NORMEN

Veileder i personvern og informasjonssikkerhet i forskningsprosjekter

Versjon 2.0

15. februar 2022

Utgitt med støtte av:

Direktoratet for e-helse

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Normen forvaltes av Styringsgruppen for Normen, etter Normens forvaltningsmodell.

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. Innbyggere og ansatte skal være trygge på at opplysninger om dem behandles på en sikker måte i helse- og omsorgssektoren. Normen skal bidra til å at virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til hverandre, ved å etablere mekanismer og regler som sørger for at behandling av helseog personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Alt om Normen, Normens krav og veiledningsmateriell finnes på www.normen.no.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knyttet til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

Publikasjonens tittel:
[Veileder i personvern og informasjonssikkerhet i forskningsprosjekter]

Utgitt:
[16.02.2022]

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

1 Innledning

1.1 Bakgrunn - Tilfredsstillende personvern og informasjonssikkerhet er forutsetninger for kvalitet og tillit

At forskningsinstitusjoner evner å behandle helse- og personopplysninger på en forsvarlig og sikker måte, er en viktig forutsetning for befolkningens tillit og vilje til å dele sine opplysninger til bruk i forskningen. Uten en forsvarlig håndtering av de registrerte og deres opplysninger, vil både tilliten og opplysningenes riktighet eller pålitelighet svekkes.

Virksomheter i helse- og omsorgssektoren er avhengige av denne tilliten for å lykkes med sine samfunnsoppdrag både som yter av helsehjelp og for å bidra med ny kunnskap gjennom forskningen.

Denne forskningsveilederen vil forhåpentligvis kunne bidra med å løfte frem noen viktige forutsetninger for å lykkes med et forskningsprosjekt, og vise hvordan forskningsdeltakernes personvern på nær sagt alle områder går hånd i hånd med et slikt mål.

God styring og kontroll i all behandling av person- og helseopplysninger er også en viktig forutsetning for at et prosjekt skal anses å være etisk og juridisk forsvarlig og publiserbart i henhold til anerkjente forskningsetiske normer.

1.2 Tema - Formålet med forskningsveilederen

Veilederen retter seg hovedsakelig mot prosjektledere i forskningsprosjekter, men kan også være nyttige for andre, som f.eks. forskere uten prosjektansvar, forskningssykepleiere, forskerstøttefunksjoner, personvernombud og ledelsen i forskningsinstitusjoner.

Veilederen tar for seg all forskning på helse- og personopplysninger, og er ikke begrenset til helseforskningslovens virkeområde. Veilederen vil også kunne brukes i prosjekter som for eksempel har til formål forskning på teknologi, biologisk materiale og ved legemiddelutprøving.

Det er mange likhetstrekk mellom forskningsprosjekter og prosjekter som har formålet kvalitetsforbedring av behandlingsforløp i helse- og omsorgstjenesten. De generelle kravene til personvern ved behandling av personopplysninger er de samme uansett formål. Det er det enkelte prosjekt som må ta stilling til om det er forskning eller kvalitetsforbedring som er formålet med behandlingen av personopplysninger. Forskjellen på forskning og kvalitetsforbedring er omtalt i punkt 6.3.1.

Veilederen skal kunne være nyttig i planleggingen av et prosjekt, gjerne før f.eks. REK har uttalt seg om hvorvidt behandlingen av helse- og personopplysninger faller innenfor helseforskningslovens virkeområde. Veilederen kan også være nyttig i planlegging og gjennomføring av kvalitetssikringsprosjekter.

Etikk eller etiske spørsmål knyttet til forskning behandles ikke i denne veilederen. For mer informasjon om forskningsetikk se nettsiden til De nasjonale forskningsetiske komiteene (www.forskningsetikk.no).

Veilederen er ikke en generell veileder i forskingsprosjekter, men begrenser seg til ivaretakelse av personvern og informasjonssikkerhet i forskningsprosjekter i helse- og omsorgssektoren.

Denne veilederen begrenser seg til ansvar og plikter knyttet til informasjonssikkerhet, personvern og datahåndtering i forskningsprosjekter.

1.2.1 Leseveiledning

I kapittel 2 til 5 gis en oversikt over noen sentrale temaer innen informasjonssikkerhet og personvern.

Veilederen har som mål å være et godt hjelpemiddel før, underveis og i avslutningen i et forskningsprosjekt. Kap. 6-8 følger derfor prosessen i et forskningsprosjekt, fordelt på planlegging, gjennomføring og avslutning. En del av virksomhetens plikter og oppgaver følger fasene i prosjektet. For en komplett oversikt over oppgaver, plikter og virksomhetens ansvar må hele veilederen leses.

1.3 Om Normen

Denne veilederen er et støttedokument under Normen som forvaltes av Styringsgruppen for Normen. Veilederen følger Normens forvaltningsmodell.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. I tillegg skal Normen bidra til å etablere mekanismer og regler som sikrer at virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knytte til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

1.4 Relevante regelverk

Krav til personvern og informasjonssikkerhet i forskningsprosjekter reguleres av en lang rekke lover, forskrifter og internasjonale konvensjoner. De mest sentrale er nevnt her.

Da personopplysingsloven og personvernforordningen ble vedtatt, ble det samtidig gjort en rekke endringer i helselovgivingen. Disse reglene utfyller og til dels skjerper enkelte av de generelle kravene i personvernregelverket. Det er lagt til grunn at helselovgivingen, etter at disse endringene ble innført, er i samsvar med personvernregelverket.[1] Dette innebærer at ved behandling av helse- og personopplysninger til forskningsformål, kan man ikke utelukkende basere seg på særlovgivingen som omtaler forskning, men man må også se til de generelle reglene i personopplysningsloven og personvernforordningen.

[1] Prop. 56 LS (2017-2018) s. 183.

1.4.1 Relevante regelverk

De er mange nasjonale og internasjonale regelverk som regulerer behandling av helse- og personopplysninger i forskning. Dette er noen av de mest relevante:

- Personopplysningsloven og personvernforordningen
- Helseforskningsloven m/ forskrift
- Helseregisterloven
- Forskrift om medisinske kvalitetsregistre
- Pasientjournalloven
- Helsepersonelloven
- Pasient- og brukerrettighetsloven
- Sikkerhetsloven
- Virksomhetssikkerhetsforskriften
- Helsinkideklarasjonen av 1964 med senere revisjoner
- EU-forordningen om medisinsk utstyr (EU/2017/745)
- Lov om legemiddelutprøving
- Biobankloven
- Vancouverkonvensjonen
- Oviedokonvensjonen med tilhørende tilleggsprotokoll om biomedisinsk forskning

1.4.2 Definisjoner og begreper i veilederen

I dette kapittelet gis det en oversikt over definisjoner og begreper som benyttes i veilederen:

Anonyme opplysninger: Kan ikke knyttes til enkeltpersoner og regnes derfor ikke som personopplysninger. Dersom helse- og personopplysninger er anonymisert, skal det ikke med rimelige hjelpemidler være mulig å tilbakeføre opplysningene til de opplysningene gjelder. Behandling av anonyme opplysninger omfattes ikke av personvernregelverket eller av regler om taushetsplikt[2], og kan samles inn, registreres, utleveres, mv. for forskningsformål.

Det er dataansvarliges ansvar å gjøre gode vurderinger av om og sikre at et datasett er anonymt før behandling av dataene kan starte. For mer informasjon om anonymisering se kap. 5.

Dersom forsker/databehandler/registereier har en koblingsnøkkel med ID til selve datamaterialet er ikke dataene anonyme, men pseudonyme.

Avidentifiserte opplysninger: Uttrykket avidentifiserte opplysninger har vært mye brukt i forskningssektoren, men er ikke videreført i dagens regelverk. Begrepet vil ikke bli brukt i denne veilederen.

Behandlingsgrunnlag: All behandling av personopplysninger må ha et rettslig grunnlag for å være lov. Den dataansvarlige må derfor ha identifisert om det finnes et

[2] Forvaltningsloven § 13 a nr. 2 og helsepersonelloven § 23 nr. 3

behandlingsgrunnlag før opplysningene hentes inn. Hvis ikke det finnes, er behandlingen av personopplysningene ulovlig.[3]

All behandling av helse- og personopplysninger må ha et tydelig avgrenset formål. Det må finnes et behandlingsgrunnlag for behandling av personopplysninger til hvert enkelt formål.

Dataansvarlig: 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. Dataansvarlig er den virksomheten som har ansvaret for behandling av helse- og personopplysninger. I praksis vil dette være øverste ledelse i virksomheten. Dataansvaret kan ikke delegeres. Tilsvarende begrep i personvernforordningen er behandlingsansvarlig. Dataansvarlig skal forstås som synonymt med personvernlovgivningens begrep «behandlingsansvarlig».

Databehandler: En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den dataansvarlige.[4] En databehandler vil typisk være en leverandør av tekniske systemer og løsninger eller en samarbeidsvirksomhet som utfører behandling av helse- og personopplysninger for dataansvarlig/forskningsansvarlig. Eksempelvis der en annen virksomhet enn forskningsinstitusjonen utfører dataanalyse eller andre behandlinger av forskningsdata på vegne av dataansvarlig. Andre eksempler vil være Tjeneste for sensitive data (TSD) ved USIT (Universitetet i Oslo), laboratorier som gjennomfører analyser (som genererer personopplysninger) på vegne av et forskningsprosjekt. Ansvar og plikter for dataansvarlig og databehandler skal avtales i en databehandleravtale. Databehandleravtalen skal sikre at helse- og personopplysningene behandles i samsvar med regelverket og at dataansvarlig beholder kontrollen over opplysningene.

Felles dataansvar: Dersom to eller flere dataansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, skal de være felles datasansvarlige. De skal på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i denne forordning, særlig med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14, ved hjelp av en ordning seg imellom, med mindre og i den grad de datasansvarliges respektive ansvar er fastsatt i unionsretten eller medlemsstatenes nasjonale rett, personvernforordningen art 24.

I forskningsprosjekter er det ofte slik at man samarbeider med andre institusjoner om f. eks analyser av humant biologisk materiale. I motsetning til bruk av en databehandler, vil samarbeidspartneren være med på å bestemme formålet med behandlingen av opplysningene, være med på publisering mv. Her vil virksomhetene ha et felles dataansvar for de dataene som genereres av analysene, ikke alle dataene i forskningsprosjektet. Ved felles dataansvar skal virksomhetene på forhånd avtale hvordan forpliktelsene etter personvernforordningen skal organiseres. Personvernlovverket krever at alle virksomhetene som har dataansvar skal kunne sikre og påvise etterlevelse. Dette betyr i praksis at virksomheter med felles dataansvar i fellesskap må gjøre vurderinger og dokumentere disse.

Forskningsansvarlig: Den forskningsansvarlige er en (fortrinnsvis) juridisk eller (unntaksvis) fysisk person med et overordnet ansvar for å tilrettelegge for at forskningen skjer på en forsvarlig måte, herunder sørge for at personvern- og informasjonssikkerhetsmessige forhold ivaretas. Den forskningsansvarlige kan delegere oppgaver til andre, så fremt den det

[3] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
[4] Personvernforordningen art. 4 nr. 8.

delegeres til har nødvendig kompetanse til å utføre oppgaven. Det er kun oppgaver som kan delegeres, ikke ansvaret. Det skal alltid oppnevnes en kontaktperson for den forskningsansvarlige for hvert forskningsprosjekt.

Dataansvarlig og forskningsansvarlig vil ikke alltid være samme virksomhet. I for eksempel oppdragsstudier, vil typisk et legemiddelfirma være oppdragsgiver/sponsor, og den som uformer protokoll, finansierer forskningsprosjektet, utformer informasjonsmateriell etc. Dersom legemiddelfirmaet er oppdragsgiver/sponsor overtar de som dataansvarlig ved overlevering av data fra helseforetaket. De bestemmer med andre ord formålet med prosjektet. På den andre siden er helseforetaket forskningsansvarlig. Det vil si at de står for selve gjennomføringen av forskningsprosjektet, herunder sørge for at nødvendige godkjenninger foreligger, rekruttering av pasienter, daglig drift av forskningsprosjektet og øvrige plikter etter helseforskningsloven m/forskrift.

Helseforetaket vil her være dataansvarlig frem til utlevering (de dataene som er lagret i kliniske systemer ved sykehuset). Deretter har prosjektet rutiner for å sende data til sponsor etter å ha innhentet dem fra prosjektdeltakere, f. eks utfylte skjemaer som sendes via programvare for datainnsamling i kliniske studier (eCRF-løsninger).

Helse- og personopplysninger

Personopplysninger er enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); Dette innebærer at opplysningene er av en slik karakter at det er mulig å identifisere enkeltpersoner, for eksempel ved at personnummer er kjent eller ved at kombinasjoner av opplysninger fører til at enkeltpersoner kan identifiseres (direkte og indirekte identifisering).

Eksempler på personopplysninger kan være navn, adresse, og fødselsnummer. Opplysninger om avdøde reguleres ikke av personvernforordningen med mindre opplysningene sier noe om gjenlevende. Dette er aktuelt ved enkelte typer behandlinger innen helse- og omsorgssektoren. Dette kan for eksempel gjelde opplysninger om arvelige sykdommer/lidelser, og gjelder ofte genetiske opplysninger. Helselovgivningen regulerer opplysninger om avdøde, og fordi disse opplysningene er underlagt taushetsplikt kan opplysninger om avdøde bare gis ut dersom det foreligger et lovlig unntak fra taushetsplikten.

Helseopplysninger er personopplysninger om en fysisk persons fysiske eller psykiske helse herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand Helseopplysninger er definert som en særlig kategori av personopplysninger etter personvernforordningen.

Denne veilederen bruker begrepet helse- og personopplysninger for å understreke at ikke all forskningsdata er helseopplysninger, men også kan inneholde personopplysninger som ikke er en særlig kategori/sensitive personopplysninger. Skillet mellom personopplysninger og særlige kategorier er avgjørende for hvilke rettslige grunnlag som gjør seg gjeldende, har konsekvenser for gjennomføring av andre typer vurderinger som må gjøres i forbindelse med forskningsprosjektet og hvilke sikkerhetskrav som må implementeres.

Analyser av og forskning på humant biologisk materiale innebærer normalt behandling av helseopplysninger.

Pseudonyme opplysninger: Pseudonymisering er behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk

av tilleggsopplysninger. Pseudonyme opplysninger regnes som helse- og personopplysninger i regelverket. Pseudonymisering av personopplysninger innebærer at enkelte direkte identifiserende kjennetegn blir erstattet med for eksempel et løpenummer el., som fremdeles fungerer som en unik identifikator. Deretter lagres koblingen mellom den identifiserte personen og koblingsnøkkel adskilt fra de pseudonymiserte dataene.

Opplysninger som ser anonyme ut for forsker vil være å regne som personopplysninger dersom de som har utlevert opplysningene til prosjektet (for eksempel et helseregister) sitter med en koblingsnøkkel. Et annet eksempel kan være IP-adresse, som er en type opplysning som kanskje ikke forteller deg hvem den registrerte er, men som nettleverandør vil kunne identifisere.

Pseudonymisering er et viktig risikoreduserende tiltak ved behandling av personopplysninger, men pseudonyme opplysninger regnes fortsatt som personopplysninger i regelverket.

2 Den registreres perspektiv i hovedfokus

Et av hovedformålene med personvernforordningen er å gi enkeltmennesket bedre kontroll over egne opplysninger og tydelige rettigheter. Dette innebærer at det må være tydelige krav til når og hvordan en virksomhet (forskningsinstitusjon/HF) kan behandle personopplysninger. Dette fokuset må man ha med seg gjennom hele forskningsprosessen dersom man skal klare å planlegge og gjennomføre behandlingen innenfor lovens rammer.

Det finnes ikke noen behandling av helse- og personopplysninger som uten videre er så samfunnsnyttig/har så stor forskningsverdi at man kan se bort fra personvernprinsippene og rettighetene som skal beskytte den registrerte. Dette er også understreket i for eksempel helseforskningslovens forskningsetiske prinsipper.

Forskningsprosjekter bør aktivt benytte seg av brukermedvirkning i alle prosjektets faser, både ved oppstart, ved endringer, gjennomføring av personvernkonsekvensvurderinger mv. Sykehus har ofte egne brukerutvalg, og i tillegg benytter mange seg av interesserorganisasjoner.

