstekrav til informasjon/dokumentasjon fra en logg i et behandlingsrettet helseregister. Det ble satt følgende minstekrav:

- navn, rolle og organisatorisk tilhørighet til den som har fått tilgang,
- hvilke opplysninger det er gitt tilgang til,
- grunnlaget for tilgangen,
- tidspunkt og varighet for tilgangen.

Videre ble det stilt krav om at logger fra et behandlingsrettet helseregister skal kunne sammenstilles med virksomhetens autorisasjonsregister med register eller liste over tilstedeværelse av personell.

Enn videre ble det stilt krav om at det jevnlig skal kontrolleres hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister. Dersom en slik kontroll utløser mistanke om at det har skjedd urettmessig tilgang, skulle virksomhetens ledelse varsles. Videre fremgikk at dersom ledelsens gjennomgang av kontrollen viser at det har skjedd en urettmessig tilegnelse av helseopplysninger, skulle Datatilsynet samt den pasienten opplysningene er knyttet til, informeres.

Forskriften fastslo at den registrerte har rett til innsyn i hendelsesregistre (logger) som gir informasjon om behandling av helseopplysninger som kan knyttes til vedkommende. Det ble presisert at den registrerte har krav på en kortfattet forklaring av tekniske uttrykk og lignende dersom vedkommende ber om det. Videre at den registrerte også har rett til å få utskrift av hendelsesregistrene. Forespørsel om innsyn og rett til utskrift av logg skulle i følge forslaget besvares uten ugrunnet opphold og senest innen 30 dager etter at henvendelsen kom inn. Videre ble det fastsatt at det ikke kan tas vederlag for dette med mindre særlige forhold tilsier det.

4.9.2 Høringsinstansenes synspunkter

Flere høringsinstanser har uttalt seg om bestemmelsene om logging.

Helse Bergen viser til at Norm for informasjonssikkerhet krever at dokumentasjon fra loggen skal oppbevares i minimum 3 måneder, og tilføyer at dette høres lite ut for "innsynsloggen". Helse Bergen mener at loggen ikke er tydelig definert som en del av journalen, og viser til at den ikke ligger i listen i forskrift om pasientjournal § 8 om hva som skal journalføres.

Kompetansesenter for IT i helse- og sosialsektoren AS (KITH) uttaler at de ikke har kommentarer til de foreslåtte bestemmelsene. KITH vil imidlertid påpeke at slike logger kan bli svært omfattende, og det vil være vanskelig for en pasient å forholde seg til utskrift av loggen som sådan. KITH viser videre til bestemmelsen i helsepersonelloven § 45 første ledd siste punktum som fastslår at det skal fremgå av journalen at annet helsepersonell er gitt tilgang til journalen. KITH foreslår derfor at det tas inn en ny bestemmelse i forskriften som setter krav til dokumentasjon i pasientjournalen ved elektronisk tilgang.

Helsedirektoratet mener at hensikten med å etablere hendelsesregistre bør fremgå klarere. Videre uttales at dette kapittelet etter direktoratets oppfatning bør beskrive

hensikten med å føre logg, og ikke detaljene for hva som skal loggføres. Direktoratet mener at detaljene bør beskrives andre steder i tilknytning til minstekrav til EPJ, og minstekrav for tilgang til virksomhetsinterne helseopplysninger på tvers av virksomheter. Direktoratet foreslår også at ordet "logg" endres til "hendelsesregister".

Folkehelseinstituttet støtter at forskriften krever at det lagres logger eller hendelsesregistre over uautoriserte og autoriserte forsøk på pålogging til helseopplysninger. Folkehelseinstituttet uttaler at logging og påfølgende sanksjoner ved påvist uautorisert tilgang, etter det instituttet kjenner til, har vist seg å være et effektivt forebyggende tiltak for å hindre uautorisert tilgang til helseopplysninger ved ulike typer helsevirksomheter.

Nasjonalt senter for telemedisin sier seg enig i at "logging og loggføring kan ses som et viktig verktøy for å sikre informasjon, og utvilsomt vil ha en sterk preventiv effekt. Senteret vil imidlertid påpeke det er et verktøy for å avdekke brudd på taushetsplikten som allerede er begått. Logging i seg selv hindrer ikke taushetsbrudd eller uautorisert tilgang, og er derfor et verktøy med begrenset verdi: Når opplysninger først er på avveier, er skaden skjedd. Senteret mener derfor at logging er et virkemiddel som må ses i sammenheng med andre virkemidler.

Ullevål universitetssykehus påpeker at gjennomgang av hva som er ikke akseptable oppslag, er svært ressurskrevende og er kun gjennomførbart med stikkprøver. Sykehuset viser til at det er flere initiativ for å forsøke å systematisere og målrette logg-gjennomganger, slik at den manuelle gjennomgangen kun blir på et håndterbart antall logger. Sykehuset mener at dette gjør at effekten av loggjennomgang foreløpig er svært begrenset.

Legeforeningen uttaler at en ordning med direkte tilgang til EPJ, både internt og på tvers av virksomhetene nødvendiggjør gode kontroll- og tilsynsordninger. Siden systemet åpner for autorisasjon på bakgrunn av roller, og ikke i alle tilfeller konkret nødvendighet, er det etter legeforeningens mening særlig viktig at man har systemer som raskt og effektivt avdekker ulovlige oppslag i EPJ. Foreningen viser til at det i forskriften stilles krav om "jevnlig kontroll". Foreningen ber departementet om å vurdere en strammere regulering, eventuelt utvide merknaden til bestemmelsen.

Datatilsynet uttaler at de støtter en tydeliggjøring av pasientens rett til å få tilgang til logg, og at prinsippet er viktig. Datatilsynet tilføyer at den direkte nytte den enkelte pasient vil ha av å få tilgang til egen logg i mange tilfeller kan diskuteres og at dette særlig gjelder hvis man ikke skjerper kravet til autentisering i pasientjournalen.

4.9.3 Departementets vurderinger og forslag

På bakgrunn av høringsuttalelser har departementet vurdert ordlyden på og strukturering av bestemmelsene om logging og dokumentasjon av tilgang til

helseopplysninger på nytt. Det vises også til den nye bestemmelsen i helseregisterloven § 13 sjette ledd som fastslår at den registrerte har rett til innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne. Videre vises til helsepersonelloven § 45 som i først ledd siste setning fastslår at det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger. Departementet foreslår at det inntas en bestemmelse – krav om dokumentasjon i behandlingsrettet helseregister av tilgang til helseopplysninger – for regelverksmessig å legge til rette for at pasientens innsynsrett i logg, jf. helseregisterloven § 13 sjette ledd kan oppfylles. Departementet foreslår også at det i forskriften tas inn en egen bestemmelse som utdyper pasientenes innsynrett.

God informasjonssikkerhet krever et sett av tiltak – både organisatoriske og tekniske. Logging eller registrering av autorisert bruk og forsøk på uautorisert bruk er et teknisk kontrolltiltak for å fange opp ulovlig bruk av systemet. Som Nasjonalt senter for telemedisin påpeker, er logging et verktøy for å avdekke brudd på taushetsplikten eller andre ulovlige handlinger som allerede er begått. Selv om logging ikke kan hindre urettmessig tilgang til helseopplysninger, mener departementet det er grunn til å tro at rutiner for loggføring – og jevnlig kontroll av logger – i stor grad kan bidra til høyning av informasjonssikkerheten og forebygging av lovbrudd.

Departementet erkjenner at det vil ta ulik tid å implementere funksjonalitet for hendelsesregistrering i det mangfold av systemer som finnes. Behovet for loggfunksjonalitet vil også variere etter virksomhetens størrelse og kompleksitet. Kravene om hendelsesregistrering i dette forslaget til forskrift tydeliggjør for leverandørene hva et EPJ – system skal inneholde og dermed hva helsevirksomheter er forpliktet til å etterspørre.

Departementet foreslår at "hendelsesregistreringen" skal lagres i to år. I denne vurderingen har departementet blant annet sett hen til at fristen for foreldelse for straffbare handlinger er 2 år når den høyeste lovbestemte straff er bøter eller fengsel inntil 1 år, jf. straffeloven § 67. (Herværende forslag til forskrift fastslår at den som forsettlig eller grovt uaktsomt unnlater å følge reglene i denne forskriften straffes med bøter eller fengsel inntil ett år eller begge deler. Dette er i samsvar med forslaget i høringsnotatet av oktober 2008. Ingen høringsinstanser hadde merknader til bestemmelsen.)

Forslaget om hendelsesregistrering og dokumentasjon er utformet noe annerledes enn i høringsnotatet av oktober 2008 – for å gjøre reglene mer tilgjengelige.

For blant annet å kunne sikre at ulike virksomheter innen helsetjenesten kan oppfylle sine informasjons- og innsynsplikter ovenfor pasienten på en noenlunde ensartet måte,

foreslår departementet at det tas inn en egen bestemmelse i forskriften om krav til dokumentasjon i behandlingsrettet helseregister, herunder elektronisk pasientjournal, av tilgang til opplysninger. Bestemmelsene i forskriften presiserer og utfyller blant annet helsepersonelloven § 45 første ledd tredje punktum, jf. tredje ledd.

5 Administrative og økonomiske konsekvenser

Forskriften skal bidra til å gi helsepersonell nødvendig elektronisk tilgang til helseopplysninger slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte uten å krenke personvernet. Et godt personvern er ikke bare begrenset til spørsmål om den enkeltes rett til å bestemme hvem som kan få tilgang til opplysningene, men innebærer også krav til hvordan helseopplysninger skal behandles, innsynsrett og sikring av opplysninger. Det er helt nødvendig for å yte god helsehjelp at det er et godt tillitsforhold mellom pasienten og helsepersonellet. Pasienten skal være trygg på at helseopplysninger skjermes for innsyn for helsepersonell som ikke trenger opplysninger om pasienten for å yte god og forsvarlig helsehjelp.

Helsedirektorat har som et ledd i arbeidet for å ivareta personvernet og den enkelte pasients rett til konfidensialitet utarbeidet Norm for informasjonssikkerhet for helsesektoren i samarbeid med representanter for sektoren. Hensikten er å bidra til tilfredsstillende informasjonssikkerhet hos den enkelte virksomhet og i sektoren generelt, samt å bidra til å etablere mekanismer hvor virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Norm for informasjonssikkerhet i helsesektoren detaljerer og supplerer øvrig regelverk. Normen er et veiledende dokument - en bransjenorm – i hva som anbefales for å oppnå tilfredsstillende informasjonssikkerhet. Det presiseres i normen at ved eventuell motstrid mellom normen og de til enhver tid gjeldende lover eller forskrifter, vil lov og forskrift gå foran normen. Alle virksomheter som inngår partneravtale med Norsk helsenett SF må i avtalen forplikte seg til å etterleve kravene i normen. De siste endringene i helseregisterloven og denne forskriften medfører at normen må oppdateres slik at det blir bedre samsvar mellom norm og regelverk.

Det er i St. meld. nr. 47 (2008—2009) Samhandlingsreformen omtalt flere innsatsområder og tiltak på e- Helseområdet. Stortingsmeldingen legger føringer for at dokumentasjon og informasjonsutveksling i all hovedsak skal foregå elektronisk. Elektronisk kommunikasjon skal i tillegg til muntlig kommunikasjon, være den normale måten å kommunisere på for helsepersonell med annet helsepersonell og med pasienter/brukere. Elektronisk samhandling mellom helsesektorens aktører foregår i dag over helsenettet som er et sikkert dedikert høyhastighetsnettverk for helsesektoren og de aktører som er tilknyttet.

Helsevirksomheter som knytter seg til helsenettet må som nevnt inngå en avtale med Norsk Helsenett SF hvor de forplikter seg til å følge normen. Det fremgår av avtalene at brudd på normen kan medføre utestenging fra helsenettet for å ivareta sikkerhet eller tilgjengelighet i nettet.

I dag er 100 % av helseforetakene tilknyttet helsenettet. Ca.46 % av kommunene, om lag 90 % av fastlegene og 80 % av fastlegekontorene er knyttet til helsenettet. I tillegg finnes det noen flere grupper av helsepersonell som har avtaler med eller utfører oppdrag/behandling for det offentlige. For disse gruppene er den prosentvise andelen av tilkoblede enheter betydelig lavere enn for fastlegene.

