Helse- og omsorgsdepartementet

HØRING

Forslag til forskrift om tilgang til helseopplysninger mellom virksomheter

19. september 2014

Høringsfrist 14. november 2014

Helse- og omsorgsdepartementet

HØRING:

FORSLAG TIL FORSKRIFT OM TILGANG TIL HELSEOPPLYSNINGER MELLOM VIRKSOMHETER

1 Høringsnotatets hovedinnhold

Helse- og omsorgsdepartementet foreslår i dette høringsnotatet en ny forskrift som regulerer adgangen til å gi tilgang mellom virksomheter – til helseopplysninger i pasientjournaler og andre behandlingsrettede helseregistre for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Formålet med forskriften er at informasjonssikkerhet og personvern skal ivaretas ved tilgang mellom virksomheter. Forskriften skal bidra til at pasienter og brukere skal kunne ha tillit til at opplysningene i systemene blir sikret på best mulig måte og ikke tilflyter uvedkommende.

Forskriften skal hjemles i pasientjournalloven § 19 (lov 20. juni 2014 nr 42 om behandling av helseopplysninger ved ytelse av helsehjelp, se Prop. 72 L (2013–2014) og Innst. 295 L (2013–2014)). Pasientjournalloven skal, sammen med den nye helseregisterloven som ble vedtatt samme dag, erstatte helseregisterloven av 2001. De nye lovene er ennå ikke trådt i kraft. Forskriften skal tre i kraft samtidig med de nye lovene.

Pasientjournalloven legger til rette for flere alternative måter å gjøre opplysninger tilgjengelige på for helsepersonell når de yter helsehjelp. Loven skal bidra til at relevante og nødvendige helseopplysninger er tilgjengelige, uavhengig av hvem som gir helsehjelpen og uavhengig av hvor opplysningene om pasienten er registrert og lagret.

Dette høringsnotatet gjelder kun ett av disse alternativene; *tilgang* for helsepersonell mellom virksomheter. Med tilgang menes her at helsepersonell gis adgang til elektronisk å hente frem helseopplysninger om pasienter. Et annet alternativ etter loven er at virksomhetene samarbeider om et felles pasientjournallsystem, se pasientjournalloven § 9. Loven § 10 åpner også for, ved forskrift, å etablere nasjonale behandlingsrettede helseregistre på bestemte områder. Nasjonal kjernejournal er allerede under utprøving og vil kunne gi tilgang til et begrenset sett kritiske helseopplysninger, jf. pasientjournalloven § 13. Opplysningene kan også utleveres på samme måte som i dag, som for eksempel ved meldingsutveksling. Videre nevnes at alternative løsninger for realisering av Meld. St. 9 (2012-2013) *Én innbygger – én journal* utredes.

Vel så viktig er det at pasientene har enkel tilgang til helseopplysninger om seg selv. Departementet og Helsedirektoratet arbeider derfor også med løsninger for å gjøre pasientjournaler elektronisk tilgjengelige for innbyggerne ved bruk av portalen www.helsenorge.no. Dette arbeidet er ikke omfattet av forskriftsforslaget.

1.1 Pasientjournalloven § 19 - tilgjengelige helseopplysninger

Pasientjournalloven omfatter behandling av helseopplysninger som er nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner.

Loven skal legge til rette for god kvalitet i helsehjelpen og god pasient- og informasjonssikkerhet. Dette forutsetter at relevante og nødvendige opplysninger er tilgjengelige for helsepersonell når de yter helsehjelp, uavhengig av hvem som gir helsehjelpen og uavhengig av hvor opplysningene om pasienten er registrert og lagret.

Pasientjournalloven legger grunnlag for at helseopplysninger skal være tilgjengelige for helsepersonell i forbindelse med helsehjelp m.m., uavhengig av organisatorisk tilknytning. Loven har nye regler i § 19 som skal legge bedre til rette for informasjonsdeling mellom helsepersonell enn helseregisterloven av 2001. Det følger av bestemmelsen at relevante og nødvendige opplysninger skal være tilgjengelige for helsepersonell når det er nødvendig for å gi pasienten best mulig helsehjelp – uavhengig av hvor pasienten tidligere har mottatt helsehjelp. Helseopplysninger kan gjøres tilgjengelige enten ved tilgang eller ved utlevering. Begrensningene knyttet til virksomhetsgrensene i helseregisterloven av 2001 § 13 ble ikke videreført i pasientjournalloven, se nærmere i punkt 2.1.

Den databehandlingsansvarlige skal bestemme på hvilken måte helseopplysningene kan gjøres tilgjengelige. Dette omfatter også om helsepersonell i andre virksomheter skal kunne gis tilgang. Opplysninger skal, som i dag, bare kunne gjøres tilgjengelige dersom de er relevante og nødvendige for å yte helsehjelp og det er sikkerhet for at opplysningene ikke kommer på avveie.

Behovet helsepersonell har for helseopplysninger ved ytelse av helsehjelp vil avhenge av den helsehjelpen som skal gis i det enkelte tilfellet, pasientens sykdomsbilde og eventuelt tidligere sykdomshistorie. Hvor pasienten mottar helsehjelpen – og tidligere har mottatt helsehjelp - vil ofte være uten betydning. Det er behovet for informasjon om pasienten for å kunne yte nødvendig helsehjelp, som skal være førende for helsepersonellets tilgang. Hvordan opplysningene skal gjøres tilgjengelige må baseres på konkrete risikovurderinger. Målet er at relevante og nødvendige helseopplysninger skal være tilgjengelige for helsepersonell slik at pasienten kan tilbys helsehjelp av god kvalitet, samtidig som pasientens vern mot at opplysninger tilflyter uvedkommende ivaretas.

I pasientjournalloven § 19 fjerde ledd er det gitt en forskriftshjemmel til å gi nærmere bestemmelser om hvordan helseopplysninger i behandlingsrettede helseregistre kan gjøres tilgjengelige. Forskriften som foreslås i dette høringsnotatet gis i medhold av denne bestemmelsen.

1.2 Forslaget til forskrift

Departementets forslag til forskrift gjelder når en virksomhet lar andre virksomheter gi helsepersonell *tilgang* til behandlingsrettede helseregistre som virksomheten er ansvarlig for (tilgang mellom virksomheter). Med tilgang menes at helsepersonell gis adgang til elektronisk å hente frem helseopplysninger om pasienten. *Utlevering* av helseopplysninger reguleres av de vanlige reglene i pasientjournalloven, helsepersonelloven og pasient- og brukerrettighetsloven. Dette har sektoren lang erfaring med allerede, og det reiser ingen nye utfordringer med hensyn til personvern og informasjonssikkerhet. Forskriften skal derfor ikke gjelde utlevering.

Formålet med forskriften er at informasjonssikkerhet og personvern skal ivaretas ved tilgang mellom virksomheter. Forskriften skal bidra til god informasjonssikkerhet slik at pasienter og brukere skal kunne ha tillit til at opplysningene i systemene blir sikret på best mulig måte og ikke tilflyter uvedkommende.

Forslaget til forskrift omhandler hvilke krav som må være oppfylt i virksomhetene for å kunne gi tilgang. Forskriften skal bare regulere tilgang til journalsystemet fra andre virksomheter (ekstern tilgang/tilgang mellom virksomheter), og ikke tilgang internt i virksomheten eller tilgang mellom virksomheter som samarbeider om et felles journalsystem (intern tilgang). Når det gjelder felles journalsystemer er det i § 9 gitt en forskriftshjemmel for å kunne gi egne bestemmelser om samarbeidet. Slike forskrifter er ikke fastsatt eller foreslått.

Virksomheter som vil gi helsepersonell fra andre virksomheter tilgang til behandlingsrettede helseregistre, må inngå en særskilt avtale om dette. Avtalepartene skal vurdere risiko for pasientenes personvern som tilgang kan føre til. Vurderingene skal minst omfatte risiko for brudd på taushetsplikt og svekket informasjonssikkerhet. Avtalen må angi hvilke behovs- og risikovurderinger som ligger til grunn for avtalen. Avtalen må også regulere hvilke journalmoduler den omfatter, og rutiner og fordeling av oppgaver for å ivareta kravene i denne forskriften.

Forskriftsforslaget stiller krav om at virksomhetene skal ha særlige rutiner for hvordan informasjonssikkerheten skal ivaretas når det gis tilgang. Tilgangen skal ikke svekke informasjonssikkerheten ved behandling av helseopplysninger i noen av virksomhetene. En virksomhet som gir annen virksomhet tilgang, skal påse at denne virksomheten ivaretar kravene til informasjonssikkerhet ved behandling av opplysninger etter forskriften.

Virksomhetene skal ha tekniske og organisatoriske løsninger som kan avgrense tilgangen til helseopplysninger til hva som er relevant og nødvendig for ytelse, administrasjon og kvalitetssikring av helsehjelp til pasienten. Forskriften vil dermed pålegge begge de databehandlingsansvarlige å etablere nødvendige organisatoriske og tekniske tiltak for tildeling og kontroll av tilgangsrettigheter til helseopplysninger.

Departementet foreslår at det forskriftsfestes at løsningene minst skal ivareta at

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

Pasienten kan kreve at helseopplysninger som kan knyttes til vedkommende sperres. Virksomhetene må da ha tekniske løsninger som gjør dette mulig før det kan gis tilgang.

Tilgang skal også følges opp og kontrolleres. Departementet foreslår at det forskriftsfestes at den databehandlingsansvarlige løpende skal kontrollere hvem som har benyttet tilgangen og hentet frem helseopplysninger. Dersom kontrollen viser at noen har tilegnet seg helseopplysninger urettmessig, skal pasienten som opplysningene gjelder varsles.

Hvis kravene i forskriften ikke er oppfylt, kan det ikke gis tilgang. Opplysningene må i stedet gjøres tilgjengelige ved utlevering hvis vilkårene for dette er oppfylt.

Reglene i forskriften skal komme i tillegg til og utfylle, de alminnelige personvernreglene som gjelder ved behandling av helseopplysninger.

2 Bakgrunn

2.1 Tilgjengelige helseopplysninger

Relevante og nødvendige pasientopplysninger skal følge pasientene og være tilgjengelige for helsepersonell som yter helsehjelp, uavhengig av hvor pasienten tidligere har fått helsehjelp og hvordan sektoren til enhver tid er organisert. Tilgjengelig relevant informasjon er nødvendig for at helsepersonell raskt kan danne seg et helhetlig bilde av pasient eller bruker, ha godt grunnlag for å velge riktig utredning, behandling eller tjeneste og unngå feilbehandling eller overbehandling. Dette bidrar også til at pasienter og brukere i større grad slipper å gjenta opplysningene hver gang de oppsøker helse- og omsorgstjenesten.

Bestemmelsene om dokumentasjon og informasjonsdeling i helsesektoren er knyttet til målet om å yte helse- og omsorgstjenester av best mulig kvalitet. Samhandlingsreformen innebærer at kommunene har fått større ansvar for å tilby flere og mer spesialiserte helse- og omsorgstjenester til innbyggerne. Det forutsetter økt samarbeid mellom ulike behandlingssteder, uavhengig av om tjenestene skal leveres av kommunal helse- og omsorgstjeneste eller av spesialisthelsetjenesten (jf. Meld. St. nr. 47 (2006–2007), helse- og omsorgstjenesteloven og folkehelseloven).

Av pasientjournalloven § 19 følger at den databehandlingsansvarlige skal sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Helseopplysninger kan gjøres tilgjengelige enten ved at helsepersonell gis autorisasjon til selv å kunne hente frem opplysningene fra journalen (tilgang), eller ved at opplysningene utleveres. En utlevering av opplysningene kan skje manuelt eller elektronisk.

Det er den databehandlingsansvarlige som bestemmer hvordan helseopplysninger kan eller skal gjøres tilgjengelige. Opplysningene kan i forbindelse med helsehjelp bare gjøres tilgjengelige dersom de er relevante og nødvendige for å yte den aktuelle helsehjelpen. Videre kan de bare gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten og helsepersonellets taushetsplikt.

Lovens utgangspunkt er at det er det reelle sikkerhetsregimet og ikke virksomhetsgrenser som er avgjørende for hvordan opplysninger kan gjøres tilgjengelige. Loven skiller ikke mellom tilgang for helsepersonell tilknyttet virksomheten eller helsepersonell tilknyttet en annen virksomhet.

Etter helseregisterloven av 2001 § 13 var utgangspunktet at bare «den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet» kunne få tilgang til helseopplysninger. Ved lovendring i 2009 ble det gitt hjemmel til å gi forskrifter om tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomhetsgrenser. Tilgang i slike tilfeller kunne bare gis etter uttrykkelig samtykke, hvis ikke det i forskriften ble gjort unntak fra samtykkekravet. Helseinformasjonssikkerhetsforskriften har regler om tilgang på tvers av virksomhetsgrenser, som er gitt i medhold av helseregisterloven § 13. Denne forskriften er imidlertid ikke trådt i kraft.

Begrensningene knyttet til virksomhetsgrensene i helseregisterloven av 2001 § 13 ble ikke videreført i pasientjournalloven. I store virksomheter, eksempelvis større helseforetak med mange enheter og flere tusen ansatte, ga begrensningen i praksis liten ekstra sikkerhet. Samtidig har regelen ført til at helsepersonell ansatt i ulike virksomheter som skal behandle samme pasient ikke får effektiv tilgang til nødvendige journalopplysninger

Tidligere foregikk mesteparten av helsehjelpen til den enkelte pasienten i en og samme virksomhet, for eksempel innenfor ett sykehus. Det var derfor naturlig at det rettslige ansvaret for behandlingen av journalopplysningene var sentrert om virksomheten. Siden helseregisterloven av 2001 ble vedtatt har det skjedd store fremskritt i medisinsk kunnskap, økt spesialisering og omorganisering av helse- og omsorgstjenestene, noe som har medført endringer i pasientforløpene. Økt spesialisering og samhandling forutsetter at flere virksomheter er løpende involvert i helsehjelpen til en og samme pasient. Dette krever i større grad dokumentasjons- og informasjonsdeling og kvalitetssikring på tvers av de involverte virksomhetene for å sikre forsvarlig helsehjelp. Omorganisering og sammenslåing av virksomheter har også ført til at mange virksomheter har blitt vesentlig større enn det som tidligere var tilfelle, noe som også gjør virksomhetsbegrepet mindre egnet som grense for hvem som skal ha tilgang til opplysninger.

Forslaget om å gjøre helseopplysninger mer tilgjengelige ved å åpne for tilgang mellom virksomheter, fikk tilslutning fra flertallet under Stortingsbehandlingen. Komiteens flertall (medlemmene fra Arbeiderpartiet, Høyre, Fremskrittspartiet, Kristelig Folkeparti, Senterpartiet og Sosialistisk Venstreparti) viste til at både tidligere meldinger og lovproposisjonen peker på betydningen av at nødvendige helseopplysninger er tilgjengelige for å yte god helsehjelp. Flertallet viste også til at

> blant annet Kreftforeningen i høringen understreker at deling av pasientopplysninger er nødvendig for å få bedre informasjonsflyt mellom leger og til pasienter, sikrere diagnostikk og bedre oppfølging og kontinuitet i behandlingen.
>
> (Innst. 295 L (2013-2014)

2.2 Personvern ved behandling av helseopplysninger

Å lagre og bruke helseopplysninger er nødvendig for å kunne yte god helsehjelp til den enkelte. I Meld. St. 11 (2012–2013) *Personvern – utsikter og utfordringar* heter det:

> For å sikre tilliten og berekrafta til den offentlege helse- og omsorgstenesta må ein ta i bruk meir moderne og effektive hjelpemiddel for informasjon og kommunikasjon. Dette skal gjerast på ein måte som tek betre vare på samspelet mellom forventninga om godt integritetsvern og god pasienttryggleik. Ein må sikre heilskapelege pasientgangar, og det må leggjast til rette for samhandling mellom helsearbeidarar, som blir alt meir spesialiserte.

Stortinget sluttet seg til dette i sin behandling av meldingen den 28. mai 2013.