Når man planlegger en behandling av personopplysninger, må man derfor i hovedsak navigere og ta valg ut ifra hvorvidt personvernet til den registrerte ivaretas tilstrekkelig.

2.1 Personvernprinsippene

Personvernforordningen artikkel 5 bygger på noen grunnleggende prinsipper som virksomheten og forsker må sørge for å ivareta ved en behandling av personopplysninger.

Overholdelse av prinsippene skal sørge for at all behandling av personopplysninger er forutsigbar og forholdsmessig for den registrerte.

Dataansvarlig må sikre at egen virksomhet opptrer i henhold til personvernprinsippene, se Normen kapittel 2.2.[5] Personvernforordningen generelt og prinsippene angitt i artikkel 5 spesielt gjelder for behandling av helse- og personopplysninger uansett formål, som behandling i forbindelse med at det gis helsehjelp og behandling av personopplysninger til kvalitetssikringsarbeid og forskning. Nasjonal helselovgivning fastsetter på sin side konkrete rammer for behandlingen av person- og helseopplysninger innen helse- og omsorgssektoren, og går derfor foran eller supplerer personopplysningsloven og personvernforordningen.

Det er også lagt inn flere henvisninger til personvernprinsippene i lovgivning som regulerer behandling av person- og helseopplysninger i helse- og omsorgstjenesten generelt, og innen helseforskning. For eksempel henviser helseforskningsloven § 32 til personvernprinsippene i personvernforordningen artikkel 5, og presiserer at medisinsk og helsefaglig forskning skal være i samsvar med disse.[6]

For utfyllende informasjon om prinsippene, se Normens faktaark om personvernprinsippene.

2.2 Behandlingsgrunnlag

All behandling av helse- og personopplysninger i forskning må ha et lovlig grunnlag. Dette kalles behandlingsgrunnlag. Dataansvarlig må sørge for å vurdere og dokumentere at prosjektet har behandlingsgrunnlag i personvernforordningen artikkel 6 og eventuelt artikkel 9, samt i supplerende nasjonal rett.

De lovlige grunnlagene for behandling av helse- og personopplysninger er angitt i personvernforordningen art. 6, og unntak fra forbudet mot å behandle særlige kategorier av personopplysninger i art. 9. For enkelte behandlingsgrunnlag og for unntak fra forbudet mot å behandle særlige kategorier av personopplysninger, herunder helseopplysninger, forutsetter personvernforordningen at behandlingen i en del tilfeller suppleres av nasjonal lovgivning. For helseopplysninger vil dette supplerende rettsgrunnlaget for eksempel finnes i personopplysningsloven, helseforskningsloven, helseregisterloven, pasientjournalloven og i helsepersonelloven.

Som regel vil formålet med en behandling være styrende for hvilket behandlingsgrunnlag som kan anvendes. I noen tilfeller vil det ikke være mulig å finne et gyldig behandlingsgrunnlag uten at forskningsprosjektet endres i sin utforming/innretning.

For mer veiledning om behandlingsgrunnlag og de ulike alternativene i artikkel 6 og 9, se Normens kapittel 4.1. og faktaark 56 om Formål og behandlingsgrunnlag.

Helseopplysninger i pasientjournalsystemer og medisinske kvalitetsregistre er underlagt taushetsplikt etter helsepersonelloven. Dersom det er aktuelt å bruke helseopplysninger fra pasientjournaler eller medisinske kvalitetsregistre, vil det som regel kreves pasientens samtykke eller et vedtak om dispensasjon fra taushetsplikt. Både pasientens samtykke og vedtak om dispensasjon fra taushetsplikten vil oppfylle rettslige krav til behandlingsgrunnlag og unntak fra taushetsplikten. Til formålet forskning er det REK som gir vedtak om dispensasjon fra taushetsplikten.

[5] Normen v6.0 Kapittel 2.2 Dataansvarliges ansvar

[6] Tilsvarende henvisning for ivaretakelse av personvernprinsippene i helseregistre, finnes i helseregisterloven § 6 første ledd.

For medisinsk og helsefaglig forskning på mennesker, humant biologisk materiale eller helseopplysninger, gjelder helseforskningsloven. Det følger av loven at medisinske og helsefaglige forskningsprosjekter skal ha forhåndsgodkjenning fra REK, jf. helseforskningsloven § 9 og 33. Med medisinsk og helsefaglig forskning menes virksomhet som utføres med vitenskapelig metodikk for å skaffe til veie ny kunnskap om helse og sykdom, jf. lovens § 4a.

I tabellen under er det gitt eksempler på behandlingsgrunnlag knyttet til ulike formål. Enkelte behandlingsgrunnlag er beskrevet under. Merk at tabellen er veiledende, og at det må gjøres en vurdering av behandlingsgrunnlag for hvert enkelt forskningsprosjekt.

Både helseforskningsloven og helsepersonelloven stiller tilleggskrav til behandlingen av helse- og personopplysninger utfra kilden til informasjon (for eksempel pasientjournalsystem, helseregistre eller andre kilder) om virkeområdet for lovverkene. Kravene i lovverket vil ikke alltid være supplerende rettsgrunnlag, men kunne være tilleggskrav som stilles til behandlingen av personopplysninger.

Behandling/aktivitet	**Behandlingsgrunnlag i personvernforordningen**	**Supplerende rettsgrunnlag / tilleggskrav**
Helseforskning basert på samtykke	Artikkel 6 nr. 1 a Artikkel 9 nr. 2 a	Helseforskningsloven §§ 9, 10. Helsepersonelloven § 22 for bruk av opplysninger fra pasientjournalsystemer og helseregistre.
Helseforskning og annen forskning basert på dispensasjon fra taushetsplikten	Artikkel 6 nr. 1 e Artikkel 6 nr. 3 Artikkel 9 nr. 2 j	Helsepersonelloven § 29 og/eller helseregisterloven § 19 e (vedtak om dispensasjon fra taushetsplikten fra REK).
Behandling av personopplysninger i de forskriftsregulerte sentrale helseregistrene[7]	Artikkel 6, nummer 1 c Artikkel 9, nr. 2 i	Helseregisterloven og de ulike forskriftene til det enkelte register, for eksempel Kreftregisterforskriften § 3-1 jf. helseforskningsloven §§ 19-19h.

[7] For en oversikt over de sentrale helseregistrene, se: https://www.fhi.no/div/datatilgang/om-sentrale-helseregistre/

Bruk av medisinske kvalitetsregistre der formålet er forskning[8]	Artikkel 6 nr. 1 e Artikkel 9 nr. 2 h og j	Helseregisterloven og forskrift om medisinske kvalitetsregistre § 1-4 og forskriftens kap. 4
Kvalitetssikring i helse- og omsorgstjenesten	Artikkel 6 nr. 1 c Artikkel 6 nr. 1 e Artikkel 9 nr. 2 h	Helsepersonelloven § 26 (intern kvalitetssikring) eller § 29 og helseregisterloven § 19 e (Kvalitetssikring på tvers av helseforetak etter vedtak fra Helsedirektoratet)

2.2.1 Samtykke

Det kreves samtykke fra deltakere i medisinsk og helsefaglig forskning med mindre annet følger av lov, jf. helseforskningsloven § 13).

I personvernforordningen er de ulike behandlingsgrunnlagene sidestilt. I både nasjonale og internasjonale normer for forskning er imidlertid samtykke ansett som hovedregel, der dette kan innhentes uten betydelige problemer for gjennomføring av forskningen. I tråd med personvernforordningens formål om å gi den registrerte bedre kontroll over egne personopplysninger, vil samtykke ofte være det mest hensiktsmessige behandlingsgrunnlaget.

Samtykke er det behandlingsgrunnlaget som gir den registrerte størst reell medvirkning og kontroll med egne opplysninger.

I forskning som forutsetter involvering av forskningsdeltakerne direkte i form av intervensjon, vil samtykke være helt avgjørende for gjennomføring av prosjektet. Andre behandlingsgrunnlag vil først og fremst være aktuelle i forbindelse med gjenbruk av person- og helseopplysninger som allerede er innhentet (for eksempel opplysninger i ulike typer registre).

Kravene til et gyldig samtykke etter helseforskningsloven § 13 er de samme kravene som stilles til et gyldig samtykke etter personvernforordningen, jf. helseforskningsloven, som sier at et samtykke skal være en tydelig bekreftelse der den registrerte på en frivillig, spesifikk, informert og utvetydig måte gir sitt samtykke til behandling av vedkommende sine personopplysninger. Det er ikke tilstrekkelig med det som kalles et passivt samtykke. Fordi det stilles krav om at et samtykke skal gis gjennom en aktiv handling, vil ikke passivt samtykke oppfylle kravene til et gyldig samtykke. Dataansvarlige skal også kunne påvise at samtykke er innhentet. Dette betyr at samtykket må dokumenteres. Ved bruk av

[8] Oversikt over medisinske kvalitetsregistre: https://www.kvalitetsregistre.no/registeroversikt

helseopplysninger fra pasientjournalsystemer og helseregistre, må i tillegg kravene i helsepersonelloven § 22 være oppfylt.

2.2.1.1 Ujevnt maktforhold – når samtykke ikke er gyldig

Når helsepersonell dokumenterer opplysninger om helsehjelpen i et pasientjournalsystem er det til helsehjelpsformål, dvs. for å kunne gi forsvarlig behandling og oppfølgning til pasienten. Dersom den samme behandleren ønsker å bruke opplysningene til forskning, er utgangspunktet at pasienter, brukere og pårørende i helse- og omsorgstjenesten står i et avhengighetsforhold til helsepersonellet og helse- og omsorgstjenesten. Ofte kan de betraktes som en sårbar gruppe, og det bør derfor gjøres grundige vurderinger av om et samtykke kan fungere som lovlig behandlingsgrunnlag.

Dersom maktforholdet er ujevnt, betyr det at man ikke kan være sikker på at et samtykke er gitt frivillig. I disse tilfellene skal det informerte samtykket innhentes av en annen som forskningsdeltakeren ikke har slikt forhold til, jf. for eksempel helseforskningsloven § 13, 3 ledd. Dette kan for eksempel være tilfelle der behandlende lege skal gjennomføre en klinisk studie som involverer pasienten. Da kan det være hensiktsmessig at samtykket innhentes av noen andre enn den behandlende legen, som pasienten vil ha et uproporsjonalt maktforhold til. Ikke alle lege-pasientforhold vil innebære et slikt avhengighetsforhold.

For eksempel kan forskningsdeltakere som er svært syke eller mentalt redusert lettere føle seg presset til å gi samtykke til deltakelse i forskningsprosjekter. For prosjekter som faller inn under helseforskningsloven, er det REK som vurderer hvorvidt det foreligger et slikt avhengighetsforhold i forbindelse med godkjenning av prosjektet. For forskning som faller utenfor helseforskningslovens virkeområde, må virksomheten selv foreta vurderingen. I vurderingen legges det vekt på hvor nært behandleren-pasientforholdet er, om forskningsprosjektet har betydning for pasientens sykdom og pasientens tilstand. Det må vurderes om det er usannsynlig at samtykket er gitt frivillig med hensyn til alle omstendigheter som kjennetegner den bestemte situasjonen.[9] Dersom det foreligger et slikt avhengighetsforhold som kan medføre at forskningsdeltakeren vil kunne føle seg presset til å gi samtykke, må en annen forsker innhente samtykket.[10]

Videre bør det ikke utgjøre et gyldig rettslig grunnlag for behandling av personopplysninger i et bestemt tilfelle dersom det er en klar skjevhet mellom den registrerte og den dataansvarlige, dvs. den virksomheten som er ansvarlig for behandlingen av opplysningene og pasienten.

I situasjoner hvor samtykke av ovennevnte grunn ikke kan være behandlingsgrunnlag, bør man likevel sørge for at den registrerte opplever å ha reell medvirkning. Det vil da være naturlig å gi deltagerne informasjon om prosjektet, og sikre at deltagerne får reservasjonsrett der det er mulig.

2.2.1.2 Bredt samtykke

Et samtykke skal ifølge både helseforskningsloven og personvernforordningen bygge på spesifikk informasjon om et konkret prosjekt/forskningsformål. Ifølge helseforskningslovens §14, jf. §13 er det adgang til å avgi et bredt samtykke til at humant biologisk materiale og helseopplysninger kan brukes til nærmere bestemte, bredt definerte forskningsformål. Det følger av helseforskningsloven § 14, at: «Den regionale komiteen for medisinsk og

[9] Personvernforordningens fortalepunkt 43.
[10] Ot.prp.nr.74 (2006–2007) Om lov om medisinsk og helsefaglig forskning (helseforskningsloven)

helsefaglig forskningsetikk kan sette vilkår for bruk av bredt samtykke og kan pålegge prosjektleder å innhente nytt samtykke dersom komiteen finner det nødvendig».

Personvernforordningen anerkjenner også at det innen vitenskapelig forskning kan være vanskelig å avgrense og definere et nøyaktig angitt formål i forkant av en innsamling av personopplysninger. Dette indikerer at det også for annen forskning enn helseforskning er anledning til å innhente et samtykke til visse områder innen vitenskapelig forskning når dette er i samsvar med anerkjente etiske standarder for vitenskapelig forskning.

Både helseforskningsloven og personvernforordningen stiller krav om en viss avgrensning, og det er ikke anledning til å innhente bredt samtykke til bruk i forskning generelt. Samtykke må med andre ord tilfredsstille kravene til et gyldig samtykke etter personvernregelverket.

2.2.2 Supplerende rettsgrunnlag: Dispensasjon fra taushetsplikten

Helseopplysninger i pasientjournaler og helseregistre er underlagt taushetsplikt, og kan ikke utleveres til forskning uten at det både foreligger et rettslig grunnlag og et unntak fra helsepersonellovens regler om taushetsplikt.

Både samtykke og dispensasjon fra taushetsplikten kan være både et rettslig grunnlag og unntak fra taushetsplikten. Dersom det ikke foreligger et gyldig samtykke i samsvar med personvernforordningen og helsepersonelloven, må det søkes om dispensasjon fra taushetsplikten. Dispensasjon fra taushetsplikten er nødvendig for å forske på humant biologisk materiale eller helseopplysninger som allerede er samlet inn, uten å be om samtykke. Helsepersonelloven § 29 gjelder for bruk av helseopplysninger fra pasientjournalsystemer og andre behandlingsrettede helseregistre, og helseregisterloven § 19 e gjelder ved bruk av helseopplysninger fra helseregistre. Det er REK som behandler slike søknader, både for medisinsk og helsefaglig forskning og for annen forskning, og Helsedirektoratet som behandler søknader til f.eks. kvalitetsforbedringsformål. For medisinsk og helsefaglig forskning søkes det normalt samtidig om etisk forhåndsgodkjenning for prosjektet.

Selv om REK treffer vedtak om dispensasjon fra taushetsplikten, er utgangspunktet at pasienten skal informeres om at informasjon blir henholdsvis utlevert og samlet inn, jf. pasient- og brukerrettighetsloven § 3-6 tredje ledd og personvernforordningen artikkel 13 til 15.

2.2.2.1 Eksempler på supplerende rettsgrunnlag fra helselovgivningen

Helsepersonelloven § 29 gir adgang til å bruke helseopplysninger uten hinder av taushetsplikten til blant annet forskningsformål. I disse tilfellene skal det søkes REK[11] om dispensasjon. De er gitt myndighet til å bestemme at helseopplysninger i pasientjournaler og andre behandlingsrettede helseregistre kan eller skal gis til bruk i forskning. Dispensasjonsmyndigheten gjelder både for opplysninger som skal brukes til medisinsk og helsefaglig forskning og annen type forskning.

Ved tilgjengeliggjøring av opplysninger fra helseregistre som reguleres av helseregisterloven, gjelder dispensasjonsbestemmelsen i helseregisterloven § 19 e. Prosjekter som faller inn under unntaket fra taushetsplikten vil typisk være omfattende forskningsprosjekter, ofte med

[11] Myndigheten er delegert fra Helsedirektoratet til REK, se forskrift 2. juli 2009 nr. 0989 om delegering av myndighet til den regionale komiteen for medisinsk og helsefaglig forskningsetikk.

svært mange registrerte/registerstudier hvor det å kontakte samtlige personer i utvalget vil utgjøre en uforholdsmessig arbeidskrevende oppgave.