De organisatoriske og administrative kravene i foreliggende forslag vil i all hovedsak tydeliggjøre kravene i gjeldende regelverk. Personopplysningsforskriften vil gjelde som utfyllende bestemmelser til den nye forskriften. Forskrift som her sendes på høring er imidlertid noe mer detaljert og bedre tilpasset helsesektorens virkelighet enn personopplysningsforskriften.

Forskriften medfører at en del bestemmelser i normen nå blir bindende gjennom forskrift, og ikke bare avtalerettslig. Departementet må derfor kunne legge til grunn at en rekke aktører allerede har implementert mange av de nye kravene i forskriften.

Departementet er imidlertid usikker på om alle virksomheter som er tilknyttet Norsk Helsenett SF har implementert beslutningsstyrt tilgang til helseopplysninger. Det vises til normen punkt 5.2. 3. der det fremgår at tilgang skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten. Departementet ber at om høringsinstansene som denne forskriften vil gjelde for, i sitt høringssvar gir tilbakemelding på om de har implementert beslutningsstyrt tilgang i sin virksomhet, eventuelt på hvilke tidspunkt dette kan forventes implementert.

Forskriften har både krav for informasjonssikkerhet internt i en virksomhet og bestemmelser om tilgang til helseopplysninger i behandlingsrettede helseregistre på tvers av virksomhetsgrenser. Det er viktig å merke seg at forskriften ikke stiller krav om at helsevirksomheter skal kunne åpne for eller inngå avtale med annen virksomhet om direkte elektronisk tilgang på tvers av virksomheten. Forskriftens krav må imidlertid være oppfylt at virksomheten skal kunne inngå en slik avtale.

Departementet antar at forskriften innebærer at tilpasninger må gjøres i mange elektroniske pasientjournalsystemer for å imøtekomme kravene til sikkerhet. Noen endringer må trolig også gjøres av de virksomheter som i dag ved avtale har forpliktet seg til å følge norm for informasjonssikkerhet, jf. departementets spørsmål i avsnittet ovenfor. Særlig i elektroniske pasientjournalsystemer av eldre dato kan det være vanskelig å oppnå de krav til sikkerhet som settes i ny forskrift. For de eldre systemene må det gjøres en avveining for hvert system mellom nytte og kostnad ved å beholde systemet, kontra å foreta en nyanskaffelse.

Leverandørene vil trenge tid på å gjøre de nødvendige tilpasninger i EPJ -systemene slik at systemene følger krav i regelverket. Leverandørene vil i første hånd bære mye av utviklingskostnadene. Virksomhetene trenger på sin side tid til å implementere nye

krav gjennom tilpasninger i EPJ -systemene eller foreta nødvendig nykjøp. Kostnadene er vanskelig å beregne fordi variasjonene i de EPJ -systemer som brukes er store og fordi kravene i forskriften er kombinasjon av helt nye krav, tydeliggjøring av allerede eksisterende krav i regelverket og krav som noen av aktørene ved avtale med helsenettet har forpliktet seg til å følge. Kostnadene kan, fordi nyutvikling må til, fordeles over en viss tid.

Departementet mener at investering i e –Helse, herunder utvikling av elektroniske pasientjournalsystemer, må oppfattes som et virkemiddel og en naturlig del av privat og offentlig tjenesteyting av helsehjelp.

Departementet foreslår at kravene i forskriften kan settes i kraft på forskjellig tidspunkt. Departementet antar at kravene i forskriften kapittel I, II, III og V allerede kan settes i verk fra 1. juli 2011. Departementet ber om høringsinstansenes vurdering av om og eventuelt når egen virksomhet antas å kunne ha implementert de ulike kravene i forskriften. Departementet forutsetter at kravene gjennomføres innenfor de gitte budsjettrammer i helsevirksomhetene.

6 Merknader til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Kapittel 1 Innledende bestemmelser

Merknader til § 1
Forskriftens formål er todelt.
Første punktum fastslår at formålet med forskriften er å gi helsepersonell nødvendig tilgang til helseopplysninger slik av helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas, jf. helseregisterloven § 1 første punktum.

Begrepet helsepersonell er nærmere definert i helsepersonelloven § 3. Helsepersonell er personer med autorisasjon etter helsepersonelloven § 48 eller lisens etter helsepersonelloven § 49. Personell i helsetjenesten eller i apotek som ikke er autorisert, eller har lisens, regnes som helsepersonell dersom de utfører handlinger som kommer inn under begrepet helsehjelp. Det samme gjelder elever og studenter som i forbindelse med helsefaglig opplæring utfører helsehjelp.

Begrepet helseopplysninger sikter til opplysninger som nevnt i helseregisterloven § 2 nr. 1. I følge denne definisjonen er helseopplysninger 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, dvs. taushetsbelagte opplysninger i henhold til helsepersonelloven, omfattes av gruppen helseopplysninger.

Andre punktum fastslår at formålet med forskriften er å bidra til god informasjonssikkerhet. God informasjonssikkerhet krever ivaretakelse av opplysningenes konfidensialitet, kvalitet, integritet og tilgjengelighet, jf. helseregisterloven § 16, samt sporbarhet. Det vises til punkt 4.1.3. Ivaretakelse av disse elementene vil sette krav til konfigurasjon (utstyr og program samt sammenkoblinger mellom disse) og organiserte rutiner for behandling av helseopplysninger. Ved fastsettelse av handlingsregler og rutiner må virksomhetens sikkerhetsmål og –strategi og resultatet av risikovurderinger legges til grunn.

Begrepet konfidensialitet sikter til at informasjon skal sikres mot å bli gjort tilgjengelig for uvedkommende, blant annet at reglene om taushetsplikt i helsepersonelloven skal overholdes. For vide tilgangsrettigheter og for omfattende autorisasjoner kan forårsake tap av konfidensialitet.

Begrepet integritet innebærer at den registrerte informasjonen skal sikres mot å bli endret, ødelagt eller gå tapt. To faktorautentisering (system der to forskjellige metoder blir brukt i autentiseringsprosessen) og kvalifisert sertifikat vil høyne integriteten.

Tilgjengelighet innebærer at de registrerte opplysningene skal være tilgjengelige når helsepersonell har behov for det for å kunne vurdere/gi helsehjelp. Uhensiktsmessig konfigurasjon, mangelfulle tilgangsrettigheter, tilfeldige feiloperasjoner og ulike former for teknisk svikt kan være årsak til tap av tilgjengelighet.

Begrepet kvalitet sikter til at opplysningene skal være korrekte og oppdaterte.

Både kravet til tilgjengelighet og kravet til kvalitet forutsetter at helseopplysningene registreres og struktureres på en slik måte at det er lett å finne frem til relevant informasjon.

Merknader til § 2
Bestemmelsen fastslår at forskriften gir regler om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre som skjer med hjemmel i helseregisterloven § 6 og helsepersonelloven § 46. Begrepet behandlingsrettet helseregistre sikter til alle registre som inneholder personidentifiserbar informasjon om pasienter og som benyttes for å yte helsehjelp eller administrere slik hjelp. Elektroniske pasientjournalsystemer (EPJ-systemer), pasientadministrative systemer (PAS), røntgeninformasjonssystemer (RIS) medisinske bildearkivsystemer (PACS), laboratoriedatasystemer, små avdelingsvise kliniske systemer og en rekke andre typer spesialsystemer benyttes ved behandling av helseopplysninger i slike registre.

Merknader til § 3
Bestemmelsen definerer fem ord eller uttrykk som brukes i forskriften. Det er autentisering, autorisasjon, tilgang til helseopplysninger, direkte tilgang til helseopplysninger og sperrede opplysninger.

Med begrepet autentisering menes den prosess som må gjennomføres for å bekrefte en påstått identitet. Et krav til autentisering kan ha ulike sikkerhetsnivå. To-faktor autentisering er et system der to forskjellige metoder blir brukt i autentiseringsprosessen. Å bruke to eller flere faktorer (multi-faktor) i en autentiseringsprosess gir et høyere nivå av sikkerhet. Krav til autentiseringsstyrke for tilgang til helseopplysninger innen egen virksomhet er inntatt i forskriften kapittel IV, og krav til autentisering for tilgang til helseopplysninger i annen virksomhet/ekstern virksomhet er inntatt i kapittel V.

Begrepet autorisasjon defineres som en person som i en bestemt rolle gis bestemte rettigheter til lesing, registrering, redigering, retting, sletting, sperring eller annen behandling av helseopplysninger. I høringsnotatet var det tilføyet en setning om at autorisasjon bare kan gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra tjenestelige behov og er i henhold til bestemmelser om taushetsplikt. Denne setningen – som formulerer et krav til autorisasjonen – er flyttet til kapittel III.

Direkte tilgang til helseopplysninger betyr at helsepersonell fra et behandlingsrettet helseregistersystem kan logge seg rett på et annet behandlingsrettet helseregistersystem. Uttrykket omfatter både situasjoner der pålogging skjer fra et helseregistersystem til et annet internt i en virksomhet, og der pålogging skjer mellom virksomheter.

Kapittel 4 Generelle krav til informasjonssikkerhet

Merknader til § 4
Bestemmelsen fastslår at virksomheter som tar i bruk behandlingsrettede helseregistre skal sørge for at systemet som tas i bruk sikrer forsvarlig informasjonssikkerhet. Kravet til forsvarlighet innebærer at helseopplysninger som registreres gis nødvendig vern (krav til konfidensialitet), integritet, kvalitet, tilgjengelighet og sporbarhet, jf. formålet med forskriften. Kravet til forsvarlig system innebærer blant annet at systemet må kunne "sperre" helseopplysninger fra innsyn fra annet helsepersonell, i den grad pasienten motsetter seg at det gis tilgang til dem. Kravet til forsvarlig system innbærer også at man må sikre at helsepersonell kan få tilgang til nødvendige opplysninger dersom "nettet er nede", under driftstans, oppgraderinger av nettet etc. Kravet om forsvarlighet kan ivaretas ved gode beredskapsrutiner som enten sikrer manuell håndtering av pasientopplysninger eller tilgang til opplysninger i en teknisk offline løsning. Kravet til forsvarlighet innebærer også at pasientens innsynsrett i logg, jf. forskriften § 34, etterleves.

Merknader til § 5
Første ledd
Første ledd innebærer at alle virksomheter, som tar i bruk et behandlingsrettet helseregister, skal ha en overordnet strategi og målsetting for informasjonssikkerheten i virksomheten. Bestemmelsen stiller krav om at det skal foreligge styrende dokumenter for behandling av helseopplysninger for alle nivåer i virksomheten. Risikovurderinger og de dokumenter som utarbeides, jf. forskriften § 6 vil utgjøre viktige premisser for utarbeidelse av de skriftlige dokumentene som kreves etter denne bestemmelse.

Innenfor den statlige spesialisthelsetjenesten sikter virksomhet til det helseforetaket som er databehandlingsansvarlig for behandlingen av opplysningene. De ulike helseforetakene er ikke en homogen gruppe, og kan ha ulik intern organisering. Et helseforetak kan være meget stort, og omfatte flere "undervirksomheter". For eksempel består Oslo Universitetssykehus HF av Oslo universitetssykehus Aker, Ullevål universitetssykehus og Oslo Universitetssykehus Rikshospitalet. Oslo universitetssykehus Aker er i seg selv en stor virksomhet og er lokalisert på 16 ulike steder i Oslo og Akershus. Oslo Universitetssykehus Rikshospitalet består av Rikshospitalet, Radiumhospitalet og Epilepsisenteret. Sunnås sykehus HF er eksempel på et mindre helseforetak.

Innen den kommunale helsetjenesten vil virksomhetene som oftest være mye mindre. En allmennlege, tannlege, fysioterapeut eller annen privat helsetjeneste i kommunen vil for eksempel være virksomhet i forhold til denne bestemmelsen. Det samme vil enkelte private legespesialister som driver egen virksomhet.

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

Departementet vil i den forbindelse vise til helseregisterloven § 6 andre ledd andre punktum som fastslår at helseforetaket og kommunen kan delegere databehandlingsansvaret. Departementet legger til grunn at databehandlingsansvaret delegeres til det nivået som har de beste forutsetninger for å utføre den databehandlingsansvarliges oppgaver (rettigheter og plikter) mest effektivt. Det presiseres at det er utøvelsen av oppgaver som delegeres. En delegering vil ikke frita den databehandlingsansvarlige fra noe ansvar. Det rettslige ansvaret vil fortsatt ligge hos den databehandlingsansvarlige.

