DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT

Rundskriv

Nr.	Vår ref	Dato
I-3/2019	19/1728	12. april 2019

Informasjonshåndtering i spesialisthelsetjenesten

I dette rundskrivet gjør Helse- og omsorgsdepartementet rede for noen av de viktigste reglene om informasjonshåndtering i spesialisthelsetjenesten. Departementet erfarer at det kan være uklarheter og ulike oppfatninger knyttet til forståelse og praktisering av reglene om taushetsplikt, personvern og informasjonssikkerhet.

Reglene må forstås og praktiseres i lys av at gode helsetjenester forutsetter at relevante pasientopplysninger kan deles. Helsepersonell har behov for opplysningene til å gi helsehjelp, til å kvalitetssikre helsehjelpen som gis og til egen læring. Virksomhetene har behov for opplysninger for å vite at de gir forsvarlig helsehjelp, og som grunnlag for systematisk arbeid med kvalitetsforbedring og pasientsikkerhet. Forskere har behov for opplysningene for å utvikle bedre helsetjenester. Dette forutsetter også at forskningsresultatene formidles og deles. Det er et økende behov for tilgjengeliggjøring av data mellom virksomheter ved ytelse av helsehjelp, og til kvalitetsforbedring, analyser og forskning.

Regelverket skal ikke være til hinder for innovasjon og bruk av ny teknologi som kan gi pasientene bedre helsehjelp. Regelverket er utarbeidet og vedtatt for å ivareta pasientens interesser. Helsehjelp, forskning og kvalitetsforbedring er alltid en balansegang mellom personvern og pasientsikkerhet. Virksomhetenes IKT-systemer kan og må utformes innenfor regelverket på en måte som sikrer at helsepersonell kan utveksle informasjon. Medisinsk kunnskap og data skal kunne nyttiggjøres på best mulig måte for pasientene og befolkningen.

Postadresse	Kontoradresse	Telefon*	Avdeling	Saksbehandler
Postboks 8011 Dep 0030 Oslo postmottak@hod.dep.no	Teatergt. 9 www.hod.dep.no	22 24 90 90 Org no. 983 887 406	Helserettsavdelingen	Sverre Engelschiøn 22 24 87 50

Dette stiller krav til informasjonshåndteringen i alle ledd. I praksis kan samspillet mellom pasientens ønske om konfidensialitet, gode dokumentasjonsrutiner og at informasjon er tilgjengelig for helsepersonellet være utfordrende. I en digital hverdag er personvern, informasjonssikkerhet og taushetsplikt avgjørende for at pasienter og pårørende skal ha tillit til helse og omsorgstjenesten. Tillit er en forutsetning for at de ønsker å dele nødvendige opplysninger med helsepersonellet. Dette krever at helseopplysninger ikke kommer på avveie, ikke endres urettmessig og er tilgjengelige ved behov. Pasientsikkerhet i en digital hverdag er på denne måten avhengig av egnede informasjonssikkerhetstiltak. Det er som hovedregel nødvendig med samtykke fra pasienten for å kunne bruke helseopplysninger til noe annet enn helsehjelp og for å kunne dele dem med andre.

Departementet ønsker å slå fast de grunnleggende rettslige utgangspunktene med hensyn til informasjonshåndtering. Reglene følger av EUs personvernforordning som gjelder som norsk lov, og av helsepersonellovens regler om taushetsplikt. Vi har også relevante regler i pasientjournalloven, helseregisterloven, helseforskningsloven mv. og i flere forskrifter. Forordningen krever at all behandling av personopplysninger har rettslig grunnlag i forordningen og eventuelt i norsk lov. Dersom det etter norske regler er lov til å behandle opplysningene, kan det legges til grunn at dette gir tilstrekkelig grunnlag også etter forordningen.

Departementet har igangsatt en vurdering av om det er behov for lov- eller forskriftsendringer. Dette gjelder særlig om helsepersonelloven § 29 c i tilstrekkelig grad ivaretar behovet for læringsarbeid og kvalitetssikring. Eventuelle forslag til regelverksendringer vil på vanlig måte bli sendt på offentlig høring.

Med hilsen

Kari Sønderland (e.f.)
ekspedisjonssjef

Sverre Engelschiøn
fagdirektør

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer

Innhold

1. Pasientsikkerhet og personvern ved ytelse av helsehjelp 4
2. Forholdet mellom helselovgivningen og personvernforordningen 5
3. Ansvar og roller 7
3.1 Virksomhetsansvar 7
3.2 Dataansvar 8
3.3 Helsepersonellets individansvar 9
3.4 Personvernombudet 10
4 Opplysninger til bruk i læringsarbeid og kvalitetssikring 10
5 Personopplysninger vs anonyme opplysninger 13
5.1 Anonyme opplysninger 13
5.2 Pseudonyme opplysninger 14
6 Deling av forskningsdata og publisering av forskningsresultater 15
6.1 Krav om samtykke eller annet rettslig grunnlag 16
6.2 Gyldig samtykke 17
6.3 Atferdsnorm for helseforskning 18

1. Pasientsikkerhet og personvern ved ytelse av helsehjelp

All pasientbehandling forutsetter behandling av helseopplysninger om pasienten. God pasientsikkerhet krever at opplysninger lagres og deles mellom helsepersonell. Pasientsikkerhet handler om å unngå unødig skade på pasient som følge av helsetjenestens ytelser eller mangel på ytelser. Mangelfull informasjon og svikt i overganger innad og mellom helsetjenestenivå er dokumentert som en av de største risikoområdene for god pasientsikkerhet. Forholdet mellom pasientsikkerhet og den enkeltes personvern er balansert på et overordnet nivå i regelverket.

Departementet mener at regelverket ikke er til hinder for å gi helsepersonell som skal behandle en pasient, adgang til alle nødvendige helseopplysninger om den de skal behandle. I tilfeller der dette ikke har grunnlag i lov eller forskrift, er det nødvendig å innhente pasientens samtykke. Feilaktig tolkning av personvernkravene og helselovgivningen kan få negative konsekvenser for den enkelte pasients helsehjelp. Det er derfor viktig å sikre god forholds-messighet mellom hensynet til personvern og hensynet til pasientsikkerhet.

