Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren

Veilederen er et støttedokument til Norm for informasjonssikkerhet

Utgitt med støtte av:

Helsedirektoratet

Versjon 1.2

www.normen.no

Merknad 24.03.2019: Dokumentet er ikke oppdatert fra siste versjon av Normen (5.3), ny personopplysningslov, endringer i helselovgivningen, eller EUs personvernforordning

INNHOLD

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for Normen (dato)
1.0	Første utgave av veilederen	Februar 2010
1.1	Oppdatering av terminologi og referanser	Sekretariatet Jan. 2011
1.2	Oppdatert referanser i definisjon "taushetsplikt"	Sekretariatet 6.jun 2013

1 INNLEDNING

1.1 Bakgrunn

Forskningsprosjekter i helse- og omsorgssektoren medfører bruk av *helse- og personopplysninger* som krever at personvern og informasjonssikkerhet blir ivaretatt på en tilfredsstillende måte. Bakgrunnen for en egen veileder for personvern og informasjonssikkerhet er å gi råd for å ivareta krav til administrative og tekniske løsninger.

Veilederen er et bidrag til prosjektene slik at ansvarlige i institusjonene enkelt kan sette seg inn i gjeldende krav.

Veilederen er ikke en generell veileder i gjennomføring av forskningsprosjekter.

Veilederen bygger på den nye helseforskningsloven med forskrifter. Målsettingen er å forenkle regelverket og formaliteter, samtidig som hensynet til personvern og informasjonssikkerhet ivaretas.

Viktige endringer vedrørende personvern og informasjonssikkerhet i forhold til tidligere lovgivning er at:
- Alle forskningsprosjekter krever forhåndsgodkjenning fra de Regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK)
- Alle forskningsprosjekter skal ha *forskningsansvarlig* og egen *prosjektleder*
- Alle forskningsprosjekter skal meldes til REK når de er avsluttet

1.2 Formålet med veilederen

Veilederen skal være til hjelp for å etablere tilfredsstillende informasjonssikkerhet i forskningsprosjekter.

1.3 Om veilederen

Veilederen er utarbeidet for styringsgruppen for Norm for informasjonssikkerhet (Normen) med støtte fra Helsedirektoratet av selskapene Advokatfirmaet Wiegaard, INCERTUS og INFOSEC.

Veilederen er utarbeidet i samarbeid med representanter fra sektoren (se kap. 5.4).

Veilederen bør leses i sin helhet ettersom de samlede krav og anbefalinger er dokumentert i flere kapitler.

Veilederen er utarbeidet som et støttedokument til Normen. Veilederen inneholder referanse til faktaark i Normen som er relevante for forskningsprosjekter (se kap. 4). *Virksomheter* tilknyttet *helsenettet* er gjennom tilknytningsavtalen forpliktet til å følge Normen.

Veilederen gjelder medisinsk og helsefaglig forskning på:

- *helse- og personopplysninger* om enkeltindivider (kvantitative og kvalitative studier)
- humant biologisk materiale (*forskningsbiobank*)

Ved forskning på direkte identifiserbare *helse- og personopplysninger* gjelder Normen i tillegg, se også figur i kapittel 3.2.2. Forskning på *anonymiserte* data er ikke underlagt krav til informasjonssikkerhet og er følgelig ikke behandlet i veilederen.

Medisinsk og helsefaglig forskning kan deles inn i flere undergrupper, f.eks.:
- Grunnforskning og anvendt forskning
- Fri forskning og oppdragsforskning
- Nasjonale og internasjonale forskningsprosjekter

Regelverkets krav til personvern, informasjonssikkerhet, søknads r og prosedyrekrav i denne forbindelse, vil gjøre seg gjeldende uavhengig av slike kategoriseringer.

Det er *prosjektleders* ansvar å påse at personvern og informasjonssikkerhet er ivaretatt i forskningsprosjektet.

Veilederen er et dynamisk dokument og vil oppdateres i samsvar med utvikling i regelverket.

1.4 Målgruppe og hvilken hjelp veilederen gir

Målgruppen for veilederen er *prosjektleder* for forskningsprosjektet.

Andre brukere av veilederen er:
- Sikkerhetsansvarlig
- *Forskningsansvarlig*
- REK
- *Personvernombud*
- Forsker

Veilederen angir krav til informasjonssikkerhet før oppstart, under gjennomføring og ved avslutning av forskningsprosjektet. Informasjonssikkerheten må ivaretas i alle fasene.