Andre ledd

Andre ledd fastslår at alle nivåer i virksomheten skal ha skriftlige rutiner for behandling av helseopplysninger, og at rutinene skal ha utgangspunkt i den overordnede planen, jf. første ledd. Dersom et helseforetak eller en virksomhet er delt inn i flere undervirksomheter, divisjoner, avdelinger etc., skal hver enhet ha skrevne rutiner, med planen for overordnet nivå som overbygning. De konkrete rutinene må forholde seg til den eller de organisatoriske deler av virksomheten de er skrevet for. Dette er ikke til hinder for at for eksempel to poster har samme plan/rutiner. I hvilken grad risikovurderinger, planer og rutiner gjelder for hele virksomheten eller deler av virksomheten, vil blant annet være avhengig av virksomhetens art og karakter. Det som kreves er at planen er så konkret at den gir hvert enkelt helsepersonell - på hvert nivå og i hver organisatorisk del i helsetjenesten - tilstrekkelig veiledning slik at

vedkommende har kunnskap om hvordan han eller hun kan/skal behandle helseopplysninger i utføringen av egne arbeidsoppgaver. Det må gå klart frem av planen hvor vedkommende kan henvende seg dersom vedkommende synes noe er uklart/etterspør kunnskap om muligheter og begrensinger, eller mener det bør gjøres endringer i autorisasjonen etc.

I enkeltmannsbedrifter, små lege- og tannlegevirksomheter, fysioterapivirksomheter eller lignende - som består av bare en enhet/et nivå – kan det trolig være tilstrekkelig å forholde seg til et dokument hvor overordnet sikkerhetsstrategi, målsetting og rutiner fremgår samlet. Dette vil imidlertid ikke være tilstrekklig for større virksomheter og helseforetak.

De skrevne rutinene skal være levende dokumenter som raskt kan tilpasses ved endringer i risikovurderingen, personellsituasjonen eller lignende.

Tredje ledd
Tredje ledd fastslår at det klart skal fremgå av planverket hvem som er ansvarlig for de ulike deler av informasjonssikkerheten. Angivelsen kan knyttes til en bestemt(e) rolle(r) eller en bestemt stilling eller stillinger. I et stort helseforetak kan det være mange som får tildelt et slikt ansvar, mens i mindre virksomheter vil dette ansvaret kunne innehas av en eller noen få personer/stillinger. I alle tilfeller må det være slik at alle ansatte og ev. andre som arbeider i virksomheten må være kjent med hvem som til enhver tid har ansvarsrollen, hvor og til hvem de kan henvende seg, for eksempel hvis det er behov for å gjøre endringer i autorisasjonen.

Tilgangsstyringen skal bygge på konkrete risikovurderinger. De dokumenter som utarbeides på basis av risikovurderinger vil legge premisser for det videre arbeidet med tilgangsstyringen, og de rutiner som for øvrig etableres for å sikre god informasjonssikkerhet.

Merknader til § 6
Bestemmelsen fastslår at den databehandlingsansvarlige skal etablere internkontroll etter helseregisterloven § 17. Bestemmelsen tilsvarer personopplysningsforskriften § 3-1. Kravene til rutiner for oppfyllelse av den databehandlingsansvarliges plikter og de registrertes rettigheter i tredje ledd er tilpasset kravene i forskriften her, og er derfor utformet noe annerledes enn i personopplysningsforskriften § 3-1 tredje ledd.

Merknader til § 7
Den databehandlingsansvarlige for behandlingen av helseopplysninger vil alltid være et eget rettssubjekt og ofte vil dette være en juridisk person. For behandling av helseopplysninger innen et helseforetak vil helseforetaket være databehandlingsansvarlig, jf. helseregisterloven § 6. Det vises til merknader til

forskriften § 5 om delegasjon av databehandlingsansvaret. Det må presiseres at en delegering av databehandlingsansvaret ikke vil frata den som delegerer noe rettslig ansvar. Det er bare ansvaret for å utføre oppgavene som tilligger den ansvarlige som delegeres.

Bestemmelsen her utfyller dette og fastslår at informasjonssikkerhet i virksomheten er et ledelsesansvar. Utfyllende bestemmelser om sikkerhetsledelse følger av personopplysningsforskriften § 2-3.

Det kan for øvrig vises til helseregisterloven § 21 nr. 2 som fastslår at enhver som ber om det kan kreve å få informasjon om hvem som har det daglige ansvaret for å oppfylle den databehandlingsansvarliges plikter.

Merknader til § 8
Hovedfokus i denne forskriften er den delen av informasjonssikkerheten som gjelder tilgangsstyring, tilgang til helseopplysninger og vern av den enkelte pasients personvern og vern mot spredning av helseopplysninger, men innholder også viktige generelle bestemmelser om informasjonssikkerhet.

For å sikre god informasjonssikkerheten generelt, gjelder bestemmelsene om informasjonssikkerhet og internkontroll i personopplysningsforskriften utfyllende til denne forskriften.

Kapittel 3 Krav om system for utstedelse av autorisasjoner og krav til autentisering

Bestemmelsene i dette kapittelet pålegger plikter og rettigheter til den databehandlingsansvarlige og den/de som utsteder autorisasjoner samt knytter disse til bestemte identiteter ved autentisering.

Merknader til § 9
Første ledd pålegger den databehandlingsansvarlige for virksomheten å etablere nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av autorisasjoner (tilgangsrettigheter). Bestemmelsen gjelder behandling av helseopplysninger innen forskriftens virkeområde, jf. forskriften § 2.

Det følger av bestemmelsen at tildeling av autorisasjon består av to ledd, en administrativ/organisatorisk del og en teknisk del. Det administrative arbeidet består i å bestemme innholdet i autorisasjonen, det vil si hvilke rettigheter og plikter et bestemt helsepersonell skal ha i forhold til behandling av helseopplysninger. Innholdet i autorisasjonen må ta utgangspunkt i hvilken rolle vedkommende skal ha i virksomheten. En bestemt tjenesteyter kan ha ulike roller i virksomheten. En beslutning om innholdet i en autorisasjon, som skal knyttes til den enkelte rolle

tjenesteyteren har, er en helsefaglig oppgave, og må besluttes av en som er tildelt dette som oppgave og er autorisert for oppgaven. Beslutningen må tas ut ifra vedkommende tjenesteyters ansvar og oppgaver i virksomheten og de risikovurderinger som er foretatt, jf. andre ledd. Helsepersonell som gis myndighet til å treffe beslutning om innholdet i en autorisasjon, må ha helsefaglig kompetanse, god kjennskap til virksomhetens organisering og ulike roller, samt gis nødvendig opplæring.

Den tekniske delen av autorisasjonen består i å gjennomføre dette teknisk i systemet.

Andre punktum fastslår at autorisasjonen skal bidra til å sikre at informasjonssikkerheten, herunder bestemmelsene om taushetsplikt og pasientens rett til konfidensialitet, blir ivaretatt. Det følger av dette at et overordnet formål med tilgangsstyringen er at den skal hindre urettmessig tilegnelse av helseopplysninger. Samtidig skal systemet være slik at helsepersonell har tilgang til nødvendige helseopplysninger når det er nødvendig for ytelse av forsvarlig helsehjelp.

Andre ledd
Andre ledd fastslår at tilgangsstyringen skal bygge på konkrete vurderinger av om det kan skje urettmessig tilegnelse av helseopplysninger. Bestemmelsen må ses i sammenheng med forskriften § 5 som fastslår at det skal utarbeides styrende dokumenter og rutiner for behandling av helseopplysninger for alle nivåer i virksomheten. Kravet om konkrete risikovurderinger innebærer at det skal gjennomføres risikovurderinger for eller på alle nivåer i virksomheten. Bestemmelsen innebærer blant annet at den som treffer beslutning om innholdet i autorisasjonen må ta risikovurderingene i betraktning ved utstedelse av autorisasjon.

Merknader til § 10
Første ledd
Bestemmelsen fastslår grunnkrav til virksomhetenes tilgangsstyring. Det følger av bestemmelsen at den databehandlingsansvarlige skal sørge for at virksomhetens tilgangsstyring sikrer og begrenser tilgangen til helseopplysninger til hva som er nødvendig og tilstrekkelig for formålet med tilgangen. Tilgangen skal vurderes og konfigureres med hensyn til:

a) antall registrerte det gis tilgang til
b) mengde informasjon om den enkelte det gis tilgang til og
c) varighet av tilgangen.

Bestemmelsen setter ikke noen maksimumskrav til antall registrerte et bestemt helsepersonell kan gis tilgang til, eller mengde informasjon han eller hun kan gis tilgang til i et konkret tilfelle. Bestemmelsen krever imidlertid at den databehandlingsansvarlige har et meget gjennomtenkt og bevisst forhold til dette ved

utstedelse av autorisasjoner, og at innholdet i autorisasjonen vurderes ut ifra vedkommendes helsepersonells stilling og rolle i virksomheten. Den databehandlingsansvarlige må selv tallfeste eller konkretisere hvilke parametre tilgangen skal vurderes og konfigureres med utgangspunkt i.

Andre ledd
Første punktum fastslår at enhver autorisasjon skal være tidsbegrenset og bare omfatte slik behandling av helseopplysninger som er nødvendig og relevant for å nå det angitte formålet med tilgangen, som må ligge innenfor forskriftens formål. Autorisasjonen skal følge rollen og ikke personen. Å være lege vil for eksempel ikke være tilstrekkelig for å bli autorisert for en bestemt type tilgang til helseopplysninger. Vedkommende helsepersonell må først bli tilsatt i en rolle/få en rolle. Det er først når vedkommende helsepersonell, for eksempel "overlege ved medisinsk avdeling A", får denne rollen, at vedkommende får de autorisasjoner som følger rollen. Opptrer overlegen i en annen rolle, for eksempel forsker, vil han eller hun ikke kunne bruke den samme tilgangsrettigheten/autorisasjon som vedkommende har i helsehjelpsøyemed.

Andre punktum krever at det enkelte helsepersonells tjenstlige behov for tilgang til helseopplysninger jevnlig skal vurderes og oppdateres. Jevnlig er et skjønnsmessig uttrykk, og må ta utgangspunktet i organisasjonens art og oppbygging. 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.

Tredje ledd
Tredje ledd krever at beslutningsgrunnlaget for virksomhetens tilgangsstyring og konfigurering dokumenteres, og at denne dokumentasjonen inngår i virksomhetens internkontrollsystem.

Merknader til § 11
Bestemmelsen krever at helsepersonellets oppgaver i virksomheten og reglene om taushetsplikt er utgangspunktet for hva personellet autoriseres til.

Bestemmelsen fastslår at autorisasjon bare kan gis i den grad det er nødvendig for tjenesteyters arbeid, er begrunnet ut fra tjenstlig behov og er i henhold til bestemmelser om taushetsplikt. Dette innebærer at den som utsteder autorisasjonen må ha oversikt over vedkommende helsepersonells arbeidsavtale, oppgaver og ansvarsportefølje ved utstedelse av autorisasjonen.

Uttrykket "tilfredsstiller bestemmelser om taushetsplikt" angir de ytre rammer for tildeling av autorisasjoner. Informasjonssystemet og hvordan dette i praksis kan/vil fungere vil legge premisser for tilgangsstyringen. Etterlevelse av bestemmelsene om taushetsplikt forutsetter at de elektroniske systemene som benyttes, i større eller

mindre grad kan skreddersy ulike tilgangsbehov. Det innebærer at systemene må kunne gi en differensiert mulighet for tilgangsstyring slik at en ved korrekt bruk av systemet kan hindre at noen får tilgang til andre opplysninger enn de som de etter gjeldende regelverk skal ha tilgang til. Det enkelte systemets funksjoner - muligheter og begrensninger – må utnyttes meget bevisst i den praktiske tilgangsstyring.

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 som utgangspunkt gis en meget begrenset tilgang (autorisasjon), i tillegg til at virksomheten organiseres slik at det er tilrettelagt for meget 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 databehandlingsansvarliges ansvar å avpasse de tekniske og organisatoriske tiltakene til hverandre, slik at kravene til informasjonssikkerheten i virksomheten etterleves.