I pasientjournalloven er samspillet synliggjort i formålsbestemmelsen. Behandling av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet, ved at relevante og nødvendige opplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell. Samtidig skal vernet mot at opplysninger gis til uved-kommende ivaretas. Behandlingen av helseopplysningene skal sikre pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning (se § 1). Videre er formålet med spesialisthelsetjenesteloven blant annet å bidra til at tjenestetilbudet blir tilpasset pasientenes behov, og bidra til at tjenestetilbudet blir tilgjengelig for pasientene (se § 1-1).

Ivaretakelse av pasientens personvern vil samtidig være viktig for pasientsikkerheten, for eksempel ved at journalopplysningene er relevante, korrekte og oppdaterte. God informasjonssikkerhet for pasientjournaler og ved bruk av medisinsk utstyr er en forutsetning for å kunne utøve forsvarlige helsetjenester. Ved bruk av medisinsk utstyr og teknologi med mangelfull sikkerhet, kan helsepersonell støte på utfordringer både i personvernlovgivningen og forsvarlighetskravet i helseretten. Dette gjelder ikke minst sikkerhet for at relevante opplysninger er tilgjengelig når det er behov for det eller at de har blitt endret utilsiktet. Videre er helsepersonellets taushetsplikt et viktig personvernelement, og en forutsetning for det nødvendige tillitsforholdet mellom pasienter og helsepersonell.

Det vil i enkelte situasjoner være utfordringer mellom det å gi pasientbehandling på en arbeidseffektiv, helsefaglig fornuftig og sikker måte og ivaretagelse av pasientens personvern. Et motsetningsforhold kan bli særlig fremtredende når de ulike IKT-systemene ikke fungerer godt nok sammen eller det er organisatoriske forhold ved helseforetaket som ikke er tilpasset behovene for informasjonsdeling, internt eller mellom virksomheter.

I mangel av effektive og tilpassede IKT-løsninger har det hendt at helsepersonell i akuttsituasjoner har hatt behov for å sende røntgenbilder og EKG via sine telefoner for å innhente råd fra kollegaer. Dette er en uheldig praksis, men kan ut fra en nødrettsbetraktning av og til være nødvendig for å gi pasienten trygg og rask behandling. At helsepersonellets privattelefon og utradisjonelle tiltak benyttes i kritiske situasjoner kan forsvares i enkelttilfeller, men når dette går over i en systematisk praksis berører det virksomhetens systemansvar etter spesialisthelsetjenesteloven § 2-2 og § 3-2. Virksomhetsansvaret er omtalt i kapittel 3.

Det er ulikheter i IKT-infrastruktur og organisatoriske forhold ved helseforetakene. Regelverket stiller gjennomgående funksjonelle krav som *forsvarlig helsehjelp* og *egnet sikkerhetsnivå*, men i liten grad konkrete krav til virkemidler for å oppnå disse målene. Ulikheter i IKT-infrastruktur og organisatoriske forhold kan kreve ulike vurderinger og ulike kompenserende sikkerhetstiltak for å ivareta forsvarlighetskravet og pasientens personvern.

Utvikling og implementering av effektive systemer som ivaretar både pasientsikkerhet og personvern på en god måte forutsetter et samarbeid mellom helsepersonell, personer med IKT-kompetanse og juridisk kompetanse. For å kunne ivareta pasientene på en god måte må de kompenserende sikkerhetstiltakene tilpasses de reelle forholdene ved det enkelte foretak. For å kunne oppfylle regelverkets krav og belyse mulighetene er det nødvendig å skille mellom hvilke problemstillinger som skyldes teknologiske utfordringer ved det enkelte helseforetaket, organisatoriske forhold og begrensninger som følger av regelverket. I tillegg er helseforetakene avhengig av velfungerende rutiner og internkontroll som sikrer at beslutningene tas på riktig nivå, et nivå hvor det totale bildet er synlig.

Se også Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.

2. Forholdet mellom helselovgivningen og personvernforordningen

I spesialisthelsetjenesten behandles helseopplysninger i forbindelse med helsehjelp, kvalitetsforbedring, forskning, statistikk, helseanalyser mv. EUs personvernforordning, personopplysningsloven og helselovene setter vilkår for all behandling av helseopplysninger.

Helseopplysninger er "personopplysninger om en fysisk persons fysiske eller psykiske helse, medregnet om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand" (jf. pasientjournalloven § 2 b og helseregisterloven § 2 a). Av personvernforordningen artikkel 4 nr. 1 følger at:

> *Personopplysninger* er enhver opplysning om en identifisert eller identifiserbar fysisk person ("den registrerte"); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet

Av samme artikkel i nr. 2 følger at:

> *Behandling* er enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Behandling er et begrep som tradisjonelt sett har en helt annen betydning i helsesektoren. Behandling av opplysninger må skilles fra behandling av pasienter ved sykdom. Det er viktig å merke seg at behandling av opplysninger i helsetjenesten omfatter alt fra registrering av pasientopplysninger i journalen, oppslag i journal og deling av opplysninger om pasienten mellom helsepersonell som yter helsehjelp til pasienten – til innsamling, lagring og analyse av opplysninger i forskningsprosjekter og formidling av forskningsresultater.

Personvernforordningen gjelder som norsk lov fra 20. juli 2018. Personvernforordningens regelsett er innarbeidet som en del av helselovgivningen og innebærer at det norske personvernregelverket er samordnet med EU-regelverket. Forordningen er "hovedloven" om de materielle reglene om personvern og informasjonssikkerhet, og skal legges til grunn ved all behandling av helseopplysninger. Forordninger skal gjennomføres "som sådan" i nasjonal rett og er gjort gjeldende som norsk lov uten omskrivninger i medhold av personopplysningsloven § 1. Helse- og omsorgsdepartementet kan derfor ikke avgi autoritative tolkningsuttalelser om hvordan forordningen skal forstås og praktiseres. Det er Datatilsynet som fører tilsyn med etterlevelsen av personvernforordningen og personopplysningsloven. Helse- og omsorgsdepartementet kan derfor ikke avgi autoritative tolkningsuttalelser om hvordan forordningen skal forstås og praktiseres.

Vi har flere lover og en rekke forskrifter som gir særregler om behandling av helseopplysninger og som utfyller kravene i personvernforordningen. Departementet forvalter denne typen regler i helselovgivningen. Fortolkningsoppgaven er i all hovedsak delegert til Helsedirektoratet, men for enkelte bestemmelser er dette delegert til Direktoratet for e-helse. Helsetilsynet fører tilsyn med helse- og omsorgstjenestene.