I helse- og omsorgssektoren har det vært lagt særlig vekt på konfidensialitetsaspektet ved personvern. Dette har sammenheng med den sterke taushetsplikten som gjelder for helse-

personell. Dette har bidratt til at regelverket har vært innrettet mot å hindre uautorisert bruk og at uvedkommende får tilgang til helseopplysninger.

Personvern er imidlertid mer enn hensynet til konfidensialitet. Et formål med personvernlovgivningen er også å sikre at personopplysninger blir brukt på rett måte. Viktige personvernhensyn er at opplysninger skal være korrekte og oppdaterte, og tilgjengelige for rett person til rett tid. Godt personvern krever at alle hensynene ivaretas. I pasientbehandling kan tilgang til journalopplysninger være kritisk. Manglende tilgjengelighet til oppdaterte og korrekte opplysninger om pasienten kan føre til dårligere pasientbehandling og i verste fall feil behandling eller skade.

Innebygget personvern betyr at hensynet til personvernet skal være en del av alle ledd i utviklingen og bruken av informasjonsteknologi. Dette betyr for eksempel at forhåndsdefinerte standardinnstillinger i teknologisk utstyr, system og program settes til det mest personvernvennlige nivået. På denne måten er brukeren sikret et best mulig personvern selv om han eller hun ikke gjør noen endringer i forhåndsdefinerte brukerinnstillinger. For IKT i helse- og omsorgssektoren innebærer dette at pasientene skal være sikret et godt personvern uten at den enkelte selv eller helsepersonell aktivt må endre innstillinger (se Meld. St. 11 (2012–2013) *Personvern – utsikter og utfordringar*).

Det er et mål at prinsippene for innebygget personvern skal inngå som naturlige elementer i utviklingen og implementeringen av elektroniske løsninger i hele sektoren. Ved at personvern og funksjonalitet ses i sammenheng i utviklings - og implementeringsfasen vil det være mindre risiko for at personvernfremmende funksjonalitet slås av for at systemet skal fungere mer effektivt.

Lovgivning og regulering er imidlertid ikke tilstrekkelig for å kunne sikre et godt personvern. Integrering av personvern må være en del av det daglige arbeidet.

3 Gjeldende rett - informasjonsdeling mellom helsepersonell

Pasientjournalloven er en spesiallov for behandling av helseopplysninger som er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner. Pasientjournalloven ble vedtatt av Stortinget 20. juni 2014, men er ikke trådt i kraft. Loven vil tre i kraft samtidig med at forskriften som her er på høring, trer i kraft. Pasientjournalloven omtales i det følgende som gjeldende rett.

Ettert pasientjournalloven § 19 skal helseopplysninger gjøres tilgjengelige for helsepersonell og annet samarbeidende helsepersonell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner. Bestemmelsen gjelder personell innenfor egen virksomhet, så vel som utenfor egen virksomhet. Det er bare opplysninger som er relevante og nødvendige som kan gjøres tilgjengelige.

Helseopplysninger kan gjøres tilgjengelige enten ved 1) at helsepersonell gis autorisasjon til selv å kunne hente frem opplysningene, eller ved 2) at opplysningene utleveres. En utlevering av opplysningene kan skje manuelt eller elektronisk.

Tilgjengeliggjøring av helseopplysninger reguleres av regler om taushetsplikt, sperring av opplysninger og generelle personvernregler, både i pasientjournalloven og andre lover. Opplysninger i behandlingsrettede helseregistre kan bare gjøres tilgjengelige i lovbestemte tilfeller. Aktuelle bestemmelser ved ytelse av helsehjelp er helsepersonelloven §§ 25 og 45, og § 26 for administrering og kvalitessikring av helsehjelpen. Kravene til informasjonssikkerhet, risikovurderinger og internkontroll skal også sikre at opplysninger om den enkelte pasient ikke gjøres tilgjengelige for uvedkommende.

De grunnleggende kravene til personvern og informasjonssikkerhet ved tilgjengeliggjøring av helseopplysninger følger av pasientjournalloven, personopplysningsloven, helsepersonelloven mv. Hva disse kravene innebærer når det gis tilgang mellom virksomheter, er drøftet i forarbeidene til pasientjournalloven (Prop 72 L (2013–2014) punkt 11.3). Det forutsettes i Prop. 72 L (20013–2014) at det vil bli utarbeidet forskrifter med nærmere regler om hvordan opplysningene kan gjøres tilgjengelige, se punkt 3.5.4.

3.1 Taushetsplikt

Reglene om taushetsplikt er bestemmende for når og til hvem helseopplysninger kan gjøres tilgjengelige for. Enhver som behandler helseopplysninger etter loven har taushetsplikt, jf. pasientjournalloven § 15 som viser til helsepersonelloven §§ 21 flg. I tillegg til en plikt til å tie, innebærer taushetsplikten en aktiv plikt til å hindre at helseopplysninger gjøres tilgjengelige for uvedkommende. Det er også forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger fra behandlingsrettede helseregistre uten at det er begrunnet i helse- og omsorgstjenester til den enkelte, administrasjon av slike tjenester eller har særskilt hjemmel i lov eller forskrift, jf. pasientjournalloven § 16. Unntak fra taushetsplikt må ha særlig hjemmel.

3.2 Hvordan opplysningene kan gjøres tilgjengelige

Helsepersonell skal gis relevante og nødvendige opplysninger om pasienten de skal yte helsehjelp til, samtidig som de ikke skal gis opplysninger ut over det som er nødvendig eller opplysninger om andre pasienter. Pasientjournalloven § 19 bestemmer ikke hvordan opplysningene skal gjøres tilgjengelige. Det er den databehandlingsansvarlige som bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige, for eksempel om det skal gis tilgang til virksomhetens journalsystem eller om opplysningene skal utleveres på papir eller ved elektronisk oversendelse. Den databehandlingsansvarlige må derfor foreta en nøye vurdering av på hvilken måte opplysninger skal kunne deles mellom virksomheter.

Måten databehandlingsansvarlige gir helsepersonell opplysninger på kan være forskjellig for ulike typer personell basert på blant annet hyppigheten av behov for opplysninger, hvilke type opplysninger det er behov for og hvilke sikkerhetstiltak som er mulig å iverksette. Personell som meget sjelden har behov for innsyn i opplysninger om en pasient kan kanskje enklest få opplysningene utlevert, mens personell som til daglig har behov for opplysninger kan gis tillatelse til elektronisk å hente dem frem. Opplysninger som oppfattes som mindre følsomme, slik som opplysninger om stråledoser, blodtype eller komplikasjoner ved intubering, kan være mer egnet for tilgang enn opplysninger som pasienten oppfatter som mer følsomme. Dette er vurderinger den databehandlings-ansvarlige er nærmest til å foreta.

Uavhengig av hvordan opplysningene gis skal det fremgå av journalen at annet helse-personell er gitt helseopplysninger, jf. helsepersonelloven § 45 og pasientjournal-forskriften § 8 bokstav l. Spørsmålet om deling av helseopplysninger skal være en del av kommunikasjonen mellom pasienten og helsepersonellet. Pasienten skal informeres om dette i samsvar med pasientjournalloven § 18 og personopplysningsloven §§ 19 og 20.

Helseopplysninger i journalen kan ikke gjøres tilgjengelige hvis pasienten motsetter seg det, jf. pasientjournalloven § 17. Den registrertes rett til å motsette seg at opplysninger gjøres tilgjengelige for annet helsepersonell omfatter helseopplysninger i alle typer behandlingsrettede helseregistre.

3.3 Kravet til forsvarlige journal- og informasjonssystemer

Virksomhetens journalsystemer skal understøtte pasientforløp i klinisk praksis. De skal være utformet og organisert slik at krav til tilgjengeliggjøring av opplysninger, informasjonssikkerhet mv. kan oppfylles, jf. pasientjournalloven § 7.

Helseinstitusjoner som omfattes av spesialisthelsetjenesteloven skal sørge for at journal- og informasjonssystemene ved institusjonen er forsvarlige, jf. § 3-2. Virksomheten skal ta hensyn til behovet for effektiv elektronisk samhandling ved anskaffelse og videreutvikling av sine journal- og informasjonssystemer.

Helse- og omsorgstjenesteloven har bestemmelser som slår fast kommunens overordnede ansvar for helse- og omsorgstjenester. Kommunen skal blant annet sørge for at journal- og informasjonssystemene i virksomheten er forsvarlige, jf. helse- og omsorgstjenesteloven

§ 5-10. Kommunen skal ta hensyn til behovet for effektiv elektronisk samhandling ved anskaffelse og videreutvikling av sine journal- og informasjonssystemer. Dette gjelder tilsvarende for virksomheter som har avtale med kommunen om å yte helse- og omsorgstjenester.

3.4 Informasjonssikkerhet

Det er avgjørende for et velfungerende helsetjenestetilbud at pasientene har tillit til at informasjonen om dem blir håndtert på en god måte. Dersom befolkningen kvier seg for å bruke helse- og omsorgstjenesten av frykt for at opplysninger om dem skal komme på avveie, vil vi ha store utfordringer med å gi et godt helse- og omsorgstjenestetilbud.

Etter pasientjournalloven § 22 skal den databehandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet. Informasjonssikkerhet handler om å sikre opplysningenes konfidensialitet, integritet og tilgjengelighet. Tilfredsstillende informasjonssikkerhet omfatter også elementer som systemets oppetid, motstandsdyktighet mot hacking (datasnoking) internt fra så vel innenfra som utenfra osv.

Virksomhetens egne sikkerhetskrav må knyttes til virksomhetens oppgaver, organisering, arbeidsprosesser og andre forhold som påvirker opplysningenes sikkerhet. Flere regelverk stiller krav til sikring av informasjon.

Et gjennomgående krav er at sikringen skal være basert på risikovurderinger. Informasjonssikkerhet er en dynamisk prosess, og de sikkerhetstiltakene som brukes i dag er ikke nødvendigvis tilfredsstillende i fremtiden, ved endret organisasjonsstruktur, endrede arbeidsprosesser osv. Bruk av IKT-systemer i helse- og omsorgssektoren er i stadig utvikling og vil reise nye sikkerhetsutfordringer som må ivaretas.

3.5 Vilkår for tilgang mellom virksomheter

I det følgende gjøres det rede for vilkårene for å kunne gi tilgang mellom virksomheter. Krav til informasjonssikkerhet, tilgangsstyring, pasientens selvbestemmelsesrett og internkontroll som vilkår for å gi tilgang mellom virksomheter, følger av pasientjournalloven § 19 om tilgjengeliggjøring av helseopplysninger, i tillegg til de øvrige kravene i pasientjournalloven, personopplysningsloven og helsepersonelloven. Det er ikke gitt egne regler om tilgang. Kravene som gjelder ved tilgang mellom virksomheter må utledes av de generelle reglene som gjelder både utlevering og tilgang, ved så vel internt som ekstern informasjonsdeling. I forarbeidene til pasientjournalloven er det gjort nærmere rede for hva disse kravene innebærer ved tilgang mellom virksomheter (Prop. 72 L (2013-2014) punkt 11.3.7).

3.5.1 Bare opplysninger som er relevante og nødvendige for helsehjelpen

Det overordnede kravet er at helseopplysninger bare skal gjøres tilgjengelige for helsepersonell som trenger opplysningene i en aktuell pasientbehandling. Taushetsplikten er avgjørende for hvilke opplysninger som kan gjøres tilgjengelige for hvem. Opplysninger

skal kun gjøres tilgjengelige for helsepersonell som har et tjenstlig behov for opplysningene. Dette er formulert i pasientjournalloven § 19 som et krav om at opplysningene skal være relevante og nødvendige for å yte, kvalitetssikre eller administrere helsehjelpen til den enkelte pasient.

3.5.2 Risikovurdering og tilgangsstyring

En virksomhet som vil gi andre virksomheter tilgang må ha vurdert risikoen ved dette og ha iverksatt eventuelle nødvendige tiltak for å begrense risikoen. Virksomheten må vurdere om kravene til konfidensialitet og tilgjengelighet er ivaretatt. Virksomheten må sikre at helsepersonell bare gis tilgang til opplysninger om pasientene som er nødvendige og relevante for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt. Videre må helsepersonell som gis tilgang kunne identifisere seg for systemet på individnivå.

Virksomhetene har ansvaret for å vurdere akseptabelt nivå når det gjelder kravene for tilgjengelighet og konfidensialitet i helsetjenesten, før opplysninger gjøres tilgjengelige. Dette følger av databehandlingsansvaret. En databehandlingsansvarlig kan derfor bare gi tilgang til virksomheter som har etablert tilfredsstillende system for tilgangsstyring og kontroll. Den databehandlingsansvarlige må vurdere om det i virksomheten som får tilgang, finnes systemer som i tilstrekkelig grad ivaretar taushetsplikten og lovens øvrige krav. Denne virksomheten må ha tilstrekkelig tilgangsstyring og andre sikkerhetstiltak slik at den totale sikkerheten ikke blir dårligere. Hvis sikkerheten ikke er god nok, må helseopplysningene i stedet gjøres tilgjengelige ved at opplysningene utleveres.

I praksis vil tilgang utenfra kunne skje ved at de involverte virksomhetene avtaler og organiserer dette på virksomhetsnivå. Dette inkluderer fordeling av roller og oppgaver for å sørge for tilfredsstillende sikkerhet og ivaretakelse av pasientens rettigheter. Det lovpålagte ansvaret kan ikke avtales bort, men gjennomføring av oppgavene og ansvarsforholdet mellom avtalepartene bør fremgå av avtalen. Det er ikke nødvendig at tilgangen avtales fra gang til gang for hver pasient. Heller ikke er det nødvendig å navngi på forhånd helsepersonellet som kan gis tilgang.

Den databehandlingsansvarlige i virksomheter som gis tilgang, får et selvstendig ansvar for å styre tilgangen i egen virksomhet. Det følger av personopplysningsforskriften § 2-15 at den databehandlingsansvarlige bare kan overføre helseopplysninger elektronisk til virksomheter som har tilfredsstillende informasjonssikkerhet. Denne virksomheten vil ha ansvaret for sin interne tilgangsstyring og for at de øvrige vilkårene for å få opplysningene er oppfylt. Blant annet har helsepersonell bare tillatelse til elektronisk å hente frem nødvendige og relevante opplysninger om pasienter de har et behandlingsforhold til.

Det å gi helsepersonell tillatelse til selv å hente frem relevante og nødvendige helseopplysninger om en pasient, krever at den databehandlingsansvarlige har systemer som kan understøtte dette. Virksomheten må sette inn tilstrekkelig med tiltak for tilgangsstyring. Videre stilles det krav til oppfølging og kontroll. Virksomheten må følge opp egne hendelser, kontrollere bruken av systemene og sørge for klar ansvarsfordeling for oppfølging av hendelser som involverer flere virksomheter. Helsepersonell må få opp-

læring i bruken av systemene. Virksomheten må ha tiltak som kan avdekke eventuell urettmessig tilegnelse av opplysninger.

3.5.3 Pasientens selvbestemmelse og rett til informasjon

I pasient- og brukerrettighetsloven er det lovfestet et generelt krav om samtykke som rettsgrunnlag for å yte helsehjelp. Det følger av § 4-2 at samtykke til helsehjelp kan gis uttrykkelig eller stilltiende. Videre i bestemmelsen fastslås den praktiske hovedregelen om samtykke ved konkludent atferd. Det vil si at pasienten ved sin handlemåte tilkjennegir at vedkommende samtykker til helsehjelp.

Pasientens samtykke til helsehjelp innebærer som hovedregel også forutsetningsvis at helsepersonell kan innhente helseopplysninger som anses nødvendige for å yte helsehjelp, jf. helsepersonelloven §§ 25 og 45. Helsehjelp innebærer også at helsepersonellet kan innhente opplysninger som er registrert ved andre virksomheter der pasienten tidligere har fått helsehjelp, dersom det er nødvendig for å yte helsehjelpen. Pasientens adgang til å motsette seg dette følger av pasientjournalloven § 17 bokstav a og helsepersonelloven §§ 25 og 45. Dette gjelder selv om opplysningene er nødvendige for å yte helsehjelp.