Merknader til § 12
Bestemmelsen pålegger den databehandlingsansvarlige å sørge for nødvendig opplæring og informasjon. Det følger av forskriften § 10 at den enkelte tjenesteyters behov for tilgang til helseopplysninger i tjenesten skal vurderes og om nødvendig oppdateres, jevnlig. Videre følger det av forskriften § 11 at ingen kan autoriseres for tilgang til helseopplysninger i videre omfang enn det som følger av reglene om taushetsplikt. På tross av dette vil det likevel være en noe videre teknisk mulighet for tilgang til elektronisk lagrede helseopplysninger enn hva en streng overholdelse av taushetsplikten skulle tilsi. Begrunnelsen for dette er at kravet til informasjonssikkerhet også setter krav til opplysningens tilgjengelighet. Videre er det slik at helsepersonell ikke på forhånd helt eksakt kan avgrense hvilke opplysninger som er nødvendige for å kunne vurdere helsehjelpen. 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. Det er først og fremst i pasientens interesse at nødvendige og tilstrekkelige helseopplysninger er til stede for helsepersonell – som grunnlag for helsefaglige vurderinger – i samspillet mellom helsepersonell og pasient. Det er ikke til å unngå at helsepersonell i enkelte tilfeller får kunnskap om helseopplysninger de strengt tatt ikke har behov for. I tillegg til at journalsystemet har tekniske sperrer for tilgang til helseopplysninger må helsepersonell derfor også ha kunnskap, og en adferd, som gjør at opplysningenes konfidensialitet og pasientens integritet ivaretas. Det vises videre til forskriften § 18 som fastslår at ingen kan gjøre bruk av en tildelt autorisasjon i videre omfang enn det som følger av reglene om taushetsplikt. Den

databehandlingsansvarlige må sørge for at helsepersonell er seg bevisst innholdet i denne bestemmelsen og hva den i praksis innebærer.

I denne sammenheng er det også viktig at helsepersonell gis kunnskap om at pasienten har rett til å reservere seg mot at opplysninger deles, og at systemet er lagt til rette for at helsepersonell effektivt kan bidra til at en ev. reservasjon fra pasienten kan etterleves gjennom mulighet for sperring av de aktuelle opplysningene. Det vises til forskriften §§ 29 og 30.

Merknader til § 13
Bestemmelsen krever at alle som skal gis autorisasjon entydig skal identifiseres som en bestemt tjenesteyter i en bestemt rolle. Bestemmelsen pålegger virksomheten en plikt til å utstede et "identifikasjonsdokument" til helsepersonell på basis av to forhold: 1) Identitet – tjenesteyter og 2) Identitet – tjenesteyters rolle. Kravet til autentisering for tilgang til helseopplysninger internt i virksomheten følger av forskriften § 18 og for tilgang til helseopplysninger i ekstern virksomhet av forskriften § 25.

Bestemmelsen forutsetter at et bestemt helsepersonell kan ha ulike roller i en virksomhet - i ulike tidsrom og ut fra ulike oppgaver vedkommende blir satt til. 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 tjenesteyters rolle som er bestemmende for innholdet/omfanget av autorisasjonen, og ikke hvem personen er eller hvilke faggruppe han eller hun tilhører. Det vises for øvrig til merknadene til forskriften § 10.

Merknader til § 14
Bestemmelsen regulerer hvem som kan autoriseres og innholdet i en autorisasjon når formålet er å yte forsvarlig helsehjelp til pasienten.

Første ledd
Første ledd første punktum fastslår at autorisasjon kan gis til helsepersonell som har behov for det for å kunne yte forsvarlig helsehjelp til pasient. Vilkårene for tilgang til helseopplysninger i pasientbehandlingsøyemed/for å tilby helsehjelp til pasient følger av helsepersonelloven §§ 25 og 45. Bestemmelsen innebærer at 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. Begrepet autorisasjon er nærmere definert i forskriften § 3 nr. 2.

Det følger av andre punktum at autorisasjonen skal gis det innhold som er nødvendig for at helsepersonell skal kunne ivareta sine oppgaver og sitt ansvar ovenfor pasienten på en forsvarlig måte. Det innebærer at en autorisasjon - i tillegg til å kunne differensiere hvilke opplysninger det gis tilgang til, også må kunne differensieres i

forhold til oppgaver som skal utføres: skal man bare kunne lese opplysningene, eller skal man også kunne skrive, kopiere, rette eller slette etc. En konkret autorisasjon må derfor kunne omfatte en eller flere av de elementer en autorisasjon kan bestå i.

Bestemmelsen forutsetter eller krever at en pasients journal kan struktureres slik at det er mulig å autorisere for særskilte deler av journalen. For eksempel må en journal kunne deles slik at den gjør et skille mellom opplysninger om somatisk helsehjelp og opplysninger fremkommet når psykisk/psykiatrisk helsehjelp er gitt. Dette kan gjøres ved å strukturere journalen etter sted/avdeling og emne. Inndeling på en slik måte – etter avdeling eller tema - gjør det mulig å gi tilgang til bare somatiske helseopplysninger eller bare opplysninger om den registrertes psykiske helse. En finere inndeling enn nevnt må også være mulig. Det må også kunne være mulig å avgrense særskilte opplysninger eller notater fra innsyn, for eksempel slik at autorisasjon til å behandle helseopplysninger registrert på bakgrunn av gynekologisk helsehjelp ikke uten videre også innebærer at ansatt på ortopedisk kirurgisk avdeling har tilgang til opplysningene. I særskilte tilfeller kan det imidlertid være nødvendig å gi tilgang til opplysninger innenfor begge fagområdene. Det kan være hensiktsmessig å gjøre en tilsvarende inndeling også for andre og mer spesifikke fagområder.

Andre ledd

Andre ledd gjelder virksomhet som ønsker å samarbeide med annen virksomhet slik at helsepersonell i virksomheten kan gis direkte tilgang til helseopplysninger i samarbeidende virksomhet. Bestemmelsen fastslår at direkte tilgang til helseopplysninger i ekstern virksomhet krever at det i eget system er en eksplisitt mulighet til å autorisere en bruker for rett til å forespørre informasjon i ekstern virksomhet. Hensikten med bestemmelsen er å forhindre at alle tjenesteytere som har et tjenstlig behov for direkte tilgang til helseopplysninger i egen virksomhet, automatisk kan forespørre informasjon i ekstern virksomhet. Direkte tilgang til opplysninger på tvers av virksomheter forutsetter mer finmasket tilgangsstyring enn omtalt i merknadene ovenfor, jf. forskriften kapittel V. Tilgang til helseopplysninger forutsetter også at opplysningene er registrert på en standardisert måte.

Tredje ledd

Tredje ledd fastslår at helsepersonells medhjelper kan gis elektronisk tilgang til helseopplysninger dersom det er nødvendig for utførelse av medhjelperens oppgaver ovenfor pasienten. Helsepersonells medhjelper er nærmere omtalt i helsepersonelloven § 5. Nevnte bestemmelse i helsepersonelloven 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 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 utdannelse, dels være medhjelper for lege med instruksjonsmyndighet.

Et annet eksempel på helsepersonells medhjelper er personell ved et sykehus som skal skrive inn et journalnotat etter et diktafonopptak eller skanne journaldokumenter som foreligger på 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.

Fjerde ledd
Fjerde ledd har en tilsvarende bestemmelse, som tredje ledd har for medhjelpere, for elever og studenter.

Kasuistikker og individuelle sykehistorier om typiske og atypiske sykdomsforløp er en viktig kilde til læring i diagnostikk, kunnskap om differensialdiagnostikk, ulike behandlingsalternativer etc. Fremstilling av ulike sykehistorier og sykdomsforløp kan derfor være en viktig kilde til kunnskap for så vel elever og studenter som for ferdig utdannet helsepersonell. Det samme kan fremvising og tolkning av ulike radiologiske bilder, røntgenbilder og annen billeddiagnostikk. Bruk av journalopplysninger, radiologiske bilder etc. i undervisning og kvalitetssikring må skje innenfor gjeldende bestemmelser om taushetsplikt. Informasjonssystemet bør derfor ha en funksjonalitet som innebærer at opplysninger og bilder som brukes til undervisning i størst mulig grad kan fremstå som anonyme for mottakerne/tilhørerne. Dersom informasjonssystemet ikke har en slik funksjonalitet må det innhentes samtykke fra pasienten for å bruke opplysningene i undervisningsøyemed.

Merknader til § 15
Bestemmelsen fastslår at autorisasjon kan gis til personell i pasientadministrasjonen som har behov for det for å kunne administrere helsehjelp til pasient. Helsepersonelloven § 26 andre ledd fastsetter en ramme for hvilke opplysninger dette kan være. Det er pasientens personnummer 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. (Departementet mener at personnummer i helsepersonelloven § 26 andre ledd må forstås som fødselsnummer).

Merknader til § 16
Bestemmelsen fastslår at personell som skal bistå med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr bare kan gis autorisasjon i den grad det er nødvendig for å ivareta den aktuelle oppgaven. Helsepersonelloven § 25 andre ledd er rettsgrunnlaget for at tilgang til helseopplysninger i dette tilfelle kan gis uten hinder av taushetsplikt. Når en feil i et elektronisk system har oppstått, kan det være vanskelig å avgjøre om og hvilke journalopplysninger vedkommende reparatør må "sveipe innom "for å kunne avhjelpe feilen. (I utgangspunktet skal det være ingen). I praksis må derfor slikt personell i noen tilfeller ha ganske vide, men svært tidsbegrenset autorisasjoner, når det gjelder hvilke journalopplysninger vedkommende kan få tilgang til. Det er spesielt viktig at disse autorisasjonene blir registrert og fulgt opp med kontroll av hvordan autorisasjonen blir benyttet, jf. forskriften § 33.

Merknader til § 17
Bestemmelsen pålegger den databehandlingsansvarlige å føre et register over utstedte autorisasjoner. Registeret skal inneholde informasjon om hvem som er tildelt autorisasjon, til hvilken rolle autorisasjonen er tildelt, formålet med den, tidspunktet for når den ble gitt, varighet og om et eventuelt tilbakekall av autorisasjonen.

Kapittel IV Tilgang til helseopplysninger i behandlingsrettet helseregister

Bestemmelsene i dette kapittel pålegger plikter og rettigheter til personell som er tildelt autorisasjon etter forskriften kapittel III – det vil si helsepersonells og administrativt personells bruk av en tildelt autorisasjon.

Merknader til § 18
Bestemmelsen fastslår at enhver som gis elektronisk tilgang til helseopplysninger skal autentisere seg som en bestemt tjenesteyter i en bestemt rolle.

Den tekniske tilgangen til pasientopplysninger vil – selv ved krav om beslutningsstyrt tilgang, jf. forskriften § 19 – i enkelte tilfeller favne noe videre enn hva som strengt tatt er relevant og nødvendig for den helsehjelp som skal ytes. Det er bakgrunnen for bestemmelsen her om at ingen kan gjøre bruk av en tildelt autorisasjon i videre utstrekning enn det som følger av reglene om taushetsplikt i helsepersonelloven. Søk etter tilgang til helseopplysninger om pasienter en ikke er involvert i helsehjelp til, kan rammes av forbudet i helsepersonelloven § 21 a om forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger.

Merknader til § 19
Første ledd
Første punktum fastslår at helsepersonell som yter helsehjelp til pasient bare har tilgang til helseopplysinger som er nødvendige og relevante for å kunne yte helsehjelpen. Det følger av andre punktum at tilgangen skal følge av en konkret beslutning om at en bestemt pasient skal gis helsehjelp – før helsepersonell gis tilgang til opplysningene. Bestemmelsen innebærer at dersom det ikke er tatt noen beslutning om at en bestemt pasient skal gis helsehjelp, vil helsepersonell ikke ha lovlig tilgang til registrerte opplysninger om vedkommende pasient i henhold til denne bestemmelsen. Tredje punktum fastslår at bestemmelsen også gjelder for helsepersonells medhjelper, elever og studenter.

Hjemmelen for at det kan gis tilgang til helseopplysninger etter denne bestemmelsen er helsepersonelloven §§ 25 og 45.