Usikkerhet i fortolkningen og ulik praktisering av reglene mellom virksomheter og mellom land, kan skape unødvendige uklarheter i avveiningen mellom pasientsikkerhet og personvern. Det er derfor viktig at helseforetakene har tilgang til og bruker juridisk kompetanse til å vurdere de juridiske implikasjonene i den daglige driften. Når juristene ved et helseforetak opplever usikkerhet ved tolkningen av helselovgivningen og juridisk litteratur eller andre rettskilder ikke gir svar, kan det være naturlig å rette en henvendelse til eget regionalt helseforetak, eventuelt til Helsedirektoratet eller Direktoratet for e-helse.

Ved spørsmål om personvernforordningen som ikke avklares internt i organisasjonen, herunder personvernombudet, kan det rettes spørsmål til Datatilsynet. Dersom utfordringen gjelder forholdet mellom helselovgivningen og personvernforordningen, er det naturlig at

saken vurderes av jurister med helserettsfaglig kompetanse og Datatilsynet. Personvernombudet vil kunne ha en rolle i denne dialogen. Denne form for samarbeid kan bidra til viktig erfaring og god veiledning i avveiningen mellom pasientsikkerhet og personvern. Ansvaret for de endelige beslutningene skal likevel alltid ligge hos ledelsen i helseforetaket, se kapittel 3.

3. Ansvar og roller

Ved ethvert helseforetak skal ansvar og oppgaver være tydelig avklart. Det bør ikke være tvil om hvem som skal ta hvilke beslutninger. Det er særlig tre former for ansvar som er relevant ved informasjonshåndtering i spesialisthelsetjenesten; *virksomhetsansvar* etter spesialisthelsetjenesteloven mv., *dataansvar* etter personvernlovgivningen og *helsepersonellets individansvar* etter helsepersonelloven. *Personvernombudets* rolle er også relevant. Ved deling av opplysninger og annen informasjonshåndtering i spesialisthelsetjenesten har alle disse aktørene en rolle og et ansvar.

3.1 Virksomhetsansvar

Eiere og ledere i helsetjenesten har et generelt ansvar for at tjenestenes drift gjennomføres innen lovfastsatte rammer, herunder legge til rette for at personell som utfører tjenestene blir i stand til å overholde sine lovpålagte plikter. Vi viser særlig til helsepersonelloven § 16, spesialisthelsetjenesteloven § 2-2, jf. §§ 2-1e, 3-4a og 3-2, og helse- og omsorgstjenesteloven § 4-1, jf. § 5-10. I forskning skal institusjonen etter forskningsetikkloven § 5 og helseforskningsloven § 5 sikre at forskningen er forsvarlig og skjer i henhold til anerkjente forskningsetiske normer.

Det følger videre av pasientjournalloven § 19 at virksomheten (den dataansvarlige) 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. Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp, jf. helsepersonelloven § 25.

Det er den dataansvarlige som bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Det er imidlertid en forutsetning at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten. Hvordan opplysninger kan gjøres tilgjengelig er altså avhengig av kvaliteten og mulighetene i IKT-systemene hos både avgiver og mottaker. Videre følger det av spesialisthelsetjenesteloven § 3-2 at helseforetak skal sørge for at journal- og informasjonssystemene ved institusjonen er forsvarlige. Det skal tas hensyn til behovet for effektiv elektronisk samhandling ved anskaffelse og videreutvikling av journal- og informasjonssystemer.

Av forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten følger at den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter i tråd med denne forskriften og at medarbeiderne i virksomheten medvirker til dette, jf. § 3. I denne forskriften betyr styringssystem for helse- og omsorgstjenesten den del av virksomhetens styring som omfatter hvordan virksomhetens aktiviteter planlegges, gjennomføres, evalueres og korrigeres i samsvar med krav fastsatt i eller i medhold av helse- og omsorgslovgivningen, jf. § 4. Plikten til å planlegge omfatter å ha oversikt over og beskrive virksomhetens mål, oppgaver, aktiviteter og organisering. Det skal klart fremgå hvordan ansvar, oppgaver og myndighet er fordelt og hvordan det skal arbeides systematisk for kvalitetsforbedring og pasient- og brukersikkerhet i virksomheten, jf. § 6 bokstav a. Av § 7 bokstav a følger plikt til å sørge for at virksomhetens oppgaver, organisering og planer er kjent i virksomheten og gjennomføres. Minst en gang i året skal det gjøres en systematisk gjennomgang av hele styringssystemet, jf. § 8 bokstav f.

Virksomheten har videre en plikt til å rette opp uforsvarlige og lovstridige forhold, jf. forskriften § 9. I dette ligger å sørge for korrigerende tiltak som bidrar til at helse- og omsorgslovgivningen etterleves, inkludert faglig forsvarlige tjenester, og at systematisk arbeid for kvalitetsforbedring og pasient- og brukersikkerhet gjennomføres. Det ligger også en plikt til å forbedre nødvendige prosedyrer, instrukser, rutiner eller andre tiltak for å avdekke, rette opp og forebygge overtredelse av helse- og omsorgslovgivningen, inkludert krav til faglig forsvarlighet og systematisk arbeid for kvalitetsforbedring og pasient- og brukersikkerhet. For at virksomheten skal kunne følge regelverket på en smidig måte, må det legges til rette for at virksomhetens ansatte enkelt kan melde om avvik og uønskede hendelser –uten frykt for represalier. Meldinger om avvik og uønskede hendelser må brukes til læring og forbedring på systemnivå. Dette inkluderer også risikofaktorer forbundet med samhandling internt og eksternt, jf. § 6 bokstav e. Ved brudd på personopplysningssikkerheten skal i alminnelighet Datatilsynet varsles.

3.2 Dataansvar

Enhver behandling av helseopplysninger må kunne knyttes til en behandlingsansvarlig. I helselovgivningen betegnes den behandlingsansvarlige som dataansvarlig. Ingen kan behandle helseopplysninger uten at det er klart hvem som er dataansvarlig.

Det er virksomheten – helseforetaket, eventuelt regionalt helseforetak, som er dataansvarlig. Det følger av personvernforordningen artikkel 4 nr. 7 at den behandlingsansvarlige (dataansvarlige) er

> en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.