Det kreves ikke uttrykkelig samtykke fra pasienten for å gi tilgang mellom virksomheter. Forutsetningen i helseregisterloven av 2001 § 13 om et frivillig, uttrykkelig og informert samtykke for at samarbeidende helsepersonell i andre virksomheter skal kunne få tilgang, ble ikke videreført i pasientjournalloven (Prop 72 L (2013–2014 punkt 11.3.5 og 11.3.6). Det ble vist til at helsepersonellovens samtykkekrav fortsatt skal gjelde og at pasienten vil ha rett til å motsette seg tilgang. Dette fikk støtte av flertallet i Stortinget:

> Komiteen har forståelse for at dette kan være en ordning som sikrer pasientens råderett over egne journalopplysninger.
>
> Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Fremskrittspartiet og Kristelig Folkeparti, mener imidlertid at det vil medføre unødig tidsbruk når alle journaler før bruk må avsjekkes mot et forventet aktivt samtykke. Flertallet slutter seg derfor til departementets forslag om å lovfeste pasientens rett til å motsette seg at helseopplysninger i journalen gjøres tilgjengelig for annet helsepersonell, se forslag til pasientjournallov § 17 bokstav a, der det henvises til helsepersonelloven §§ 25 og 45, samt pasient- og brukerrettighetsloven § 5-3. Det vil etter komiteens mening være avgjørende at den enkelte pasient/bruker får god informasjon om hva reservasjonsretten innebærer, hva slags opplysninger man kan reservere for innsyn, og hvordan helsevesenet håndterer og sikrer slike opplysninger. (Innst. 295 L (2013-2014)).

Pasienten har etter pasientjournalloven § 18 rett til informasjon og innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logg). Pasienten skal så langt råd er gjøres kjent med at det utleveres opplysninger i samarbeidsøyemed (Ot.prp. nr. 13 (1998–1999) merknadene til §§ 25 og 45 i kapittel 12). Pasienten skal også informeres om retten til å motsette seg behandling av helseopplysninger, og hvordan dette kan gjøres rent praktisk.

Dette følger av personopplysningsloven § 19 første ledd bokstav e om informasjonsplikt med hensyn til forhold som gjør den registrerte i stand til å bruke sine rettigheter etter loven på best mulig måte.

3.5.4 Forskriftshjemmel

Pasientjournalloven § 19 gir hjemmel til å gi nærmere bestemmelser om hvordan helseopplysnimger i behandlingsrettede helseregistre kan gjøres tilgjengelige. Departementet forutsatte at det skulle gis forskrifter om tilgang mellom virksomheter før pasientjournalloven § 19 om tilgjengeliggjøring av helseopplysninger ved helsehjelp trer i kraft:

> Departementet er enig i at det kan være behov for å regulere sikkerhetskravene nærmere hvis virksomheter skal gi personell i andre virksomheter tilgang til konkrete opplysninger fra journalen. Det bør fastsettes nærmere regler for å sikre at det i slike situasjoner finnes systemer som i tilstrekkelig grad ivaretar taushetsplikten, konfidensialitet og lovens øvrige krav.
>
> Departementet har derfor kommet til at det skal utarbeides forskrift om hvordan informasjon kan gjøres tilgjengelig og deles på en måte som sikrer personvernet og begrenser tilgangen til det som er nødvendig, se forslaget til pasientjournallov § 19 siste ledd. Forskriften skal gi regler som utfyller lovens vilkår for å kunne gjøre opplysningene tilgjengelige for personell i andre virksomheter. Departementet vil blant annet sette krav til de ansvarlige for virksomheten og til risikovurderingen når det gis tilgang til behandlingsrettede helseregistre for helsepersonell i andre virksomheter. Slik forskrift skal tre i kraft samtidig med ny pasientjournallov. (Prop. 72 L (2013–2014) punkt 11.3)

Departementets forslag om å åpne for tilgang mellom virksomheter fikk flertallets tilslutning under Stortingsbehandlingen av pasientjournalloven. Stortinget fremhevet samtidig personvernkravene og behovet for forskrifter:

> Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Fremskrittspartiet, Kristelig Folkeparti, Senterpartiet og Sosialistisk Venstreparti, mener at de teknologiske løsningene som i dag er tilgjengelig, også vil kunne gi et godt vern for personsensitive opplysninger i pasientjournal og helseregistre.
>
> Flertallet vil understreke at behandling og bruk av helseopplysninger alltid må skje på en måte som sikrer pasienters og brukeres personvern.
>
> (…)
>
> Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Fremskrittspartiet, Kristelig Folkeparti og Senterpartiet, påpeker at lovforslaget forutsetter at deling av informasjon krever en viss grad av struktur. Det vil si at databehandlingsansvarlige som ikke har journaler som er tilstrekkelig strukturerte, heller ikke kan åpne for tilgang mellom virksomheter.
>
> (Innst. 295 L (2013–2014), komiteens merknader i innledningen)

Flertallet i komiteen forutsatte videre at bare virksomheter som har moderne og sikre journalsystemer, vil kunne ta i bruk de mulighetene som loven gir. Samtidig ble det bemerket at

> departementet vil stille krav om at virksomheter som ønsker å ta i bruk de mulighetene loven åpner for, vil måtte påregne kostnader for tilpasning av de tekniske systemene og eventuelle organisatoriske endringer.
>
> (Innst. 295 L (2013–2014), komiteens merknader om IKT og informasjonssikkerhet)

Komiteen fremholdt at departementet kan gi forskrift om nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger etter loven. Dette innebærer ifølge flertallet

> bestemmelser blant annet om:
>
> - tilgangsstyring og tilgangskontroll
> - system for administrasjon av autorisasjoner for tilgang til helseopplysninger
> - register over og kontroll av autorisasjon
> - opplæring av ansatte
> - krav til kommunikasjonen
> - autentiseringsløsning
> - elektronisk signatur
> - funksjon for at pasienten kan motsette seg utlevering eller tilgang til helseopplysninger
> - sporbarhet
> - langtidslagring
> - nærmere krav til dokumentasjon av tilgang til og utlevering av helseopplysninger (logg)
> - innhold og lagringstid for logg
>
> Flertallet legger til grunn at departementet gjennom forskrift vil stille tydelige krav i tråd med dette for å sikre at både innhold, teknologi og kultur i helsetjenesten er innrettet slik at det understøtter lovens intensjon. Flertallet vil understreke betydningen av at regelverket til enhver tid ivaretar et godt og framtidsrettet personvern, at man sørger for gode og forutsigbare rammebetingelser for utviklere av systemer og legger til rette for den teknologiske utviklingen i sektoren. Her må det spesielt legges vekt på sikkerhet og personvern i all kommunikasjon der pasientopplysninger er involvert, og at løsningene må være brukervennlige og effektive. Flertallet vil understreke viktigheten av at departementet påser at dette arbeidet prioriteres i hele helsesektoren.
>
> (Innst. 295 L (2013–2014), komiteens merknader om IKT og informasjonssikkerhet)

4 Regulering i andre land

Elektroniske pasientjournalsystemer, både i primær- og spesialisthelsetjenesten, er tatt i bruk og har stor utbredelse i flere andre land. I flere land er det er også lagt til rette for at helseopplysninger skal kunne følge pasienten i et behandlingsforløp.

4.1 Danmark

Danmark har, som Norge, lokale elektroniske pasientjournalsystemer i den enkelte virksomhet. Regelverket legger til rette for at det kan samarbeides om journalløsninger for en pasient for flere offentlige sykehus i en region.

Sunnhetsloven («Sundhedsloven» fra 2007) har som formål å fremme befolkningens helse samt å forebygge og behandle sykdom, lidelse og funksjonsnedsettelse for den enkelte. Den inneholder blant annet bestemmelser om organisering av helsetjenesten og behandling av pasientopplysninger.

I dag har helsepersonell adgang til elektronisk å innhente opplysninger om en pasients helsetilstand, private forhold og andre fortrolige opplysninger, når det er nødvendig i forbindelse med aktuell behandling av pasienten. Dette gjelder uavhengig av virksomhetsgrenser og hvor pasienten tidligere har fått helsehjelp. Opplysningene kan innhentes i felles nasjonale registre eller hos andre i helsevesenet. Annet helsepersonell kan i forskrift gis samme adgang til å innhente opplysninger elektronisk. Det foreligger ikke et krav om samtykke fra pasienten for å innhente disse opplysningene, men pasienten har rett til å reservere seg mot at opplysningene innhentes. Reservasjonsretten gjelder informasjonsdeling både internt i virksomheten og mellom virksomheter.

4.2 Sverige

I Sverige benyttes det lokale elektroniske pasientjournalsystemer i den enkelte virksomhet. Det er imidlertid etablert nasjonale tjenester for å sikre kommunikasjon mellom virksomheter, blant annet Nationell Pasientöversikt (NPÖ), elektroniske resepter mm.

Reglene for behandling av pasientopplysninger i helsetjenesten er samlet i pasientopplysningsloven («patientdatalagen» fra 2008). Formålet med loven er å få en samlet regulering av informasjonshåndteringen i helsesektoren, og legge til rette for nødvendig informasjonsdeling mellom behandlere samtidig som både hensynet til personvern og pasientsikkerhet ivaretas.

Utgangspunktet er at opplysninger kan deles elektronisk med helsepersonell i andre virksomheter, men pasienten kan motsette seg dette ved å sperre opplysningene. Da vil ikke helsepersonell i andre virksomheter ha tilgang til dem. I tillegg skal pasienten ha gitt sitt samtykke til behandling i en gitt behandlingssituasjon før helsepersonell gjør oppslag i journalsystem i annen virksomhet.

Loven regulerer grunnleggende prinsipper som gjelder for håndteringen av pasientopplysninger innenfor helsesektoren. Den nærmere detaljreguleringen skjer i forskrifts form.

4.3 Finland

I Finland benyttes flere ulike journalsystemer, men det er innført krav om at alle pasient-opplysninger skal lagres i én sentral database, det såkalte pasientarkivet. Arkivet driftes av Folkepensionsanstalten (Kela) og er en del av de nasjonale elektroniske tjenestene (KanTA).

Klientopplysningsloven («Lagen om klientuppgifter» fra 2007) skal fremme sikker elektronisk behandling av pasientopplysninger innen helse- og sosialtjenesten, og etablere det nasjonale arkivet. Loven krever at alle elektroniske pasientjournalsystemer skal ha en datastruktur som muliggjør bruk, utlevering, lagring og beskyttelse av elektroniske journaldokumenter i det landsdekkende arkivet. Lagring i det sentrale arkivet skal skje når pasientbehandlingen er ferdig lokalt og pasienten skrives ut.

Det er kun helsepersonell med reelt behov for pasientens opplysninger som får tilgang til opplysninger i det sentrale arkivet, og strukturen i journalsystemet skal kunne begrenses slik at behandler kun får tilgang til pasientopplysninger som er nødvendig for å yte den konkrete tjenesten. Alle oppslag i journalsystemer skal registreres (logges).

Videre fastsetter loven at utlevering av pasientopplysninger fra arkivet kan skje etter pasientens samtykke eller med hjemmel i lov. Pasienten kan samtykke til utlevering av informasjon for en enkelt hendelse (for eksempel pasientbehandling) eller for et helt behandlingsforløp. Samtykket kan når som helst trekkes tilbake.

5 Departementets vurderinger

Departementet foreslår at det gis nærmere bestemmelser i forskrift som fastsetter vilkår for tilgang mellom virksomheter til behandlingsrettede helseregistre. Med tilgang menes at helsepersonell gis adgang til elektronisk å hente frem helseopplysninger om pasienter.

5.1 Behovet for nærmere regler

Forskriften skal ifølge departementets forslag hjemles i den nye pasientjournalloven § 19 om helseopplysninger ved helsehjelp. Det følger av denne bestemmelsen at den databehandlingsansvarlige skal sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Den databehandlingsansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Det er en forutsetning at det gjøres innenfor rammene av taushetsplikten og på en måte som ivaretar kravene informasjonssikkerhet. Se nærmere i punkt 3.5.

Pasientjournalloven § 19 åpner for å gi helsepersonell tilgang til et behandlingsrettet helseregister uavhengig av helsepersonellets organisatoriske tilknytning. Opplysningene kan gjøres tilgjengelige ved at det gis tilgang mellom virksomheter. Forskriften som foreslås i dette høringsnotatet skal gi nærmere regler om hvordan opplysningene kan gjøres tilgjengelige.

Tilgang til helseopplysninger mellom virksomheter gir personvernutfordringer som virksomhetene ikke har erfaring med. I forbindelse med den offentlige høringen av forslaget til pasientjournallov var det flere, også fra de store sykehusene som særlig ønsket lovendringen, som mente at det burde utarbeides nærmere regler om hvilke tiltak og forutsetninger som måtte være på plass før det kunne gis tilgang mellom virksomheter. Departementet og flertallet i komiteen under Stortingsbehandlingen la til grunn at det skulle vedtas slike forskrifter, se punkt 3.7.

Departementet mener at det ikke vil være hensiktsmessig med konkrete tekniske krav i forskriften. Vi må ha fleksible regler som tar høyde for den teknologiske utviklingen og at de skal gjelde for ulike virksomheter, behov og løsninger. I forslaget til forskrift er det derfor lagt særlig vekt på organisatoriske forhold og funksjonskrav fremfor konkrete tekniske krav til løsningene. Det stilles krav til vurderinger, rutiner, kontroll osv. Flere av kravene, som for eksempel pasientens rett til sperring og til innsyn i logg, forutsetter imidlertid at virksomhetene også har tekniske løsninger som gjør dette mulig.

5.2 Ulike former for informasjonsdeling

Når flere virksomheter behandler samme pasient i samme behandlingsforløp, kan tilgjengelighet for nødvendige og relevante helseopplysninger og effektiv informasjonsutveksling ivaretas på flere måter. Pasientjournalloven åpner for ulike måter å dele informasjonen på mellom virksomheter.

Opplysninger i virksomhetens journaler kan gjøres tilgjengelige for annet helsepersonell ved at opplysninger *utleveres* eller ved at helsepersonell gis *tilgang*. Helseregisterloven av 2001 fikk ved lov 19. juni 2009 nr. 68, et tillegg med hjemmel til å vedta forskrifter om tilgang mellom virksomheter etter samtykke fra pasienten. Helseinformasjonssikkerhets-forskriften fra 2011, som har regler om dette, er imidlertid ikke trådt i kraft. Opplysningene kunne dermed bare gjøres tilgjengelige for annet helsepersonell i andre virksomheter ved å utlevere opplysningene ved meldinger, brev, telefon osv. Pasient-journalloven § 19 åpner for at opplysningene også kan gjøres tilgjengelige ved at det gis tilgang til journalen mellom virksomheter uten å innhente pasientens samtykke først.

En annen måte å dele informasjon mellom virksomheter er at to eller flere virksomheter samarbeider om et felles journalsystem for virksomhetene, jf. pasientjournalloven § 9. Et felles journalsystem kommer i stedet for virksomhetens egen journal. Forskriften som departementet nå foreslår vil imidlertid ikke regulere samarbeid mellom virksomheter om behandlingsrettede helseregistre, se punkt 5.5 om forskriftens saklige virkeområde. Det er i stedet gitt en egen forskriftshjemmel i pasientjournalloven § 9 for å regulere samarbeidet. Slike forskrifter er ikke fastsatt.

Hvilken måte som velges for informasjonsdelingen vil avhenge av virksomhetenes behov for samarbeid og helsehjelpens (behandlingens) karakter, de organisatoriske og teknologiske løsningene og hvordan de ulike måtene kan ivareta taushetsplikten og oppfylle kravene til informasjonssikkerhet og personvern.

5.3 Sammenhengen med dokumentasjonsplikten

All pasientbehandling skal journalføres i samsvar med dokumentasjonsplikten i helse-personelloven §§ 39 og 40. Alle som bidrar i helsehjelpen til en pasient, må imidlertid ikke dokumentere. Dette følger av helsepersonelloven § 39 andre punktum som fastslår at plikten til å føre journal ikke gjelder for samarbeidende helsepersonell som gir hjelp etter instruksjon eller rettledning fra annet helsepersonell.