I tillegg til veilederen er det utarbeidet et faktaark som skal være en bro mellom denne veilederen og den enkelte forsker (se Faktaark 40 – Informasjonssikkerhet i forskningsprosjekter).

1.5 Definisjoner

Definisjoner er hentet fra Normen. Nye begrep er definert og samlet etter definisjoner fra Normen.

Definerte ord er markert med *kursiv* i teksten.

Definisjoner fra Normen (av 2. juni 2010)

Med "***anonymisert***" menes i Normen *helse- og personopplysninger* der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson (jf. helseregisterloven § 2 nr 3.). Opplysninger om en person regnes som *anonymisert* dersom identifiseringen krever uforholdsmessig stor arbeidsinnsats eller uforholdsmessige store kostnader.

Med "***autentisering***" menes i Normen prosessen som gjennomføres for å bekrefte en påstått identitet.

Med "***autorisere/autorisert/autorisasjon***" menes i Normen at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, retting, sletting og/eller sperring av *helse- og personopplysninger*. *Autorisasjon* kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra *tjenstlig behov* og er i henhold til bestemmelser om *taushetsplikt*.

Med "***avidentifisert***" menes i Normen *helse- og personopplysninger* der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet (jf. helseregisterloven § 2 nr. 2). For å regnes som *avidentifiserte*, skal dataene være bearbeidet slik at de uten løpenummer fremstår som anonyme.

Avidentifiserte data er *anonyme* hvis filen med *koblingsnøkler* er fjernet.
Det må vurderes i hvert enkelt tilfelle om opplysningene er *avidentifiserte* eller ikke.

Som en "tommelfingerregel" kan et datasett anses som *avidentifisert* selv om følgende felter er inkludert i datasettet:

- Adressedata
  - bo- og fødestedsfylke
  - fødeland/etnisitet (ved små grupper skal grupper slås sammen)
  - adresseinformasjon i form av sammenslåinger (av kommuner, bydeler el.)
- Beregnede tidsintervaller, f.eks.:
  - svangerskapslengde
  - alder
  - observasjonstid
- Grupperte yrkesopplysninger
- Institusjonens (sykehus, skole e.l.) størrelse angitt i størrelsesgrupper
- *Koblingsnøkkel* som er unikt for hvert prosjekt

Dette vil imidlertid ikke alltid gjelde dersom pasienten har en meget sjelden sykdom/diagnose og/eller forskeren har egne data, som kan kobles på de *forskningsdata* som utleveres.

Med "***avvik***" menes i Normen enhver håndtering av *helse- og personopplysninger* som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd.

Med "***behandling***" menes i Normen enhver formålsbestemt bruk av *helse- og personopplysninger*, som f.eks. innsamling, registrering, sammenstilling, lagring og

utlevering eller en kombinasjon av slike bruksmåter, jf. helseregisterloven § 2 nr. 5 og personopplysningsloven § 2 nr. 2).

Med "***databehandler***" menes den som *behandler helse- og personopplysninger* på vegne av den *databehandlingsansvarlige*, jf. helseregisterloven § 2 nr. 9 og personopplysningsloven § 2 nr. 5). Det presiseres at en *databehandler* er en ekstern person eller *virksomhet* utenfor den *databehandlingsansvarliges virksomhet*. Det vil si at den *databehandlingsansvarliges* egne medarbeidere ikke er dennes *databehandlere*.

Med "***databehandlingsansvarlig***" menes den som bestemmer formålet med *behandlingen* og hvilke hjelpemidler som skal brukes, hvis ikke *databehandlingsansvaret* er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 nr. 8 og personopplysningsloven § 2 nr. 4) (her benyttes begrepet "behandlingsansvarlig"). Det presiseres at det er *virksomheten* som er *databehandlingsansvarlig* for *behandling* av *helse- og personopplysninger.* Ansvaret skal ivaretas av den daglige ledelsen av *virksomheten*, og *virksomheten* er pliktsubjekt.

*"**helse- og personopplysninger**"* benyttes i Normen som en fellesbetegnelse for *helseopplysninger* og/eller *personopplysninger* innenfor Normens virkeområde.

Med "***helsenettet***" menes nettverket som tilbys av Norsk Helsenett SF.

*Med "**helseopplysninger**" menes i* Normen *taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson, jf. helseregisterloven § 2 nr. 1*.

Med "***hendelsesregistrering***" menes i Normen registrering av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

Med "***integritet***" menes i Normen at *helse- og personopplysninger* må være sikret mot utilsiktet eller *uautorisert* endring eller sletting.

Med *"**internkontroll**"* menes i Normen 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.