Det er den dataansvarlige som har ansvaret for personvernet ved behandling av helseopplysninger. Den dataansvarlige har også ansvaret for at de registrerte får oppfylt sine personvernrettigheter, for eksempel når de ber om innsyn i opplysninger om seg selv. Den dataansvarlige kan inngå avtale med en databehandler, som da behandler opplysningene på vegne av den dataansvarlige.

Se også ny forskrift om pasientjournal § 3 om dataansvarlig og Kongelig resolusjon (PRE-2019-03-01-168 Fastsettelse av ny forskrift om pasientjournal), hvor dataansvar omtales særskilt.

3.3 Helsepersonellets individansvar

Det enkelte helsepersonell har ansvar for å opptre i samsvar med lovpålagte krav, først og fremst å yte forsvarlige helsetjenester. Av helsepersonelloven § 4 følger det at "(H)elsepersonell skal utføre sitt arbeid i samsvar med de krav til faglig forsvarlighet og omsorgsfull hjelp som kan forventes ut fra helsepersonellets kvalifikasjoner, arbeidets karakter og situasjonen for øvrig."

Forsvarlighetskravet er en rettslig standard. Det konkrete innholdet i forsvarlighetskravet kan bare fastsettes i det enkelte tilfellet vurdert på bakgrunn av de foreliggende omstendigheter, for eksempel gjennom tilsynsmyndighetenes virksomhet eller domstolsavgjørelser. Forsvarlighetskravet er knyttet til hva som kan forventes på bakgrunn av det enkelte personells kvalifikasjoner og bakgrunn. Innholdet i normen vil blant annet være avhengig av den enkeltes faglige tilhørighet, formelle og reelle kvalifikasjoner, variasjoner i personlig erfaring og kompetanse. Forsvarlighetskravet for helsepersonell er forankret i anerkjent fagkunnskap, herunder vitenskapelig forskning og erfaringsbasert systematisert kunnskap, faglige retningslinjer og allmenngyldige samfunnsetiske normer.

Krav til forsvarlighet innebærer at helsepersonellet må innrette seg etter sine faglige kvalifikasjoner og respektere begrensninger i egen kompetanse, jf. § 4 andre ledd. Det fremgår uttrykkelig at helsepersonell skal innhente bistand eller henvise pasienten videre der dette er nødvendig og mulig. Plikten til å samarbeide og samhandle med annet kvalifisert personell dersom pasientens behov tilsier dette understrekes også.

Det følger av forsvarlighetskravet at personellet har en plikt til å innhente nødvendig informasjon om pasienten før helsehjelp gis. Det må innhentes tilstrekkelig informasjon til at beslutning om og gjennomføring av hjelp etter loven kan gjøres forsvarlig.

Helsepersonells individansvar omfatter blant annet også lovpålagt taushetsplikt, en plikt til å dokumentere "relevante og nødvendige opplysninger om pasienten og helsehjelpen", gi innsyn i journal til de har som har krav på det, og dele opplysninger med annet helsepersonell "når dette er nødvendig for å kunne gi forsvarlig helsehjelp", jf. helsepersonelloven §§ 39, 40, 25 og 45.

Av helseforskningsloven § 5 første ledd følger at "(M)edisinsk og helsefaglig forskning skal organiseres og utøves forsvarlig." I bestemmelsens tredje ledd er det presisert at medisinsk og helsefaglig forskning "skal vareta etiske, medisinske, helsefaglige, vitenskapelige og personvernmessige forhold."

Etter forskningsetikkloven § 4 skal den enkelte forsker opptre med aktsomhet for å sikre at all forskning skjer i henhold til anerkjente forskningsetiske normer. Dette gjelder også under forberedelser til forskning, rapportering av forskning og andre forskningsrelaterte aktiviteter.

3.4 Personvernombudet

Personvernombudet har en selvstendig rolle og skal gi råd og veiledning, men det er ledelsen ved helseforetaket som er ansvarlig for beslutningene. Ombudet har en rådgivende rolle ved helseforetakene og har blant annet i oppgave å informere om gjeldende personvernlovgivning. Ansvaret for et helseforetaks beslutninger kan ikke plasseres hos personvernombudet, men ligger alltid hos virksomhetens ledelse.

Personvernombudets stilling og oppgaver er beskrevet direkte i personvernforordningen artikkel 38 og 39. I tillegg er ombudet pålagt særlige oppgaver gjennom personopplysningsloven § 9 og taushetsplikt gjennom personopplysningsloven § 18.

Virksomhetens ledelse skal sikre at personvernombudet ikke mottar instrukser om utførelsen av oppgaven. Personvernombudet kan ikke straffes eller avsettes for å utføre sine oppgaver. Ombudet rapporterer direkte til det høyeste ledelsesnivå i virksomheten. Se personvernforordningen artikkel 37, 38 og 39, datatilsynet.no, Artikkel 29-gruppen *Guidelines on Data Protection Officers ('DPOs')*, 5. april 2017 og Norm for informasjonssikkerhet og personvern faktaark nr. 35.

I mange virksomheter har personvernombudet også andre oppgaver. Av forordningen artikkel 38 nr. 6 følger at den dataansvarlige skal sikre at disse oppgavene ikke fører til interesse-konflikt.

4. Opplysninger til bruk i læringsarbeid og kvalitetssikring

Helsepersonell som tidligere har tatt del i undersøkelse eller behandling av en pasient kan i ettertid ha behov for å gjøre seg kjent med taushetsbelagte opplysninger om pasienten, for eksempel ved innsyn i pasientens journal. Dette vil typisk gjelde der hvor man ønsker å få avklart om de vurderingene som ble gjort, om de tiltakene man iverksatte eller om de rådene man ga, var riktige. En slik adgang er avgjørende for læring og for kvalitetssikring av helsehjelpen.

Helsepersonelloven § 29 c åpner for innsyn i eller tilgjengeliggjøring av taushetsbelagte opplysninger for slikt formål. Bestemmelsen lyder:

> § 29 c. Opplysninger til bruk i læringsarbeid og kvalitetssikring
> Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger etter særskilt anmodning gjøres tilgjengelige for annet helsepersonell som tidligere har ytt helsehjelp til pasienten i et konkret behandlingsforløp, for kvalitetssikring av helsehjelpen eller egen læring. Behandlingen av anmodningen kan automatiseres. Første punktum omfatter opplysninger som er nødvendige og relevante for formålet. I pasientens journal skal det dokumenteres hvem opplysninger har blitt gjort tilgjengelige for, og hvilke opplysninger som har blitt gjort tilgjengelige, jf. § 40.