Det skal som hovedregel kun være én journal i hver virksomhet om samme pasient, for å unngå dobbeltregistrering. Om spesialisten skal føre journal og hvilke journalsystem opplysningene skal føres i, vil avhenge av hvilken virksomhet spesialisten er tilknyttet og utfører arbeidet for.

Dokumentasjonsplikten etter helsepersonelloven §§ 39 og 40 skal gjennomføres i den journalen virksomheter etablerer for dette formålet. Helsepersonell verken kan eller skal gjennomføre sin dokumentasjonsplikt i andre virksomheters journaler som det gis tilgang til.

5.4 Formål – informasjonssikkerhet og personvern

Departementet foreslår at formålet med forskriften skal være at informasjonssikkerhet og personvern blir ivaretatt ved tilgang mellom virksomheter til behandlingsrettede helse-registre, se formålsbestemmelsen i forskriften § 1.

Det er en viktig forutsetning for å kunne gi forsvarlig helsehjelp, at opplysninger om pasienten er tilgjengelige der pasienten får helsehjelp. Det er viktig at helsepersonellet gis enkel tilgang til nødvendige og relevante opplysninger slik at pasientens behov for helsehjelp kan ivaretas, og at informasjonsutvekslingen skjer på en effektiv og sikker måte. Kravet om tilgjengelighet av helseopplysninger er regulert i pasientjournalloven § 19 og helsepersonelloven.

For at helsetjenesten skal kunne yte gode helsetjenester til pasientene er det også viktig at pasientene har tillit til helsetjenesten. Denne tilliten må også gjelde behandlingen av pasientopplysninger. Pasientopplysninger må være tilgjengelige for helsepersonell som har behov for det for å gi helsehjelp til pasienten. Samtidig skal opplysningene ikke komme i hendene på uvedkommende. Det skal tas hensyn til at mange pasienter ikke ønsker at andre skal få kunnskap om ens sykdom og plager, bortsett fra de som må vite det av hensyn til helsehjelpen. Det er derfor viktig at pasientens rett til konfidensialitet og selvbestemmelse ivaretas dersom det gis tilgang. Pasientene skal få informasjon om at ansatte i andre virksomheter kan gis tilgang til journalen, se punkt 5.9.2 og 5.10. Pasientens rett til å motsette seg at opplysninger tilgjengeliggjøres må gjennomføres i systemet, se punkt 5.9.2. Videre skal all tilgang til systemet logges, slik at pasienten skal kunne få se hvem som har hentet frem opplysninger fra registeret, se punkt 5.10 og 5.12.

Ivaretakelse av disse forutsetningene krever god informasjonssikkerhet. Dagens kommunikasjons- og informasjonsteknologi gjør det mulig å sikre opplysningene, inkludert kontrollmuligheter, og å ivareta hensynet til pasientens rett til konfidensialitet ved tilgang til helseopplysninger mellom virksomheter.

5.5 Definisjoner

Departementet har vurdert om det er behov for en egen bestemmelse som definerer nøkkelbegreper i forskriften. Begrep som helsehjelp, databehandlingsansvarlig og behandlingsrettet helseregister er definert i pasientjournalloven. Disse begrepene skal forstås på samme måte i forskriften. Det er derfor ikke nødvendig å gjenta definisjonene i forskriften. Begrepet tilgang er derimot et nøkkelbegrep i forskriften som vi ikke finner igjen i loven. Dette begrepet blir derfor definert i forskriften § 2.

5.6 Virkeområdet – tilgang mellom virksomheter

Departementet foreslår at loven skal gjelde når tilgjengeliggjøring av helseopplysninger etter pasientjournalloven § 19 skjer ved tilgang mellom virksomheter, se forslaget til forskrift § 2.

5.6.1 Helsehjelp

Formålet med tilgang innen rammene av forskriften skal være å yte, administrere eller kvalitetssikre helsehjelp til den enkelte pasient. Dette henger sammen med at forskriften skal sikre personvernet i de nye situasjonene som oppstår som følge av pasientjournalloven § 19. Denne bestemmelsen gjelder tilgjengelige helseopplysninger ved helsehjelp.

Virkeområdet for forskriften og virkeområdet for pasientjournalloven § 19 som forskriften er hjemlet i, må korrespondere.

Helsehjelp er definert i pasientjournalloven § 2 "handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende, rehabiliterende eller pleie- og omsorgsformål, og som utføres av helsepersonell, jf. helsepersonelloven § 3 første ledd".

Forskriften vil ikke regulere eventuell tilgang til helseopplysninger for andre formål enn helsehjelp, som for eksempel for forskning.

5.6.2 Tilgang

Departementet foreslår at forskriften skal regulere tilgang mellom virksomheter til behandlingsrettede helseregistre. Tilgang defineres i forskriften som det at helsepersonell gis adgang til elektronisk å hente frem helseopplysninger om pasienter. Dette for å markere at det er elektroniske journalsystemer det er tale om, med muligheter for selv å logge seg inn for å hente frem opplysninger. Forskriften vil ikke regulere en eventuell tilgang til papirjournaler.

Forskriften bør etter departementets vurdering ikke regulere tilgjengeliggjøring av opplysninger på andre måter enn ved tilgang. Opplysninger som er blitt hentet frem i journalen av helsepersonellet i en virksomhet der opplysningene er registrert, og som deretter er blitt utlevert ved brev, meldingsutveksling, per telefon eller på andre måter, vil derfor ikke bli regulert av forskriften. Det samme gjelder helseopplysninger som hentes frem ved hjelp av automatiske spørre-svar funksjoner. Utlevering av helseopplysninger vil bli regulert av de vanlige reglene i pasientjournalloven, helsepersonelloven og pasient- og brukerrettighetsloven. Dette har sektoren lang erfaring med allerede, og det reiser ingen nye utfordringer med hensyn til personvern og informasjonssikkerhet.

Departementet mener at forskriften bare bør regulere lesetilgang, dvs. at helsepersonell i andre virksomheter bare skal kunne hente frem, men ikke registrere eller endre opplysninger i registeret. Dette følger av ordlyden i § 2 om forskriftens virkeområde. Bakgrunnen for dette er å sikre at relevante og nødvendige opplysninger om pasienten og helsehjelpen blir nedtegnet korrekt. For pasienten er det viktig å kunne forholde seg til én virksomhet og et naturlig utgangspunkt er da den virksomheten som pasienten har fått helsehjelp. Det skal være enkelt å få innsyn i hva som er gjort og hvor, slik at det skal være enkelt blant annet å kreve retting og eventuell sletting i journalnotater.

Dette er også viktig for å unngå dobbeltregistreringer. Det er helsepersonellet som gir pasienten behandling som skal føre journalen. Annet helsepersonell som også gir pasienten behandling, skal føre i journalsystemet i sin virksomhet. Dette følger av dokumentasjonsplikten. Virksomheter som har behov for føre i samme journal, kan i stedet etablere felles journalsystemer etter pasientjournalloven § 9.

Det kan imidlertid tenkes situasjoner der det kan være hensiktsmessig om personell i virksomheten som får tilgang etter forskriften også får en begrenset skrivetilgang, ved at de gis mulighet til å gjøre for eksempel påtegninger eller markeringer på røntgenbilder. Et eksempel hvor dette kan være aktuelt, er innenfor radiologien: En pasient er innlagt på et

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

Dette bør i tilfelle begrenses til registreringer som er nødvendige for forståelsen av de vurderingene som er gjort. Disse registreringene skal ikke erstatte virksomhetens egen journalføringsplikt.

Departementet ber om høringsinstansenes synspunkter på om det bør åpnes for en begrenset skriveadgang i tilknytning til at det gis tilgang.

5.6.3 Mellom virksomheter

Forslaget gjelder tilgang *mellom* virksomheter. Virksomhetene står ikke overfor en ny situasjon med den nye loven når det gjelder intern tilgang. De generelle reglene i pasientjournalloven, personopplysningsloven og helsepersonelloven vil gjelde på samme måte som tidligere. Flere av kravene som er tatt inn i denne forskriften vil likevel også være relevante ved intern tilgang. Det gjelder blant annet begrensningen til kun å gi tilgang til nødvendige og relevante helseopplysninger og pasientens rett til å motsette seg at opplysninger gjøres tilgjengelige.

Behovet for tilgang til helseopplysninger i andre virksomheter vil være ulikt avhengig av type virksomhet, pasientgrunnlaget og hvor tett samarbeidet er om pasienten. Eksempler kan være samarbeid mellom helseforetak ved funksjonsfordeling, samarbeid mellom sykehus og fastlege, samarbeid mellom fastlege og helse- og omsorgstjenesten i kommunen eller mellom helseforetak og helse- og omsorgstjenesten i kommunen. Samarbeidet kan omfatte pasienter med store og kompliserte behov, som kan trenge helsehjelp dels fra pleie- og omsorgstjenesten i kommunen, dels fra fastlege, dels fra sykehus. Det kan omfatte palliativ behandling hjemme, kronisk syke, rehabilitering osv.

Tilgangen trenger ikke å gjelde gjensidig mellom virksomhetene. Pasientjournalloven § 19 åpner for eksempel også for at en fastlege skal ha tilgang til helseopplysninger om fastlegens pasienter på sykehuset uten at sykehuset får tilgang til fastlegens journalsystem. Departementet mener at det samme bør gjelde for tilgang etter forskriften.

Begrepet virksomhet tilsvarer her juridiske enheter i helsetjenesten. Eksempler på slike juridiske enheter er kommuner og helseforetak. Det kan også være private virksomheter som private sykehus eller privatleger som er selvstendig næringsdrivende (i mange tilfeller er dette fastleger). Databehandlingsansvaret følger som hovedsak virksomhetsgrensene. Den databehandlingsansvarlige har ansvaret for at behandlingen av personopplysninger følger reglene i denne forskriften og annet regelverk. De daglige oppgavene, men ikke ansvaret, kan delegeres til underordnede enheter og personer den databehandlingsansvarlige har instruksjonsmyndighet over. Dette forslaget til forskrift gjelder for de tilfeller der den databehandlingsansvarlige ikke har slik instruksjonsmyndighet over helsepersonell i andre virksomheter som skal få tilgang til opplysningene.

Forskriften som departementet nå foreslår vil ikke regulere tilgang innenfor virksomhetens interne journal, eller tilgang for virksomheter som samarbeider om en pasients journal etter pasientjournalloven § 9. Når det gjelder journaler en eller flere virksomheter samarbeider om, vil personell i alle de samarbeidende virksomhetene ha tilgang fordi journalføringsplikten skal gjennomføres i dette systemet. En slik journal skal komme i stedet for virksomhetens interne journal. Forskriften skal ikke regulere samarbeid mellom virksomheter om behandlingsrettede helseregistre. Dette er foreslått presisert i forskriften § 2.

To eller flere virksomheter som sammen etablerer et journalsystem etter pasientjournalloven § 9 kan imidlertid inngå avtale om tilgang for virksomheter utenfor samarbeidet. Forskriften vil i tilfelle regulere denne tilgangen.

5.7 Informasjonssikkerhet

Det følger av pasientjournalloven at helseopplysninger alltid må sikres på en tilfredsstillende måte. Både pasientene og helsepersonellet som benytter informasjonen skal kunne ha tillit til at helseopplysninger behandles med diskresjon og respekt, og at informasjonen ikke endres eller tilflyter uvedkommende. Samtidig må opplysningene være tilgjengelige for personell som har behov for informasjonen i sitt arbeid. Den databehandlingsansvarlige har plikt til å innrette seg på en måte som gjør at disse kravene ivaretas.

God informasjonssikkerhet oppnås ved hjelp av planlagte og systematiske tiltak. Basert på risikovurderinger må den databehandlingsansvarlige sørge for teknologiske og organisatoriske tiltak for å sikre tilfredsstillende beskyttelse av helseopplysningene med hensyn til konfidensialitet, integritet og tilgjengelighet, jf. pasientjournalloven § 22.

Forskriften skal fastsette særlige vilkår for å kunne gi tilgang mellom virksomheter, se forslaget til § 3. Forskriften regulerer enkelte tekniske og organisatoriske forutsetninger som må være på plass før en virksomhet kan gi andre tilgang. Kravene i forskriften kommer ikke i stedet for andre sikkerhetskrav, men i tillegg til disse. Departementet foreslår at dette presiseres i forskriften.

Departementet foreslår at forskriften uttrykkelig krever at begge virksomhetene skal ha rutiner og systemer som gir tilfredsstillende informasjonssikkerhet. Det omfatter tilgangsstyring, tekniske muligheter for sperring av helseopplysninger samt dokumentasjon, oppfølging og kontroll av tilgang, på et nivå som minst ivaretar kravene i forskriften. Departementet viser til personopplysningsforskriften § 2-15 som sier at den databehandlingsansvarlige bare kan overføre helseopplysninger elektronisk til virksomheter som har tilfredsstillende informasjonssikkerhet.

Med uttrykket begge virksomheter siktes det til avtalepartene, dvs. virksomhetene som inngår avtale med hverandre, både den virksomheten som gir tilgang til andre virksomheter og den virksomheten som får tilgang. En virksomhet kan imidlertid inngå avtaler om tilgang med flere virksomheter, eventuelt med likelydende avtaler dersom disse ut fra risikovurderinger vil oppfylle kravene.

Det er bare virksomheter som har moderne og sikre journalsystemer, som kan oppfylle forskriftens krav og som vil kunne gi tilgang mellom virksomheter. Dette kan kreve tilpasninger i de tekniske systemene og organisatoriske endringer. Deling av informasjon krever en viss grad av struktur. Journalsystemet må kunne gjøre et skille mellom opplysninger som kan deles og opplysninger som ikke kan deles. Databehandlingsansvarlige som ikke har journaler som er tilstrekkelig strukturerte, kan heller ikke åpne for tilgang mellom virksomheter.

Begge virksomhetene vil fortsatt ha ansvaret for informasjonssikkerheten knyttet til opplysningene som det gis tilgang til. Det er viktig å presisere at det ikke er tale om noen overføring av ansvar for opplysningene det gis tilgang til. Begge virksomhetene er ansvarlige for sin egen tilgangsstyring, ivaretakelsen av taushetsplikten og generelt for sin egen behandling av de opplysningene de får tilgang til.

For at en virksomhet skal kunne gi personell i andre virksomheter tilgang til helseopplysninger, må det være en forutsetning at dette ikke svekker informasjonssikkerheten i noen av virksomhetene, jf. Prop. L 72 (2013-2014) punkt 11.3.6 og merknadene til § 19 i punkt 24.1. Departementet foreslår at dette presiseres i forskriften, se forslaget til § 5.

Departementet foreslår videre at det forskriftsfestes at de databehandlingsansvarlige i virksomhetene skal ha særlige rutiner for hvordan informasjonssikkerheten skal ivaretas ved tilgang mellom virksomhetene. En virksomhet som lar en eller flere andre virksomheter gi sitt helsepersonell tilgang, skal påse at disse har tilfredsstillende informasjonssikkerhet for opplysninger det gis tilgang til, se forslaget § 5. Virksomheten som har opplysningene registrert, må derfor i tillegg til å stille krav til informasjonssikkerheten i egen virksomhet, også ha kunnskap om hvordan opplysningene sikres hos virksomheten som gis tilgang. Dette kan gjelde både tekniske og organisatoriske forhold. Eksempler kan være hvordan virksomhetene ivaretar tilgangsstyring, hvordan systemene sikres fysisk og rutiner for å fjerne tilgang når ansatte bytter oppgaver eller slutter.

Gjennomføring av kravet innebærer at den databehandlingsansvarlige som gir tilgang til opplysningene må ha kunnskap om tilgangsstyringen og andre forhold som kan påvirke informasjonssikkerheten i den virksomheten som får tilgang. Kunnskap om den eksterne virksomhetens sikkerhetsmål og sikkerhetsstrategi for å ivareta tilfredsstillende informasjonssikkehet vil være premisser i vurderingen av om det vil være hensiktsmessig å gi tilgang og eventuelt i hvilket omfang.