2.2.3 Personopplysningsloven §§ 8 og 9

Både personopplysningsloven §§ 8 og 9 gjelder behandling av personopplysninger for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål. Lovens § 8 viser til personvernforordningen artikkel 6 som kun gjelder personopplysninger. Bestemmelsen gjelder ikke for særlige kategorier opplysninger, herunder helseopplysninger. Skal forskningsprosjektet behandle særlige kategorier av personopplysninger, kan kun § 9 brukes som rettslig grunnlag. Bestemmelsen åpner på nærmere vilkår for behandling av særlige kategorier av personopplysninger, uten at den registrerte samtykker, for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål, jf. forordningen artikkel 9 nr. 2 bokstav j.

Personopplysningsloven § 8 gir supplerende rettsgrunnlag for behandling av personopplysninger som er nødvendig for formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål på grunnlag av artikkel 6 nr. 1 bokstav e, jf. nr. 3.

Når behandling av helse- og personopplysninger skjer med grunnlag i disse bestemmelsene, innebærer det at man ikke må innhente samtykke fra den registrerte, men behandlingen skal være omfattet av nødvendige garantier i samsvar med personvernforordningen artikkel 89 nr. 1, se under. Dersom opplysningene er omfattet av annen lovhjemlet taushetsplikt, må det søkes om dispensasjon.

For behandling av opplysninger som faller inn under § 9, stilles det i tillegg krav om at det må være i samfunnets interesse at behandlingen gjennomføres, og den dataansvarlige har plikt til å rådføre seg med personvernombudet før behandlingen starter. Det vil fortsatt være den behandlingsansvarliges ansvar å sørge for at behandlingen er lovlig.

Personvernforordningen artikkel 89 – nødvendige garantier

Dersom behandlingsgrunnlaget er artikkel 6 nr.1 e og artikkel 9 nr. 2 j) (allmennhetens interesse), følger det at virksomheten også må oppfylle artikkel 89 om nødvendige garantier. Det må gjøres en avveining mellom samfunnets interesse av behandlingen av personopplysninger og den enkeltes rettigheter og friheter. Videre må virksomheten kunne påvise hvordan nødvendige garantier er ivaretatt. Eksempler på tiltak kan være pseudonymisering og dataminimering. Tiltak kan være av både teknisk og organisatorisk art. I prosjekter som skal ha tilgang til taushetsbelagte opplysninger, er artikkel 89 ikke et alternativ til dispensasjon fra taushetsplikten.

I kommentarutgaven til personvernforordningen utdypes tolkningen av hva som regnes som nødvendige garantier.[12] Med nødvendige garantier menes her at de alminnelige reglene i personvernforordningen også gjelder for behandling av opplysninger i forbindelse med arkiv, forskning og statistikk. Prinsippet om dataminimering nevnes spesielt. Dataminimering betyr i praksis at det ikke skal behandles flere personopplysninger enn nødvendig og heller ikke

[12] Åste Marie Bergseng Skullerud mfl., Personopplysningsloven. Lovkommentar, Personopplysningsloven, Juridika (kopiert 10. november 2021)

lenger enn nødvendig. Pseudonymisering er et tiltak som kan benyttes dersom det ikke er mulig å benytte opplysninger som ikke lenger kan identifisere enkeltpersoner (anonyme opplysninger).

Bestemmelsen legger opp til at dersom formålet kan oppnås med anonyme opplysninger, så skal behandlingen skje på den måten.

Det er ikke fastsatt detaljerte nasjonale krav som skal sikre at behandling av personopplysninger til forskningsformål skjer i samsvar med personvernforordningen. Dette betyr at det er den dataansvarliges ansvar å iverksette nødvendige tiltak for at behandlingen skal foregå innenfor rammene av personvernforordningen.

Personvernforordningen åpner opp for at det kan fastsettes unntaksbestemmelser fra enkelte av de registrertes rettigheter. Unntakene må fastsettes i nasjonal rett, og må ivareta de rettighetene og garantiene som er nedfelt i artikkel 89 nr. 1 i personvernforordningen. Eksempler på slike nasjonale unntaksbestemmelser finnes i personopplysningsloven §§ 16 og 17.

I spørsmålet om hvorvidt en unntaksbestemmelse kan gjøres gjeldene, forutsettes det at forskningen ikke kan oppnås, gjennomføres eller i alvorlig grad bli hindret, hvis rettighetene gjøres gjeldende.

Unntak ved forskning og statistiske formål

Når personopplysninger skal brukes til vitenskapelig eller historisk forskning eller til statistiske formål, kan det gjøres unntak fra art. 15 om retten til innsyn i egne personopplysninger, art. 16 om retten til retting av personopplysninger, art. 18 om retten til begrensning i behandling og art. 21 om retten til å motsette seg visse behandlinger.

Dette er rettigheter som må antas ikke å være av vesentlig betydning for den registrerte når opplysningene behandles for forskningsformål eller statistiske formål. Da skal opplysningene ikke benyttes til noe som kan få direkte konsekvenser for vedkommende, og det er heller ikke den enkelte personen som er interessant. Det er derfor av mindre betydning for den registrerte å kunne utøve de nevnte rettighetene.

2.2.4 Den registrertes rettigheter

Som pasient og/eller forskningsdeltaker har man en rekke rettigheter som i hovedsak kan deles i to: pasientrettigheter og rettigheter etter personvernregelverket som registrert.

Pasientrettighetene finnes i pasient- og brukerrettighetsloven, og inneholder rettigheter som innsyn i journal, retten til forsvarlig helsehjelp og retten til fritt behandlingsvalg.

Rettigheter etter personvernregelverket har som mål å gi den enkelte innbygger kontroll over sine helse- og personopplysninger, og finnes i personopplysningsloven og personvernforordningens kapittel 3. Det er disse rettighetene som omtales i denne veilederen.

I et forskningsprosjekt er virksomheten ansvarlig for at forskningsdeltakeren får oppfylt sine rettigheter. I Normen kap. 4 er disse formulert som plikter for virksomheten.

For en generell innføring i de registrertes rettigheter som følger av personvernforordningen, se Normens «Veileder for rettigheter ved behandling av helse- og personopplysninger». Veilederen inneholder også oversikt over hvilke unntaksbestemmelser som finnes og i hvilke

tilfeller de kan benyttes. Informasjon om pasientrettigheter generelt finnes i pasient- og brukerrettighetsloven med kommentarer på Helsedirektoratets nettsider.

2.2.4.1 Informasjon (artikkel 13 og 14)

Dersom det skal behandles personopplysninger, har de personene det skal behandles opplysninger om en grunnleggende rett til informasjon om den planlagte behandlingen av personopplysninger. Det er også gjennom denne informasjonen at den registrerte gjøres kjent med sine øvrige rettigheter, eventuelle unntak fra rettigheter og hvordan man skal gå frem for å benytte seg av de rettighetene vedkommende har.

Hva retten til informasjon innebærer i detalj, omtales i personvernforordningens artikkel 13 og 14. Artikkel 13 gjelder hvilken informasjon som skal gis når personopplysninger innhentes fra den registrerte selv. Artikkel 14 gjelder hvilken informasjon som skal gis dersom personopplysningene ikke innhentes fra den registrerte. Bestemmelsene angir også tidspunktet for når informasjonen skal gis.

Når personopplysninger innhentes fra den registrerte: Informasjon skal gis på et tidspunkt som setter den registrerte i stand til å lese og vurdere egen deltakelse, uten press fra den som ber om samtykke. I praksis gis ofte informasjon sammen med samtykkeskjema.

Når personopplysninger innhentes fra andre enn den registrerte selv: Informasjonen skal gis innen rimelig tid etter at personopplysningene er samlet inn, senest innen en måned, idet det tas hensyn til de særlige forholdene opplysningene er behandlet under.

Vær oppmerksom på at informasjonen den registrerte får vil danne rammene for hva opplysningene kan brukes til/hvordan personopplysningene kan behandles. Dersom behandlingen har flere formål, er det derfor viktig å informere om samtlige formål. Et sekundært formål kan for eksempel være at personopplysningene ønskes brukt til oppfølgingsstudier/nye prosjekter, og at en derfor planlegger å lagre personopplysningene videre etter at det opprinnelige formålet er fullført, og kanskje også utlevere personopplysningene til nye forskningsformål ved andre forskningsinstitusjoner.

2.2.4.2 Innsyn (artikkel 15)

Forskningsprosjekter som behandler helse- og personopplysninger, har ifølge personvernlovgivningen plikt til å gi de registrerte innsyn i disse opplysningene.

I tillegg gir helseforskningsloven forskningsdeltakere rett til innsyn i sikkerhetstiltakene for behandlingen av helseopplysningene. Denne innsynsretten gjelder bare så lenge innsynet ikke svekker sikkerheten.[13]

2.2.4.3 Retting (artikkel 16)

Den registrerte har i tillegg en rett til å be om retting etter personvernforordningen artikkel 16. Den registrerte har også denne retten når hennes personopplysninger behandles i helseforskning, behandlingsrettede helseregistre og andre helseregistre

2.2.4.4 Sletting (artikkel 17)

Sletting av personopplysninger er et endelig tiltak som ikke kan omgjøres. Virksomhetens plikt til å slette personopplysninger, og unntakene fra plikten, er derfor grundig regulert i personvernlovgivningen.

[13] HFL § 40

Personvernforordningen definerer ulike situasjoner der virksomheten har en plikt til å slette personopplysninger. De mest aktuelle tilfellene for helse- og omsorgssektoren er:

- Personopplysningene er ikke lenger nødvendige for formålet
- Behandlingen av personopplysninger er basert på samtykke og samtykket trekkes tilbake
- Personopplysningene har blitt behandlet ulovlig
- Personopplysningene må slettes for å oppfylle en rettslig forpliktelse
- Personopplysningene må slettes fordi en registrert protesterer mot behandlingen og protesten tas til følge etter en konkret vurdering

Personvernforordningen inneholder flere unntak fra plikten til å slette personopplysninger som er beskrevet over. Et eksempel er når lagring er nødvendig for arkivering i allmenhetens interesse, vitenskapelige eller historiske forskningsformål eller statistiske formål. Unntaket gjelder så lenge sletting i alvorlig grad vil hindre at formålene nås. Dette unntaket kan være aktuelt for helse- og personopplysninger som behandles i forskriftsregulerte helseregistre og helserelaterte forskningsprosjekter.

Personvernforordningens artikkel 85 slår fast at nasjonal lovgivning kan fastsette unntaksbestemmelser som blant annet gjelder retten til sletting, når formålet er å bringe personvernforordningene i samsvar med ytrings- og informasjonsfriheten. Dette omfatter behandlinger i form av akademiske ytringer. Anledning til å gjøre unntak fremgår av personopplysningsloven § 3, jf. personvernforordningen art. 17 (3). En vurdering av unntaksbestemmelsen fra retten til sletting må alltid inneholde en avveining mot personvernet, jf. art 85(2). Opplysninger som har inngått i analyse, publiseringer eller er anonymisert kan ikke kreves slettet, jf. helseforskningsloven § 16, tredje og fjerde ledd. Det kan imidlertid kreves at det ikke forskes mer på opplysningene fremover i tid. Dette unntaket er særlig relevant for kliniske studier, som legemiddelutprøving, av hensyn til etterprøvbarhet, bivirkninger mv.

2.2.4.5 Protest (artikkel 21)

Retten til å protestere mot en behandling av personopplysninger gjelder for behandlinger med grunnlag i personvernforordningen art. 6 nr. 1 bokstav e) (allmennhetens interesse) eller f) (berettiget interesse). Allmennhetens interesse er et behandlingsgrunnlag som benyttes innen forskning, særlig i forbindelse med prosjekter av stort omfang og hvor forsker ikke innhenter opplysningene fra den registrerte selv. Berettiget interesse er sjelden relevant i forskningssammenheng.

Med behandlingsgrunnlag i allmennhetens interesse har den registrerte til enhver tid, av grunner knyttet til den enkeltes særlige situasjon, rett til å protestere mot behandling av personopplysninger om vedkommende. Protesten skal tas til følge, og personopplysningene skal følgelig slettes, med mindre prosjektleder/forskningsansvarlige kan påvise at det foreligger tvingende nødvendige grunner for behandlingen, som går foran den registrertes interesser, rettigheter og friheter. Implisitt i dette ligger det at forsker/dataansvarlige må foreta en vurdering av hver enkeltstående protest. Den registrertes situasjon skal tas med i vurderingen og veies opp mot viktigheten/samfunnsnytten av at opplysningene om den registrerte behandles.

2.2.5 Retten til å motsette seg behandling av helseopplysninger i behandlingsrettet helseregister (Rett til sperring/reservasjon)

Helselovgivingen inneholder regler som gir pasienten en rett til å motsette seg deling av helseopplysninger i behandlingsrettede helseregistre. Rettigheten omtales ofte som en rett til å "sperre journalen", eller som «reservasjonsrett». Retten til å motsette seg behandling av helseopplysninger følger av blant annet pasientjournalloven § 17.[14]

For å gjøre retten reell er det viktig at pasienter får informasjon om at de har en slik rett og hvordan de kan utøve den. Virksomheten må derfor gi informasjon om retten til å motsette seg behandling av helseopplysninger. REK har også mulighet til å sette som vilkår for dispensasjon at prosjekter må sende ut et reservasjonsskriv til de registrerte. Virksomheter som behandler helse- og personopplysninger i forskriftsregulerte helseregistre, må være oppmerksomme på at det finnes egne regler om den registrertes rett til å motsette seg behandling av helseopplysninger i slike registre. Rettigheten gjelder der registeret skal behandle navn, fødselsnummer og andre direkte personidentifiserende kjennetegn uten den registrertes samtykke.

Retten til å reservere seg har som formål å ivareta den enkeltes selvbestemmelsesrett slik at personvernulempene ved å etablere et personidentifiserbart register blir mindre i forhold til nytten av registeret.

Å utlevere person- og helseopplysninger fra behandlingsrettede helseregistre til forskningsformål, krever både et unntak fra taushetsplikten som samtykke eller dispensasjon fra taushetsplikten i kombinasjon med et gyldig behandlingsgrunnlag.

[14] Retten til å reservere seg fremgår også av pasient- og brukerrettighetsloven og i enkelte forskrifter som regulerer kvalitetsregistre.

3 Overordnet om virksomhetens ansvar og plikter

For å kunne planlegge og gjennomføre forskningsprosjekter på en god måte, er det avgjørende med god styring og kontroll. Både personvernforordningen og helselovgivningen har regler for hva og hvordan virksomheten skal jobbe med dette.

Forskningsinstitusjonen har ansvaret for informasjonssikkerheten og vil i de fleste tilfeller allerede ha ivaretatt dette gjennom institusjonens internkontrollsystem og etablering av nødvendige tiltak. Dette gjelder bl.a.: styringssystem for informasjonssikkerhet, avtalemaler, diverse prosedyrer, nivå for akseptabel risiko, risikovurdering, konfigurasjonskontroll, tekniske sikkerhetstiltak, hendelsesregistrering, og innsynsrett. Prosjektleder har likevel et selvstendig ansvar for å sette seg inn i og følge de krav som gjelder ved etablering og i den daglige drift av prosjektet.

I multisenterstudier, er det viktig at prosjektleder avklarer med sine prosjektmedarbeidere i andre institusjoner hvilke krav som gjelder for informasjonssikkerhet i prosjektet. Her er det viktig at dataansvarlig/forskningsansvarlig institusjon der prosjektet og prosjektleder har sin forankring leder an arbeidet med informasjonssikkerhet og sikrer at alle samarbeidende institusjoner får tilgang til relevant dokumentasjon og retningslinjer for personvern og informasjonssikkerhet. Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt og stiller krav til styring og kontroll, både organisatoriske-, tekniske- og prosesskrav.

Dette kapittelet omtaler noen av virksomhetens plikter og viktige roller. Flere av virksomhetens og prosjektets plikter og oppgaver behandles i kapitlene 6-8.

3.1 Internkontroll

Den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll). Bestemmelsene som omhandler den dataansvarliges ansvar for internkontroll, fremgår av personvernforordningens artikkel 24. I henhold til helseforskningsloven er det overordnede ansvar lagt til den forskningsansvarlige institusjon.