Bestemmelsen forskriftsfester såkalt beslutningsstyrt tilgang: Når det treffes en beslutning om å yte helsehjelp til pasient og denne beslutningen registreres, innebærer det samtidig en registrering av hvor denne helsehjelpen skal tilbys og herunder hvilke helsepersonell man forventer vil bli delaktig i ytelse av helsehjelpen. Det kan være medisinsk avdeling, hjerte medisinsk avdeling, kirurgisk avdeling, ortopedisk avdeling, ev. post etc. Videre kan det være klart eller sannsynlig at pasienten vil motta helsehjelp fra anestesiavdeling, operasjonsavdeling, radiologisk avdeling eller andre fagspesialiserte avdelinger. Når en beslutning om helsehjelp registreres i pasientens journal, vil det samtidig åpnes for at en eller flere helsepersonell, i de ulike avdelingene som vil bidra ved gjennomføring av helsehjelpen, gis tilgang til nødvendige og relevante opplysninger om pasienten. Hvor mange tjenesteytere som vil få tilgang til helseopplysninger ved beslutningsstyrt tilgang vil blant annet bero på hvordan tilgangsstyringen konfigureres. Det vises til forskriften §§ 9 og 10.

Andre ledd
Andre ledd gjelder helsepersonell som på selvstendig grunnlag kan treffe beslutning om at en pasient skal tilbys helsehjelp. Bestemmelsen fastslår at helsepersonell som på selvstendig grunnlag kan treffe beslutning om helsehjelp, kan gis tilgang til nødvendige og relevante helseopplysninger om de pasienter vedkommende har rett og plikt til å treffe slik beslutning om. Det skal fremgå av journalen hvem som har truffet beslutningen om helsehjelp. Det er det enkelte helsepersonells rolle innen virksomheten som er avgjørende for hvilke typer eller hva slags helsehjelp tjenesteyteren kan treffe beslutning om, og hvilke typer eller hva slags helsehjelp tjenesteyteren kun kan delta ved gjennomføringen av.

Tredje ledd
Tredje ledd bestemmer at helsepersonellets tilgang til helseopplysningene varer så lenge det er nødvendig for helsehjelpen. Dette dekker også tiden det tar å dokumentere/registrere opplysningene. 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.

Fjerde ledd
Fjerde ledd fastslår at tilgang til helseopplysninger etter denne bestemmelsen bare gjelder dersom pasienten ikke har motsatt seg, eller motsetter seg, at tilgang til de aktuelle opplysninger gis. Bestemmelsen bidrar til å oppfylle pasientens rett til å reservere seg mot at opplysninger deles med annet helsepersonell. Bestemmelsen gjelder også for helsepersonell som på selvstendig grunnlag kan treffe beslutning om helsehjelp til pasienten. I praksis innebærer bestemmelsen at opplysninger pasienten har motsatt seg kan deles med annet helsepersonell, må sperres. Annet helsepersonell må da som hovedregel ha et uttrykkelig samtykke fra pasienten for å få tilgang til opplysningene. Det vises til forskriften §§ 29 og 30.

Selv om alle helseopplysninger regnes som sensitive opplysninger, vil det ofte være slik at noen helseopplysninger fremstår som mer sensitive enn andre. Opplysninger om blodgruppe, eventuelle allergier, bruk av hjertemedisiner, blodfortynnende medisiner etc. vil sjelden regnes som meget sensitive, og det må antas at det vil høre til sjeldenhetene at en pasient reserverer seg mot at annet helsepersonell kan få tilgang til slike opplysninger. Opplysninger om tidligere psykisk sykdom, visse smittsomme sykdommer, særskilt ømtålige spørsmål etc. kan det hende pasienten vil føle belastende kan bli delt med annet helsepersonell. Det er derfor viktig at helsepersonell ved registrering av opplysninger har et bevisst forhold til hvilke opplysninger som bør eller kan deles med annet helsepersonell og opplysninger som ikke bør eller kan deles med annet helsepersonell.

Dersom opplysningene kan antas å være følsomme for pasienten eller det kan antas at pasienten vil føle seg ubekvem dersom opplysningene ble kjent av andre, skal helsepersonellet gjøre pasienten oppmerksom på at han eller hun kan kreve opplysningene sperret. Det kan tenkes tilfeller der pasienten på grunn av sin fysiske eller psykiske tilstand ikke er i stand til å ta stilling til om opplysningene bør sperres. Dersom opplysningene i sist nevnte tilfeller ikke kan antas å være nødvendig for annet helsepersonell bør opplysningene som et utgangspunkt sperres.

Pasientens rett til å reservere seg mot at annet helsepersonell gis tilgang til helseopplysninger er ikke absolutt. Det kan tenkes tilfeller hvor helsepersonell bør ha tilgang til opplysninger selv om pasienten motsetter seg det. I enkelte tilfelle vil det kunne være av stor betydning at helsepersonell får kjennskap til tidligere sykdomshistorie eller behandling. En forutsetning for at helsepersonell skal få tilgang til opplysninger i slike tilfeller er at *"tungtveiende private eller offentlige interesser gjør det rettmessig å gi opplysninger videre"*, jf. helsepersonelloven § 23 nr. 4. Hvorvidt det kan gis tilgang til helseopplysninger på dette grunnlaget må besluttes av det helsepersonell som har ansvaret for helsehjelpen. Dette gjelder med de begrensninger som følger av forskriften § 29 tredje ledd. Det følger av forskriften § 29 tredje ledd at dersom helsepersonell mener at opplysninger ikke kan antas å være påtrengende nødvendig i en akutt situasjon for å kunne yte forsvarlig helsehjelp, så er det heller ikke nødvendig at annet helsepersonell som gis tilgang til opplysninger i journalen i en akuttsituasjon får kunnskap om at opplysninger er sperret.

Merknader til § 20
Første ledd
Første ledd gir personell som administrerer helsehjelp til pasient elektronisk tilgang til de pasientadministrative opplysinger som er nødvendige og relevante for å kunne administrere helsehjelpen. Helsepersonelloven § 26 andre ledd angir den ytre rammen for hvilke opplysninger dette er.

Andre ledd
Andre ledd fastslår at forskriften § 19 andre, tredje og fjerde ledd gjelder tilsvarende for pasientadministrasjonens tilgang til opplysninger. Rammen for hvilke opplysninger pasientadministrasjonen kan gis tilgang til følger av helsepersonelloven § 26 andre ledd.

Merknader til 21
Bestemmelsen fastslår at personell som skal bistå med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr bare har tilgang til de helseopplysninger som er nødvendig for å kunne ivareta den aktuelle oppgaven. Bestemmelsen er en "sikkerhetsbestemmelse." I utgangspunktet legges til grunn at service på det elektroniske systemet bør kunne utføres uten at det gis tilgang til helseopplysninger.

Kapittel VI Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

Merknader til § 22
Bestemmelsen regulerer direkte tilgang til helseopplysninger på tvers av virksomheter.

Første ledd
Første ledd krever at avtale må være inngått mellom den virksomhet som har databehandlingsansvaret for behandlingen av opplysningene og den virksomhet som gis lesetilgang til opplysningene. Avtale om tilgang til helseopplysninger på tvers av virksomheter kan bare inngås der formålet er ytelse av helsehjelp til pasient.

Bestemmelsen fastslår at avtalen bare kan omfatte strukturerte helseopplysninger som på forhånd er vurdert å kunne deles med annet helsepersonell.

Andre ledd
Andre ledd fastslår at det skal fremgå av avtalen hvilke type helsehjelp avtalen gjelder. Behovet for og omfanget av avtalen må være fundert på konkrete behovs- og nødvendighetsvurderinger. At det generelt kan oppstå en situasjon der det kan være "kjekt å ha" tilgang på tvers er ikke nok. Behovet for tilgang på tvers av virksomhetsgrenser (for eksempel mellom to helseforetak eller mellom et helseforetak og en kommunal virksomhet) må vurderes opp mot andre muligheter for kommunikasjon mellom virksomhetene, for eksempel meldingsutveksling. Elektronisk meldingsutveksling vil fortsatt være en viktig samhandlingsform, og i mange tilfeller den mest hensiktsmessige. Dette gjelder også ved kommunikasjon internt i virksomheten. Det er ikke slik at kommunikasjon internt alltid bør skje ved direkte tilgang, også internt kan meldingsutveksling være et hensiktsmessig kommunikasjonsmiddel, som for eksempel mellom ulike sykehus innen samme helseforetak.

Databehandlingsansvarlige som åpner for direkte tilgang til helseopplysninger fra ekstern virksomhet - må forsikre seg om - før avtale inngås - at informasjonssikkerheten i den virksomheten som gis tilgang er god nok. Det skal derfor fremgå av avtalen hvilke forutsetninger som ligger til grunn for avtalen, blant annet hvilke tekniske løsninger som skal benyttes ved slik tilgang. Det innebærer blant annet at den databehandlingsansvarlige som gir tilgang må ha kunnskap om tilgangsstyringen, eller hva som kan skje med de opplysningene det gis tilgang til, i den virksomheten som gis tilgang. Den databehandlingsansvarlige må også kunne sette vilkår for behandlingen av opplysningene i den virksomheten som gis tilgang.

Det skal også fremgå av avtalen at den virksomheten som får tilgang skal etablere internkontrollsystem for å sikre at helseregisterloven, forskriften og avtalens forutsetninger overholdes. Både den databehandlingsansvarlig og den som gis tilgang - vil kunne bli holdt ansvarlig ved overtredelse av avtalen, helseregisterloven og forskriften, jf. helseregisterloven § 34 og forskriften § 35.

Tredje ledd
Tredje ledd fastslår at avtale inngås mellom den virksomhet som har databehandlingsansvaret for behandlingen av opplysningene og den virksomhet som gis tilgang til opplysningene. Kravet til nødvendighetsvurdering og at avtalene konkretiseres i forhold til type helsehjelp, forutsetter bilaterale avtaler.

Den databehandlingsansvarlige som i henhold til avtale gir annen databehandlingsansvarlig (og helsepersonell ved denne virksomheten) tilgang til helseopplysninger i sin virksomhet, kan ikke fraskrive seg databehandlingsansvaret ved avtale. Avtalen mellom de to virksomhetene må derfor sette vilkår for når tilgang til helseopplysninger kan gis.

Den virksomheten som gis tilgang vil enten være databehandlingsansvarlig eller databehandler. Både som databehandler og databehandlingsansvarlig vil virksomhetene ha ansvar for informasjonssikkerheten, jf. helseregisterloven § 16. Det avgjørende for om man er databehandler eller databehandlingsansvarlig i den enkelte situasjon vil være avhengig av hvilke av de to virksomhetene som bestemmer formålet med tilgangen og den enkelte behandlingen av helseopplysninger i et konkret tilfelle. Eksempler:

- Virksomhet 1 ber virksomhet 2 om en annenhåndsvurdering av et røntgenbilde, og gir virksomhet 2 tilgang til røntgenbildet. Virksomhet 1 bestemmer her formålet med tilgangen og er databehandlingsansvarlig for opplysningene. Virksomhet 2 behandler dataene på vegne av virksomhet 1 og er databehandler. Vedkommende helsepersonell i virksomhet 2 som gjør denne vurderingen kan ikke behandle dataene til noe annet enn den forespurte annenhåndsvurdering.

- Dersom virksomhet 2 har en pasient til behandling i sin virksomhet og ber om tilgang til helseopplysninger om pasienten i virksomhet 1, er det virksomhet 2 som bestemmer formålet med behandlingen av opplysningene. Virksomhet 1 vil være ansvarlig for at tilgang faktisk er gitt. Virksomhet 2 vil imidlertid være ansvarlig for den videre bruken av opplysningene.

Helseforetakene er databehandlingsansvarlige for de behandlingsrettede helseregistrene innenfor helseforetaket, jf. helseregisterloven § 6 og helseforetaksloven § 9. Det innebærer at det regionale helseforetaket, selv om de står som eier av foretaket, ikke kan instruere et helseforetak om å inngå avtale om tilgang på tvers av virksomhetens grenser. Helseforetaket er eget rettssubjekt, jf. helseforetaksloven § 6.

Merknader til § 23
Bestemmelsen åpner for skrivetilgang eller anmerkningstilgang på tvers av virksomheter innenfor særskilte områder etter avtale. Bestemmelsen har et begrenset virkeområde.

Et eksempel på hvor bestemmelsen vil kunne anvendes, er innenfor radiologien. En pasient er for eksempel innlagt på et sykehus for å ta MRT (magnetresonanstomografi), CT (computer tomografi) 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 ev. endringer/funn ligger. Dersom det gjøres en anmerkning/tolkning av bildet, må det også registreres/fremgå hvem det er som har gjort denne anmerkningen/tolkningen.