Tilfredsstillende informasjonssikkerhet krever organisatoriske så vel som tekniske og fysiske tiltak. Organisatoriske tiltak omfatter klare ansvarslinjer, gode rutiner hos alle som bruker systemet, risikovurderinger, dokumentasjon av informasjonssystemene m.v. Alle i virksomheten må være kjent med egne arbeidsoppgaver, plikter og rettigheter. Tilfredsstillende informasjonssikkerhet kan ikke alene ivaretas eller måles ut fra den tekniske funksjonaliten et elektronisk system har.

De ulike virksomhetene i helsetjenesten er svært forskjellige, både i størrelse, innhold og kompleksitet. For eksempel består Oslo universitetssykehus HF i dag av flere sykehus, blant andre Ullevål, Rikshospitalet og Aker, som til sammen har rundt 22 000 ansatte.

Samtidig kan en tannlege- eller legevirksomhet, fysioterapeutvirksomhet, psykolog-virksomhet kanskje ha to eller tre ansatte. De organisatoriske tiltakene som må til for å sikre tilfredsstillende informasjonssikkerhet i disse virksomhetene vil kreve ulik tilnærming. Informasjonssikkerhetstiltakene må derfor være tilpasset virksomhetens art, aktiviteter og størrelse.

Nødvendige rutiner må alltid utarbeides ved behov, noe som ikke kan detaljreguleres i regler som skal gjelde for alle virksomheter. Det er blant annet på denne bakgrunn at departementet foreslår at det i forskriften kun settes krav til at det skal foreligge rutiner, men at det er virksomheten selv som må utarbeide innholdet i rutinene. Rutiner må gjelde for alle nivåer i virksomheten. Ledelsen i virksomheten må kunne dokumentere hvordan regelverket er implementert i egen virksomhet – der tilgang til helseopplysningene faktisk blir gitt. Det er ikke nok å ha et overordnet regelverk og forutsette at det etterleves nedover i virksomheten.

5.8 Risikovurdering

Tilfredsstillende informasjonssikkerhet forutsetter gode risikovurderinger. Personopplysningsforskriften § 2-4 stiller krav til at det skal gjennomføres risikovurderinger for å kartlegge sannsynligheten for, og konsekvenser av, sikkerhetsbrudd. En forutsetning for å kunne ha en forsvarlig risikostyring, er at det finnes noen kriterier å styre etter. Akseptabelt risikonivå skal fastlegges for alle sikkerhetsbehov, inkludert konfidensialitet, tilgjengelighet og integritet. Kryssende hensyn må identifiseres og prioriteringen mellom forskjellige behov må fremgå i beskrivelsen av akseptabelt risikonivå.

Departementet foreslår at det forskriftsfestes at tilgang mellom virksomheter skal baseres på vurderinger av den risikoen for pasientenes personvern i begge virksomhetene som tilgang mellom virksomhetene kan føre til. Vurderingene skal omfatte tilgangsstyringen og ivaretakelsen av helsepersonellets taushetsplikt, informasjonssikkerheten og øvrige krav. Det skal foretas risikovurderinger av sannsynligheten for at en urettmessig tilegnelse av helseopplysninger kan skje, og eventuelle konsekvenser hvis det skjer. Det er en ledelsesoppgave å vurdere hvilken risiko som er akseptabel. Gjennomføring av risikovurderinger forutsetter god kjennskap til virksomhetens organisering og rutiner.

Basert på risikovurderingene skal den databehandlingsansvarlige avpasse de tekniske og organisatoriske tiltakene til hverandre, slik at kravene til informasjonssikkerheten i virksomheten etterleves og at målene for virksomheten nås.

Når det gis tilgang til behandlingsrettede helseregistre for personell i andre virksomheter, vil avveiningen mellom konfidensialitet, integritet og tilgjengelighet være særskilt viktig. Akseptabelt risikonivå vil være betinget av hvilke opplysninger og behandlinger av disse som berøres, akseptable nivåer for sannsynlighet og konsekvens, prioritering mellom forskjellige sikkerhetsbehov og en overordnet beskrivelse av risikoreduserende tiltak. Risiko betegner her forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvensene en slik hendelse vil medføre.

Risikovurdering må alltid gjennomføres før det kan besluttes å gi personell i andre virksomheter tilgang. Det er likevel ikke nok å gjøre en slik vurdering bare ved i verksettelsen av tilgangen. Dersom det oppstår endringer i forhold som kan påvirke informasjonssikkerheten, må risikoen vurderes på nytt. Eksempler på endringer som krever ny risikovurdering og ledelsesgodkjenning kan være organisasjonsendringer i egen virksomhet eller virksomheten som har fått tilgang, endringer i trusselbildet, endringer i egne IKT-systemer eller IKT-systemer hos virksomheten som har fått tilgang eller endring i klassifisering av opplysninger.

5.9 Avtale

Departementet foreslår at virksomheter som lar andre virksomheter gi sitt helsepersonell tilgang må ha inngått en særskilt avtale om dette. Se forslag til forskrift § 3. Hva avtalen minst skal inneholde foreslås regulert i § 4.

Personopplysningsforskriften § 2-15 om sikkerhet hos andre virksomheter krever at det inngås avtale med klare ansvars- og myndighetsforhold når opplysninger overføres elektronisk.

Kravet om avtale skal ikke komme i stedet for andre sikkerhetskrav, men i tillegg. Avtalen må holde seg innenfor lovens og forskriftens rammer. Det må følge av avtalen hva tilgangen gjelder og hvilke journalmoduler tilgangen omfatter. Behovet for og virkeområdet for avtalen skal være fundert på konkrete behovs- og nødvendighetsvurderinger. Avtalen kan for eksempel avgrenses til bestemte pasientgrupper eller bestemte fagsystemer. Det bør også fremgå av avtalen hvilke forutsetninger som ligger til grunn for avtalen, blant annet hvilke tekniske løsninger som skal benyttes av partene ved slik tilgang. Dette inkluderer informasjon om tilgangsstyring og informasjonssikkerhet. Avtalen skal angi relevante risikovurderinger av betydning for pasientens personvern.

Databehandlingsansvarlige som åpner for tilgang til helseopplysninger for ekstern virksomhet, skal vurdere om virksomheten som vil få tilgang har tilfredsstillende informasjonssikkerhet. Det er en forutsetning at tilgangen ikke vil svekke informasjonssikkerheten i noen av virksomhetene. Se forslaget til forskrift § 5.

Det må også kunne avtales vilkår for behandlingen av opplysningene i den virksomheten som får tilgang. Avtalen skal angi rutiner og fordeling av oppgaver for å ivareta kravene i denne forskriften. Den databehandlingsansvarlige kan ikke fraskrive seg ansvaret ved avtale. Departementet viser her til at begge parter vil ha ansvar for informasjonssikkerheten. Både den databehandlingsansvarlige og den som gis tilgang vil kunne bli holdt ansvarlig ved overtredelse av regelverket for den del avtalen gjelder. Se også forslaget § 5 tredje ledd som sier at en virksomhet som gir annen virksomhet tilgang, skal påse at denne virksomheten ivaretar kravene til informasjonssikkerhet, ved behandling av opplysninger etter forskriften.

Dersom to virksomheter som samarbeider om journal etter § 9, ønsker å gi en tredje virksomhet tilgang kan dette gjøres i avtale etter denne forskriften. Det vil si avtale

mellom fellesskapet, som den ene parten, og den tredje virksomheten, som den andre parten.

5.10 Tilgangsstyring

Departementet foreslår at det forskriftsfestes at begge virksomhetene skal ha tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger i samsvar med krav som følger av forskriften § 7 andre ledd. Forskriften vil dermed pålegge begge de databehandlingsansvarlige å etablere nødvendige organisatoriske og tekniske tiltak for tildeling og kontroll av tilgangsrettigheter til helseopplysninger.

Departementet foreslår at det forskriftsfestes at løsningene minst skal ivareta at

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

5.10.1 Tekniske og organisatoriske løsninger

Den databehandlingsansvarlige skal, på bakgrunn av risikovurderinger, etablere et system for tilgangsstyring. Tilgangsstyringen skal både begrense mulighetene for urettmessig tilegnelse og endring av opplysninger, og den skal sikre at helsepersonell har tilgang til relevante og nødvendige helseopplysninger når det er nødvendig for at en pasient skal kunne få forsvarlig helsehjelp. Det innbærer at det skal være enkelt for helsepersonell å finne relevant informasjon, samtidig som urettmessige forsøk på å tilegne seg opplysninger skal hindres.

Tilgangsstyringssystemet må være slik at risikoen for at helsepersonell kan få tilgang til helseopplysninger om pasienter de ikke er involvert i helsehjelpen til, blir minst mulig.

Tilgangsstyringen skal bygge på risikovurderinger og skal bidra til å sikre at informasjonssikkerheten, inkludert bestemmelsene om taushetsplikt og pasientens rett til konfidensialitet, blir ivaretatt. Hva som kreves for å kunne gi tilgang, hvem som skal kunne få tilgang og til hvilke opplysninger i hvilke systemer tilgang skal gis, må vurderes konkret for den enkelte virksomhet. En gjennomtenkt tilrettelegging og organisering av tilgangen er avgjørende for god informasjonssikkerhet. Dette gjelder særlig de store virksomhetene. I mindre virksomheter – hvor bare en eller to har tilgang til journalsystemet – må dette kunne gjøres ganske enkelt.

Den organisatoriske tiltaksdelen innebærer blant annet å bestemme hvilke rettigheter og plikter helsepersonellet skal ha. Andre organisatoriske tiltak er å sikre at data-behandlingsansvarlig og databehandler har tilstrekkelig kompetanse, innarbeiding av rutiner og holdninger i virksomheten, osv.

Den tekniske delen består i å gjennomføre tiltak som gjør at funksjonalitet som skal gi tilgang, logge tilgang og kontrollere tilgang, implementeres i systemet i tråd med

spesifikasjonen og at nødvendige sikringstiltak iverksettes. Teknisk sikring gjelder tilgangskontroller ved bruk av passord eller lignende. Det skal settes tekniske skranker for de muligheter helsepersonell har til å logge inn i et IT-system og behandle helseopplysninger.

Teknisk mulighet til å lese journalopplysninger er ikke det samme som å ha lov til lese i journalnotater. Lovlig tilgang til helseopplysninger krever at reglene om taushetsplikt etterleves. Regler om taushetsplikt og forbudet mot urettmessig tilegnelse av helseopplysninger, følger av pasientjournalloven §§ 15 og 16, jf. helsepersonelloven §§ 21 flg. For tilgang til helseopplysninger i journal og journalopplysninger vil reglene i helsepersonelloven §§ 25 og 45 være relevante.

I tillegg må det sørges for fysisk sikring av systemets omgivelser ved for eksempel adgangskontroll og lås på døren.

Virksomheten må vurdere hvor lenge en tilgang skal være gyldig. For to virksomheter som regelmessig behandler de samme pasientene gjennom et behandlingsforløp, kan en fast ansatt med faste oppgaver gis tilganger av lengre varighet enn om samarbeidet er mer sporadisk eller personell ofte skifter roller.

Dersom utstyret eller de tekniske hjelpemidlene som brukes ikke har tilstrekkelig differensiert teknisk tilgangsstyring, må den databehandlingsansvarlige vurdere risikoen for at personell i andre virksomheter kan få tilgang til opplysninger de ikke skal ha, og om informasjon må gis på annen måte, for eksempel ved meldingsutveksling.

5.10.2 Pasientens rett til å motsette seg at opplysninger gjøres tilgjengelige

Det er et viktig prinsipp at pasientens selvbestemmelsesrett må ivaretas dersom det gis tilgang. I pasientjournalloven § 17 er det presisert at pasienten eller brukeren har rett til å motsette seg at helseopplysninger gjøres tilgjengelige etter § 19. Bestemmelsen viser til helsepersonelloven §§ 25 og 45 og til pasient- og brukerrettighetsloven § 5-3. Det følger av helsepersonelloven at med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til pasient gis nødvendige og relevante helseopplysninger. Pasienten skal så langt råd er gjøres kjent med at det utleveres opplysninger i samarbeidsøyemed, og kan motsette seg dette. I særlige tilfeller vil det kunne tenkes at pasienten ikke kan motsette seg tilgang eller utlevering, for eksempel i forbindelse med tvangsinnleggelser ved psykiatriske institusjoner. Se nærmere i merknadene til §§ 25 og 45 i Ot.prp. nr. 13 (1998–1999) og Prop. 72 L (2013–2014) punkt 11.1.2 om helsepersonellovens samtykkekrav og retten til å motsette seg informasjonsdeling.

Departementet foreslår at det presiseres i forskriften at tilgangsstyringen må ivareta at det bare gis tilgang dersom pasienten ikke har motsatt seg eller motsetter seg at opplysningene gjøres tilgjengelige. Pasientens rett til å motsette seg at opplysninger tilgjengeliggjøres, må gjennomføres i systemet slik at retten blir reell. Sikring av retten til å motsette seg at helsepersonellet kan tilegne seg informasjon, må gjøres på flere nivåer.

En måte er tekniske mekanismer for å sperre opplysninger mot at andre skal kunne lese journalen. Det innebærer at pasientens rett til å motsette seg at opplysninger gjøres

tilgjengelige for annet helsepersonell, ivaretas av systemet. Det må derfor etableres tekniske løsninger som gjør denne retten effektiv. Det foreslås derfor å stille krav om at begge virksomhetene skal ha tekniske og organisatoriske løsninger som avgrenser tilgangen, se forskriften § 7.

Dette er imidlertid ikke nok. I tillegg skal pasienten alltid ha anledning til å til å si til sin behandler at vedkommende ikke skal lese informasjon om han eller henne som er ned-tegnet andre steder. Dette ivaretas ved organisatoriske løsninger og interne rutiner. Pasienten skal så langt råd er gjøres kjent med at det vil bli innhentet opplysninger i samarbeidsøyemed, og kan motsette seg dette. Det ivaretas ved informasjon til pasienten, se punkt 5.11 og forskriften § 8.

5.10.3 Bare nødvendige og relevante opplysninger

Det følger av pasientjournalloven § 19 at opplysningene bare kan gjøres tilgjengelige når de er relevante og nødvendige. Det er kun de som har et tjenstlig behov som skal få opplysningene, og de skal ikke få flere opplysninger enn det som er relevant og nødvendig for å yte helsehjelpen.

Departementet foreslår at det forskriftsfestes at løsningene skal ivareta at helsepersonell kun skal ha tilgang til helseopplysninger som er relevante og nødvendige for helsehjelpen til den enkelte pasienten. Dette gjelder opplysninger for å yte, kvalitetssikre eller administrere helsehjelpen. I Prop. 72 L (2013–2014) punkt 11.3.4 gjøres det nærmere rede for hva som menes med relevante og nødvendige helseopplysninger.

Kravet om at det bare kan gis tilgang til nødvendige og relevante opplysninger for å kunne gi helsehjelp til pasienten, innebærer at journalen må ha struktur som gjør at denne funksjonen kan oppfylles. Lite struktur og stor grad av løpende prosatekst vil kunne gjøre det vanskelig å begrense tilgangen til det som er relevant og nødvendig. Dette vil imidlertid gjelde uansett om det er internt i en virksomhet eller tilgang fra personell i andre virksomheter. Det er en ekstra utfordring når det gis tilgang for personell i andre virksomheter ved at det må være effektiv tilgangsstyring i begge virksomheter. Hos begge virksomheter må kravet til kvalitet og struktur være ivaretatt.

Ved tilgang til opplysningene må systemene som benyttes kunne gi en differensiert mulighet for tilgangsstyring slik at en kan hindre at helsepersonell får tilgang til opplysninger som ikke er relevante og nødvendige for helsehjelpen. Det enkelte systemets funksjoner og muligheter må gjenspeiles/utnyttes i den praktiske tilgangsstyringen.

5.10.4 Autorisasjon og autentisering

Departementet foreslår at forskriften skal sette krav til autorisasjoner som gir tilgang til helseopplysninger mellom virksomheter. Departementet foreslår at det forskriftsfestes at helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet skal

- beskrive rettigheter og plikter som følger av autorisasjonen,
- være i samsvar med helsepersonellovens regler om taushetsplikt,
- dokumenteres i virksomhetens autorisasjonsregister,

- tidsbegrenses, og
- vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold.