Med "***konfidensialitet***" menes i Normen at *helse- og personopplysninger* må være sikret mot at uvedkommende får kjennskap til opplysningene.

Med "***konfigurasjon***" menes i Normen informasjonssystemets utforming inklusive både teknisk utstyr og programvare.

Med "***konfigurasjonsendring***" menes i Normen en endring av informasjonssystemets utforming som følge av installasjon, oppgradering eller fjerning av utstyr eller programvare.

Med "***kvalitet***" menes i Normen at *helse- og personopplysninger* må være korrekte, oppdaterte, samt relevante og tilstrekkelige som grunnlag for å yte helsehjelp.

Med "***personopplysninger***" menes opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1.

Med "***personvernombud***" menes i Normen en formelt oppnevnt kontakt for personvern og informasjonssikkerhet internt mot *databehandlingsansvarlig* (*virksomhetens* ledelse) og ansatte og eksternt mot Datatilsynet og *den registrerte* (*pasienter*, inkluderte i studier og egne ansatte).

Med "***pseudonymisering***" menes i Normen prosessen der identiteten til *helse- og personopplysninger* skjules, men likevel slik at helseopplysningene er individualisert og det lar seg gjøre å følge hver person gjennom behandling av *helse- og personopplysninger* uten at identiteten røpes (jf. helseregisterloven § 2 nr. 4).

Med "***register***" menes i Normen en logisk sammenstilling av opplysninger. En database eller et regneark er en teknisk løsning for et *register*.

Med "***sikkerhetsnivå 4***" menes i Normen to-faktor *autentisering* hvor en faktor er dynamisk basert på kvalifiserte sertifikater og ellers tilfredsstiller kravene til sikkerhetsnivå 4 i "Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor".

Med "***taushetsplikt***" menes i Normen lovpålagt eller avtalt plikt til å hindre at andre får adgang eller kjennskap til *helse- og personopplysninger*, jf. helsepersonelloven § 21, helseregisterloven § 15, helse- og omsorgstjenesteloven § 12-1 og forvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften § 2-9. *Taushetsplikt* innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

Med "***tekniske tiltak***" menes i Normen tiltak av teknisk karakter som ikke kan påvirkes eller omgås av medarbeidere, og ikke er begrenset av handlinger som den enkelte forutsettes å utføre. Eksempler på slike tiltak kan være *autentisering* på *sikkerhetsnivå 4* eller *konfigurering* av en brannmur slik at den kun tillater bestemt trafikk eller en meldingstjeneste som er laget slik at alle meldinger automatisk blir kryptert.

Med "***tilgang***" menes i Normen at *helse- og personopplysninger* om en eller flere bestemte *pasienter/brukere* er eller gjøres tilgjengelige for *autorisert* personell. Beslutning om *tilgang* til *behandlingsrettede helseregistre* skal treffes etter en konkret vurdering basert på at det ytes helsehjelp til *pasienten. Tilgang* til *fagsystemer* i forbindelse med ytelser til *pasient/bruker* skal iverksettes basert på *tjenstlig behov*. *Tilgang* i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra *tjenstlig behov*.

Med "***tilgjengelighet***" menes i Normen at *helse- og personopplysninger* som skal *behandles*, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Med "***virksomhet***" menes i Normen juridisk enhet som helseforetak, *kommune*, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse m.v.

Nye definisjoner i denne veilederen

Med "***forskningsansvarlig***" menes institusjon eller en annen juridisk eller fysisk person som har det overordnede ansvaret for forskningsprosjektet, og som har de nødvendige forutsetningene for å kunne oppfylle den *forskningsansvarliges* plikter.

Med "***forskningsbiobank***" menes en samling humant biologisk materiale og opplysninger som direkte fremkommer ved analyse av dette materialet, og som anvendes eller skal anvendes til forskning (se behandlingsbiobankloven § 2).

Med "***forskningsdata***" menes *helse- og personopplysninger* om, eller humant biologisk materiale fra, en *forskningsdeltager* som skal inngå i forskning.

Med "***forskningsdeltager***" menes det enkeltindivid (den personen) hvis opplysninger det forskes på.

Med "***forskningsfil***" menes et uttrekk av *helse- og personopplysninger* som skal benyttes i et forskningsprosjekt. *Helse- og personopplysningen* i *forskningsfilen* er vanligvis ikke direkte identifiserbar. *Forskningsfilen* kan bestå av personidentifiserbare, *pseudonymiserte, avidentifiserte* eller *anonyme helse- og personopplysninger*.