Merknader til § 24
Første ledd
Første ledd fastslår tekniske forutsetninger for at to virksomheter kan inngå avtale om lesetilgang på tvers av virksomhetene. Det kreves at journalføringen kan struktureres og er strukturert på en slik måte at det er mulig å bare gi tilgang til et avgrenset sett av klinisk informasjon - som før tilgang gis er vurdert at kan deles med annet helsepersonell i ekstern virksomhet ved direkte tilgang.

Andre ledd
Andre ledd forutsetter at en også tar organisatoriske elementer med i vurderingen av informasjonssikkerheten. Bestemmelsen fastslår at avtale om lese- og eventuelt skrivetilgang mellom to virksomheter (egne rettssubjekter) bare kan inngås dersom gjennomføring av avtalen ikke svekker informasjonssikkerheten ved noen av virksomhetene. Det innebærer at enhver databehandlingsansvarlig nøye må vurdere om det er hensiktsmessig å inngå en slik avtale og eventuelt i hvilke omfang. En forutsetning for å inngå avtale, er at begge parter i avtalen er kjent med hverandres sikkerhetsmål og sikkerhetsstrategi.

For helseinstitusjoner som har et meget fast og formelt samarbeid om oppgavedeling innenfor en bestemt gren av medisinen kan det vurderes som mest formålstjenelig å inngå en slik avtale. For andre helseinstitusjoner kan det kanskje være mest formålstjenlig å basere seg på meldingsutveksling. Når det gjelder kommunikasjon mellom fastleger og helseforetak antar departementet at det i mange tilfeller kan være mest hensiktsmessig å kommunisere via utveksling (epikriser og henvisninger) av meldinger. Det samme gjelder mellom fastlegen 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.

Merknader til § 25
Bestemmelsen fastslår at enhver som gis tilgang til helseopplysninger i et behandlingsrettet helseregister i ekstern virksomhet, §§ 22 og 23, skal autentisere seg ved bruk av kvalifisert sertifikat. Kvalifisert sertifikat er nærmere regulert i esignaturloven § 4.

Godt sikkerhetsnivå for tilgang til helseopplysninger på tvers av virksomheter kan etter omstendighetene etableres selv om en ved autentiseringen ikke har benyttet kvalifisert sertifikat. Dette kan for eksempel gjelde der to helsevirksomheter har felles database med logiske skiller mellom de ulike helseforetakene. Departementet har derfor vurdert om kravet om bruk av kvalifisert sertifikat bør være absolutt, eller om det kan åpnes for unntak der begge virksomheter har god tilgangsstyring og et høyt sikkerhetsnivå selv om autentiseringen ikke skjer ved bruk av kvalifisert sertifikat. Det som er avgjørende for om unntak ev. skal kunne gjøres er at det gjennom risikoanalyse kan dokumenteres at sikkerheten er god.

I herværende utkast til forskrift har departementet som et utgangspunkt ikke åpnet for at det kan gjøres unntak fra kravet om bruk av kvalifisert sertifikat. Departementet ber om kommentarer fra høringsinstansene på dette spørsmål.

Merknader til § 26
Første punktum fastslår at en forespørsel om og tilgang til helseopplysninger i annen virksomhet skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet. Dette innebærer at helsepersonell som ønsker tilgang til helseopplysninger i ekstern virksomhet må begynne prosessen med først å bli autentisert og autorisert for innsyn i egen virksomhet. Tilgang til opplysninger i den eksterne virksomheten kan bare gis der det tjenstlige behovet er identifisert og dokumentert i egen virksomhet. Andre punktum presiserer at forespørselen og tilgang til helseopplysninger bare kan omfatte en person om gangen. Videre fremgår av tredje punktum at forespørselen samt beslutningen om å etterkomme den, eller ikke, skal registreres. Forespørselen vil skje mot forhåndsvurderte og strukturerte opplysninger, jf. forskriften § 22 første ledd andre punktum og § 24 første ledd. Ved behov for gjentatt tilgang til helseopplysninger om samme pasient, skal det gjøres en ny forespørsel.

Det følger av bestemmelsen at dersom helsepersonellet som har ekstern lesetilgang ikke lenger yter eller skal yte helsehjelp til pasienten, pasienten er for eksempel utskrevet eller flyttet, skal det heller ikke lenger være mulig for vedkommende helsepersonell å forespørre om tilgang til helseopplysninger i den eksterne virksomheten.

Merknader til § 27
Første punktum fastslår at tilgang til helseopplysninger på tvers av virksomheter bare kan gis etter uttrykkelig, informert og frivillig samtykke fra den registrerte, jf. helseregisterloven § 2 nr. 11. 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. Et samtykke kan når som helst trekkes tilbake.

Andre punktum fastslår at samtykket skal dokumenteres. Slik dokumentasjon kan skje som avkrysning/anmerkning i journalen både i den virksomheten som gir tilgang og den virksomheten som ber om tilgang. Samtykket må innhentes fra pasienten i den aktuelle behandlingssituasjonen det er behov for opplysningene. Pasientens uttrykkelige samtykke kan avgis i muntlig eller skriftlig form. Helsepersonell som mottar samtykke og således gis tilgang til opplysningene må dokumentere/anmerke at samtykket er mottatt. Anmerkningen må kunne tilbakeføres til en konkret navngitt person.

Aktuelt helsepersonell i den virksomhet som gis tilgang vil for øvrig ha alminnelig journalføringsplikt. Det innebærer blant annet at bakgrunnen for helsehjelpen, opplysninger om pasientens sykehistorie, og utveksling av informasjon med annet helsepersonell, jf. journalforskriften § 8, skal beskrives. Der bakgrunnsopplysninger og opplysninger om tidligere sykehistorie er opplysninger som er blitt kjent ved tilgang til annet journalsystem, skal dette fremgå.

Ved journalføringen er det en plikt til å informere pasienten etter helseregisterloven § 23.

Det følger av dette at et elektronisk journalsystem som åpner for tilgang på tvers må ha funksjonalitet for registrering av samtykke (når dette er innhentet). Det bør i tillegg ha funksjonalitet for registrering av at pasienten er informert, jf. helseregisterloven § 23. I den forbindelse kan det også vises til forskrift om pasientjournal § 8 bokstav j tredje punktum der det fremgår at journalen skal inneholde opplysninger om pasientens samtykke eller reservasjon vedrørende informasjonsbehandling.

Merknader til § 28
Bestemmelsen åpner for at det kan gjøres unntak fra kravet om uttrykkelig samtykke. Det følger av bestemmelsen at dersom pasienten på grunn av sin fysiske eller psykiske tilstand ikke er i stand til å gi et uttrykkelig samtykke, og det må antas at pasienten ville ha gitt et slikt samtykke dersom han eller hun hadde vært i stand til å gi et slikt samtykke, kan tilgang til opplysningene – fra ekstern virksomhet likevel gis. Det skal

fremgå av det aktuelle registeret (det registeret det gis tilgang til) at uttrykkelig samtykke ikke er gitt, og begrunnelsen for det.

Merknader til § 29
Første ledd
Det følger av bestemmelsen at helseopplysninger den registrerte har motsatt seg eller motsetter seg at andre får tilgang til, jf. helsepersonelloven §§ 25 og 45, skal sperres.

Andre ledd
Bestemmelsen åpner for at den registrerte kan bestemme om sperringen kun skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for den eller de den registrerte selv bestemmer, eller om de bare skal være tilgjenglig etter samtykke.

Selv om alle helseopplysninger regnes som sensitive personopplysninger, kan noen helseopplysninger føles mer sensitive enn andre. Hvilken blodgruppe vi har, om vi har brukket et ben, er operert for blindtarmbetennelse eller har fjernet mandlene vil kanskje et fåtall av oss synes er ubehagelig at andre kan få kunnskap om. Mottar vi behandling for Hiv/aids, har gjennomført flere aborter, er innlagt på grunn av "nervøst sammenbrudd" er det kanskje flere av oss som vil forbeholde slike opplysninger til et fåtall helsepersonell – og eventuelt bare til de som vi vet er der for å hjelpe oss og vi har et personlig og tillitsfullt forhold til. Denne bestemmelsen legger til rette for at den registrerte (pasienten) selv kan ha kontroll med hvilke opplysninger annet helsepersonell kan få tilgang til.

Tredje ledd
Det følger av tredje ledd at dersom de opplysninger den registrerte krever sperret, skal det fremgå av journalen at slike opplysninger er sperret. Opplysninger om blodgruppe, medikamenter, og da særlig blodfortynnende medikamenter, hjerte og/eller lungesvikt, at pasienten tidligere har vært vanskelig å intubere, eventuelt allergier er eksempler på slike opplysninger. Det må kunne antas at det er sjeldent at en pasient ønsker å sperre slike opplysninger, og særlig etter at pasienten er informert om at slike opplysninger ikke bør sperres av hensyn til senere helsehjelp. Annerledes kan det stille seg med opplysninger om sykdommer som smitter gjennom blod. Dersom den registrerte (pasienten) ber om at opplysninger om smittsomme sykdommer sperres i henhold til første og andre ledd, bør journalen gi informasjon om at det finnes sperrede opplysninger.

Merknader til § 30
Det fremgår av bestemmelsen at tilgang til sperrede opplysninger kan skje dersom tungtveiende grunner taler for det, jf. pasientrettighetsloven § 5–3. En akuttsituasjon hvor det kreves at pasienten øyeblikkelig legges i narkose for å kunne opereres kan være eksempel på en slik situasjon. Det må være det helsepersonellet som har ansvaret for pasienten i akuttsituasjonen - og som på selvstendig grunnlag kan treffe beslutning om helsehjelpen - 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.

Merknader til § 31
Bestemmelsen krever at det i behandlingsrettede helseregistre skal finnes dokumentasjon av hvem som har hatt tilgang til opplysningene i registrene, i hvilket tidsrom den enkelte har hatt tilgang, og hva som er grunnlaget for tilgangen. Det er ikke nok bare å skrive helsehjelp. Type helsehjelp må angis. Bestemmelsen representerer en konkretisering av helsepersonelloven § 45 første ledd tredje punktum.

Registreringen av grunnlaget for tilgangen skal inkludere tilstrekkelige opplysninger til at det er mulig å fastslå hvilken bestemmelse i denne forskriften det er som danner grunnlaget for tilgangen. Dette innebærer blant annet:

- For tilgang etter § 19 skal det inngå referanse til den beslutning om helsehjelp som legitimerer tilgangen.
- For tilgang etter § 20 skal det fremgå den pasientadministrasjon som nødvendiggjorde tilgangen.
- For tilgang etter § 21 skal den aktuelle bistanden fremgå.
- For tilgang etter §§ 22 og 23 skal det inngå referanse til forespørselen om tilgang, jf. forskriften § 26.

For pasienten skal dokumentasjonen av tilgang gi en kortfattet oversikt over hvem som har hatt tilgang til journalen, når de har hatt tilgang samt hvorfor de har hatt tilgang. Ettersom dokumentasjonen vil være betydelig mer oversiktlig enn registreringen i hendelsesregistrene, kan det antas at den vil være et godt hjelpemiddel for pasienter som ønsker å få klarlagt om noen uberettiget har tilegnet seg opplysninger i journalen.

Hendelsesregistreringene/loggene kan eventuelt (inntil de er slettet) benyttes som et supplement til denne dokumentasjonen dersom det er behov for mer detaljert informasjon om hvilke opplysninger i journalen som har vært omfattet av et tilfelle av tilgang. Dokumentasjonen etter denne bestemmelsen er en del av "pasientens journal"

og berøres ikke av at korresponderende bestemmelser i hendelsesregisteret, jf. forskriften § 32, blir slettet etter 2 år.

Merknader til § 32
Første ledd
Første ledd krever at det lagres hendelsesregistre over uautoriserte forsøk på pålogging til systemer som inneholder helseopplysninger og over autoriserte påloggingер til slike systemer. For å oppfylle dette formålet må virksomheten ha flere hendelsesregistre, jf. flertallsformen. Hendelsesregistrene etter denne paragrafen er ikke en del av den enkelte pasients journal/behandlingsrettede helseregister.