Helsepersonell og annet personell må være autorisert for tilgang til helseopplysningene. Autorisasjonen skal angi hvilke plikter og rettigheter den enkelte har. Dersom helsepersonell gis adgang til elektronisk å hente frem informasjon om pasienter i andre virksomheters systemer må dette fremgå av autorisasjonen.

Når det gis tilgang til helseopplysninger, er det viktig at det er stor grad av sikkerhet for at personen som gis tilgang faktisk er den vedkommende utgir seg for å være. Autentisering er bevis for at oppgitt identitet er korrekt, og skal skje ved sikker autentiseringsløsning. Det innbærer at den elektroniske identifikasjonen må være av tilstrekkelig kvalitet og styrke for å sikre rett identitet på personen og at det kan brukes som bevis i en rettssak. I tillegg vil autentiseringen bidra til å sikre at hendelsesregistreringen (loggen) viser hvem som har hatt tilgang til opplysningene. For kommunikasjon mellom forskjellige virksomheter må identifisering (navngivning) gi mening på tvers av virksomheter.

Enhver som gis tilgang til helseopplysninger skal kunne identifiseres som en bestemt person med bestemte rettigheter og plikter. Det kan altså ikke etableres noen form for «felleskonto» som gir personell i en virksomhet tilgang til opplysninger i en annen virksomhet uten at deres identitet er sikker.

5.11 Informasjon til pasienten

Departementet foreslår en egen bestemmelse i forskriften som presiserer virksomhetens plikt til å informere pasientene om at det kan gis tilgang til journalen fra andre virksomheter, jf. forslaget § 8. Pasientens rett til innsyn i logg er foreslått presisert i forskriften § 10.

Det er avgjørende at pasienten er klar over om helsepersonell i andre virksomheter enn der de får behandling kan få tilgang til journalopplysningene. Denne informasjonen trenger pasienten både når opplysningene journalføres, og senere når de får behandling i en annen virksomhet der det blir aktuelt å søke frem opplysninger fra den virksomheten der pasienten tidligere har fått behandling. Pasienten har et særlig behov for informasjon i lys av at tilgang mellom virksomheter ikke er betinget av pasientens samtykke. Pasienten har imidlertid rett til å motsette seg at det gis tilgang eller at opplysningene tilgjengeliggjøres på andre måter, se punkt 5.11.

Pasienten har etter pasientjournalloven § 18 rett til informasjon og innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logg). Innsynsretten gjelder alle tilfeller der noen har lest, søkt eller på annen måte tilegnet seg, brukt eller besittet helseopplysninger fra behandlingsrettede helseregistre, enten dette er rettmessig eller ikke. Det følger av denne bestemmelsen og av § 6 om rett til å behandle helseopplysninger, at den databehandlings-

ansvarlige har både rett og plikt til å registrere hvem som har hatt tilgang til eller fått utlevert opplysninger.

Det følger av forarbeidene til helsepersonelloven at pasienten så langt råd er skal gjøres kjent med at det utleveres opplysninger i samarbeidsøyemed. Se nærmere i Ot.prp. nr. 13 (1998–1999) merknadene til §§ 25 og 45 i kapittel 12.

Pasienten skal også informeres om retten til å motsette seg behandling av helseopplysninger, og hvordan dette kan gjøres rent praktisk. Slik informasjon er avgjørende for at reservasjonsretten skal være rell, se Prop. 72 L (2013–2014) punkt 18.1.2. Dette følger av personopplysningsloven § 19 første ledd bokstav e om informasjonsplikt med hensyn til forhold som gjør den registrerte i stand til å bruke sine rettigheter etter loven på best mulig måte.

Departementet foreslår på denne bakgrunn at begge databehandlingsansvarlige skal ha informasjonsplikt, både den virksomheten som gir tilgang og den som får tilgang. Den databehandlingsansvarlige i virksomheter som lar andre virksomheter gi sitt helsepersonell tilgang skal informere pasienten blant annet om hvilke virksomheter som gis tilgang, hvilke opplysninger tilgangen omfatter, og at pasienten kan motsette seg at det gis tilgang. Virksomheter som henter frem opplysninger skal også informere pasienten om dette.

5.12 Sperring av helseopplysninger

En forutsetning for å kunne ivareta pasientens ønske, er at det elektroniske systemet kan sperre de aktuelle opplysningene for innsyn. Med sperring menes en teknisk løsning der journalopplysninger gjøres utilgjengelig for enkeltpersoner, grupper av helsepersonell eller helsepersonell i andre virksomheter enn der journalnotatene er nedtegnet.

Fra pasientens ståsted vil dette kunne sikre tilliten til at opplysningene ikke kommer på avveie. Enkelte vil nok særlig oppleve muligheten til å kunne sperre som viktig i forbindelse med løsninger for tilgang mellom virksomheter. Fra helsepersonellets ståsted vil det være at stor betydning at det elektroniske systemet utformes slik at det støtter etterlevelse av regelverket.

Departementet foreslår derfor at det tas inn en bestemmelse i forskriften om at pasienten kan kreve at helseopplysninger som kan knyttes til vedkommende sperres. Virksomhetene må da ha på plass tekniske løsninger som gjør dette mulig før det kan gis tilgang, se forskriften § 7 første ledd bokstav b og § 9.

Dette vil gi pasienten en rett til å få opplysninger teknisk sperret i systemet. Pasienten kan selv bestemme om opplysningene skal sperres for all tilgang fra personell utenfor den aktuelle virksomheten eller om for eksempel personell i enkelte virksomheter skal kunne få tilgang.

Retten til å motsette seg at opplysninger gjøres tilgjengelige for annet helsepersonell gjelder med de forbeholdene som følger av pasientjournalloven § 17, jf. pasient- og brukerrettighetsloven § 5-3 og helsepersonelloven §§ 25 og 45. Dette innebærer at retten til å motsette seg at opplysninger gjøres tilgjengelige for andre ikke er absolutt. Det kan

være tilfeller der opplysningene ut fra hensynet til forsvarlig helsehjelp, likevel bør gis. Retten til sperring for tilgang til helseopplysninger mellom virksomheter etter denne forskriften bør imidlertid etter departementets vurdering være absolutt.

Dersom sperrede opplysninger likevel må gjøres tilgjengelige fordi tungtveiende grunner taler for det, jf. pasient- og brukerrettighetsloven § 5-3, må dette skje ved utlevering. Pasienten skal da informeres om at sperrede opplysninger utleveres, hvorfor de utleveres og til hvem.

5.13 Logging og dokumentasjon av tilgang

Etter forslaget § 10 skal all tilgang registreres automatisk i systemet. Krav om logging følger også indirekte av innsynsretten etter pasientjournalloven § 18. Her kan det også vises til de mer generelle bestemmelsene i personopplysningsforskriften § 2-14 om registrering av uautorisert bruk av informasjonssystem og § 2-16 om registrering av autorisert og forsøk på uautorisert bruk.

Logging av informasjon om hvem som har hentet frem taushetsbelagte opplysninger, er et viktig tiltak for å bedre informasjonssikkerheten. Det er et sentralt element i personvernet at den enkelte skal ha rett til og reell mulighet til å ha kontroll over helseopplysninger om seg selv. Informasjon om hvem som har hatt tilgang til helseopplysninger om en via innsyn i logg, vil bidra til å øke pasientens kontroll med opplysningene og sikre personvernet på en bedre måte. Logging er imidlertid et supplement til god tilgangsstyring, og kommer ikke i stedet for andre sikkerhetstiltak eller tilgangsstyring.

All tilgang til systemene bør være sporbar slik at behandlingen av opplysningene kan dokumenteres i ettertid ved for eksempel logganalyser. Autentiseringen bidrar til å sikre at loggen viser hvem som har hatt tilgang til hvilke opplysninger. Loggen skal være et verktøy til å avdekke mulig urettmessig tilgang til opplysningene og å forebygge og forhindre at gjentagelse av sikkerhetsbrudd i informasjonssystemene skjer. Loggen er også nødvendig for at pasientene skal kunne få innsyn i hvem som har hatt tilgang til opplysningene. Når en behandling av opplysninger skjer mellom virksomheter, må en kunne spore informasjonsflyten i begge virksomhetene.

Departementet foreslår at det fastsettes i forskriften at det skal registreres automatisk når personell fra andre virksomheter henter frem opplysninger i et behandlingsrettet helseregister. Dette betyr at virksomheten må ha en løsning for elektronisk logging av all tilgang til journalen. Loggen skal ikke kunne føres manuelt. All tilgang skal logges også når det er gitt tilgang til personell utenfor virksomheten. Hvis tilfredsstillende loggsystem ikke er etablert, kan det ikke gis tilgang.

Det må etableres funksjonalitet for logging av alle oppslag i systemene, både interne oppslag og ved oppslag fra andre virksomheter. All tilgang til systemene skal være sporbar slik at behandlingen av opplysningene kan dokumenteres i ettertid ved for eksempel logganalyser.

Departementet mener at loggen minst skal inneholde informasjon om

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

Dette skal bare være minimumskrav. For å kunne oppfylle kravene om oppfølging og kontroll av tilgang kan det være nødvendig også å inkludere annen informasjon i loggen, for eksempel mer detaljert knytning mellom hendelsene og opplysningene. Dette må vurderes konkret av den databehandlingsansvarlige. Virksomhetene bør søke å finne fram til løsninger som er best mulig egnet til å avdekke urettmessig tilgang til helseopplysninger.

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

Departementet foreslår at det også presiseres i forskriften at pasienten har rett til innsyn i og utskrift av loggen. Dette kravet skal fortolkes i samsvar med pasientjournalloven § 18 om innsyn. Innsynsretten gjelder alle pasienter som er registrert i et behandlingsrettet helseregister hos den databehandlingsansvarlige. Det stilles ikke krav om at en må være pasient *når* en ber om dokumentasjon av tilgang. Pasienten kan også be om innsyn etter at behandlingen er avsluttet.

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

5.14 Oppfølging og kontroll av tilgang

Effektiv bruk av loggsystemer forutsetter at virksomheten har rutiner for når, hvor ofte og eventuelt på hvilke vilkår kontrollen av tilgangen skal foretas. Rutinene skal bygge på konkrete risikovurderinger, og vil blant annet være avhengig av hvordan tilgangsstyringen er innrettet. Kontroll skal alltid foretas dersom det foreligger mistanke om at noen ulovlig har tilegnet seg helseopplysninger. Som nevnt i punkt 5.13 skal all tilgang til systemene være sporbar.

Urettmessig tilgang til helseopplysninger som oppdages ved kontroll, skal håndteres som avvik etter personopplysningsforskriften § 2-6. Samtidig skal pasienten dette gjelder informeres. Logging og kontroll av autorisert og uautorisert tilgang er kontrolltiltak overfor de ansatte i henhold til arbeidsmiljøloven kapittel 9, og den databehandlings-

ansvarlige må informere de ansatte og drøfte med tillitsvalgte etter arbeidsmiljøloven § 9-2.

5.15 Internkontroll

Alle virksomheter i helse- og omsorgssektoren skal ha en systematisk tilnærming i etterlevelsen av regelverk. Når det gjelder informasjonssikkerhet følger kravet om internkontroll av pasientjournalloven § 23. Personopplysningsforskriften § 2-15 har utdypende regler om internkontroll i §§ 3-1 og 3-2.

Dersom det besluttes at personell fra andre virksomheter skal gis tilgang til bestemte opplysninger i et behandlingsrettet helseregister, skal internkontrollen også omfatte dette. Internkontroll skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen skal være tilpasset virksomhetens risikovurdering og være en integrert del av virksomhetens helhetlige styringssystem.

Å etablere god risikostyring er viktig. Det er ikke tilstrekkelig å kun utarbeide dokumentasjon. Sikringstiltak må henge sammen med risikovurderingene og dokumentasjonen skal være en aktiv støtte for bruk av systemet. Det må være klart hvilke risikovalg som er tatt når retningslinjene er utformet og ledelsen må ha gitt klare føringer med hensyn til hvilket risikonivå som kan aksepteres.

Siden kravet om internkontroll følger av de alminnelige reglene, mener departementet at det ikke er behov for å forskriftsfeste dette særlig. En egen forskriftsbestemmelse om dette vil ikke stilles andre krav enn de som følger av de alminnelige reglene i pasientjournal-loven § 19.

6 Administrative og økonomiske konsekvenser

Forskriften stiller krav til virksomheter som ønsker å gjøre helseopplysninger i egen virksomhet tilgjengelig for personell i annen virksomhet, ved at helsepersonell gis adgang til elektronisk å hente frem opplysningene. Forskriften pålegger ingen virksomheter plikt til å tilgjengeliggjøre opplysninger på denne måten.

7 Merknader til de enkelte bestemmelsene

Til § 1 Formål

Formålet med forskriften er å ivareta informasjonssikkerhet og personvern ved tilgang mellom virksomheter til behandlingsrettede helseregistre. Hva som menes med tilgang er definert i § 2. Personvern og informasjonssikkerhet er i viktige elementer for å ivareta pasientsikkerheten. God informasjonssikkerhet krever ivaretakelse av opplysningenes konfidensialitet, integritet og tilgjengelighet. Det følger av pasientjournalloven at det er den databehandlingsansvarlige som bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige for helsepersonell ved ytelse av helsehjelp, og at opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten. Tilgang mellom virksomheter forutsetter risikovurderinger, rutiner og gode tekniske og organisatoriske løsninger.

Se nærmere om formålet i punkt 5.4. Se også Prop. 72 L (2013-2014) punkt 9.3.3.

Til § 2 Saklig virkeområde

Første ledd

Forskriften gjelder når tilgjengeliggjøring av helseopplysninger etter pasientjournalloven § 19 skjer ved tilgang mellom virksomheter. Begrepet tilgang defineres i § 2 andre ledd.

Forskriften gjelder tilgang til behandlingsrettede helseregistre. Med behandlingsrettet helseregister menes pasientjournal- og informasjonssystem eller annet register, fortegnelser eller lignende, der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner (jf. pasientjournalloven § 2 bokstav d).

Videre gjelder forskriften når helsepersonell skal yte, kvalitetssikre eller administrere helsehjelp til en enkelt person. Begrepet helsehjelp skal forstås på samme måte som etter helsepersonelloven § 3 og pasientjournalloven § 2. Helsehjelp er definert i pasient-journalloven § 2 som ”handlinger som har forebyggende, diagnostisk, behandlende, helse-bevarende, rehabiliterende eller pleie- og omsorgsformål, og som utføres av helse-personell, jf. helsepersonelloven § 3 første ledd”.

Dette innebærer at det ikke kan gis tilgang mellom virksomheter etter forskriften dersom formålet er kvalitetssikring av helsehjelpen som sådan, undervisning eller forskning. Dette er samme virkeområde som pasientjournalloven § 19.

Forskriften gjelder tilgang *mellom* virksomheter. Forskriften gjelder dermed for data-behandlingsansvarlige som legger opp til at helsepersonell i andre virksomheter kan gis tilgang til virksomhetens behandlingsrettede helseregistre. Forskriften gjelder for de tilfeller der den databehandlingsansvarlige ikke har instruksjonsmyndighet over helsepersonellet som får tilgang til opplysningene.

Begrepet virksomhet tilsvarer her juridiske enheter (egne rettssubjekter) i helsetjenesten. Databehandlingsansvaret følger som hovedsak virksomhetsgrensene. Dette gjelder både

offentlige og private virksomheter. Eksempler på slike juridiske enheter er kommuner, helseforetak og fastleger.

Tilgangen trenger ikke å gjelde gjensidig mellom virksomhetene. To virksomheter kan også avtale at den ene virksomheten kan gis tilgang til et behandlingsrettet register i en virksomhet den samarbeider med, samtidig som den andre virksomheten ikke åpner for slik tilgang. Forskriften åpner for eksempel for at en fastlege skal ha tilgang til helseopplysninger om fastlegens pasienter på sykehuset uten at sykehuset får tilgang til fastlegens journal.