Internkontroll skal være formalisert, og dokumentasjon om internkontrollen skal til enhver tid være oppdatert og lett tilgjengelig for alle ansatte. Informasjonssikkerhet og personvern bør inngå som en del av den totale internkontrollen i virksomheten, og det er disse områdene som denne veilederen fokuserer på.

Internkontroll er alle planlagte og systematiske tiltak som skal sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lovgivningen. Det inkluderer både helselovgivningen og lovgivning som ikke kun gjelder for helse- og omsorgssektoren, så som personvernregelverket og internasjonale konvensjoner som er inkorporert i nasjonal lovgivning.

De fleste forskningsprosjekter innen helse- og omsorgssektoren vil være organisert under en virksomhet (ansvarlig institusjon) som i henhold til Normen skal ha etablert et styringssystem for informasjonssikkerhet. Styringssystem for informasjonssikkerhet er et verktøy for å sikre internkontroll slik at virksomhetens data behandles iht. gjeldende krav. Det anbefales at det eksisterende styringssystemet i forskningsinstitusjonen gjøres gjeldende for det aktuelle forskningsprosjektet, og at prosjektleder undersøker hvilke interne rutiner som eksisterer hos den enkelte virksomheten.

For mer veiledning om internkontroll i helse- og omsorgssektoren, se Normens veileder om internkontroll.

3.2 Roller og ansvar

Både personvernforordningen og helseforskningsloven (med forskrift om organisering av helseforskning) slår fast at dataansvarlig er ansvarlig for personvernet og informasjonssikkerheten i virksomheten.[15] Virksomheten skal påse at nødvendige tiltak er iverksatt for å ivareta dette.

Dataansvarlig skal videre påse at behandlingen av helse- og personopplysninger og informasjonssikkerheten organiseres slik at det er tydelig hvem som har ansvar for de ulike deler av behandlingen. Ansvar og organisering skal dokumenteres før behandling av helse- og personopplysninger begynner. I de fleste tilfeller vil rollen som forskningsansvarlig og dataansvarlig være sammenfallende og knyttet til det institusjonelle ansvar.

Ansvaret for personvern og informasjonssikkerhet innebærer både et overordnet ansvar for at virksomheten har tilfredsstillende og dekkende internkontroll for personvern informasjonssikkerhet iht. Normen, og et ansvar for at ledere på alle nivåer, ansatte/medarbeidere, innleid personell og leverandører er kjent med og følger de spesifikke krav og plikter som gjelder i virksomheten.

Det er viktig at roller og ansvar i prosjektet er tildelt og avklart før oppstart, slik at det er enighet og forutsigbarhet om hvordan ansvar og oppgaver er fordelt. Roller og ansvar er ofte formelt regulert i lovverk, slik som i helseforskningsloven, men også i forskningsinstitusjoners egne rutiner og retningslinjer. Virksomhetens interne rutiner vil både klargjøre hvordan virksomheten har fordelt de lovpålagte rollene og oppgavene, men også andre roller og oppgaver som er tilpasset virksomhetens størrelse, art og omfang. Undersøk derfor hvordan dette er regulert i din virksomhet.

3.2.1 Bruk av personvernombudet

I henhold til personvernforordningen har mange virksomheter i helsesektoren plikt til å oppnevne et personvernombud. Ombudets oppgaver inkluderer å gi opplæring, råd og anbefalinger om personvern til dataansvarlig, samt kontrollere etterlevelse av regelverket. Personvernombudet har en uavhengig rolle og kan ikke instrueres, men har ikke beslutningsmyndighet. I alle tilfeller er det dataansvarlig som har ansvaret for at helse- og personopplysninger behandles i samsvar med regelverket. Mange virksomheter har etablert forskningsstøttefunksjoner som også bistår med råd og veiledning som ledd i formalisering og gjennomføring av forskningsprosjekter.

[15] Jf, Forskrift om organisering av helseforskning § 3, om forskningsansvarliges plikter.

Personvernombudet og forskningsstøtteenheter sitter på verdifull kompetanse som bør benyttes i alle faser av et forskningsprosjekt. Organisering og arbeidsdeling mellom personvernombudene og forskningsstøtteenhetene skal være angitt i styrende dokumenter for den enkelte institusjon.

En rekke virksomheter har, i tillegg til personvernombud, avtale med eksterne virksomheter (for eksempel NSD/SIKT sin personverntjeneste) som bistår med vurderinger, protokoll for forskningsprosjekter og personvernkonsekvensvurdering der det er nødvendig.

Under planleggingsfasen er det lurt å legge frem prosjektet for virksomhetens personvernombud eller forskningsstøtteenhet, som kan komme med gode innspill og råd for behandlingen av helse- og personopplysninger i prosjektet. Dersom det er vanskelig å avgjøre hva slags type prosjekt det er snakk om, kan personvernombudet være et veldig godt sted å begynne. Personvernombudet kan bistå med kompetanse som den enkelte forsker ikke har dybdekunnskap om. Ved behandling av særlige kategorier av personopplysninger er man pålagt å rådføre seg med personvernombudet, men mange venter unødvendig lenge før de kontakter denne fagkompetansen. En rådføring med personvernombudet kan bidra til å sikre forutsigbarhet i prosjektet, og kan hjelpe prosjektleder med å identifisere utfordringer som må håndteres på et tidlig tidspunkt.

Personvernombudet og forskningsstøtteenhetene vil også ha god kjennskap til rutinene for behandling av personopplysninger i virksomheten, og kan gi opplæring om dette.

Ved utførelse av en personvernkonsekvensvurdering (DPIA), skal personvernombudet involveres og gi en uttalelse om gjennomføring/konklusjon. Det er alltid ledelsen som skal ta stilling til risikoen som er identifisert gjennom personvernkonsekvensvurdering og eventuelt beslutte at behandlingen av personopplysninger kan gjennomføres.

Det er gjort enkelte unntak i lovgivningen fra rådføringsplikten med personvernombudet, for eksempel helseforskningsloven § 33. Sjekk allikevel hvilke rutiner virksomheten har for når personvernombudet skal involveres. Ofte vil en forskningsstøtteenhet bidra med avklaring rundt behov for særskilt personkonsekvensvurdering eller rådføringsplikt før prosjektet forelegges personvernombudet.

Mange virksomheter har en egen informasjonssikkerhetsleder, som gir råd og veiledning rundt risikovurdering ved bruk av IKT- verktøy ved behandling av person- og helseopplysninger i forskning.

3.2.2 Prosjektleders ansvar

I de fleste forskningsprosjekter og andre typer prosjekter er det vanlig at det er oppnevnt/utpekt en prosjektleder. At en navngitt person med riktig kompetanse har et overordnet daglig ansvar for driften av et forskningsprosjekt, er hensiktsmessig av flere grunner, ikke minst i kommunikasjon med vurderingsinstanser og opp mot egen ledelse. Det vil også være betryggende for forskningsdeltakerne å ha en navngitt person å forholde seg til dersom de skulle ha behov for å nå dataansvarlig, for eksempel for å benytte seg av sine rettigheter eller ved spørsmål om prosjektet. Det er imidlertid kun helseforskningsloven som stiller krav om en prosjektleder. Prosjektleder for et helseforskningsprosjekt har i henhold til helseforskningsloven ansvar for den daglige driften av prosjektet og for at prosjektet drives ut fra "etiske, medisinske, helsefaglige, vitenskapelige, personvern- og

informasjonssikkerhetsmessige forhold".[16] Prosjektleder skal ha akademisk kompetanse (i praksis vil dette bety ph.d-grad eller tilsvarende) som kreves for å gjennomføre prosjektet på en forsvarlig måte.

Prosjektleder har ihht § 5 i forskrift om organisering av helseforskning, ansvar for blant annet følgende:

- Å sørge for at etiske, medisinske, helsefaglige, vitenskapelige, personvern- og informasjonssikkerhetsmessige forhold ivaretas i den daglige driften
- Å innvolvere den forskningsansvarlige i forskningsprosjektet før oppstart
- Å sørge for nødvendig forhåndsgodkjenning fra REK og eventuelt andre vurderingsinstanser
- Å sørge for at forskningsprosjekter gjennomføres i henhold til godkjent forskningsprotokoll
- Kommunikasjon med offentlige innstanser og forskningsansvarlig(e).

For mer konkret veiledning om hvilke oppgaver som normalt vil tilfalle en prosjektleder i et forskningsprosjekt hvor det behandles person- og helseopplysninger, se kapittel 6-8.

3.2.3 Den enkelte forskers ansvar

Ved gjennomføring av forskningsprosjektet plikter prosjektleder og de øvrige prosjektmedarbeidere å:

- gjøre seg kjent med prosedyrer i styringssystemet for informasjonssikkerhet og personvern
- ivareta taushetsplikten og personvernet
- påse at formålet med innhenting av helse- og personopplysninger er i samsvar med samtykkeerklæring, eventuelt annet lovlig behandlingsgrunnlag
- følge reglene for bruken av koblingsnøkkel i henhold til forhåndsgodkjenningen fra REK
- følge prosedyrene for sikring av forskningsfil
- ta del i opplæring i informasjonssikkerhet og personvern (f.eks. sette seg inn i sikkerhetsinstruksen)
- følge prosedyrene for bruk av utstyr og spesielt bærbart datautstyr
- følge prosedyrene for bruk av flyttbare datamedia (f.eks. minnepinner)
- følge prosedyrene for eventuell overføring av forskningsdata til utlandet
- følge prosedyrene om forskningsdeltageren krever innsyn i forskningsdataene
- følge prosedyrene dersom forskningsdeltageren trekker samtykket
- ikke benytte tradisjonelle e-postløsninger ved overføring av identifiserbare eller pseudonyme forskningsdata

I forskningsprosjekter som gjennomføres som samarbeid mellom flere institusjoner (multisenterstudier), er det viktig at den enkelte prosjektmedarbeider gjør seg kjent med og

[16] Jf. Forskrift om organisering av medisinsk og helsefaglig forskning § 5.

følger opp de prosedyrer som gjelder i egen institusjon. Merk at, i tråd med bestemmelser som gjelder den dataansvarlige, både i personvernforordningen og helseforskningsloven, kan datasansvarlig ikke delegere ansvar, kun oppgaver. Ansvaret som er beskrevet i kapitlene om henholdsvis prosjektleders og den enkelte forsker ansvar, skal derfor forstås som et ”sørge-for-ansvar”.

3.3 Risikostyring og risikovurderinger

Alle virksomheter skal etablere tekniske og organisatoriske tiltak som er egnet for å håndtere risiko på en tilfredsstillende måte. Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten vurdere tiltakene opp mot virksomheten, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv.[17]

Risikovurderingene skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger. Risikovurderinger skal gjennomføres før behandling av helse- og personopplysninger starter, og ved endringer av behandlinger som kan påvirke sikkerheten. I forskningsprosjekter vil kravet om risikovurdering i stor grad bli ivaretatt gjennom de formelle godkjenningsprosesser og kravet om intern melding om bruk av person- og helseopplysninger.

Det er dataansvarlig som er ansvarlig for at det gjennomføres risikovurdering ved ny og endret bruk av IKT-verktøy som behandler helse- og personopplysninger i forskning. Risikovurderinger dokumenterer at dataansvarlig har iverksatt tilstrekkelige tiltak og at behandlingene utføres innenfor virksomhetens nivå for akseptabel risiko. Normens kapittel 5 om sikkerhetskrav inneholder sikkerhetstiltak som anses egnet for å oppnå tilfredsstillende sikkerhet, men det kan være aktuelt med mer omfattende tiltak, basert på den risiko som skal vurderes.

Mange tekniske løsninger og systemer som tas i bruk av forskere vil allerede ha vært risikovurdert av virksomheten, og vil finnes i oversikter over systemer som er godkjent for bruk til gitte formål, for eksempel lagring av forskningsdata. Undersøk derfor hvilke systemer som allerede er tilgjengelige i virksomheten før behandlingen av personopplysninger starter. Dersom et forskningsprosjekt har behov for løsninger som ikke allerede er anskaffet og risikovurdert av virksomheten, er det viktig at behovet spilles inn til IT/sikkerhetsavdeling og sikkerhetsansvarlig. På denne måten vil systemet kunne risikovurderes i henhold til virksomhetens interne retningslinjer, og virksomhetens kontroll over systemer og løsninger bevares.

Relevante momenter i risikovurderingen er:

- Bruk av teknisk utstyr (f.eks. lagring i nettverk, sikring av bærbart utstyr, nettverk for overføring av data, opptaksutstyr for bilde og lyd)
- Eksterne aktører angriper via internett eller eksterne linjer
- Metode for autorisasjon og tilgangsstyring til forskningsdata for medarbeidere i det enkelte forskingsprosjektet
- Om forskningsfilen er tilstrekkelig pseudonymisert
- Bruk av koblingsnøkkel med vekt på samtidighet mellom koblingsnøkkel og forskningsfil

[17] Se Normen kapittel 3

- Om koblingsnøkkel og / eller forskningsfil oppbevares mobilt (på reise eller hjemmekontor) må metoden for sikring risikovurderes, idet mobilt utstyr generelt gir større risiko
- Om koblingsnøkkelen er sikret slik at personell utenfor forskningsprosjektet ikke får innsyn eller kontroll over den
- Om koblingsnøkkelen er sikret slik at personell i forskningsprosjektet ikke får kontroll over den utenom fastlagte prosedyrer
- Skyløsninger for lagring av forskningsdata

Ulike risikovurderinger innen både informasjonssikkerhet og personvern vil måtte sees i sammenheng gjennom prosjektets livsløp, og det vil ofte være hensiktsmessig å oppdatere eksisterende risikovurderinger ettersom nye vurderinger ferdigstilles, for å sikre at alle relevante risikomomenter er ivaretatt.

Ved ny og endret bruk av IKT-verktøy for behandling av person- og helseopplysninger i prosjektet, vil det også stilles krav til en egen risikovurdering.

For generell veiledning om risikostyring og risikovurdering, se Normens veileder om risikostyring.

3.4 Vurdering av personvernkonsekvenser

Dersom det er sannsynlig at en behandling medfører høy risiko for de registrertes rettigheter og friheter, er den dataansvarlige pålagt å gjennomføre en personvernkonsekvensvurdering etter art. 35 i personvernforordningen.

Enhver behandling av personopplysninger innebærer en viss risiko for at rettigheter og friheter etter personvernforordningen ikke ivaretas. Plikten til å gjennomføre en vurdering av personvernkonsekvenser gjelder ikke for enhver risiko. Risikoen skal være «høy». Formålet med personvernforordningen er blant annet å ivareta de registrertes rettigheter og friheter og sikre at nødvendige vurderinger og tiltak er dokumentert (ansvarlighet). I vurderingen av om det skal gjøres en personvernkonsekvensvurdering, er det konsekvensen og sannsynligheten for *avvik* fra målet (ivaretagelse av rettigheter og friheter) som skal vurderes som større enn normalt. Ved tvil bør det gjennomføres en personvernkonsekvensvurdering.

Direktoratet for E-helse har utgitt en mal for personvernkonsekvensvurdering med tilhørende veiledning for utfylling (publiseres i 2022). Se også Datatilsynets nettside for utdypende informasjon om når og hvordan en personvernkonsekvensvurdering skal gjennomføres og Normens veileder i risikostyring.

3.4.1.1 Hva er en personvernkonsekvensvurdering?

Personvernkonsekvensvurdering er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak.

Personvernkonsekvensvurderinger skal minst inneholde

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger

- beskrivelse av formålet med behandlingen av personopplysninger
- en vurdering av om behandlingene av helse- og personopplysninger er nødvendige og står i rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

3.4.1.2 Når skal det gjennomføres en personkonsekvensvurdering?

Momenter som slår fast eller taler for at det skal gjennomføres en personvernkonsekvensvurdering:

- Behandlingen er oppført i Datatilsynets liste over behandlingsaktiviteter som alltid innebærer høy risiko for de registrertes rettigheter og friheter (krever alltid personvernkonsekvensvurdering/DPIA).
- Et av de alternative kravene i personvernforordningens Artikkel 35 (3) er oppfylt
- Krav i artikkel 29-gruppens veileder er oppfylt. I veilederen er det lagt til grunn ni relevante kriterier for å avgjøre hvorvidt en behandling vil føre til høy risiko eller ikke. Det er vanlig å gjennomføre en personvernkonsekvensvurdering /DPIA dersom to eller flere kriterier er oppfylt, men dette er ikke absolutt. Virksomheten må gjøre en konkret vurdering. Kravet til en god begrunnelse for ikke å gjøre en DPIA blir høyere jo flere kriterier som er oppfylt.
- Virksomheten har tidligere utført en DPIA for behandlingen av personopplysninger, og ser et behov for å oppdatere med en ny personvernkonsekvensvurdering.
- Virksomheten har tidligere hatt konsesjon fra Datatilsynet eller godkjenning fra REK som er datert før juli 2018.