Det må føres hendelsesregistre over alle uautoriserte forsøk på pålogging og autoriserte påloggingер til systemer som benyttes for å behandle helseopplysninger. Opphenting av helseopplysninger fra eget system mot en felles database for helseopplysninger skal ha tilsvarende registreringer over uautoriserte forsøk og autoriserte påloggingер.

Hvor mange hendelsesregistre det er behov for og hvilke opplysninger de bør inneholde, vil variere blant annet med virksomhetens størrelse og hvilke tekniske løsninger virksomheten benytter. Forskriften stiller derfor ikke konkrete krav verken når det gjelder antall hendelsesregistre eller hvilke opplysninger som skal inngå. Det er opp til den enkelte databehandlingsansvarlige å sikre at registreringen av hendelsene /loggingen gir tilstrekkelig detaljert informasjon slik at konkrete mottiltak kan settes i verk dersom forholdene gjør dette nødvendig. Videre må databehandlingsansvarlig sikre at opplysningene som registreres/logges er tilstrekkelige til entydig å avgjøre hvilke tidsrom den enkelte bruker har vært pålogget, hvor de har vært pålogget fra samt hvilke systemer de har benyttet mens de har vært pålogget.

I tillegg til ovennevnte må det også føres hendelsesregistre som kan gi kunnskap om i hvilken grad personell som er pålogget har benyttet seg av sin mulighet for tilgang til opplysinger i behandlingsrettede helseregistre, hvilke opplysninger de har lest eller slått opp– og på hvilket tidspunkt.

Andre ledd
Andre ledd stiller krav om hvilken informasjon som skal registreres i et hendelsesregister. Stikkordsmessig kan dette oppregnes i:hvem – hvorfra – hvorfor - hva og når.

Tredje ledd
Tredje ledd krever at hendelsesregistrene fra de behandlingsrettede helseregistrene skal kunne sammenstilles med virksomhetens autorisasjonsregistre og med register eller liste over tilstedeværelse av personell. Det kreves ikke at slik sammenstilling må

skje elektronisk, selv om dette kan være det mest effektive. Inntil systemer for elektronisk sammenstilling av slike opplysninger er på plass, må sammenstillingen kunne gjøres manuelt. Kobling mot autorisasjonsregisteret eller listen over tilstedeværelse av personell skal gjøres ved mistanke om snoking eller ved rutinemessig kontroll av dette.

Fjerde ledd
Fjerde ledd krever at opplysningene i hendelsesregisteret skal bevares i minst to år før de kan slettes.

Merknader til § 33
Bestemmelsen krever at hendelsesregistreringer jevnlig skal følges opp og kontrolleres. Det gjelder både dokumentasjon etter forskriften § 31 og § 32. Dersom en slik kontroll utløser mistanke om at det har skjedd urettmessig tilgang, skal virksomhetens ledelse varsles. Dersom gjennomgang av kontrollen viser at det har skjedd en urettmessig tilegnelse av helseopplysninger, skal Datatilsynet informeres, jf. personopplysningsforskriften § 2–6. Videre skal pasienten opplysningene er knyttet til, informeres.

Merknader til § 34
Bestemmelsen gir den registrerte innsynsrett i logger som gir informasjon om behandling av opplysninger som kan knyttes til vedkommende. Det innebærer at vedkommende pasient vederlagsfritt skal kunne kreve informasjon om hvem, hvorfra, hva, hvorfor og når tilgang til opplysninger om vedkommende er gitt.

Denne bestemmelsen må ses i sammenheng med bestemmelsen i forskriften § 31 om dokumentasjon i behandlingsrettet helseregister (elektronisk pasientjournal) av tilgang til opplysninger. Bestemmelsene gir imidlertid også innsynsrett i hendelsesregistreringer etter § 32. Sistnevnte registreringer kan slettes etter 2 år.

Merknader til § 35
Bestemmelsen fastslår at den som forsettlig eller grovt uaktsomt unnlater å følge reglene i denne forskriften straffes med bøter eller fengsel inntil ett år eller begge deler. Fristen for foreldelse er 2 år, jf. straffeloven § 67.

Merknader til § 37
Det følger av første og andre punktum at departementet bestemmer når forskriften trer i kraft samt at en beslutning om ikrafttredelse kan omfatte hele eller deler av helsetjenesten. De ulike virksomheter innen helsetjenesten har kommet ulikt langt i å ta i bruk elektroniske systemer som tilfredsstiller forskriftens krav til funksjonalitet. Blant annet gjelder dette krav til teknisk funksjonalitet som beslutningsstyrt tilgang, muligheten til å sperre opplysninger samt kravene til logging og dokumentasjon av

tilgang. Forskriften åpner også for at en kan skille mellom ulike virksomheter innen kommunehelsetjenesten og spesialisthelsetjenesten.

Tredje punktum fastslår at de enkelte bestemmelsene i forskriften kan settes i kraft på ulike tidspunkt. Kapittel V som gir bestemmelser for tilgang til helseopplysninger på tvers må settes i kraft i sin helhet.

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

Fastsatt ved kgl. res. …..med hjemmel i helseregisterloven §§ 13, 16 og 17, helsepersonelloven §§ 40, 45 og 46 og pasientrettighetsloven § 5-1. Fremmet av Helse- og omsorgsdepartementet

Kapittel 1 Innledende bestemmelser

§ 1 *Forskriftens formål*

Formålet med forskriften er å gi helsepersonell nødvendig tilgang til helseopplysninger slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas. Videre er formålet å bidra til god informasjonssikkerhet.

§ 2 *Forskriftens virkeområde*

Forskriften gir regler om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre som skjer med hjemmel i helseregisterloven § 6 og helsepersonelloven § 46.

§ 3 *Definisjoner*

I forskriften menes med

1. *autentisering:* Prosess som gjennomføres for å bekrefte en påstått identitet.
2. *autorisasjon:* En person i en bestemt rolle gis bestemte rettigheter til lesing, registrering, redigering, retting, sletting, sperring eller annen behandling av helseopplysninger.
3. *tilgang til helseopplysninger:* Helseopplysninger om en eller flere bestemte pasienter er eller gjøres tilgjengelig for autorisert personell, jf. punkt 2.
4. *direkte tilgang til helseopplysninger:* Helsepersonell kan logge seg rett inn på et behandlingsrettet helseregistersystem og fra dette systemet logge seg rett inn på andre behandlingsrettede helseregistersystemer, internt i virksomheten eller i ekstern virksomhet. Pålogging kan skje fra den interne virksomhetens helseregistersystem eller fra den eksterne virksomhetens system.

a. *sperrede helseopplysninger:* Helseopplysninger som pasienten etter helsepersonelloven §§ 25 eller 45 har motsatt seg eller motsetter seg at andre gis tilgang til.

Kapittel II Generelle krav til informasjonssikkerhet

§ 4 *Krav om forsvarlige systemer*

Virksomheter som tar i bruk behandlingsrettede helseregistre, skal sørge for at systemene som tas i bruk sikrer forsvarlig informasjonssikkerhet.

§ 5 *Krav til planlegging, organisering og rutiner*

Virksomhet som tar i bruk behandlingsrettede helseregistre, skal utarbeide en overordnet strategi og målsetting for informasjonssikkerheten i virksomheten. Det skal utarbeides informasjonssikkerhetsplaner og styrende dokumenter for behandlingen av helseopplysninger for alle nivåer i virksomheten.

Alle nivåer i virksomheten skal ha skriftlige rutiner for behandling av helseopplysninger. Rutinene skal ha utgangspunkt i den overordnede planen, jf. første ledd.

Det skal klart fremgå av planverket hvem som til enhver tid er ansvarlig for de ulike deler av informasjonssikkerheten.

Tiltak som faller inn under paragrafen her skal integreres i virksomhetens internkontrollsystem.

§ 6 *Krav om internkontroll*

Databehandlingsansvarlig skal etablere internkontroll i samsvar med helseregisterloven § 17. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve kravene i helseregisterloven og i denne forskriften.

Kravet til internkontroll innebærer at den databehandlingsansvarlige blant annet skal ha kjennskap til gjeldende regler om behandling av helseopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av reglene samt ha denne dokumentasjonen tilgjengelig for de den måtte angå.

Den databehandlingsansvarlige skal ha rutiner for oppfyllelse av sine plikter og de registrertes rettigheter etter det til enhver tid gjeldende regelverk, herunder ha rutiner for

- administrasjon og kontroll av autorisasjoner etter kapittel III,
- administrasjon, kontroll og oppfølging av logg etter kapittel VI,
- innhenting av samtykke etter § 29,
- oppfyllelse av henvendelser fra den registrerte om innsyn i logg etter § 36 og
- avdekking, oppretting og forebygging av overtredelser av forskriften.

Databehandlere som behandler helseopplysninger på oppdrag fra den databehandlingsansvarlige, skal behandle opplysningene i samsvar med rutiner den databehandlingsansvarlige har oppstilt.

§ 7 *Sikkerhetsledelse*

Den som har den daglige ledelse av virksomheten som den databehandlingsansvarlige driver, har ansvaret for at informasjonssikkerheten i virksomheten er god og at bestemmelsene i helseregisterloven og denne forskriften følges.

§ 8 *Forholdet til personopplysningsforskriften*

Bestemmelsene i personopplysningsforskriften om informasjonssikkerhet gjelder som utfyllende bestemmelser til denne forskriften.

Kapittel III Krav om system for utstedelse av autorisasjoner og krav til autentisering

§ 9 *Krav om system for administrering av autorisasjoner*

Den databehandlingsansvarlige skal etablere nødvendige organisatoriske og tekniske tiltak for tildeling, administrasjon og kontroll av autorisasjoner. Autorisasjonen skal bidra til å sikre at informasjonssikkerheten, herunder bestemmelsene om taushetsplikt og pasientens rett til konfidensialitet, blir ivaretatt.

Den enkelte autorisasjon skal bygge på konkrete risikovurderinger for urettmessig og uriktig behandling av helseopplysninger.

§ 10 *Krav til tilgangsstyringen – forholdet til taushetsplikt*

Den databehandlingsansvarlige skal sørge for at virksomhetens tilgangsstyring sikrer og begrenser tilgangen til de helseopplysninger som er relevante og nødvendige for formålet med tilgangen. Tilgangen skal vurderes og konfigureres med hensyn til:

a) antall registrerte det gis tilgang til
b) mengde informasjon om den enkelte det gis tilgang til og
c) varighet av tilgangen.

Enhver autorisasjon skal være tidsbegrenset og bare omfatte slik behandling av helseopplysninger som er relevant og nødvendig for å nå det angitte formålet med tilgangen. Den enkelte tjenesteyters behov for den aktuelle autorisasjonen i tjenesten skal vurderes og oppdateres jevnlig.

Virksomheten skal dokumentere vurderingene etter andre ledd. Dokumentasjonen skal inngå i virksomhetens internkontrollsystem.

§ 11 *Vilkår for utstedelse av autorisasjon*

Autorisasjon kan bare gis i den grad det er nødvendig for tjenesteyters arbeid, er begrunnet i tjenstlige behov og tilfredsstiller bestemmelser om taushetsplikt. Grunnlaget for tilgangen skal dokumenteres.

Ingen kan autoriseres for tilgang til helseopplysninger i videre omfang enn det som følger av reglene om taushetsplikt i helsepersonelloven.

§ 12 *Krav om opplæring*

Den databehandlingsansvarlige skal sørge for at enhver som gis autorisasjon, får nødvendig opplæring og informasjon om hvordan autorisasjonen skal brukes, og om dens begrensninger og muligheter. Opplæringen skal som hovedregel gis før autorisasjon utstedes, eller i spesielle tilfelle så snart som mulig etter at autorisasjonen er utstedt. Opplæringen skal gjentas slik at kunnskapen holdes vedlike.

§ 13 *Krav om autentisering*

Enhver som gis autorisasjon, skal entydig identifiseres som en bestemt tjenesteyter i en bestemt rolle.

§ 14 *Autorisasjon for ytelse av helsehjelp*

Autorisasjon kan gis til helsepersonell som har behov for det for å kunne yte forsvarlig helsehjelp til pasient. Autorisasjonen skal gis det innhold som er nødvendig for at helsepersonellet skal kunne ivareta sine oppgaver og sitt ansvar ovenfor pasienten på en forsvarlig måte.