For en utførlig redegjørelse for bestemmelsen vises det til Helsedirektoratets Rundskriv IS-8/2012 *Helsepersonelloven med kommentarer*. Som det fremgår må flere vilkår være oppfylt for å kunne gjøre seg kjent med taushetsbelagte opplysninger:

- Formålet med å gjøre seg kjent med taushetsbelagte opplysninger må være *læringsarbeid eller kvalitetssikring* av helsehjelpen. Et ønske om innsyn som er begrunnet i andre formål må vurderes etter annet regelverk.
- Det er *ikke krav om å innhente samtykke* fra pasienten først. Dersom en pasient eksplisitt har motsatt seg slikt innsyn i ettertid, må dette respekteres.
- Det helsepersonell som ønsker å gjøre seg kjent med taushetsbelagte opplysninger må ha ytt helsehjelp til pasienten i *et konkret behandlingsforløp*. Bestemmelsen gir ikke rett til taushetsbelagte opplysninger om behandlingsforløp som helsepersonellet ikke selv har vært involvert i og det kan uansett bare utleveres opplysninger som er *nødvendige og relevante* for læringsarbeid eller kvalitetssikring av helsehjelpen.
- Det helsepersonell som ønsker å gjøre seg kjent med taushetsbelagte opplysninger må *særskilt anmode* om dette.
- Vurdering av en slik anmodning kan skje *automatisert*, det vil si uten at en fysisk person i hvert enkelt tilfelle må ta stilling til anmodningen. Hensikten med en slik ordning er å lette administrasjonen og å gi lettere tilgang for helsepersonell så fremt bestemmelsens øvrige vilkår er oppfylt. Den dataansvarlige må i så fall bestemme hvilke prosesser som skal følges, innenfor rammene av reglene om taushetsplikt og informasjonssikkerhet, inkludert pasientens rett til vern mot spredning av taushetsbelagte opplysninger.
- Med *tilgjengeliggjøring* menes at opplysningene gjøres tilgjengelige ved utlevering eller ved at helsepersonellet gis tilgang til å søke opp de aktuelle opplysningene i systemet, jf. pasientjournalloven § 19. Bestemmelsens ordlyd er altså teknologinøytral ved at den uttrykkelig åpner for at helsepersonellet også kan få opplysninger ved at det gis tilgang, fremfor ved utlevering av data på minnepinne, utskrift, muntlig eller annet.

- Når helsepersonell gis tilgang på denne måten, må det aksepteres en viss grad av søking etter "nødvendige og relevante" helseopplysninger i pasientens journal. Dermed må en slik løsning kunne innebære at det enkelte helsepersonell også vil kunne få tilgang til opplysninger som ut fra en streng fortolkning ikke er nødvendige og relevante for læringsarbeid eller kvalitetssikring av helsehjelpen. Se også pasientjournalloven § 19 om tilgang i forbindelse med aktuell helsehjelp, der avgrensningen "relevante og nødvendige helseopplysninger" må tolkes på samme måte.
- Bestemmelsen åpner også for at det kan gis innsyn eller utleveres opplysninger fra *annet helseforetak eller andre deler av helse- og omsorgstjenesten* enn der hvor helsepersonellet arbeider. Dette vil typisk gjelde situasjoner hvor pasienten etter innledende undersøkelse eller behandling ved et helseforetak henvises eller overføres til et annet helseforetak for videre undersøkelse eller behandling. Et annet eksempel er der hvor ambulansepersonell eller innleggende fastlege/legevaktslege ber om opplysninger fra et helseforetak for å få avklart om deres vurderinger eller behandlingsmessige tiltak i ettertid viste seg å være riktige.
- I pasientens journal skal det blant annet *dokumenteres* hvem opplysninger har blitt gjort tilgjengelige for, se pasientjournalloven § 22 og den nye pasientjournalforskriften § 14 (i kraft 1. juli 2019).

Spørsmål om innsyn i journalopplysninger etter helsepersonelloven § 29 c er ikke utelukkende et spørsmål om hva regelverket åpner for. Slike innsyn er også betinget av at de tekniske løsningene gir tilgang til de opplysningene bestemmelsen gir unntak for. Det er for eksempel ikke gitt at pasientjournalsystemene ved de ulike helseforetakene er så integrerte at det er mulig med direkte elektronisk tilgang til journaler ved ulike foretak. Selv om bestemmelsen åpner for at det kan gis innsyn/utleveres opplysninger fra annet helseforetak, kan det være tekniske eller sikkerhetsmessige krav eller løsninger som gjør det vanskelig for det enkelte helsepersonell med "direkte oppslag" i pasientens journal hos et annet helseforetak. Her kan man oftere måtte basere seg på løsninger som innebærer at helsepersonell ved aktuelle helseforetak på forespørsel må ta stilling til hvilke opplysninger som kan utleveres.

Helsedirektoratet har i en tolkningsuttalelse 12. mars 2019 vurdert lovens ordning med automatisering av anmodninger om å gjøre seg kjent med taushetsbelagte pasientopplysninger. I den forbindelse har direktoratet vurdert om det er adgang til slikt innsyn basert på en skriftlig rutine hvor innsyn automatisk godkjennes etter generelle kriterier som virksomheten har fastsatt. Etter direktoratets vurdering er det tvilsomt at kun en skriftlig rutine hvor innsyn godkjennes etter gitte kriterier uten at det foretas en konkret vurdering, vil være tilstrekkelig for å kunne oppfylle de krav som lovgiver har stilt til automatisering av behandling av anmodning om innsyn etter bestemmelsen. Departementet er enig i direktoratets fortolkning og legger til grunn at slike skriftlige rutiner i så fall må suppleres med elektroniske elementer som god tilgangsstyring, logging av innsyn og samtidig dokumentasjon av formålet med innsynet.

Departementet har igangsatt en vurdering av om helsepersonelloven § 29 c i tilstrekkelig grad ivaretar behovet for læring og kvalitetssikring. Eventuelle forslag til endringer vil på vanlig måte bli sendt på offentlig høring.