Forskriften regulerer ikke tilgang innenfor virksomhetens interne journal. Forskriften gjelder heller ikke tilgang mellom virksomheter til en felles journal som virksomhetene samarbeider om etter pasientjournalloven § 9, se forskriften § 2 tredje ledd.

I punkt 5.6.3 drøftes hva som menes med tilgang mellom virksomheter.

Andre ledd

Tilgang betyr at helsepersonell gis adgang til elektronisk å hente frem informasjon om pasienter. Forskriften gjelder dermed ikke der helseopplysninger gjøres tilgjengelige ved at de utleveres, som for eksempel ved elektronisk melding.

Med tilgang siktes det bare til lesetilgang og ikke skrivetilgang. Forskriften gir ikke hjemmel til å la helsepersonell i andre virksomheter registrere, endre eller legge til opplysninger i journalen. Helsepersonell i andre virksomheter som får tilgang vil imidlertid ha rett til å skrive eller kopiere inn opplysningene i sin egen journal, i samsvar med dokumentasjonsplikten etter helsepersonelloven § 39. Departementet ber imidlertid høringsinstansene vurdere hvorvidt det også skal kunne åpnes for en begrenset skrivetilgang, se punkt 5.6.2.

Tredje ledd

Forskriften regulerer ikke tilgang til helseopplysninger mellom virksomheter som samarbeider om et felles behandlingsrettet helseregister etter pasientjournalloven § 9. Tilgang til et behandlingsrettet helseregister etter § 9 fra de samarbeidende virksomhetene anses som intern tilgang fra begge eller alle virksomheter som samarbeider om registeret. Personell i begge virksomhetene vil ha lese- og skrivetilgang, fordi dokumentasjonsplikten skal gjennomføres i dette systemet. Vilkårene for samarbeid om felles journal reguleres i stedet av pasientjournalloven § 9 og eventuelle forskrifter i medhold av denne

To eller flere virksomheter som etablerer felles journalsystem etter pasientjournalloven § 9 kan imidlertid inngå avtale om tilgang for virksomheter utenfor samarbeidet. Forskriften om tilgang mellom virksomheter vil i tilfelle regulere denne tilgangen.

Til § 3 Grunnvilkår for tilgang mellom virksomheter

Den databehandlingsansvarlige kan bare la andre virksomheter gi sitt helsepersonell tilgang dersom kravene i forskriften §§ 3 til 11 er oppfylt. Bestemmelsen regulerer grunnvilkårene som må være oppfylt for at tilgang mellom virksomheter skal kunne gis.

Det foreslås ingen hjemmel til å dispensere fra kravene.

Dersom vilkårene i forskriften ikke er oppfylt, kan det ikke gis tilgang mellom virksomhetene. Opplysningene kan da i stedet utleveres hvis grunnvilkårene i pasientjournalloven § 19 er oppfylt.

Med databehandlingsansvarlig menes den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, og den som i eller i medhold av lov er pålagt et databehandlingsansvar, jf. pasientjournalloven § 2. 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. En delegering av de daglige oppgavene vil ikke frata den som delegerer noe rettslig ansvar.

For det første må de databehandlingsansvarlige i virksomhetene ha inngått avtale om tilgang i samsvar med § 4. Avtalepartene skal vurdere risiko for pasientenes personvern som tilgang kan føre til. Vurderingene skal minst omfatte risiko for brudd på taushetsplikt og svekket informasjonssikkerhet.

For det andre skal begge virksomhetene ha rutiner og systemer som gir tilfredsstillende informasjonssikkerhet og tilgangsstyring. Tekniske muligheter for sperring av helseopplysninger samt dokumentasjon, autentisering og oppfølging, og kontroll av tilgang skal minst ivareta kravene i §§ 5 til 11.

Med uttrykket begge virksomheter siktes det til avtalepartene, dvs. både den virksomheten som gir tilgang til andre virksomheter og den virksomheten som får tilgang. En virksomhet kan imidlertid inngå avtaler om tilgang med flere virksomheter, eventuelt med likelydende avtaler dersom disse ut fra risikovurderinger vil oppfylle kravene.

Avtalen skal være basert på vurderinger av risikoen for pasientenes personvern i begge virksomhetene som tilgang mellom virksomhetene kan føre til. Risiko betegner her forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvensene en slik hendelse vil medføre. Vurderingene skal omfatte tilgangsstyringen og ivaretakelsen av helsepersonellets taushetsplikt, informasjonssikkerheten og øvrige krav.

Risikovurdering må alltid gjennomføres før det kan besluttes å gi personell i andre virksomheter tilgang. Det er ikke nok å gjøre en slik vurdering bare ved iverksettelsen av tilgangen. Dersom det oppstår endringer i forhold som kan påvirke informasjonssikkerheten, må det gjennomføres ny risikovurdering. Gjennomføring av risikovurderinger forutsetter god kjennskap til virksomhetens organisering og rutiner. Eksempler på endringer som krever ny risikovurdering og ledelsesgodkjenning kan være organisasjonsendringer i egen virksomhet eller virksomheten som har fått tilgang, endringer i trusselbildet, endringer i egne IKT-systemer eller IKT-systemer hos virksomheten som har fått tilgang eller endring i klassifisering av opplysninger. Se nærmere om risikovurderingen i punkt 5.8.

Det er bare virksomheter som har moderne og sikre journalsystemer, som vil kunne gi tilgang mellom virksomheter. Dette kan kreve tilpasning av de tekniske systemene og

eventuelle organisatoriske endringer. Når det gis tilgang mellom virksomheter vil avveiningen mellom konfidensialitet, integritet og tilgjengelighet være særskilt viktig. Akseptabelt risikonivå vil være betinget av hvilke opplysninger og behandlinger av disse som berøres, akseptable nivåer for sannsynlighet og konsekvens, prioritering mellom forskjellige sikkerhetsbehov og en overordnet beskrivelse av risikoreduserende tiltak. En beskrivelse av akseptabelt risikonivå skal være en del av grunnlaget for gjennomføring av risikovurderingen. Det er en ledelsesoppgave å vurdere hvilken risiko som er akseptabel. Se nærmere om kravene til informasjonssikkerhet i § 5 og punkt 5.7.

Andre ledd

Reglene i forskriften kommer i tillegg til, og utfyller, de alminnelige personvernreglene i pasientjournalloven, personopplysningsloven (med personopplysningsforskriften) og andre lover som gjelder ved behandling av helseopplysninger.

Til § 4 Avtalens innhold

Første ledd

Det følger av § 3 at virksomheter som skal gi andre virksomheter tilgang må inngå avtale om dette. Dette følger av at den databehandlingsansvarlige som gir tilgang fortsatt vil ha et ansvar for opplysningenes sikkerhet etter forskriften § 5 andre ledd. Databehandlingsansvarlig kan ikke fraskrive seg dette ansvaret ved avtale. Samtidig vil den databehandlingsansvarlige som gis tilgang være ansvarlig for sin behandling av opplysningene. Se nærmere i punkt 5.7 og merknadene til § 5.

Andre ledd

Kravene i § 4 andre ledd bokstavene a til c angir minstekrav til avtalens innhold. Begge de databehandlingsansvarlige kan sette ytterligere krav til den andre virksomheten som vilkår for å åpne for tilgang.

Bokstav a

Det følger av bestemmelsen at avtalens virkeområde må angis og avgrenses, dvs. hva avtalen gjelder.

Bokstav b

Behovet for og virkeområdet for avtalen skal være fundert på konkrete behovs- og nødvendighetsvurderinger. Avtalen skal derfor angi de behovs- og risikovurderingene som ligger til grunn for avtalen. At det generelt kan oppstå en situasjon der det kan være ”kjekt å ha” tilgang til opplysninger i annen virksomheten er ikke nok.

Bokstav c

Avtalen skal redegjøre for hvilke journalmoduler avtalen gjelder. Behandlingsrettet helseregister er et vidt begrep. Helseopplysninger kan være registrert i mange ulike systemer, og inkluderer også røntgen- og informasjonssystemer (RIS), medisinske bildearkivsystemer (PACS), laboratoriedatasystemer, anestesijournaler, medikasjons- og kurvesystemer, pleieplaner, små avdelingsvise kliniske systemer og andre typer

spesialsystemer. En avtale mellom virksomheter etter denne forskriften kan omfatte en eller flere av virksomhetens interne systemer eller av felles journalsystemer etter pasientjournalloven § 9.

Bokstav d

Bestemmelsen fastslår at avtalen skal omfatte krav om rutiner og fordeling av oppgaver for å ivareta kravene i denne forskriften. Dette henger sammen med blant annet forskriften § 5 som setter krav til rutiner.

Til § 5 Informasjonssikkerhet

Bestemmelsen regulerer kravene til informasjonssikkerhet i begge virskomhetene. Informasjonssikkerhet omfatter blant annet konfidensialitet, integritet og tilgjengelighet ved behandling av helseopplysninger, se pasientjournalloven § 22. Etter tradisjonell informasjonssikkerhetsmetodikk skal sikkerhetsmål beskrive hva som ønskes oppnådd sikkerhetsmessig og understøtte og sikre virksomhetens drift, allmenne tillit og omdømme i det offentlige rom, ved å forebygge og begrense konsekvensene av uønskede hendelser. Sikkerhetsstrategien beskriver hvilke tiltak som skal gjennomføres for å oppnå sikkerhetsmålene.

Bestemmelsen kommer i tillegg til pasientjournalloven § 22 og tydeliggjør at det skal foreligge styrende dokumenter for behandling av helseopplysninger for alle nivåer i virksomheten. Disse må baseres på risikovurderinger for virksomheten. Se nærmere i punkt 5.7.

Første ledd

Begge virksomhetene skal ha rutiner for hvordan informasjonssikkerheten skal ivaretas. Rutinene skal blant annet omfatte krav til risikovurdering, fysisk sikring, organisering, revisjon og avvikshåndtering. Rutinene skal omfatte alle behandlingsrettede helseregistre virksomheten (eller virksomhetene som samarbeider om behandlingsrettet helseregister etter pasientjournalloven § 9) avtaler at det kan gis tilgang til.

Dersom en virksomhet er delt inn i flere undervirksomheter, divisjoner, avdelinger eller lignende, skal hver enhet ha skrevne rutiner, med planer for overordnet nivå som overbygning. De konkrete rutinene må forholde seg til den eller de organisatoriske deler av virksomheten de er skrevet for. I hvilken grad risikovurderinger, planer og rutiner gjelder for hele virksomheten eller deler av den, vil blant annet være avhengig av avtalen etter forskriften § 4, virksomhetens art og karakter.

Planen må være så konkret at det er klart hvilke opplysninger det kan gis tilgang til, til hvem tilgang kan gis, på hvilke vilkår og hvem som avgjør om tilgang skal gis.

Rutinene for å ivareta informajonssikkerheten ved tilgang mellom virksomheter skal bygge på og utfylle, virksomhetens interne rutiner. Rutinene må implementeres i de konkrete rutinene til den eller de organisatoriske deler av virksomheten de gjelder for. De skrevne rutinene skal være levende dokumenter som raskt kan tilpasses ved endringer i risikovurderingen, organisering av virksomheten eller lignende.

Andre ledd

Tilgangen mellom virksomhetene skal ikke svekke informasjonssikkerheten ved behandling av opplysningene i noen av virksomhetene. Dette stiller krav til informasjonssikkerheten både i virksomheten som gir tilgang og i virksomheten som får tilgang.

Tredje ledd

En virksomhet som gir annen virksomhet tilgang, skal påse at denne virksomheten ivaretar kravene til informasjonssikkerhet, ved behandling av opplysninger etter forskriften. Den databehandlingsansvarlige som åpner for tilgang til helseopplysninger for ekstern virksomhet, må påse at virksomheten den inngår avtale med har tilfredsstillende informasjonssikkerhet. Denne "påse-plikten" korresponderer med pasientjournalloven § 22 fjerde ledd som sier at virksomheten har en aktiv plikt til å påse at mottaker av helseopplysninger har tilfredsstillende informasjonssikkerhet. Her kan det også vises til personopplysningsforskriften § 2-15 om sikkerhet hos andre virksomheter ved elektronisk overføring av personopplysninger.

Til § 6 Krav til autorisasjonen for tilgang til helseopplysninger i annen virksomhet

Helsepersonell og annet personell må være autorisert for å kunne få tilgang til helseopplysninger, se forskriften § 7 andre ledd bokstav c. En autorisasjon gir bestemte plikter og rettigheter til å behandle helseopplysninger.

Forskriften § 6 setter krav til autorisasjoner som gir tilgang til helseopplysninger mellom virksomheter. Bestemmelsen fastslår innledningsvis at helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet må ligge innenfor rammen av hva som er avtalt mellom virksomhetene.

Et eksempel: Det følger av forskriften § 4 at avtalen mellom virksomhetene skal angi hvilke journalmoduler avtalen gjelder. Autorisasjonen for tilgang til helseopplysninger i den andre virksomheten må da avgrenses til disse modulene. Autorisasjonen kan ikke omfatte tilgang til helseopplysninger som ikke er omfattet av avtalen. Hvis avtalen ikke omfatter journalene til avdelingen for psykisk helsevern og rus, kan autorisasjonen heller ikke omfatte tilgang til disse opplysningene.

Bokstav a

Rettigheter og plikter som følger av autorisasjonen skal beskrives i autorisasjonen. Bestemmelsen bidrar til å tydeliggjøre skillet mellom tilgang til helseopplysninger i egen virksomhet og tilgang mellom virksomheter. Helsepersonells tjenstlige behov for tilgang mellom virksomheter vil ofte være begrenset sammenlignet med behovet for tilgang i egen virksomhet. Rettighetene til å behandle opplysningene vil også være mer begrenset. Autorisasjonen som gjelder tilgang mellom virksomheter vil omfatte lesetilgang (dvs. rett til å søke og hente frem opplysninger og eventuelt føre eller kopiere dem inn i egen journal). Autorisasjonen kan eventuelt også gi rett til å sperre for videre lesing. Autorisasjonen kan ikke omfatte redigering, retting, sletting osv. fordi det ikke er adgang til å gi skrivetilgang, jf. merknadene til § 2. Se imidlertid punkt 5.6.2 om eventuell begrenset skrivetilgang.

En autorisasjon må også omfatte informasjon om hvorvidt og i hvilken grad den som er autorisert for tilgang mellom virksomheter også kan åpne for at annet helsepersonell i virksomheten kan få tilgang til opplysningene.

Bokstav b

Autorisasjonen skal være i samsvar med helsepersonellovens regler om taushetsplikt, jf. blant annet helsepersonelloven §§ 25 og 45. Bestemmelsen krever at autorisasjonen avviser eller ikke åpner for en forespørsel om å hente fram helseopplysninger mellom virksomheter dersom pasienten opplysningene gjelder har motsatt seg det, jf. forskriften § 9 første ledd.

Bokstav c

Autorisasjonen skal dokumenteres i virksomhetens autorisasjonsregister. Bestemmelsen forutsetter at den databehandlingsansvarlige har rutiner for å oppdatere og vedlikeholde informasjon om utstedte autorisasjoner, og at denne oppbevares. Dokumentasjonen skal gi informasjon om hvem som er tildelt autorisasjon og hva den medfører av rettigheter og plikter. Bestemmelsen må ses i sammenheng med § 11 om oppfølging og kontroll av tilgang.

Forskriften stiller ikke krav til hvor eller hvordan informasjonen oppbevares, og det vil være opp til virksomheten å vurdere hvor det er mest hensiktsmessig med slik dokumentasjon. Arkivloven med forskrifter vil komme til anvendelse for offentlige virksomheter. Det følger av arkivloven at sletting (kassasjon) av arkivmateriale krever hjemmel i eller i medhold av lov.

Bokstav d

Den databehandlingsansvarlige skal med utgangspunkt i egen virksomhet vurdere konkret hvilken varighet autorisasjonen skal ha. Varigheten må ses i sammenheng med vedkommendes oppgaver og ansvarsområder.

Bokstav e

Autorisasjonen skal alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold.