Direkte tilgang til helseopplysninger i ekstern virksomhet, jf. forskriften kapittel V, krever at det i eget system er en eksplisitt mulighet til å autorisere en bruker for rett til å forespørre informasjon i ekstern virksomhet.

Helsepersonells medhjelper, jf. helsepersonelloven § 5, kan gis autorisasjon i den grad det er nødvendig for utførelse av medhjelperens oppgaver overfor pasienten. Medhjelperen er i slike tilfeller underlagt helsepersonellets kontroll og tilsyn.

Elever og studenter som i forbindelse med helsefaglig opplæring gir helsehjelp kan gis autorisasjon i den grad det er nødvendig for utførelsen av elevens eller studentens oppgaver overfor pasienten. Tredje ledd annet punktum gjelder tilsvarende for eleven og studenten.

§ 15 Autorisasjon for administrering av helsehjelp

Autorisasjon kan gis til personell i pasientadministrasjonen som har behov for det for å kunne administrere helsehjelp til pasient, jf. helsepersonelloven § 26 andre ledd.

§ 16 *Autorisasjon for ytelse av nødvendige støttefunksjoner*

Personell som skal bistå med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr, jf. helsepersonelloven § 25 andre ledd, kan bare gis autorisasjon i den grad det er nødvendig for å ivareta den aktuelle oppgaven.

§ 17 *Krav om register over og kontroll av autorisasjoner*

Den databehandlingsansvarlige skal føre et register over utstedte autorisasjoner (autorisasjonsregister). Registeret skal inneholde informasjon om hvem som er tildelt autorisasjon, til hvilken rolle autorisasjonen er tildelt, formålet med den, tidspunktet for når den ble gitt, varighet og om et eventuelt tilbakekall av autorisasjonen.

Kapittel IV Tilgang til helseopplysninger i behandlingsrettet helseregister

§ 18 Krav om autentisering og bruk av autorisasjonen

Enhver som gis elektronisk tilgang til helseopplysninger skal autentisere seg som en bestemt person i en bestemt rolle.

Ingen kan gjøre bruk av en tildelt autorisasjon i videre omfang enn det som følger av reglene om taushetsplikt.

§ 19 *Tilgang til helseopplysninger for ytelse av helsehjelp*

Helsepersonell som yter helsehjelp til pasient, har bare tilgang til helseopplysinger som er nødvendige og relevante for å kunne yte helsehjelpen. Tilgangen skal følge av en konkret beslutning om å yte helsehjelp til pasienten. Dette samme gjelder for helsepersonells medhjelper, elever og studenter, jf. § 14 tredje og fjerde ledd.

Helsepersonell som på selvstendig grunnlag kan treffe beslutning om helsehjelp, kan gis elektronisk tilgang til nødvendige og relevante helseopplysninger om de pasienter vedkommende tjenesteyter har rett og plikt til å treffe slik beslutning om. Det skal fremgå av journalen hvem som har truffet beslutningen.

Tilgangen til helseopplysninger etter denne bestemmelsen varer så lenge det er nødvendig for helsehjelpen.

Tilgangen til helseopplysningene gjelder bare dersom pasienten ikke har motsatt seg eller motsetter seg at tilgang til de aktuelle opplysninger gis, så fremt tungtveiende grunner ikke tilsier noe annet, jf. pasientrettighetsloven 5-3.

§ 20 *Tilgang til helseopplysninger for administrering av helsehjelp*

Personell som administrerer helsehjelp, har bare tilgang til de pasientadministrative helseopplysninger som er nødvendige og relevante for å kunne administrere hjelpen, jf. helsepersonelloven § 26 andre ledd.

§ 19 andre, tredje og fjerde ledd gjelder tilsvarende for personell i pasientadministrasjonen.

§ 21 *Tilgang til helseopplysninger for personell med støttefunksjoner*

Personell som skal bistå med elektronisk bearbeiding av opplysninger, eller som bistår med service og vedlikehold av utstyr, jf. helsepersonelloven § 25 andre ledd, har bare tilgang til de helseopplysninger som er nødvendig for å kunne ivareta den aktuelle oppgaven.

Kapittel V Tilleggsbestemmelser for direkte tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter

§ 22 *Avtale om direkte lesetilgang til helseopplysninger på tvers av virksomheter*

Helsepersonell som ikke står under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet kan, dersom det på forhånd er inngått en avtale om det, gis direkte lesetilgang til helseopplysninger i behandlingsrettet register virksomheten er ansvarlig for. Avtale om lesetilgang kan bare inngås for tilfeller der formålet med tilgangen er ytelse av helsehjelp til pasient, og kan bare omfatte strukturerte helseopplysninger som er relevante og nødvendige for å nå formålet med behandlingen av dem. Det kan bare gis tilgang til opplysninger som det på forhånd er vurdert kan deles med annet helsepersonell som skal yte eller yter helsehjelp til pasienten.

Det skal fremgå av avtalen hvilke formål (type helsehjelp) avtalen gjelder og hvilke forutsetninger som ligger til grunn for avtalen, herunder også hvilke tekniske løsninger som skal benyttes ved slik tilgang.

Avtale som nevnt i første og andre ledd, inngås mellom den virksomhet som har databehandlingsansvaret for behandlingen av opplysningene og den virksomhet som gis lesetilgang til opplysningene.

§ 23 *Avtale om skrivetilgang på tvers av virksomheter*

Dersom det er nødvendig for å utføre formålet med lesetilgang i medhold av § 22, kan det for særskilte områder avtales at helsepersonell som i en bestemt rolle gis slik tilgang, skal kunne registrere bestemte anmerkninger i det behandlingsrettede helseregister det er gitt tilgang til. Dette gjelder bare i de tilfeller der anmerkningen er nødvendig med tanke på helsehjelpen pasienten skal tilbys. Anmerkningen skal kunne føres tilbake til navngitt person.

§ 24 *Forutsetninger for å kunne inngå avtale om direkte tilgang til helseopplysninger på tvers av virksomheter*

Avtale som nevnt i §§ 22 og 23 kan bare inngås dersom begge virksomheter har tekniske løsninger som kan avgrense tilgangen til å omfatte strukturert og forhåndsvurdert klinisk informasjon om en navngitt person relatert til forespørselen.

Avtale som nevnt kan videre bare inngås dersom gjennomføring av den ikke svekker informasjonssikkerheten ved behandling av helseopplysninger ved noen av virksomhetene. Begge parter i avtalen må være kjent med den andre partens sikkerhetsmål og sikkerhetsstrategi.

§ 25 *Krav til autentisering*

Enhver som gis tilgang til helseopplysninger i et behandlingsrettet helseregister ved en ekstern virksomhet, skal autentisere seg ved bruk av kvalifisert sertifikat.

§ 26 Krav til forespørselen m.m.

En forespørsel om og direkte tilgang til helseopplysninger i annen virksomhet skal skje via autorisasjons- og autentiseringsmekanismer i regi av egen virksomhet. Forespørselen og tilgangen til helseopplysninger kan bare omfatte en person om gangen. Forespørselen samt beslutningen om å etterkomme den, eller ikke, skal registreres. Ved behov for gjentatt tilgang til helseopplysninger om samme pasient skal det gjøres en ny forespørsel.

§ 27 *Krav om samtykke*

Direkte tilgang til helseopplysninger på tvers av virksomheter kan bare gis etter uttrykkelig, informert og frivillig samtykke fra den registrerte. Samtykket skal dokumenteres.

§ 28 *Unntak fra krav om at samtykke skal være uttrykkelig*

Kravet om at samtykket skal være uttrykkelig 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 det aktuelle registeret at uttrykkelig samtykke ikke er gitt, og begrunnelsen for det.

Kapittel VI Sperring av helseopplysninger

§ 29 Sperring av helseopplysninger

Dersom den registrerte har motsatt seg eller motsetter seg at andre får tilgang til helseopplysninger, jf. helsepersonelloven §§ 25 og 45, skal opplysningene sperres.

Den registrerte kan bestemme om sperringen kun skal gjelde bestemte personer, om de sperrede opplysningene bare skal være tilgjengelige for den eller de den registrerte selv bestemmer, eller om de bare skal være tilgjenglig etter samtykke.

Dersom de opplysninger den registrerte krever sperret antas å være påtrengende nødvendig for å yte forsvarlig helsehjelp i en akutt situasjon, skal det fremgå av journalen at det er registrert opplysninger som er sperret.

§ 30 Tilgang til sperrede opplysninger

Tilgang til sperrede opplysninger kan skje dersom tungtveiende grunner taler for det, jf. pasientrettighetsloven § 5-3.

Kapittel VII Krav om logging og dokumentasjon av tilgang

§ 31 *Krav om dokumentasjon av tilgang*

Alle tilfeller av tilgang til opplysninger i et behandlingsrettet helseregister skal automatisk dokumenteres i registeret. Dokumentasjonen skal inneholde informasjon om:

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

§ 32 *Krav om hendelsesregistrering/logg*

For å avdekke uautorisert tilgang til opplysninger i behandlingsrettede helseregistre, eller forsøk på slik tilgang, skal den databehandlingsansvarlige sørge for at det lagres hendelsesregistre over uautoriserte forsøk på pålogging til systemer som benyttes til å behandle helseopplysninger og over autoriserte påloggінger til slike systemer.

Videre skal hvert enkelt tilfelle av tilgang til helseopplysninger fra et behandlingsrettet helseregister registreres i et hendelsesregister med dokumentasjon av:

a) entydig identifikasjon av den som har fått tilgang
b) stedet hvor vedkommende har vært pålogget fra
c) referanse til de opplysninger det er gitt tilgang til

d) hvilke systemer vedkommende har benyttet mens han eller hun var pålogget
e) det tidsrom vedkommende har hatt tilgang til opplysningene.

Hendelsesregistrering som nevnt skal skje uavhengig av om opplysningene ble gitt tilgang til for å leses på skjerm, skrives ut eller for å være gjenstand for andre former for behandling.

Hendelsesregistre som skal kunne sammenstilles med virksomhetens autorisasjonsregister, jf. § 17, og med register eller liste over tilstedeværelse av personell.

Dokumentasjonen som registreres kan slettes etter 2 år.

§ 33 *Oppfølging og kontroll av elektronisk tilgang*

Den databehandlingsansvarlige skal jevnlig kontrollere hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister. Dersom gjennomgang av kontrollen viser at det har skjedd en urettmessig tilegnelse av helseopplysninger, skal Datatilsynet informeres, jf. personopplysningsforskriften § 2-6. Videre skal pasienten opplysningene er knyttet til informeres.

§ 34 *Innsynsrett i logg og annen dokumentasjon av tilgang*

Den registrerte har rett til innsyn i dokumentasjon som gir informasjon om behandling av helseopplysninger som kan knyttes til vedkommende. For å gjøre tilgangsloggen forståelig for den registrerte skal det ved innsyn eller utskrift foretas sammenstilling med virksomhetens autorisasjonsregister og det behandlingsrettede helseregister tilgangsloggen gjelder. Sammenstillingen skal som et minimum inneholde følgende opplysninger:

a) navn, rolle og organisatorisk tilhørighet til den som har hatt tilgang
b) tidspunkt for den enkelte tilgang
c) hvilken type opplysninger det ble gitt tilgang til ved det enkelte tilfelle
d) registreringsdato for den enkelte opplysning det er gitt tilgang til ved det enkelte tilfelle.

Den registrerte har krav på en kortfattet forklaring av tekniske uttrykk og lignende dersom vedkommende ber om det. Den registrerte har også rett til å få utskrift av dokumentasjonen. Ved utskrift skal det kunne foretas sortering i henhold til den registrertes ønske.

Forespørsel om innsyn og rett til utskrift av dokumentasjon som nevnt skal besvares uten ugrunnet opphold og senest innen 30 dager etter henvendelsen kom inn.

Det kan ikke tas vederlag for utskrift av dokumentasjon etter denne bestemmelsen med mindre særlige forhold tilsier det.

Kapittel VIII Avsluttende bestemmelser

§ 35 *Straff*

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

§ 36 *Ikrafttredelse*

Forskriften trer i kraft fra det tidspunkt departementet bestemmer. En beslutning om ikrafttredelse kan omfatte hele eller deler av helsetjenesten. Departementet kan også beslutte at de enkelte bestemmelser i forskriften skal tre i kraft til forskjellig tid. Alle bestemmelsene i forskriften kapittel V må settes i kraft samtidig.