5. Personopplysninger vs anonyme opplysninger

Personopplysninger er opplysninger der enkeltpersoner kan identifiseres direkte eller indirekte. Helseopplysninger er en form for personopplysninger, se kapittel 2 om hva som menes med helseopplysninger og personopplysninger.

5.1 Anonyme opplysninger

Anonyme opplysninger kan ikke knyttes til enkeltpersoner og regnes derfor ikke som personopplysninger. Behandling av slike opplysninger omfattes ikke av taushetsplikten eller personvernreglene, og kan fritt innsamles, registreres, utleveres mv. Det vil derfor være viktig å vurdere om et datasett er anonymt.

Når en opplysning er anonym er forklart i punkt 26 i fortalen til EUs personvernforordning:

> "Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den [dataansvarlige] eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking. For å fastslå om midler med rimelighet kan tenkes å bli tatt bruk for å identifisere den fysiske personen bør det tas hensyn til alle objektive faktorer, f.eks. kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utvikling. Prinsippene om vern av personopplysninger bør derfor ikke få anvendelse på anonyme opplysninger, nærmere bestemt opplysninger som ikke kan knyttes til en identifisert eller identifiserbar fysisk person, eller personopplysninger som er blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres. Denne forordning gjelder derfor ikke behandling av slike anonyme opplysninger, herunder for statistiske formål eller forskningsformål."

Ved behandling av anonyme opplysninger skal det ikke, verken direkte eller indirekte, være mulig å spore opplysningene tilbake til de enkeltpersonene opplysningene knytter seg til. Den nedre grensen for når en opplysning kan anses for å være anonym må vurderes konkret. Mengden og arten av opplysninger (variabler) om samme person er av betydning ved vurderingen av om opplysningene er anonyme.

Det er likevel klart at ikke enhver teoretisk mulighet å identifisere enkeltpersoner er nok til at opplysningene ikke er anonyme. I vurderingen av om opplysningene er anonyme eller ikke, må en se hen til om det er en reell sannsynlighet for identifikasjon, og ikke om identifikasjon kun er hypotetisk mulig. Man må ta utgangspunkt i de tilgjengelige hjelpemidlene det er rimelig å ta i bruk for identifikasjon. Dersom innsatsen som skal til for å knytte en person til

et sett av opplysninger er store eller krever metoder som er svært arbeidskrevende, kostbare eller avhengig av særskilt kompetanse, vil det ikke være en personopplysning.

Den nærmere fortolkningen av forordningen og hva som kreves for at opplysningene skal regnes som anonyme, må fastslås av Datatilsynet og EU/EØS-organene. Den tidligere Artikkel 29-gruppen i EU har utgitt *Opinion 05/2014 on Anonymisation Techniques*. Se også Datatilsynets veileder *Anonymisering av personopplysninger*. Disse er eldre enn personvern-forordningen, men gir likevel relevant veiledning om anonymisering, pseudonymisering mv.

5.2 Pseudonyme opplysninger

Pseudonymisering kan redusere personvernrisikoen ved at opplysningene ikke like lett kan knyttes til et individs identitet. Dette kan redusere eller fjerne uheldige konsekvenser dersom helseopplysninger skulle komme på avveie, samtidig som det er mulig for forskningsprosjektet å finne tilbake til de enkelte individene. Forordningen fastsetter ingen plikt til å pseudonymisere personopplysninger. Pseudonymisering er imidlertid nevnt som et mulig tiltak som kan være egnet for å verne de registrertes rettigheter.

Pseudonymisering vil si at enkelte direkte personentydige kjennetegn erstattes med løpe-nummer e.l, som fremdeles vil være unike indikatorer. Pseudonymisering er i forordningen artikkel 4 nr. 5 definert som

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

Det står i fortalen punkt 28 og 29 at pseudonymisering

> kan redusere risikoene for de berørte registrerte og bidra til at [dataansvarlige] og databehandlere kan oppfylle sine forpliktelser med hensyn til vern av person-opplysninger. Hensikten med den uttrykkelige innføringen av 'pseudonymisering' i denne forordning er ikke å utelukke andre tiltak for vern av personopplysninger.
>
> For å skape insitamenter til bruk av pseudonymisering i forbindelse med behandling av personopplysninger bør pseudonymiseringstiltak som samtidig tillater en generell analyse, være mulig hos den samme [dataansvarlige] når denne har truffet de tekniske og organisatoriske tiltak som er nødvendige for å sikre at denne forordning gjennom-føres med tanke på den berørte behandlingen, og at tilleggsopplysninger som gjør det mulig å knytte personopplysningene til en bestemt registrert, lagres atskilt. Den [data-ansvarlige] som behandler personopplysningene, bør angi de autoriserte personene hos den samme [dataansvarlige].

Pseudonymiserte opplysninger er ikke anonyme opplysninger, men personopplysninger som må behandles etter personvernreglene. Dette følger av at pseudonymisering ikke utelukker at man kan finne tilbake til hvem opplysningene gjelder ved hjelp av en koblingsnøkkel ("nøkkel" eller kode). Pseudonymisering gir heller ikke i seg selv sikkerhet for at enkeltpersoner ikke vil kunne gjenkjennes på bakgrunn av variablene i datasettet. Opplysningene vil derfor kunne være indirekte identifiserbare. Større datamengder, økt digitalisering og nye tekniske løsninger betyr at risikoen for bakveisidentifisering er blitt såpass stor, at det kan være vanskelig å pseudonymisere opplysninger på en måte som umuliggjør reidentifisering.

Departementet gjør oppmerksom på at kravet om pseudonymisering i forskriftene for Reseptregisteret og IPLOS-registeret, er noe annet og strengere enn det som menes med pseudonymisering etter forordningen. I motsetning til det som gjelder etter forordningen, kan den dataansvarlige ikke ha tilgang til både navn og pseudonym. Etter forordningen er kravet bare at disse lagres og behandles atskilt.