Til § 7 Tilgangsstyring

Første ledd

Begge virksomhetene skal ha tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger i samsvar med minimumskravene i §7 andre ledd. Virksomheten som får adgang til å gi helsepersonell tilgang i en annen virksomhets behandlingsrettet helseregister, skal gjøre en særskilt vurdering av hvem i virksomheten som skal gis autorisasjon for tilgang. Bestemmelsen må ses i sammenheng med forskriften § 6 om krav til autorisasjon.

Andre ledd

Bestemmelsen fastsetter minstekravene til tilgangsstyringen i begge virksomhetene. Virksomhetene må ha tekniske og organisatoriske løsninger som gjør det mulig å etterleve kravene, jf. § 3 bokstav b.

Bokstav a
Løsningene skal være slik at de kan sikre at helsepersonell i andre virksomheter ikke skal kunne hente frem helseopplysningene, dersom pasienten har motsatt seg eller motsetter seg at opplysningene skal gjøres tilgjengelige. Bestemmelsen presiserer og utvider pasientjournalloven § 17 som gir pasienten rett til å motsette seg at helseopplysninger gjøres tilgjengelige for helsepersonell.

Løsningene som implementeres skal sikre at tilgang til opplysningene begrenses slik at den bare omfatter behandling av de helseopplysningene som er nødvendige og relevante for behandlingen av den enkelte pasienten. Det betyr at virksomheter som åpner for tilgang fra andre virksomheter kan avgrense tilgangen til å omfatte tilstrekkelig strukturerte helseopplysninger knyttet til en navngitt pasient.

Bokstav b

Det skal kun gis tilgang til opplysninger som er relevante og nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til pasienten. Det er kun de som har et tjenstlig behov som skal få opplysningene, og de skal ikke få flere opplysninger enn det som er relevant og nødvendig for å yte helsehjelpen. Det må være tale om en aktuell behandlingssituasjon.

Kravet om at det bare kan gis tilgang til nødvendige og relevante opplysninger for å kunne gi helsehjelp til pasienten, innebærer at journalen må ha struktur som gjør at denne funksjonen kan oppfylles. Ved tilgang til opplysningene må systemene som benyttes kunne gi en differensiert mulighet for tilgangsstyring slik at en ved korrekt bruk av systemet kan hindre at helsepersonell får tilgang til andre opplysninger enn de etter reglene skal ha tilgang til. Det enkelte systemets funksjoner og muligheter må gjenspeiles/utnyttes i den praktiske tilgangsstyringen.

Se nærmere i punkt 5.10.3 og Prop. 72 L (2013-2014) punkt 11.3.4 om hva som menes med relevante og nødvendige helseopplysninger.

Bokstav c

Helsepersonellet må ha autentisert seg ved bruk av en sikker autentiseringsløsning for at opplysningene skal hentes frem. Det kan bare gis tilgang til helsepersonell som er autorisert for tilgang og har autentisert seg ved bruk av sikker autentiseringsløsning. En autorisasjon skal knyttes til en entydig identifisert person og bestemme hvilke tillatelser den identifiserte personen har til å behandle helseopplysninger. Dersom en autorisasjon omfatter å gi tillatelser til andre personer til å behandle helseopplysninger skal dette fremgå av autorisasjonen.

For å sikre at helseopplysninger ikke hentes frem uautorisert, er det viktig at det er stor grad av sikkerhet for at personen som henter frem opplysningene faktisk er den vedkommende utgir seg for å være. Autentisering er bevis for at oppgitt identitet er korrekt, og skal skje ved autentiseringsmekanisme på et høyt sikkerhetsnivå. Det innbærer at den elektroniske identifikasjonen må være av tilstrekkelig kvalitet og styrke for å sikre rett identitet på personen og at det kan brukes som bevis i en rettssak.

Enhver som gis tilgang til helseopplysninger skal kunne identifiseres som en bestemt person med bestemte rettigheter og plikter. Det kan ikke etableres noen form for «felles-konto» som gir personell i en virksomhet tilgang til opplysninger i en annen virksomhet uten at deres identitet er sikker.

Se nærmere om tilgangsstyringen i punkt 5.10.

Til § 8 Informasjon til pasienten

Første ledd

Bestemmelsen presiserer den generelle informasjonsplikten som gjelder for behandling av helseopplysninger etter forskriften, jf. også personopplysningsloven §§ 19 og 20. Den databehandlingsansvarlige skal gi informasjon etter denne bestemmelsen av eget tiltak. Pasienten har i tillegg innsynsrett i blant annet logg, se forskriften § 10 andre ledd.

Andre ledd

Bokstavene a og b

Databehandlingsansvarlige i virksomheter som lar andre virksomheter gi sitt helse-personell tilgang skal blant annet informere pasienten om hvilke virksomheter som gis tilgang og hvilke opplysninger tilgangen omfatter. Bestemmelsen er en presisering av personopplysningsloven § 19 først ledd bokstav c.

Bokstav c

Pasienten skal også informeres om retten til å motsette seg tilgang, og hvordan dette kan gjøres rent praktisk. Bestemmelsen er en presisering av kravene i personopplysningsloven § 19 første ledd bokstav e om informasjonsplikt med hensyn til forhold som gjør den registrerte i stand til å bruke sine rettigheter etter loven på best mulig måte. Bestemmelsen krever at pasienten får informasjon om sin rett til å motsette seg at helsepersonell i annen virksomhet gis tilgang.

Tredje ledd

Bestemmelsen presiserer informasjonsplikten til den databehandlingsansvarlige i virksomheten som gis tilgang. Pasienten skal informeres om at virksomheten elektronisk henter frem helseopplysninger om pasienten fra annen navngitt virksomhet.

Fjerde ledd

Informasjonen til pasienten skal tilpasses pasientens forutsetninger og tilstand, og kan unnlates dersom det er klart utilrådelig ut fra pasientens tilstand. Bakgrunnen for informasjonsplikten er hensynet til pasienten, blant annet at pasienten skal kunne

kontrollere hvem som kan bli kjent med helseopplysninger om seg. Informasjon til pasienten etter fjerde ledd kan derfor ikke unnlates hvis pasienten positivt ber om slik informasjon.

Til § 9 Sperring av helseopplysninger

Første ledd

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

Bestemmelsen forutsetter at virksomheten har et system som er tilrettelagt slik at helsepersonell effektivt kan bidra til at pasientens ønske om sperring for tilgang fra andre virksomheter effektivt kan etterleves.

Bestemmelsen forutsetter at helsepersonell gis kunnskap om at pasienten har rett til å motsette seg at opplysninger i virksomheten kan hentes frem fra andre virksomheter, informerer pasienten eller brukeren om det, og allerede ved registreringen av opplysningene kan sperre dem fra at det gis slik tilgang.

Se nærmere om sperring i punkt 5.12.

Andre ledd

Det følger av bestemmelsen at dersom vilkårene i pasient- og brukerrettighetsloven § 5-3 er oppfylt kan sperrede opplysninger utleveres. Pasient- og brukerrettighetsloven § 5-3 åpner for at selv om pasienten har motsatt seg det, så kan opplysningene likevel utleveres dersom tungtveiende grunner taler for det. I praksis er «tungtveiende grunner» 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 (Ot. prp. nr. 12 (1998-1999), merknadene til § 5-3). Det innebærer at helsepersonell som har tjenstlig behov for opplysningene ikke kan gis adgang til selv å hente frem opplysningene, men i stedet få dem utlevert.

Til § 10 Dokumentasjon av tilgang

Første ledd

Bestemmelsen krever at når personell i andre virksomheter henter frem helseopplysninger fra et behandlingsrettet helseregister, skal dette dokumenteres automatisk (logg). Dokumentasjonen skal minst inneholde informasjon om hvem som har hentet frem opplysningene, personens organisatoriske tilhørighet, grunnlaget for at opplysningene er hentet frem og i hvilket tidsrom de er hentet frem.

Det vil ikke være nok bare å dokumentere at begrunnelsen er helsehjelp. Bestemmelsen må ses i sammenheng med forskriften § 11 om oppfølging og kontroll av tilgang. Registreringen av grunnlaget for tilgangen skal inkludere tilstrekkelige opplysninger til at

det er mulig å fastslå om opplysningene er innhentet i samsvar med forskriften. Videre må virksomheten med bakgrunn i dokumentasjonen, eventuelt sammen med annen dokumentasjon, kunne kontrollere om vedkommende helsepersonell, som har hentet frem opplysningen, har hatt et behandlingsforhold til pasienten.

Bestemmelsen er blant annet en konkretisering av helsepersonelloven § 45 første ledd andre punktum om at det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger.

Andre ledd

Bestemmelsen fastslår at pasienten har rett til innsyn i og utskrift av dokumentasjonen. Virksomheten har ikke anledning til å ta vederlag for innsyn i og utskrift av denne dokumentasjonen, med mindre særlige forhold tilsier det.

Se nærmere om dokumentasjon av tilgang i punkt 5.13.

Til § 11 Oppfølging og kontroll av tilgang

Bestemmelsen krever at de databehandlingsansvarlige i begge virksomhetene skal samarbeide om kontroll av tilganger. Hendelsesregistreringer skal følges opp og kontrolleres løpende.

Den databehandlingsansvarlige i virksomheten som får adgang til å gi sitt helsepersonell tilgang, skal løpende kontrollere

- hvem i egen virksomhet som elektronisk har hentet frem helseopplysninger fra annen virksomhet
- grunnlaget for at opplysningene er hentet frem
- tidsperioden opplysningene er hentet frem

Dersom kontrollen viser at noen urettmessig har hentet frem helseopplysninger skal virksomheten opplysningene er hentet fra og pasienten opplysningene gjelder, varsles. Videre skal Datatilsynet informeres, jf. personopplysningsforskriften § 2-6.

Se nærmere om kontroll av tilgang i punkt 5.14.

Til § 12 Straff

Bestemmelsen fastslår at forsettlig eller grovt uaktsomt overtredelse av bestemmelsene i forskriften § 3 første ledd, jf. §§ 4 til 11, straffes med bøter eller fengsel inntil ett år eller begge deler.

8 Forslag til forskrift om tilgang til helseopplysninger mellom virksomheter

Fastsatt av Helse- og omsorgsdepartementet xx 2014 med hjemmel i lov 20. juni 2014 om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) § 19 tredje ledd og § 22 fjerde ledd.

§ 1 *Forskriftens formål*

Formålet med forskriften er at informasjonssikkerhet og personvern blir ivaretatt når det gis tilgang til helseopplysninger mellom virksomheter for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte.

§ 2 *Saklig virkeområde*

Forskriften gjelder når tilgjengeliggjøring av helseopplysninger i behandlingsrettede helseregistre, jf. pasientjournalloven § 19, skjer ved tilgang mellom virksomheter.

Med tilgang menes at helsepersonell gis adgang til elektronisk å hente frem helseopplysninger om pasienter.

Forskriften gjelder ikke tilgang til helseopplysninger mellom virksomheter som samarbeider om et felles behandlingsrettet helseregister etter pasientjournalloven § 9.

§ 3 *Grunnvilkår for tilgang mellom virksomheter*

Tilgang mellom virksomheter kan bare gis hvis følgende vilkår er oppfylt:

a) De databehandlingsansvarlige virksomhetene må ha inngått avtale i samsvar med § 4. Avtalepartene skal vurdere risiko for pasientenes personvern som tilgang kan føre til. Vurderingene skal minst omfatte risiko for brudd på taushetsplikt og svekket informasjonssikkerhet.

b) Begge virksomhetene skal ha rutiner og systemer som gir tilfredsstillende informasjonssikkerhet og tilgangsstyring som minst ivaretar kravene i §§ 5 til 11.

Dette gjelder i tillegg til de alminnelige kravene etter pasientjournalloven, personopplysningsloven og andre lover.

§ 4 Avtalens innhold

Avtalen om tilgang mellom virksomhetene skal minst angi

a) hva avtalen gjelder,

b) hvilke behovs- og risikovurderinger som ligger til grunn for avtalen,

c) hvilke journalmoduler avtalen omfatter, og

d) rutiner og fordeling av oppgaver for å ivareta kravene i denne forskriften.

§ 5 ***Informasjonssikkerhet***

De databehandlingsansvarlige i begge virksomhetene skal ha særlige rutiner for hvordan informasjonssikkerheten skal ivaretas ved tilgang mellom virksomhetene. Rutinene skal blant annet omfatte krav til risikovurdering, fysisk sikring, organisering, revisjon og avvikshåndtering.

Tilgangen skal ikke svekke informasjonssikkerheten ved behandling av helseopplysninger i noen av virksomhetene.

En virksomhet som gir annen virksomhet tilgang, skal påse at denne virksomheten ivaretar kravene til informasjonssikkerhet, ved behandling av opplysninger etter forskriften.

§ 6 Krav til autorisasjonen for tilgang til helseopplysninger i annen virksomhet

Innenfor rammen av hva som er avtalt mellom virksomhetene etter § 4, skal helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet

a) beskrive rettigheter og plikter som følger av autorisasjonen,
b) være i samsvar med helsepersonellovens regler om taushetsplikt, jf. blant annet helsepersonelloven §§ 25 og 45,
c) dokumenteres i virksomhetens autorisasjonsregister,
d) tidsbegrenses, og
e) alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold.

§ 7 ***Tilgangsstyring***

Begge virksomhetene skal ha tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger i samsvar med kravene i andre ledd.

Løsningene skal minst ivareta at

a) opplysningene ikke gjøres tilgjengelige dersom pasienten har motsatt seg eller motsetter seg det, jf. § 9.
b) det kun gis tilgang til opplysninger som er relevante og nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til pasienten,
c) helsepersonellet er autorisert for slik tilgang, og har autentisert seg ved bruk av sikker autentiseringsløsning.

§ 8 Informasjon til pasienten

Den databehandlingsansvarlige skal informere pasienten om virksomhetens behandling av helseopplysninger etter denne forskriften.

Den databehandlingsansvarlige i virksomheter som lar andre virksomheter gi sitt helsepersonell tilgang skal informere pasienten blant annet om

a) hvilke virksomheter som gis tilgang,

b) hvilke opplysninger tilgangen omfatter, og

c) at pasienten kan motsette seg at det gis tilgang, jf. § 9.

Virksomheter som henter frem opplysninger etter denne forskriften skal informere pasienten om dette.

Informasjonen etter denne bestemmelsen skal tilpasses pasientens forutsetninger og tilstand, og kan unnlates dersom det er klart utilrådelig ut fra pasientens tilstand.

§ 9 *Sperring av helseopplysninger*

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

Dersom tungtveiende grunner taler for det, kan sperrede opplysninger gjøres tilgjengelige for annet helsepersonell ved utlevering etter pasient- og brukerrettighetsloven § 5-3. Pasienten skal da informeres om at sperrede opplysninger utleveres, hvorfor de utleveres og til hvem.

§ 10 *Dokumentasjon av tilgang*

Bruk av tilgang til helseopplysninger mellom virksomheter for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte skal dokumenteres automatisk. Dokumentasjonen skal minst inneholde informasjon om

a) person og organisatorisk tilhørighet til den som har hentet frem opplysningene ,
b) hvorfor opplysningene er hentet frem , og
c) hvilke tidsperioder vedkommende har hentet frem opplysningene.

Pasienten har rett til innsyn i og utskrift av dokumentasjonen.

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

§ 11 ***Oppfølging og kontroll av tilgang***

Avtalepartene skal samarbeide om kontroll av tilganger.

Den databehandlingsansvarlige som har adgang til å autorisere helsepersonell for tilgang, skal løpende kontrollere

a) hvem i egen virksomhet som elektronisk har hentet frem helseopplysninger fra annen virksomhet,
b) hvorfor dette er gjort, og
c) tidsperioden opplysningene er hentet frem.

Dersom kontrollen viser at noen urettmessig har hentet frem helseopplysninger skal virksomheten opplysningene er hentet fra og pasienten opplysningene gjelder, varsles. Avviket skal håndteres i samsvar med personopplysningsforskriften § 2-6.

§ 12 ***Straff***

Den som forsettlig eller grovt uaktsomt overtrer bestemmelsene i forskriften § 3 første ledd, jf. §§ 4 til 11, straffes med bøter eller fengsel inntil ett år eller begge deler.

§ 13 ***Ikrafttredelse***

Forskriften gjelder fra den tid departementet bestemmer.