På Datatilsynets liste over behandlinger som alltid krever en personvernkonsekvensvurdering, nevnes flere behandlingsaktiviteter som sannsynligvis ofte vil foregå i eller tilknyttet helse- og omsorgssektoren eller i forbindelse med forskning:

- Behandling av genetiske opplysninger i følge med minst ett annet kriterium *.
    - For eksempel behandling av genetiske opplysninger i stor skala, inkludert gensekvensering. (Særlige kategorier eller svært personlige opplysninger og stor skala.)
- Behandling av personopplysninger med innovativ teknologi i følge med minst ett annet kriterium *.
    - For eksempel behandling av helseopplysninger med innovativ velferdsteknologi som helseimplantater. (Innovativ bruk og særlige kategorier av opplysninger.)
- Behandling av personopplysninger for systematisk monitorering av ansatte.
    - For eksempel overvåking av ansattes internettaktivitet, elektroniske kommunikasjon og kameraovervåking. (Sårbare registrerte og systematisk monitorering.)
- Behandling av personopplysninger, uten samtykke, for vitenskapelige eller historiske formål i følge med minst ett annet kriterium *.

    - For eksempel behandling av helseopplysninger for forskningsformål uten den registrertes samtykke. (Evaluering og særlige kategorier av opplysninger eller svært personlige opplysninger.)

- Behandling av lokasjonsdata i følge med minst ett annet kriterium *.
    - For eksempel systematisk sammenstilling av den registrertes lokasjons- og trafikkdata fra teleoperatører eller behandling av personopplysninger om abonnentens bruk av telenettet eller teleoperatørens tjenester. (Svært personlige opplysninger og systematisk monitorering.)
- Behandling av særlige kategorier av personopplysninger eller svært personlige opplysninger i stor skala for algoritmetrening.
- Behandling av personopplysninger ved å systematisk monitorere effektivitet, ferdigheter, kunnskap, mental helse og utvikling. (Svært personlige opplysninger og systematisk monitorering).
- Innsamling av personopplysninger i stor skala gjennom «tingenes internett» eller velferdsteknologi. (Stor skala og særlige kategorier av opplysninger eller svært personlige opplysninger.)

Når Datatilsynet omtaler en type behandling «i følge med minst ett annet kriterium», viser dette til de kriteriene som fremgår av «Artikkel 29-gruppens kriterier for å vurdere behov for DPIA». Kriteriene til Artikkel 29-gruppen finnes i Datatilsynets veiledning om når man må gjennomføre en vurdering av personvernkonsekvenser.

Eksempler på når det bør vurderes å gjennomføre en personvernkonsekvensvurdering:

- Behandlingen av personopplysninger er av en slik karakter at de registrerte (prosjektdeltakere) har høye forventninger/krav til ivaretakelsen av personvernet, for eksempel sårbare grupper prosjektdeltakere (barn, psykisk syke) eller at forskningsprosjektet handler om et stigmatiserende eller svært sensitivt tema som selvmord, ME, kvinnesykdommer etc.

- De registrerte har reduserte muligheter til å utøve sine rettigheter etter personvernlovgivningen, f. eks når det er gitt en dispensasjon fra taushetsplikten, barn er prosjektdeltakere, etc.
- Store mengder data og registerstudier
- Forskningsprosjekter hvor det ikke innhentes samtykke
- Innovasjonsprosjekter hvor ny teknologi skal prøves ut (det vil være vanskelig for den registrerte å sette seg inn i omfanget)
- Opprettelse av medisinske kvalitetsregistre hvor data skal lagres over et langt tidsrom, og brukes til en rekke formål (forutsatt forhåndsgodkjenning fra REK)

3.4.1.3 Personvernkonsekvensvurdering med flere virksomheter

Utgangspunktet i personvernforordningen er at det er dataansvarlig alene som har ansvaret for å gjennomføre personvernkonsekvensvurderinger. Det finnes tilfeller der flere virksomheter deltar i en behandling som det skal gjennomføres en personvernkonsekvensvurdering for. Dette kan være virksomheter som skal gjennomføre

enkelte behandlingsaktiviteter for den dataansvarlige, for eksempel dataanalyse eller lagring, eller at virksomhetene har felles dataansvar.

Når flere virksomheter skal utføre behandlingsaktiviteter som skal dekkes av samme personvernkonsekvensvurdering, for eksempel en multisenterstudie, er utgangspunktet at hele behandlingen dekkes av en personvernkonsekvensvurdering, som gjennomføres av virksomheten som har dataansvaret.

Dersom virksomheten har felles dataansvar med en annen virksomhet, må det klargjøres hvilken(e) av partene som har ansvar for gjennomføring av personvernkonsekvensvurderingen. Ansvaret for risiko/restrisiko må også avklares. Dette skal følge av en ordning mellom partene, jf personvernforordningen artikkel 26 nr. 2.

Det kan også være hensiktsmessig å gjennomføre en personvernkonsekvensvurdering i pilotprosjekter hvor man ser at databehandlingen på sikt kan få et større omfang. Dersom man begynner å kartlegge databehandlingen på et tidlig stadium, vil det også være enklere å finne ut hvilke tiltak som kan bidra til å redusere personvernrisikoen. Det kan også oppleves mindre krevende for prosjektet dersom de gradvis gjennomfører DPIA i takt med prosjektets utvikling.

3.4.1.4 Målet med en personvernkonsekvensvurdering

En personvernkonsekvensvurdering inneholder bl.a. en vurdering av risiko. Fokus for denne vurderingen er ikke hvilken risiko virksomheten løper på egne vegne, men hvilke risikoer behandlingen av personopplysninger kan medføre for enkeltpersonene virksomheten behandler opplysninger om, eventuelt hvordan behandlingen kan påvirke andre fysiske personer. Dette vil være aktuelt i forskningsprosjekter som kan være egnet til å gjøre det vanskelig for de registrerte å håndheve sine rettigheter, eller der brudd på personopplysningssikkerheten kan oppleves ekstra belastende.

Når virksomheten starter på en personvernkonsekvensvurdering fordi man har identifisert at risikoen for personvernet er høy, må den være innstilt på å gjøre endringer/tilpasninger i den planlagte behandlingen av personopplysninger. Det er ikke nødvendigvis mulig å redusere samtlige identifiserte risikoer. Virksomheten må ha som mål å bringe den samlede risikoen til et akseptabelt nivå. Alternativet er forhåndsdrøfting med Datatilsynet eller at behandlingen ikke kan gjennomføres.

3.5 Tilgangsstyring

Prosjektleder må sørge for at alle prosjektmedarbeidere som skal ha tilgang til person- og helseopplysninger har tilganger basert på sin rolle og oppgaver i prosjektet. I helseforskning vil ofte tilgangen være i samsvar med prosjektdeltakere meldt inn til REK, så sant de har behov for tilgang.

Det er særlig viktig at forskere som også arbeider som helsepersonell i virksomheten, har en separat tilgangsrolle tilpasset forskerrollen. Samtidig må de(n) dataansvarlige ha rutiner for hvordan eksterne forskere skal gis korrekte tilganger, slik at de ikke for tilgang til flere opplysninger enn det som er nødvendig for å utføre sin rolle i prosjektet.

Prosjektleder i forskningsprosjektet skal sørge for at det etableres prosedyrer for tilgangsstyring til forskningsdata og forskningsfil, slik at kun de som er autoriserte for tilgang

får forskningstilgang i henhold til vedtatte prosedyrer i virksomheten. I mange tilfeller kan den enkelte virksomhet ha sentrale føringer for slike prosedyrer. Prosedyrene må ta hensyn til om personer som opplysningene i forskningsfilen gjelder er direkte eller indirekte identifiserbare, fordi kravet til forholdsmessig sikring gjør at sikkerhetsnivået kan være ulikt. Ved eventuell bruk av lyd- og bildeopptak må prosedyrene for tilgangsstyring omfatte dette.

For mer informasjon og veiledning, se Normens veileder for tilgangsstyring (ny utgave kommer våren 2022).

3.6 Logging

Et viktig sikkerhetstiltak er å ha kunnskap om hvem som har hatt tilgang til hvilke data og i hvilke systemer. Hva som skal logges:

a) All forskningstilgang, registrering, retting og sletting, autorisert og forsøk på uautorisert bruk og kopiering / duplisering av forskningsdata og forskningsfilen
b) All autorisert og forsøk på uautorisert bruk og kopiering / duplisering av koblingsnøkkelen eller fil med koblingsnøkler

I forsknings- og kvalitetsprosjekter hvor det er gitt dispensasjon, kan det fremstå som uklart for de registrerte hvorfor det er gjort oppslag i deres journal. Oppslaget er kodet som forskning, men det er ikke tilstrekkelig informasjon for dem til å ta stilling til innsynet og gir ingen begrunnelse for hvorfor den aktuelle personen har fått lov til å gjøre oppslaget. Derfor kan det være hensiktsmessig å henvise til prosjekttittel og formål når det gjøres oppslag i pasientens journal.

Les mer om logging i Normen, kapittel 5.4.4 og i Normens faktaark «Logging og innsyn i logg».

3.7 Opplæring av ansatte/forskere om virksomhetens rutiner for personvern og informasjonssikkerhet

Dataansvarlig skal påse at det er etablert og gjennomføres opplæring i informasjonssikkerhet og personvern i egen virksomhet. Prosjektleder på sin side skal påse at alle prosjektmedarbeidere har den nødvendige kompetanse og opplæring for å kunne gjennomføre sine oppgaver i prosjektet. Opplæringen skal fokusere på virksomhetens eventuelle sikkerhetsinstruks og områder risikovurderingen peker ut som sentrale for den enkelte medarbeider.

Opplæring skal gis:

- Før forskningsprosjektet starter
- Når det kommer nye medarbeidere i forskingsprosjektet
- Når det er påkrevet som følge av endringer i styringssystemet for informasjonssikkerhet og personvern
- Når det er påkrevet som følge av gjennomført risikovurdering

- Når det innføres nye regulatoriske krav innen informasjonssikkerhet
- Ved avvik som avdekker et behov for opplæring

4 Tilgjengeliggjøring av helse- og personopplysninger

For å kunne tilgjengeliggjøre opplysninger må virksomheten ha et lovlig behandlingsgrunnlag og følge reglene om taushetsplikt.

Dersom behandlingsgrunnlaget for eksempel omfatter et vedtak om dispensasjon fra taushetsplikt, må dispenserende myndighet kontaktes før man deler opplysninger videre, med mindre dispensasjonen allerede tillater tilgjengeliggjøringen.

Mange forskningsprosjekter gjennomføres som samarbeid mellom forskningsinstitusjoner og i slike prosjekter er deling eller tilgjengeliggjøring av forskningsdata på tvers av virksomhetene en viktig forutsetning. Mange forskningsprosjekter samler også inn verdifulle data som det kan være veldig ønskelig og viktig å kunne dele med andre forskere/institusjoner for gjenbruk til nye forskningsformål. Tilgjengeliggjøring eller deling av forskningsdata som inneholder helse- og personopplysninger er imidlertid regulert av personvernlovgivningen og det er derfor viktig at forskningsinstitusjonene er rigget for slik deling og gir sine forskere opplæring i hvordan dette kan foregå.

De ulike måtene å dele eller gjøre forskningsdata tilgjengelig på kan beskrives som

- Overføring av helse- og personopplysninger mellom samarbeidende virksomheter
- Tilgjengeliggjøring av forskningsdata til nye forskningsformål
- Tilgjengeliggjøring i form av publisering av helse- og personopplysninger
- Lagring eller arkivering etter prosjektslutt til andre fremtidige formål.

Det er de to første som omtales i dette kapitlet. Veiledning om publisering og lagring/arkivering finnes i kapittel 8 (Avslutningsfasen).

I tillegg til at lovverket regulerer ulike måter å dele eller tilgjengeliggjøre forskningsdata på, er det også andre viktige forutsetninger som påvirker nytteverdien av tilgjengeliggjøringen. Et eksempel på dette kan være de såkalte FAIR-prinsippene.

FAIR-prinsippene er et sett med veiledende arkitekturprinsipper som skal tilrettelegge for deling og gjenbruk av data gjennom at dataene er søkbare (**F**indable), tilgjengelige (**A**ccessible), understøtter interoperabilitet (**I**nteroperable) og er gjenbrukbare (**R**eusable).

Statens IKT-politikk innebærer et mål om økt gjenbruk av offentlige data.[18] Regjeringens føringer for deling av åpne offentlige data er regulert i regjeringens «Retningslinjer ved tilgjengeliggjøring av offentlige data».[19] Ifølge disse retningslinjer må data tilgjengeliggjøres på en måte som gjør det mulig for brukere å realisere verdien av dem. Dette innebærer både juridisk beskrivelse av hvordan data kan brukes og teknisk beskrivelse av hvordan data er tilgjengeliggjort. Merk at person- og helseopplysninger ikke kan regnes som åpne offentlige data, men krever at man har et formål og et behandlingsgrunnlag.

[18] IKT-politikk - regjeringen.no
[19] Retningslinjer ved tilgjengeliggjøring av offentlige data - regjeringen.no

Norges forskningsråds policy følger «åpen som standard»-prinsippet når det gjelder tilgang til forskningsdata, men skisserer samtidig hvilke unntak som gjelder.[20] Årsaker til å begrense tilgjengeligheten er blant annet sikkerhetshensyn og personvernhensyn. FAIR-prinsippene og NFR sin policy om åpne data skal derfor ikke tolkes som i konflikt med personvernregelverket. Tilgangen til forskningsdata skal være så åpen som mulig og så begrenset som nødvendig. For utfyllende veiledning, se Direktoratet for E-helses «Veileder for bruk av FAIR-prinsippene for helsedatakilder».[21]

4.1 Overføring av/tilgang til helse- og personopplysninger mellom samarbeidende virksomheter

Dersom helse- og personopplysninger skal overføres til en annen virksomhet som del av et samarbeid er det den av de samarbeidende virksomhetene som har dataansvaret, som vurderer og dokumenterer lovlig behandlingsgrunnlag. Når samarbeidende virksomhet(er) skal ha tilgang til opplysningene for å utføre oppgaver i prosjektet, løses dette ved at virksomhetene inngår en databehandleravtale med dataansvarlig. Ved å inngå en databehandleravtale, sørger dataansvarlig for at virksomheten har kontroll på hvordan opplysningene behandles av ekstern virksomhet/samarbeidende virksomhet(er). Ved slik deling mellom virksomhetene skal man også oppgi denne informasjonen til de registrerte.

Dersom samarbeidende virksomheter har felles dataansvar vil ikke databehandleravtale være nødvendig for utveksling av helse- og personopplysninger mellom disse virksomhetene. Informasjon om ansvaret for behandlingen av opplysningene skal formidles til de registrerte.

4.2 Deling av forskningsdata til nye forskningsformål

Med deling av forskningsdata til nye forskningsformål menes helse- og personopplysninger som er innsamlet for et forskningsformål, som deretter deles med andre (eksterne eller interne) til nye forskningsformål. Ved slik deling er det ikke tilstrekkelig at avsender av opplysningene har behandlingsgrunnlag. Også virksomheten som skal motta opplysningene må ha et lovlig grunnlag for å kunne motta opplysningene. Det gjelder uavhengig av om dataene deles internt i virksomheten eller til andre forskningsvirksomheter. Slik deling krever både at dataansvarlig har behandlingsgrunnlag for utleveringen og at den som mottar opplysningene har lovlig behandlingsgrunnlag for det nye formålet.