6. Deling av forskningsdata og publisering av forskningsresultater

Forskningsdata og forskningsresultater fra forskningsprosjekter i helseforetakene inneholder gjerne opplysninger om forskningsdeltakernes helse. Publisering av forskningsresultater er en påkrevet del av det å drive forskning, og nasjonalt og internasjonalt arbeides det for økt tilgjengeliggjøring og deling av forskningsdata. Taushetsplikten, personvernreglene og forskningsetikken stiller samtidig vilkår for å kunne dele forskningsdata ("rådata") eller publisere forskningsresultater hvor forskningsdeltakeren kan kjennes igjen.

Dersom opplysningene er anonyme, kan opplysningene fritt publiseres eller deles på andre måter. Opplysningene er anonyme dersom enkeltpersoner verken direkte eller indirekte kan identifiseres. Større datamengder, økt digitalisering og nye tekniske løsninger (kunstig intelligens mv.) betyr at risikoen for bakveisidentifisering er blitt såpass stor, at det blir vanskeligere å anonymisere opplysninger på en måte som umuliggjør reidentifisering. Særlig gjelder dette mindre studier, sjeldne sykdommer og studier som inkluderer genetiske opplysninger. Se kapittel 5 om personopplysninger vs anonyme opplysninger.

Dersom enkeltpersoner kan identifiseres, er det tale om helseopplysninger eller andre personopplysninger. Pseudonyme opplysninger er personopplysninger etter personvernforordningen. Publisering og annen deling av helseopplysninger må følge strenge krav knyttet til taushetsplikt og personvern. Siden enkeltpersoner kan identifiseres, er opplysningene taushetsbelagte, og all deling må ha samtykke eller annet rettslig grunnlag (se punkt 6.1). Det er helseforetakets ledelse som har det overordnede ansvaret for at disse reglene følges, samtidig som taushetsplikten er personlig og følger den enkelte forsker/helsepersonellet.

Samtykke fra forskningsdeltakerne vil som hovedregel være nødvendig. Et samtykke til å delta i et forskningsprosjekt gir ikke i seg selv rett til å dele eller publisere personopplysninger (direkte eller indirekte identifiserbare), med mindre det er konkrete holdepunkter for det. Det vil eksempelvis være relevant om forskningsdeltakerne har fått informasjon om deling av forskningsdata, om publisering av forskningsresultater og om eventuell risiko for bakveisidentifisering. Se nærmere i punkt 6.2 om kravene til gyldig samtykke.

Utvikling av en egen atferdsnorm (bransjenorm) for helseforskning kan være et viktig tiltak for å sikre riktig etterlevelse av reglene, se punkt 6.3.

6.1 Krav om samtykke eller annet rettslig grunnlag

Deling og publisering av helseopplysninger og andre personopplysninger i forskningsprosjekter må ha et rettslig grunnlag. Kravet om rettslig grunnlag følger av personvernforordningen artikkel 5 nr. 1 bokstav a, jf. artikkel 5 nr. 1, jf. artikkel 6 og 9. Utlevering og annen behandling av opplysningene vil ha rettslig grunnlag dersom behandlingen er basert på samtykke, lov, forskrift eller dispensasjon fra taushetsplikten.

Siden medisinsk og helsefaglig forskning som hovedregel er basert på forskningsdeltakernes samtykke, vil den praktiske hovedregelen være at samtykke også vil være det aktuelle rettslige grunnlaget for eventuell publisering eller annen deling av opplysningene. Et samtykke til å delta i et forskningsprosjekt gir ikke i seg selv rett til å dele, publisere eller behandle personopplysninger (dvs. opplysninger der deltakeren kan kjennes igjen) på andre måter. For at samtykket skal gi rettslig grunnlag for deling og publisering må forskningsdeltakerne ha fått informasjon om deling av forskningsdataene, om publisering av forskningsresultater og om eventuell risiko for bakveisidentifisering. Se nærmere i punkt 6.2 om vilkårene for gyldig samtykke. Dette inkluderer informasjon om hvilke formål opplysningene som deles skal kunne brukes til, om det er forskningsformål, helsehjelp til andre pasienter eller andre formål.

Forskningen kan også være basert på at REK har gitt adgang til å behandle opplysningene uten hinder av taushetsplikten, jf. helseforskningsloven § 35 og helsepersonelloven § 29. Denne dispensasjonen fra taushetsplikten vil også kunne gi rettslig grunnlag for mottakerens bruk av opplysningene i forskningen. Hvorvidt dispensasjonen også gir rettslig grunnlag for deling eller publisering av opplysningene, vil avhenge av REKs vedtak. I utgangspunktet må en legge til grunn at et slikt vedtak ikke gir rett til å dele eller publisere personopplysninger. Noe annet er det dersom det står i vedtaket at personopplysningene skal (kunne) deles eller publiseres. Da vil vedtaket gi forskeren supplerende rettsgrunnlag for å kunne dele eller publisere opplysningene. Det er da i realiteten tale om to ulike vedtak: dispensasjon til å utlevere opplysningene til forskningsprosjektet og dispensasjon til å dele eller publisere opplysninger fra forskningsprosjektet.

Behandling av helseopplysninger i forskning kan alternativt skje med grunnlag i personopplysningsloven § 9. Vilkåret er at behandlingen er nødvendig for å oppnå formålet med forskningen, og at samfunnets interesse i forskningen klart overstiger ulempene for den enkelte forskningsdeltaker. Det må iverksettes pseudonymisering eller andre nødvendige tiltak for å redusere risikoen for identifisering av forskningsdeltakerne. Behandlingen må også være i samsvar med taushetsplikten. Her kan eventuelt unntaket i helsepersonelloven § 23 nr. 3 påberopes. Det følger av denne bestemmelsen at "opplysninger kan gis videre når behovet for beskyttelse må anses ivaretatt ved at individualiserende kjennetegn er utelatt", for eksempel ved pseudonymisering.

REKs forskningsetiske vurdering og forhåndsgodkjenning etter helseforskningsloven § 33 jf. § 10 vil derimot ikke gi rettslig grunnlag etter personvernreglene i forordningen. Forhåndsgodkjenningen kan likevel være et viktig grunnlag for å fortolke om et samtykke eller et dispensasjonsvedtak også gir rett til å dele eller publisere opplysningene. Dette henger sammen med at helseforskningsloven og REK skal ivareta generelle forskningsetiske hensyn, mens forordningen bare gjelder personvern. REKs forhåndsgodkjenning fritar derfor ikke helseforetaket fra ansvaret etter personvernforordningen, for eksempel for at forskningsdeltakernes samtykke og informasjonen de har fått er tilstrekkelig.