Vær oppmerksom på at samtykker som har vært innhentet for det opprinnelige forskningsformålet må være i samsvar med utleveringen og bruk for det nye formålet. Dersom samtykket ikke dekker deling av dataene eller det ikke er gitt god nok informasjon om det nye forskningsformålet, må det gis oppdatert informasjon, eventuelt innhentes nye samtykker.

[20] 1254032061080.pdf (forskningsradet.no)
[21] Veileder for bruk av FAIR-prinsippene for helsedatakilder - ehelse

Personvernforordningens formålsbegrensningsprinsipp slår fast at virksomheten kan fortsette å behandle helse- og personopplysninger etter at formålet er oppnådd dersom behandlingen er nødvendig for å oppnå nye formål som er forenlige med det opprinnelige formålet.

I vurderingen av forenlighet skal det blant annet tas hensyn til forbindelsen mellom opprinnelige og nye formål, sammenhengen personopplysningene ble samlet inn i (herunder relasjonen mellom virksomheten og den registrerte, og den registrertes forventninger), personopplysningenes art, mulige konsekvenser av behandlingen og eventuelle garantier for personvernet. De nye formålene kan være forenlige med den opprinnelige behandlingen, hvis de er en naturlig forlengelse av de opprinnelige formålene, og den nye behandlingen ikke medfører større konsekvenser for den registrerte.

5 Anonymisering av forskningsdata

Anonymisering av helse- og personopplysninger benyttes ofte som et verktøy for å redusere/fjerne personvernulempen og slik sett åpne opp for en større mulighet til å bruke opplysningene. Flere lover og forskrifter stiller strenge krav knyttet til bruk av helse- og personopplysninger, som ikke gjelder etter at opplysningene er anonymiserte. Dette åpner for eksempel opp for en bredere bruk av opplysningene i analyser, forskning, statistikk og publisering av datasett. Anonymisering skal være en irreversibel prosess, slik at det ikke er mulig å re-identifisere den registrerte.[22]

Verken de generelle kravene i personvernforordningen eller de mer spesifikke kravene i helselovgivningen gjelder for anonymiserte personopplysninger. Når opplysningene er anonymiserte, så trenger ikke dataansvarlig lenger å vurdere behandlingens lovlighet og om den ivaretar de øvrige personvernprinsippene i personvernforordningen. Behandlingen frem til opplysningene er anonyme må likevel være i samsvar med behandlingsgrunnlaget. I tillegg utgjør det et forskningsetisk spørsmål hvorvidt man bør dele anonymiserte data uten at de registrerte er informert, når data er innsamlet basert på samtykke.[23]

Det er viktig å merke seg at anonymisering er en behandling av personopplysninger. Dersom anonymisering av personopplysningene inngår i behandlingen som personopplysningene samles inn for, så må dataansvarlig blant annet definere tydelige formål for behandlingen (anonymiseringen), samt vurdere om dataansvarlig har behandlingsgrunnlag etter personvernforordningen artikkel 6.[24]

Anonymisering er også et verktøy som kan oppfylle kravet om innbygget personvern (personvernforordningen artikkel 25).

[22] Datatilsynets veileder «Anonymisering av personopplysningene» (2015) side 6
[23] Aronsen-utvalget nedsatt av Forskningsrådet kommenter dette i rapportens pkt. 1.5
[24] Les mer om behandlingsgrunnlag i Faktaark 56 – Formål og behandlingsgrunnlag

Helse- og personopplysninger regnes som anonymiserte når de håndteres eller bearbeides slik at de ikke lenger kan knyttes til en identifisert eller identifiserbar fysisk person.[25] I dette ligger ikke et absolutt krav om at det skal være praktisk umulig å koble opplysningene til en identifiserbar person. Dataansvarlig må gjøre en tilsvarende vurdering som ved vurderingen av om en opplysning kan knyttes til en identifiserbar person slik at opplysningen skal regnes som en personopplysning. Dataansvarlig må ta utgangspunkt i de faktiske forholdene og vurdere sannsynligheten for at reidentifisering av den registrerte kan skje. I vurderingen skal dataansvarlig ta hensyn til alle tilgjengelige hjelpemidler som med rimelighet kan tenkes brukt i en slik identifisering.[26]

Anonymisering må ikke forveksles med det å pseudonymisere opplysningene.

Ved pseudonymisering bearbeides personopplysningene slik at det ikke lenger er mulig å identifisere de registrerte uten tilleggsopplysninger. Tilleggsopplysningene må beskyttes av tekniske og organisatoriske tiltak, slik at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar person.

Ved bruk av pseudonymisering, så vil personopplysningene tilsynelatende ikke kunne knyttes til en registrert. Det vil imidlertid være mulig å reidentifisere den registrerte ved å bruke tilleggsopplysninger, og det er dette som skiller resultatet etter bruk av disse verktøyene fra resultatet etter anonymisering. Etter pseudonymisering vil helse- og personopplysningene fremdeles regnes som personopplysninger, ettersom den registrerte fremdeles kan identifiseres.

Anonymisering skal være en irreversibel prosess, slik at det ikke er mulig å reidentifisere den registrerte.[27]

5.1.1 Vanlige risikofaktorer ved anonymisering av helse- og personopplysninger

Det finnes ingen universell metode for anonymisering av helse- og personopplysninger. Dataansvarlig må vurdere hva som skal til for å anonymisere hvert enkelt datasett som inneholder slike opplysninger. Dataansvarlig må blant annet ta hensyn til antallet variabler datasettet inneholder og variablenes art, opplysningenes detaljeringsgrad og hvilke tilleggsopplysninger som kan være tilgjengelig for offentligheten eller andre aktører.

Datatilsynet trekker frem tre sentrale risikoer som kan oppstå ved anonymisering av helse- og personopplysninger, og som bør brukes i vurderingen av hvor godt dataansvarlig har sikret seg mot reidentifisering:

1. Er det mulig å skille ut en enkeltperson i datasettet etter at anonymiseringen er gjennomført?
2. Er det mulig å koble flere datasett sammen og til den samme personen?
3. Er det mulig å utlede informasjon som kan knyttes til en enkeltperson fra datasettet?[28]

[25] Personvernforordningens fortalepunkt 26
[26] Datatilsynets veileder «Anonymisering av personopplysningene» (2015)
[27] Datatilsynets veileder «Anonymisering av personopplysningene» (2015) side 6
[28] Datatilsynets veileder «Anonymisering av personopplysningene» (2015) side 12

I en vurdering av om en metode eller teknikk for anonymisering er tilfredsstillende, bør dataansvarlig vurdere risikoen for reidentifisering (knyttet til det aktuelle datasettet) både før og etter at anonymiseringen er gjennomført. Ettersom omstendighetene rundt opplysningene kan endre seg i tråd med den teknologiske utviklingen og at nye tilleggsopplysninger blir tilgjengelig, så bør virksomheten også legge opp til jevnlig reevaluering av faren for reidentifisering.

Dersom det ikke ble gjort en grundig nok vurdering av dette innledningsvis, er det sannsynlig at det forskningsdeltakerne har samtykket til ikke tillater at datamaterialet lagres videre. Er anonymisering umulig, kan det være at de registrerte må få ny informasjon, eventuelt sikre nytt behandlingsgrunnlag f.eks. ved å innhente nye samtykker.

6 Planleggingsfasen

Et forskningsprosjekt består av ulike faser, som hver for seg er viktige for å sikre at et prosjekt blir gjennomført på en forsvarlig måte i tråd med gjeldende lovverk og anerkjente forskningsetiske normer.

Dette kapitlet handler om viktigheten av god planlegging, hva man må planlegge for, hvilke gevinster man oppnår ved dette, eller på den andre siden hvilke risikoer det kan innebære dersom man har det for travelt med å «komme i gang».

I planleggingsfasen må det også legges til rette for aktiviteter som skal skje i sluttfasen av et forskningsprosjekt. Dersom opplysningene for eksempel skal publiseres i etterkant eller lagres for andre forskningsformål, må dette tas høyde for i planleggingsfasen. Dersom det er ønskelig å publisere personidentifiserende eller pseudonyme opplysninger, må dette for eksempel informeres om til forskningsdeltakerne og det må innhentes samtykke til dette. I de tilfellene hvor forsker ønsker at forskningsdataene skal anonymiseres og gjenbrukes til et annet forskningsformål, må det også innhentes samtykke for dette.

6.1 Forankring hos egen ledelse/helseforetaket

Prosjektet som skal gjennomføres må ha administrativ og faglig støtte hos den øverste ledelsen i virksomheten. Som ansvarlig for all behandling av personopplysninger, skal ledelsen alltid ha oversikt over pågående aktiviteter. Ledelsen skal ha fastsatt rutiner og kontrollmekanismer som sikrer at behandlinger som ikke er forsvarlige ikke igangsettes før nødvendige tiltak er på plass.

Dette kapitlet beskriver de viktigste avklaringene forsker må gjøre og som skal forankres hos ledelsen i startfasen/planleggingen. Merk likevel at alle faser av prosjektet skal dokumenteres og være tilgjengelig for virksomhetens ledelse slik at de til enhver tid kan kontrollere at behandlingen av personopplysninger gjennomføres i tråd med forskningsprotokoll og relevante godkjenninger.

6.2 Interne retningslinjer for hvordan prosjekter skal organiseres og dokumenteres i virksomheten

Alle virksomheter som behandler helse- og -personopplysninger skal ha et internkontrollsystem som sikrer at behandlingen skjer på en lovlig måte. Dette betyr at behandlingen i seg selv må foregå innenfor rammer som er tilpasset både loven og virksomhetens ressurser, samt at det må kunne dokumenteres. Det er derfor viktig at den som skal lede prosjektet setter seg inn i de krav og forventninger som ligger til denne rollen og hva som må være på plass før prosjektet kan starte opp. Dette er ofte aktiviteter som går parallelt med arbeidet med utarbeidelse av en prosjektbeskrivelse og forskningsprotokoll.

Dokumentasjon på hvordan behandlingen skjer er viktig for å kunne påvise at man følger personvernlovgivningen. Kravet til dokumentasjon følger også av helselovgivningen. Som regel er det noen i virksomheten som har i oppgave å støtte forsker i forskningsprosessen, og de er avhengig av at forsker dokumenterer planer, godkjenninger og endringer slik at forskerstøtten kan hjelpe forsker og virksomhetens ledelse med å sikre at behandlingen skjer i tråd med juridiske og organisatoriske rammer.

Å jobbe planlagt og systematisk er viktige forutsetninger for å kunne gjenta en suksess. Dokumenter og la andre lære av det som gav resultater.

6.3 Utform prosjektbeskrivelse/ forskningsprotokoll

Utarbeidelse av prosjektbeskrivelse / forskningsprotokoll er avgjørende for at dataansvarlig institusjon skal kunne ta stilling til hvorvidt prosjektet er etisk og juridisk gjennomførbart. Dette gjelder ikke minst for å kunne dokumentere hvordan prinsippene i personvernforordningen planlegges ivaretatt i prosjektet. I helseforskningsforskriften § 8 er det angitt krav om hva en forskningsprotokoll minimum bør inneholde av informasjon. For en del prosjekter med mer kompliserte prosesser for innsamling av person- og helseopplysninger, så kan det i tillegg til forskningsprotokollen også være nødvendig å utarbeide en egen datahåndteringsplan. Det finnes flere maler tilgjengelig for dette formålet.

En prosjektbeskrivelse eller forskningsprotokoll skal inneholde en fremstilling av hvordan prosjektet tenkes gjennomført. Prosjektbeskrivelsen/forskningsprotokollen inneholder som regel tittel, et avsnitt om bakgrunn, formål og problemstilling, design, utvalg, variabler, datainnsamling, analyse, prosjektorganisasjon, personell, utstyr og ressurser, kostnader og finansieringsplan, tidsplan, publisering og etikk.

Det er også viktig å beskrive samfunnsnytten ved prosjektet, og identifisere/peke på personvernulempen og eventuelle andre ulemper/risiko for forskningsdeltakerne. Dette styrker prosjektplanen og forskers evne til å hele tiden beholde den registrertes perspektiv i fokus.

6.3.1 Avklar og beskriv prosjekttype og formål

Gjennomføringen av et prosjekt vil alltid kunne by på overraskelser, og det kan virke vanskelig, og noen ganger nærmest uhensiktsmessig å planlegge alt ned til minste detalj. Det er heller ikke alltid nødvendig. Det viktigste er at man tar utgangspunkt i hva man ønsker å oppnå, og dersom det innebærer en behandling av personopplysninger, må man sørge for at man har et lovlig behandlingsgrunnlag for alle formålene.

Ulike *typer* prosjekter kan ha mange likhetstrekk, og noen ganger kan det være vanskelig å avgjøre hvorvidt et prosjekt er helseforskning, annen forskning eller f.eks. kvalitetssikring. Dersom prosjektets formål etter dataansvarliges vurdering er tydelig, må dette også fremgå tydelig i presentasjonen av prosjektet overfor de aktuelle vurderingsinstansene. Er det avgjørende for dataansvarlig virksomhet at prosjektet vurderes som helseforskning og derav får en medisinsk etisk vurdering, da må prosjektleder sørge for at kriteriene for hva som ansees som medisinsk og helsefaglig forskning, er oppfylt og fremgår klart og tydelig.

I tillegg til at type prosjekt må avklares, er det viktig å avgrense og beskrive hva som er formålet med prosjektet. Med dette menes: *hva man ønsker å oppnå med behandlingen av personopplysningene.*

For å avgjøre hvorvidt formålet med et prosjekt kan betraktes som helseforskning, anbefales det å stille følgende kjernespørsmål:

- Er søknaden/prosjektet fremleggingspliktig etter helseforskningsloven, eller ikke?

I vurderingen av den enkelte sak er dette nøkkelspørsmål:

- Hva er formålet med prosjektet? Er formålet å skaffe til veie ny kunnskap om helse og sykdom?
- Innebærer prosjektet risikomomenter utover det som er vanlig i diagnostikk og behandling, eller fare for integritetskrenkelse?
- Kan prosjektet gjennomføres innenfor de lover og regler som gjelder for helse – og omsorgstjenesten?

6.3.1.1 Hvorfor er en avklaring viktig?

Grunnen til at det er viktig å avklare om det er helseforskning, annen forskning, kvalitetssikring, forskning på biologisk materiale eller en annen type prosjekt, samt hva som er det konkrete formålet/eller formålene, er fordi type prosjekt og formål(ene) sier noe om hvilke godkjenninger som er nødvendige og hvilke lovverk som regulerer behandlingen. Med andre ord; hva som er de juridiske rammene for behandlingen. I tillegg til de juridiske rammene kan forskningsvirksomheten ha egne interne regler eller retningslinjer på det aktuelle området, som det er avgjørende å kjenne til.

Merk at en behandling av personopplysninger kan ha flere formål, kanskje ett hovedformål og så sekundære formål man ønsker å oppfylle i tillegg. For eksempel kan et forskningsprosjekt inneholde en masteroppgave eller lignende i tillegg til forskningsformålet

En avklaring av ulike formål tidlig i prosessen gir bedre forutsetninger for å planlegge tidsbruk, hvilke instanser som må kontaktes først og hvordan prosjektdesignet kan påvirke hvorvidt det som er planlagt kan gjennomføres.

I mange tilfeller kan det være at små endringer i prosjektopplegget skiller hva som er innenfor og utenfor lovens rammer. Dette må avklares tidlig, og vil også være en god hjelp i generell prosjektstyring.

6.3.2 Avklar og beskriv ansvar og roller

Prosjekter varierer i omfang og kompleksitet, fra et avgrenset prosjekt med en forsker til de store og langvarige prosjektene hvor flere forskningsinstitusjoner er involvert. Ifølge personvernforordningen er det den som bestemmer formålet og hvordan behandlingen av personopplysninger skal gjennomføres, som er dataansvarlig.

Dersom flere virksomheter har et felles dataansvar, må dette være avklart helt i startfasen av planleggingen. Roller og ansvar er også informasjon som de fleste vurderings- eller godkjenningsinstanser ber om, og det er derfor viktig at de mottar den samme informasjonen.