Kravet om rettslig grunnlag er forklart nærmere i Prop. 56 LS (2017-2018) kapittel 6, kapittel 7 og punkt 32.3 om gjennomføringen av personvernforordningen i den nye personopplysningsloven og i helselovene.

6.2 Gyldig samtykke

Det følger av det foregående at det som hovedregel vil være nødvendig med samtykke fra forskningsdeltakerne for å kunne dele forskningsdata og publisere forskningsresultater, dersom det er tale om personopplysninger (dvs. dersom de er personidentifiserbare og derfor ikke anonyme).

Samtykket skal være en frivillig, spesifikk, informert og utvetydig viljesytring fra forskningsdeltakeren der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av helseopplysninger som gjelder vedkommende, jf. helseforskningsloven § 13 og forordningen artikkel 4 nr. 11 og 7. Samtykket må kunne dokumenteres. Det følger av dette at det er forordningens bestemmelser om samtykke som skal legges til grunn.

Samtykket skal bygge på spesifikk informasjon om et konkret forskningsprosjekt, med mindre det er adgang til å gi et bredt samtykke. Samtykket må være gitt ved en aktiv handling eller erklæring. Passivitet er derfor ikke tilstrekkelig til at samtykket er gyldig. Hva som kreves for et gyldig samtykke er nærmere forklart i personvernforordningens fortale punkt 32:

> Samtykke bør gis i form av en tydelig bekreftelse der den registrerte på en frivillig, spesifikk, informert og utvetydig måte gir sitt samtykke til behandling av

vedkommendes personopplysninger, f.eks. i form av en skriftlig, herunder elektronisk, eller en muntlig erklæring. Dette kan innebære å krysse av i en boks under et besøk på et nettsted, velge tekniske innstillinger for informasjonssamfunnstjenester eller en annen erklæring eller handling som i denne forbindelse tydelig viser at den registrerte godtar den foreslåtte behandlingen av vedkommendes personopplysninger. Taushet, forhåndsavkryssede bokser eller inaktivitet bør derfor ikke utgjøre et samtykke. Et samtykke bør omfatte alle behandlingsaktiviteter som utføres med henblikk på samme formål.

Spørsmålet i denne sammenhengen er hva forskningsdeltakerne har samtykket til. Dette avhenger først og fremst av informasjonen som ble gitt da samtykkene ble innhentet. Et samtykke til å delta i et forskningsprosjekt, er i utgangspunktet ikke også et samtykke til å publisere forskningsresultater som inneholder personopplysninger. At deltakeren også har samtykket til publisering av personopplysninger, kan bare legges til grunn dersom forskningsdeltakerne har fått informasjon om dette, med åpenhet om at også pseudonyme kan være personidentifiserbare. Det bør informeres om dette selv om risikoen for bakveis-identifisering er svært liten. Dette følger av at samtykket skal være informert, slik at forskningsdeltakerne får mulighet til å forstå konsekvensene av å delta i forskningsprosjektet.

Et samtykke til å delta i et forskningsprosjekt, vil heller ikke uten videre omfatte en adgang til å dele forskningsdataene. Det kan for eksempel være aktuelt å deponere rådataene i eksterne databaser der data fra flere forskningsprosjekter er samlet. Et annet eksempel er utlevering av data til bruk i nye forskningsprosjekter. REK/NEM har skilt mellom tilgjengeliggjøring av data for redaktører og fagfeller for publisering og annen deling av data. Begrunnelsen har vært at formålet med å publisere er forenlig med samtykket som er avgitt til forskningsformålet. Data som deles i en slik sammenheng er dessuten underlagt tilgangskontroll og taushetsplikt. Ved annen datadeling kan formålet med videre bruk være noe annet enn det samtykket har dekket. Etikk-komiteenes tilnærming fremstår som fornuftig for departementet.

Les mer om kravene til gyldig samtykke etter personvernforordningen i veiledningen: Artikkel 29-gruppen, *Guidelines on Consent under Regulation 2016/679* (28. november 2017, revidert 10. april 2018).

6.3 Atferdsnorm for helseforskning

Utvikling av en egen atferdsnorm (bransjenorm) for helseforskning kan være et viktig tiltak for å sikre riktig etterlevelse og lik fortolkning og praktisering av reglene. Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen) foreligger allerede, men omhandler ikke utfordringer og behov som særlig gjelder for helseforskningen. Det er imidlertid utarbeidet en veileder til Normen om helseforskning, men denne omtaler ikke spesifikt problemstillingene i dette rundskrivet. En europeisk atferdsnorm for helse-forskning er under utvikling (BBMRI-ERIC Code of Conduct for Health Research).

I personvernforordningen uttales at medlemsstatene og tilsynsmyndighetene skal oppmuntre til at det utarbeides atferdsnormer (artikkel 40). Aktørene kan velge å forplikte seg til atferdsnormen gjennom avtale. Aktørene kan søke om å få atferdsnormen godkjent av Datatilsynet. Overholdelse av en godkjent atferdsnorm kan brukes som en faktor for å påvise at forordningens krav til informasjonssikkerhet er oppfylt, jf. artikkel 32.

Departementet anbefaler at det utvikles en egen norsk atferdsnorm for helseforskning. En slik norm vil gi veiledning om reglene og konkret hvordan de skal etterleves. Det vil også bidra til lik praktisering av regelverket, noe som er viktig for å legge til rette for godt og effektivt forskningssamarbeid. Atferdsnormer skal utformes, fastsettes og forvaltes av aktørene i den aktuelle sektoren. Forskerne og helseforetakene kan på denne måten få et "eierskap" til regelfortolkningen, ved at normen tilpasses helseforskningens særlige utfordringer og behov og ved at det tas utgangspunkt i begreper, rammer og eksempler som er kjente.

En egen norm for behandling av personopplysninger i helseforskningen kan blant annet omhandle hvordan opplysninger skal pseudonymiseres for å redusere faren for bakveisidentifikasjon samtidig som forsknings- og publiseringsformål kan ivaretas. Et annet spørsmål som en eventuell norm bør omhandle er kravene til et gyldig samtykke og hvordan det skal informeres om deling, publisering, risikoen for bakveisidentifikasjon osv. i forbindelse med innhenting av samtykker.