At ansvar og roller er avklart og beskrevet/dokumentert, vil bidra til at man ikke ender opp i en situasjon hvor oppgaver ikke er utført, eller uenighet om eierskap til forskningsdata. Merk at det er den dataansvarlige som har det juridiske ansvaret for at personopplysningene behandles forsvarlig. Dette gjelder selv om involverte samarbeidspartnere har fått i oppgave å utføre deler av behandlingen.

6.3.3 Kartlegg og beskriv samarbeid og avhengigheter

Med avhengigheter menes de oppgavene som må utføres for at prosjektet skal kunne gjennomføres. Det er naturlig å begynne med hvem som har dataansvaret, om det benyttes databehandlere og hvilke vurderinger/godkjenninger man må innhente. Vurderinger skal alltid innhentes før en behandling av personopplysninger igangsettes. Dersom man vet at man vil måtte benytte en databehandler for deler av behandlinger, vil dette også være en avhengighet som man bør planlegge for.

Har dataansvarlig avtale med eksterne bidragsytere/forskere fra andre forskningsinstitusjoner, må slike avtaler dokumenteres. Dataansvarlig skal til enhver tid ha kontroll med behandlingen av personopplysninger. Dette er et «sørge for»-ansvar som innebærer at de må sikre at de har instruksjonsmyndighet overfor de som utfører oppgaver for dem.

Noen vanlige avhengigheter:

- Utarbeidelse av avtaler (f.eks. databehandleravtaler, samarbeidsavtaler, avtaler om overføring mellom virksomheter og til tredjeland, avtaler med registereiere)
- Innhenting av vurderinger/godkjenninger/dispensasjoner
- Kontakt med dataeier/registereiere
- Analysekompetanse dersom den ikke finnes i egen virksomhet (databehandleravtale eller ansettelsesforhold)
- Plikt til å rådføre seg med personvernombudet dersom forskningen/prosjektet innebærer en behandling av særlige kategorier av helse- og personopplysninger
- Eventuelt, krav om personvernkonsekvensvurdering (DPIA)
- Interne retningslinjer
- Taushetserklæringer

Alle avtale- eller vurderingsprosesser tar tid. Fordelen ved å investere tid i presise og gode vurderingsprosesser, er at forsker kan være tryggere på at prosjektet kan gjennomføres innenfor den tidsrammen som er planlagt. Å rette opp i feil tar erfaringsmessig mer tid.

6.4 Vurdering av personvern

Vær oppmerksom på at all behandling av personopplysninger skal vurderes etter personvernregelverket. Dette gjelder også der behandlingens formål faller innenfor helseforskningslovens virkeområde.

6.4.1 Vurder om prosjektet trenger personopplysninger

Dersom det vil være nødvendig å behandle personopplysninger kreves et lovlig behandlingsgrunnlag, samt oppfyllelse av personvernprinsippene og ivaretakelse av den registrertes rettigheter.

Vanlige vurderingsmomenter:

- Er formålet tydelig og avgrenset?
- Er behandlingsgrunnlag lovlig og i tråd med formålet?
- Er behandlingens art, omfang og sammenhengen den utføres i beskrevet/dokumentert?
- Er kilder, mottakere, informasjonssikkerhet og ansvarsforhold kartlagt og beskrevet?
- Oppfyller behandlingen personvernprinsippene
- Hvilke rettigheter følger av behandlingsgrunnlaget, og finnes det legitime unntak fra enkelte rettigheter?
- Er det utformet informasjon til de registrerte som beskriver formålet med behandlingen og hva det innebærer for dem (inkludert hvilke rettigheter de har)?
- Er behandlingen av personopplysninger nødvendig og proporsjonal?

Eksempel: Et forskningsprosjekt har kommet med en forespørsel om utlevering av journaler i forbindelse med datainnsamlingen. Selv om prosjektet har et klart avgrenset formål, så bes det likevel om journaler i sin helhet. Dette er sjeldent i tråd med samtykket prosjektdeltakerne har gitt og hva REK har godkjent. Opplysningene som innhentes fra journalene må være begrenset til det som er nødvendig for å gjennomføre formålet med forskningsprosjektet og i samsvar med samtykket som er gitt fra forskningsdeltakerne.

6.4.2 Hvem skal gjøre vurderingen?

Hvem som skal foreta vurderingen av om den planlagte behandlingen er tilstrekkelig beskrevet og om den vil kunne gjennomføres i tråd med lovkravene i personvernforordningen vil variere. Dette er det forskningsinstitusjonen/dataansvarlig som avgjør, og det er sannsynligvis beskrevet i virksomhetens interne rutiner hvordan prosjektleder skal gå frem.

Noen virksomheter har fordelt denne oppgaven til en dedikert rolle internt, mens andre har avtale med eksterne til dette.[29]

6.4.3 Involver personvernombudet i virksomheten

Personvernombudet har som hovedoppgaver å gi råd om behandling av personopplysninger, samt kontrollere virksomhetens arbeid. Ombudet er en verdifull ressurs og kan bidra med avklaringer og veiledning til hvordan et forskningsprosjekt bør planlegges og gjennomføres. For ytterligere veiledning om hvordan personvernombudets rolle og fagkompetanse kan brukes, se kapittel 3.

Ta kontakt med eget personvernombud (PVO) eller dataansvarlig for prosjektet og be om en vurdering av det rettslige grunnlaget for behandlingen av opplysningene. Før det gjennomføres behandling av særlige kategorier av personopplysninger til forskningsformål, skal den dataansvarlige rådføre seg med personvernombudet eller en annen som oppfyller vilkårene.[30] I enkelte virksomheter kan det være egne personvernrådgivere som bistår med dette, avhengig av virksomhetens interne rutiner. Personvernombudet vil også sannsynligvis kunne uttale seg om hvorvidt det vil være nødvendig med en personvernkonsekvensvurdering, også kalt DPIA.

6.4.4 Sett deg inn i virksomhetens rutiner for behandling og lagring av personopplysninger

Alle virksomheter som behandler personopplysninger som en del av normal drift, har rutiner for behandling og lagring av ulike typer personopplysninger. Noen virksomheter har egne rutiner som gjelder forskning, mens andre har generelle rutiner som gjelder behandling uavhengig av formålet med behandlingen.

For at virksomheten skal settes i stand til å etterleve regelverket er det avgjørende at forsker setter seg inn i og følger de interne retningslinjene. Slike retningslinjer er normalt utarbeidet på grunnlag av en vurdering av risiko. Dersom prosjektet ikke kan gjennomføres i tråd med de eksisterende retningslinjene i virksomheten, bør forsker kontakte IT-avdelingen/ledelsen for en avklaring av hvordan behandlingen kan gjennomføres på en måte som virksomheten kan akseptere/anser som tilfredsstillende.

6.4.5 Beskriv dataflyt/ eventuelt utform Datahåndteringsplan (DMP)

En beskrivelse av dataflyten inngår i dokumentasjonen og vurderingsgrunnlaget en trenger for å avgjøre om en behandling er lovlig etter personvernforordningen. Ofte kan det være nyttig å illustrere dataflyten i form av et skjema/tegning. Utforming av en Datahåndteringsplan er også et krav fra mange finansiører (blant annet i EU-prosjekter og prosjekter med finansiering fra Norges Forskningsråd).

Dataflyt vil også fremgå av en datahåndteringsplan. En datahåndteringsplan er et godt verktøy for å sikre god planlegging og konkretisering av prosjektopplegget, samt oppgaver og leveranser underveis.

[29] For eksempel NSD/SIKT.

[3030] Jf. personopplysningsloven § 9, 2.ledd.

Fordelen med en illustrasjon av dataflyt eller en datahåndteringsplan, kan være at det er enklere å være konkret med tanke på mulige sårbarheter eller potensielle utfordringer.

6.4.5.1 Databehandlere

Det er kun leverandører/tjenesteytere/samarbeidspartnere som behandler helse- og opplysninger på vegne av virksomheten som regnes som databehandler. Det betyr at man kun er databehandler dersom man har fått en delegert oppgave om å behandle helse- og personopplysninger fra dataansvarlig, og behandling av helse- og personopplysninger må være en del av formålet med avtalen mellom virksomhetene.

Dersom et forskningsprosjekt innebærer at dataanalyse eller annen behandling av forskningsdata skal gjennomføres av en annen virksomhet på prosjektets vegne, vil dette være et databehandlerforhold. Det kreves derfor en databehandleravtale mellom dataansvarlig for prosjektet (forskningsinstitusjonen) og virksomheten som skal behandle opplysningene.

Et annet eksempel som kan være utfordrende er multisenterstudier. Det kan være uklart hvem av samarbeidspartnerne som er ansvarlig i relasjon til prosjekter som involverer databehandlere, som for eksempel kan være leverandør av en skyløsning som benyttes for lagring av forskningsdataene. Dersom de ulike rollene/ansvarsforholdene ikke avklares på et tidlig tidspunkt, kan det medføre at flere partnere foretar de vurderingene som er pålagt dataansvarlig, uten at det er nødvendig. Det er derfor viktig å avklare ansvarsforholdene før behandlingen av helse- og personopplysninger begynner.

Hvis man benytter databehandlere, er det viktig at disse selv bidrar med informasjon om blant annet personopplysningsvern/informasjonssikkerhet ivaretas, eventuelt hvordan de etterlever de kravene som dataansvarlig stiller i databehandleravtalen.

For mer informasjon om databehandlere og databehandleravtaler, se Normens faktaark 10.

6.4.5.2 Overføring av helse- og personopplysninger utenfor EU/EØS

All overføring av helse- og personopplysninger ut av EU/EØS (omtales også som overføring til tredjeland) krever et særskilt grunnlag for å være lovlig. Med overføring menes ikke bare at data føres ut av EU/EØS, men også enhver tilgang til opplysningene fra land utenfor. Det betyr for eksempel at dersom en amerikansk leverandør av en skytjeneste har tilgang til opplysninger som ligger på deres datasentre i EU, så regnes det som en overføring etter personvernforordningen.

For at overføring av helse- og personopplysninger til tredjeland skal være lovlig, så må virksomheten benytte et gyldig overføringsgrunnlag i personvernforordningen art. 46. Det mest vanlige er standard personvernbestemmelser (Standard Contractual Clauses eller SCC). Ved bruk av SCC forplikter databehandler seg til å behandle helse- og personopplysninger i samsvar med personvernforordningen.

Det er viktig å vurdere om overføringsgrunnlaget faktisk vil ha en effekt på beskyttelsen av personopplysninger. I noen tilfeller er det ikke tilstrekkelig å ha et overføringsgrunnlag, og det vil være nødvendig å vurdere beskyttelsesnivået for helse og personopplysninger i tredjelandet det er aktuelt å overføre opplysninger til. Dette innebærer at virksomheten må undersøke tredjelandets nasjonale lovgivning og vurdere hvilken reell beskyttelse helse- og personopplysningene har. Det vil for eksempel være aktuelt å undersøke om tredjelandet har lovgiving som åpner for utlevering av informasjon til nasjonale myndigheter eller etterretning.

Standard personvernbestemmelser vil ikke være bindende for tredjelandets myndigheter og nasjonal lovgiving kan derfor gå foran disse.

Dersom man kommer frem til at beskyttelsesnivået er lavere enn i EU, må det iverksettes ytterligere tiltak, utover de tiltakene som er iverksatt ved valg av overføringsgrunnlag. Dersom det er nødvendig med ytterligere tiltak, men slike tiltak ikke iverksettes, er overføringen ulovlig og må opphøre.

For mer informasjon om overføring til tredjeland og hvilke vurderinger som må gjennomføres ved overføring til tredjeland, se Datasynets veileder for oppdatert informasjon. EDPBs anbefalinger om ytterligere tiltak inneholder mer informasjon om vurderingen av beskyttelsesnivået, samt mulige informasjonskilder.[31]

6.5 Innhent andre nødvendige godkjenninger avhengig av type prosjekt og formål

Vær nøye med å legge frem prosjektet på samme måte overfor de ulike godkjennings/vurderingsinstansene.

Fordi ulike vurderingsinstanser har et avgrenset mandat/skal gjøre en avgrenset vurdering, vil det være avgjørende at behandlingen beskrives likt overfor de ulike instansene.

Eksempel: Et forskningsprosjekt som skal få utlevert helseopplysninger fra et sentralt helseregister, legger prosjektet frem for både REK, dispenserende myndighet, registereier og den som skal vurdere behandlingen etter personvernforordningen.

REK gjøre en forskningsetisk medisinsk vurdering og vurderer behovet for en dispensasjon fra taushetsplikten for utlevering av opplysninger fra registeret.

Registereier vurderer søknad om data fra registeret, inkludert utformer en avtale som sier noe om hvordan opplysningene skal behandles ved prosjektslutt.

Den som vurderer personvernet, tar stilling til nødvendig behandlingsgrunnlag og sikring av opplysningene underveis i prosjektet.

Dersom forsker har beskrevet behandlingen likt overfor disse instansene, vil man kunne være sikker på at alle nødvendige vurderinger er gjort. Dersom man derimot har presentert ulike variabellister eller beskrevet dataflyten på en ikke konsistent måte, vil sjansen være stor for at vurderingene ikke dekker alle nødvendigheter. Se for deg at variabellisten ovenfor REK er mer detaljert enn den som legges frem for den som vurderer personvernet. Vurderingen av personvernet slår fast at det ikke skal behandles detaljerte opplysninger som vil kunne være indirekte identifiserbare for forsker. Man betrakter risikoen for den registrertes rettigheter og friheter som lav. I realiteten har forsker kanskje søkt REK om dispensasjon fra taushetsplikten på grunnlag av en variabelliste som viser at forsker ber om å få utlevert svært identifiserende helseopplysninger. Konsekvensen kan være at det ikke gjøres en påkrevet personvernkonsekvensvurdering (DPIA) eller at sikkerheten ikke er ivaretatt i tilstrekkelig grad. Dette kan få konsekvenser både for den registrerte, for virksomheten og for forsker.

[31] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Hvem er dispenserende myndighet?		
Dispenserende myndighet	Prosjekttype/type dispensasjon	Kreves det tilleggsgodkjenning fra andre instanser?
REK	Medisinske og helsefaglige forskningsprosjekter	
	Utprøvende behandling med annet primært formål enn å gi helsehjelp til en enkelt pasient	
	Generelle forskningsbiobanker	
	Dispensasjon fra taushetsplikt med hjemmel i forvaltningsloven §13 d og helsepersonelloven § 29, 1. ledd, for forskningsformål. Dispensasjon fra taushetsplikt med hjemmel i helseregisterloven § 19e	
	Bruk og utlevering av personidentifiserbare opplysninger og indirekte identifiserbare opplysninger fra ett eller flere (koblete) sentrale/lovbestemte helseregistre Utlevering av humant biologisk materiale til utlandet, jf. helseforskningsloven § 29	
	Klinisk utprøving av medisinsk og annet utstyr	Krever også godkjenning fra Statens legemiddelverk
	Klinisk utprøving av legemidler	Krever også godkjenning fra Statens legemiddelverk dersom hensikten er å undersøke eller etterprøve kunnskap om legemidlenes • effekter eller påvirkning av fysiologisk funksjon • interaksjoner • bivirkninger • opptak, fordeling, metabolisme og utskillelse

		• terapeutiske verdi
Helsedirektoratet	Dispensasjon fra taushetsplikten for å innhente og behandle opplysninger blant annet på tvers av virksomheter, dersom formålet blant annet er statistikk, helseanalyser, utvikling og bruk av klinisk beslutningsstøtteverktøy, kvalitetsforbedring, planlegging, styring eller beredskap, jf. helsepersonelloven § 29.	
Eget helseforetak (Det er ikke tale om en dispensasjon, men må vurderes av dataansvarlig selv.)	Intern kvalitetssikring, jf. helsepersonelloven § 26 og pasientjournalloven § 6.	
	Opprettelse av medisinske kvalitetsregistre, jf. forskrift om medisinske kvalitetsregistre.	

6.5.1 Helseforskning/REK

Vurderingen til REK er en medisinsk-etisk vurdering og behandlingen av personopplysninger også krever en vurdering etter personvernforordningen. Tidligere ga godkjenning fra REK også behandlingsgrunnlag for behandlingen av helse- og personopplysninger, men etter innføringen av personvernforordningen er det dataansvarlig som må identifisere rett behandlingsgrunnlag.

Prosjektleder/ansvarshavende skal søke om forhåndsgodkjenning av:

- Medisinske og helsefaglige forskningsprosjekter
- Generelle forskningsbiobanker
- Dispensasjon fra taushetsplikt med hjemmel i forvaltningsloven § 13d og helsepersonelloven § 29 1.ledd, for annen type forskning
- Klinisk utprøving av medisinsk og annet utstyr
- Utlevering av humant biologisk materiale til utlandet
- Bruk av registerdata (helseregistre)

Ved søknad til REK om godkjenning av forskningsprosjektet vil prosjektleder være ansvarlig for å sannsynliggjøre at studiens nytteverdi og kvalitet og forskernes kompetanse er så høy at det er forsvarlig å gjennomføre studien.

6.5.1.1 Prosjekter som ikke er fremleggingspliktige for REK

Dersom forskningen ikke har til hensikt å frembringe ny kunnskap om helse og sykdom skal ikke prosjektet legges frem for REK for godkjenning/medisinsk etisk vurdering.

Dersom det er usikkerhet om hvorvidt prosjektet er fremleggelsespliktig for REK, kan prosjektleder sende inn en fremleggelsesvurdering, som gir REK grunnlag for videre veiledning om prosjekttype. Fremleggingsvurderinger vurderes fortløpende av REK, utenom de faste komitemøtene.

Dersom prosjektet skal behandle helse- og personopplysninger, skal prosjektet vurderes etter personvernforordningen og personopplysningsloven. Dette kan for eksempel være helsetjenesteforskning, der man skal forske på selve helse- og omsorgstjenesten med vitenskapelig metode og det innhentes helseopplysninger. Det kan være forskning på hvordan helsepersonell kommuniserer med pasienter, prioriteringer osv.

6.5.2 Intern kvalitetssikring

Dataansvarlig må selv påse at det gjøres en vurdering etter personvernforordningen og at behandlingsgrunnlag kan fastsettes.

6.5.3 Kvalitetssikring/kvalitetsforbedring på tvers av helseforetak

Ved kvalitetssikring på tvers av helseforetak skal det søkes Helsedirektoratet om dispensasjon fra taushetsplikten. Virksomhet sørger for vurdering etter personvernforordningen.

6.5.4 Forskning på biologisk materiale

Prosjektet legges frem for REK. Ved behandling av personopplysninger må virksomheten sørge for vurdering etter personvernforordningen.

6.5.5 Klinisk utprøving av medisinsk eller annet utstyr

En ny EU-forordning for utprøving av medisinsk utstyr trådte i kraft 26. mai 2021. Prosjekter som faller innenfor lovens saklige virkeområde, skal legges frem for REK for en forskningsetisk vurdering. Statens legemiddelverk (SLV) er fag- og tilsynsmyndighet for medisinsk utstyr, og en uttalelse fra SLV kan innhentes vedrørende om prosjektet faller innenfor den nye EU-forordningen for utprøving av medisinsk utstyr (Medical Device Regulation (MDR) 2017/745).

Kliniske utprøvinger av medisinsk utstyr kan være søknads- eller meldepliktig til SLV. Sørg for å undersøke dette tidlig i planleggingen av prosjektet. For mer informasjon, se SLV sin nettside.

Dersom det behandles personopplysninger i forbindelse med prosjektet, må dataansvarlig i tillegg sørge for en vurdering etter personvernforordningen (GDPR)

6.5.6 Legemiddelutprøving

Kliniske utprøvinger av legemidler må godkjennes av Legemiddelverket før de kan gjennomføres. Det er innført et mer eller mindre felles regelverk for Europa, med formål å

sikre forsøkspersonenes rettigheter og sikkerhet. De samme kravene gjelder for alle studier, uavhengig av om studien gjennomføres av legemiddelindustrien eller forskere ved en forskningsinstitusjon.

Klinisk utprøving av legemidler innebærer en plikt til å ha beredskap for uønskede hendelser som kan påvirke pasientsikkerheten/sikkerheten til deltakerne. Det er derfor nødvendig å registrere og oppbevare personidentifiserende opplysninger om deltakeren i hele prosjektperioden og i 15 år etter prosjektslutt. Slike prosjekter innebærer derfor alltid en behandling av personopplysninger og dataansvarlig virksomhet må vurdere og dokumentere etterlevelse av personvernforordningens bestemmelser.

6.5.7 Forskning på registeropplysninger

Et forskningsprosjekt som skal innhente og behandle personopplysninger fra et eller flere helseregistre, vil som regel ikke ha direkte kontakt med de registrerte. Utlevering av opplysningene fra registereier krever dispensasjon fra taushetsplikten. Det første som bør avklares er imidlertid hvorvidt formålet med behandlingen av helse- og personopplysninger faller innenfor helseforskningslovens virkeområde. Dersom REK slår fast at prosjektet regnes som helseforskning, vil som regel REK samtidig ta stilling til og avgjøre om dispensasjon kan innvilges.

For dispensasjon fra taushetsplikten for utlevering fra registre som SSB forvalter, søkes det direkte til SSB som også er dispenserende myndighet for disse registrene.

All behandling av personopplysninger i helseregistre skal vurderes etter personvernforordningen. Merk at for medisinske kvalitetsregistre kan helseopplysninger samles inn og behandles uten den registrertes samtykke på bestemte vilkår, jf. forskrift om medisinske kvalitetsregistre § 3-2. Vær også oppmerksom på at noen registereiere/registerforvaltere kan kreve at det er gjennomført en personvernkonsekvensvurdering etter personvernforordningens artikkel 35 før de foretar en vurdering av hvorvidt personopplysninger fra registeret kan utleveres, da behandlingen vil innebære en høy risiko for de registrertes rettigheter og friheter.

6.5.8 Opprettelse av register for konkret forskningsformål

Dersom det skal opprettes et register i forbindelse med/for å oppfylle et konkret forskningsformål, og formålet faller innenfor helseforskningslovens virkeområde, skal prosjektet legges frem for REK for vurdering.

Selve etableringen av et medisinsk kvalitetsregister faller utenfor helseforskningslovens virkeområde og skal ikke godkjennes av REK. Opprettelsen skal vurderes av dataansvarlig selv etter forskrift om medisinske kvalitetsregistre. Det skal sendes søknad til REK når opplysninger fra disse prosjektene skal behandles i forbindelse med forskning.

Dataansvarlig skal sørge for en vurdering av behandlingen av personopplysninger etter personvernforordningen.

6.5.9 Opprettelse av register (permanent eller langvarig) til andre og udefinerte forskningsformål

Dersom det skal opprettes et register (med særlige kategorier personopplysninger) som skal brukes til fremtidige og ikke definerte forskningsformål, innebærer dette som regel at behandlingen vil pågå over lang tid, eller kanskje regnes som et permanent register. Slike behandlingsformål vil sannsynligvis innebære en høy risiko for de registrertes rettigheter og friheter, og en personvernkonsekvensvurdering (DPIA) etter personvernforordningens artikkel 35 vil være nødvendig.[32]

7 Gjennomføringsfasen

7.1 Alltid i tråd med prosjektbeskrivelse, godkjenninger og vurderinger

Gjennomføringen av et forskningsprosjekt skjer ikke alltid helt etter planen. Overraskende funn, utfordringer knyttet til datainnsamlingen, endret ressurssituasjon eller behovet for ytterligere data/mer omfattende datagrunnlag, er bare noe av det som kan avdekkes i løpet av gjennomføringen. Resultatet er ofte at det må gjøres endringer i prosjektopplegget.

7.2 Endringer underveis i prosjektet

Ved behov for å gjøre endringer i gjennomføringen er det viktig å huske at alle godkjenninger eller vurderinger, samtykker etc. er basert på den opprinnelige beskrivelsen av hvordan behandlingen skulle gjennomføres. Ved vesentlige endringer vil det derfor være nødvendig med nye vurderinger.

Noen vanlige endringer som kan ha en påvirkning på personvernet, informasjonssikkerheten eller rettighetene og friheten til de registrerte, kan være f. eks:

- Utsettelse av prosjektslutt/forlengelse av behandlingen
- Nye/flere prosjektmedarbeidere
- Nye datainnsamlinger
- Nye utvalg
- Endringer i tekniske løsninger som benyttes
- Endring i rekrutteringsmetode
- Nye typer personopplysninger / flere variabler, mer detaljerte data enn planlagt

For helseforskningsprosjekter vil blant annet følgende endringer utløse behovet for godkjenning fra REK:

[32] Se eget kapittel om personvernkonsekvensvurdering

- Endringer i design og analyse
- Ny kunnskap om risiko, ulempe og/eller nytte for forskningsdeltakerne og/eller andre
- Endring av prosjektleder, forskningsansvarlig(e), ansvarshavende for forskningsbiobank eller prosjektmedarbeider
- Utsettelse eller forlengelse av prosjektperioden
- Økning i antall forskningsdeltaker
- Endring i rekrutteringsprosedyre
- Endring i inklusjons og eksklusjonskriterier.
- Innholdsmessig endring av forespørsel om deltakelse (informasjonsskriv)
- Endringer i gitte vilkår for dispensasjon fra taushetsplikt (f.eks. hvem som skal ha tilgang til personidentifiserbare opplysninger)
- Endring av oppbevaring og behandling av helseopplysninger eller biologisk materiale

Dersom det er uklart hvorvidt en endring er av vesentlig karakter, bør forsker rådføre seg med personvernombudet eller annen person med tilsvarende kompetanse. Alternativt be om en uttalelse fra de aktuelle vurderingsinstansene.

7.2.1 Vurderinger må alltid gjøres før endringen gjennomføres

Be om ny vurdering før endringen gjennomføres. Avvent alltid tilbakemelding/svar på søknad om endring. Det er ikke tilstrekkelig å dokumentere at ny søknad er sendt inn.

7.2.2 Den registrertes perspektiv – endringer innebærer ofte vilkår

Endringer i gjennomføringen av behandlingen av personopplysninger kan for eksempel innebære at tidligere innhentet samtykke ikke vil være dekkende for den nye behandlingen/endringen. Dersom dette er tilfellet, vil et vilkår for endringen kunne være at det gis ny informasjon. Dersom endringen er igangsatt før dette er vurdert, vil videre behandling ikke ha et lovlig behandlingsgrunnlag.

Den registrertes perspektiv er igjen styrende og verdifullt i en vurdering av hvorvidt endringen i vesentlig grad også innebærer en endring personvernet til den registrerte.

Innebærer endringen at behandlingen ikke lenger er like forutsigbar, oversiktlig og eller rettferdig?

Bruk personvernprinsippene som rettesnor i denne vurderingen.

8 Avslutningsfasen

Dette kapittelet omhandler aktivitetene publisering og arkivering, som typisk skjer i avslutningsfasen av et forskningsprosjekt.

Deling og anonymisering er omtalt i egne kapitler, men vil også være relevante aktiviteter i avslutningen av et prosjekt.

Når prosjektet er avsluttet, skal prosjektleder sende sluttmelding på eget skjema til REK senest seks måneder etter at godkjenningsperioden er utløpt, jf. Helseforskningsloven § 12. Dersom prosjektet ikke igangsettes eller gjennomføres skal prosjektleder også sende melding om dette via sluttmeldingsskjemaet.

I tillegg skal studien registreres som avsluttet hos andre steder den er registrert, for eksempel helsenorge.no.

Det er viktig å ha lagt til rette for disse aktivitetene i avslutningsfasen allerede i planleggingsfasen av prosjektet. For eksempel vil gjenbruk av og publisering av ikke-anonyme data kreve at virksomheten har et behandlingsgrunnlag. Dersom behandlingsgrunnlaget er basert på samtykke fra forskningsdeltakere, må slik viderebehandling være dekket av samtykket som er blitt gitt til prosjektet, eventuelt må samtykke innhentes. Samtykket bør være basert på god informasjon til forskningsdeltaker om hva publiseringen innebærer og hvordan eventuell deling av data skal skje, og for hvilke formål.

8.1 Publisering

Publisering i denne veilederen innebærer offentliggjøring, utgivelse eller kunngjøring.

Utgangspunktet for all forskning er at det foreligger en plikt til å publisere forskningsresultatene, uavhengig av forskningens resultat. Plikten til å publisere er begrunnet i forskerens akademiske frihet, forskningens samfunnsnytte og rettigheter for forsker og forskningsinstitusjon. Ny kunnskap om helse av betydning for samfunnet skal deles og være tilgjengelig av hensyn til etterprøvbarhet. Personvernhensyn tilsier at forskningsresultater ikke kan publiseres helt fritt, og det finnes krav i lovgivingen til hvordan forskningsdata skal publiseres. Graden av åpenhet vil være avhengig av hva slags data det er snakk om, hvem som får tilgang og på hvilke vilkår.

Forskning regnes som akademiske ytringer og har et særskilt vern etter personopplysningsloven § 3. Ved publisering av forskning må det gjøres en avveining mellom samfunnsnytten til forskningen og personvernet til forskningsdeltakerne.

Prosjektleder må ta stilling til publisering allerede i planleggingsfasen, og legge til rette for dette i en datahåndteringsplan eller lignende. For helseforskningsprosjekter vil REK i sitt vedtak kunne legge føringer eller stille krav for publisering av forskningsresultatene, for eksempel at opplysningene skal fremstå som anonyme.

Publisering av forskning som inneholder helse- og personopplysninger er en behandling av personopplysninger som krever behandlingsgrunnlag etter personvernforordningen. Ofte vil behandlingsgrunnlaget være samtykke fra forskningsdeltaker. Dersom det planlegges å publisere anonyme forskningsdata, må samtykket spesifisere dette. Samtykket bør også

informere om hvilke type data man planlegger å publisere og at det kan være en risiko for identifisering. Tilgjengeliggjøring av data for redaktører og fagfeller før publisering i vitenskapelige tidsskrift krever ikke spesifikt samtykke.[33]

I vurderingen av om hvilke data som skal publiseres og i hvilken form, bør blant annet følgende vurderes:

- Skal det publiseres pseudonyme eller anonyme data? Hvis pseudonyme, hvor store er risikoen for bakveisidentifisering av den enkelte? Her vil det være aktuelt å vurdere typen data, størrelsen på studien og utvalget, og det foreligger offentlige tilgjengelige opplysninger om utvalget, om det omtales lett gjenkjennelige ytre tegn
- Bør man bruke aggregerte data (anonyme opplysninger)?
- Kan det innhentes samtykke fra forskningsdeltakeren?
- Hvilken form skal dataene publiseres i, for eksempel tabeller og figurer?
- Hvor mye data er det nødvendig å publisere for å dokumentere resultatet av forskningen?

8.2 Arkivering

Helse- og personopplysninger som inngår i et forskningsprosjekt skal ikke oppbevares lengre enn det som er nødvendig for å gjennomføre prosjektet, jf. helseforskningsloven § 38. Langtidsarkivering av data utover prosjektets varighet forutsetter behandlingsgrunnlag, for eksempel REK-godkjenning eller samtykke. For enkelte typer forskningsprosjekter vil behandlingsgrunnlaget være basert på krav i nasjonal lovgiving. Ved klinisk utprøving av legemidler skal både sponsor og utprøver oppbevare dokumenter av vesentlig betydning for den kliniske utprøvingen i minst femten år etter at forsøket er avsluttet.[34]

REK kan bestemme at dokumenter som er nødvendige for etterkontroll av prosjektet, skal oppbevares i fem år eller mer etter at sluttmelding er sendt. Dersom dokumenter skal lagres i mer enn fem år, kan REK stille vilkår knyttet til lagringen.

Med mindre opplysninger ikke skal oppbevares videre i henhold til arkivloven eller annen lovgiving, skal opplysningene deretter anonymiseres eller slettes. Eventuelt skal data leveres tilbake til dataeier.

Arkivering av data har ofte som hensyn å sikre etterprøvbarhet av data, analyser og forskningsresultatet. Ved arkiveringen må det derfor sørges for at data arkiveres på et format som er tilgjengelig lesbart frem i tid.

[33] Rundskriv om informasjonshåndtering i spesialisthelsetjenesten.
[34] Forskrift om klinisk utprøving av legemidler til mennesker § 8-2.

9 Vedlegg: Eksempel på utfylt personvernkonsekvensvurdering

Dette vil bli publisert i en oppdatert versjon av veilederen, når Direktoratet for e-helses mal er publisert.

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no