Med "***forskningsresultat***" menes det endelige resultatet av forskningsprosjektet som gjøres åpent tilgjengelig for allmennheten.

Med "***forskningstilgang"*** menes at *forskningsdata* eller *forskningsfil* gjøres tilgjengelige for *autorisert* personell.

Med "***koblingsnøkkel***" menes en annen personentydig kode som refererer til de identifiserende opplysningene som gjør det mulig å identifisere et enkeltindivid i en *avidentifisert* fil.

Med "***multisenterstudie***" menes et forskningsprosjekt der flere *virksomheter* er involvert i selve forskningen, og hver *virksomhet* har egen *prosjektleder*.

Med "***nøkkelfil***" menes et *register* over *koblingsnøkler*.

Med "***PKI/Public Key Infrastructure***" menes en teknologi for utstedelse, administrasjon og bruk av digitale sertifikater over datanett. Anvendelsesområder for *PKI* er *autentisering* (legitimering av en person, organisasjon eller gjenstands identitet), digital signatur (av dokumenter eller programvare) og verifisering av dataintegritet.

Med "***prosjektleder***" menes en fysisk person med ansvar for den daglige driften av forskningsprosjektet, og som har de nødvendige forskningskvalifikasjonene og erfaringer for å kunne oppfylle *prosjektlederens* plikter.

2 PRINSIPPER FOR FORSKNING OG RETTSLIG UTGANGSPUNKT

Medisinsk og helsefaglig forskning er i helseforskningsloven § 4 definert som "*virksomhet som utføres med vitenskapelig metodikk for å skaffe til veie ny kunnskap om helse og sykdom*." Siktemålet med forskningen er økt kunnskap, bedre diagnostikk og bedre pasientbehandling. Norske sykehus har etter spesialisthelsetjenesteloven plikt til å drive forskning.

2.1 Regler for personvern og informasjonssikkerhet

Forskning på *personopplysninger*, herunder *helseopplysninger*, krever normalt samtykke fra personer det forskes på. Samtykke vil da være behandlingsgrunnlaget for forskningen. Et samtykke må være frivillig, uttrykkelig og informert. Viktigste utgangspunkt for å innhente et korrekt samtykke, er at informasjonen som gis er uttømmende. Videre, frivillighet innebærer blant annet at pasienter ikke må settes i en presset situasjon. Med begrepet uttrykkelig sikter lovgiver til at samtykket skal være tydelig og konkret i forhold til formålet som er definert. Vær oppmerksom på at dersom formålet for prosjektet endrer seg eller utvides, kan det utløse behov for ny informasjon og nytt samtykke fra de berørte.

I Norge og internasjonalt gjelder prinsippet om forskningsfrihet. Forskningsmiljøene skal selv bestemme hva de vil forske på og hvordan denne forskningen i store trekk skal foregå. Premissene for forskningen er likevel rettslig regulert. Forskning innen medisin og helsefag omfatter grupper og enkeltindivider, humant biologisk materiale og *helse- og person-opplysninger*. Personvern og informasjonssikkerhet må derfor være en integrert del av forskningsprosjektet. Hovedreglene om medisinsk og helsefaglig forskning finnes i helseforskningsloven.

Helseforskningsloven bestemmer at reglene i personopplysningsloven og i personopplysningsforskriften vedrørende personvern og informasjonssikkerhet gjelder.

Normen er et sett med regler som aktører i helse-, omsorgs- og sosialsektoren er blitt enig om at skal være retningsgivende, og er basert på eksisterende lovverk. Dette innebærer at personvernet og informasjonssikkerheten i forskningsprosjektene blir ivaretatt på en god og helhetlig og juridisk riktig måte ved at Normen blir fulgt.

Følgende rangering gjelder:
1. Helseforskningsloven m/ forskrifter
2. Normen
3. Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren (dette dokumentet)
4. Faktaark (se kap. 4)

Prosjektleder skal følge kravene fastsatt i pkt. 1 til 4, mens den enkelte forsker vil finne tilstrekkelig veiledning i Faktaark 40 - Informasjonssikkerhet i forskningsprosjekter.

2.2 Forhåndsgodkjenning fra REK

Helse- og personopplysninger kan bare *behandles* og brukes hvis det foreligger et såkalt behandlingsgrunnlag, dvs. en rettslig hjemmel til å innhente og bruke opplysninger og biologisk materiale til et bestemt formål. *Behandling* av *helse- og personopplysninger* uten et behandlingsgrunnlag er forbudt.

Forskningsprosjekter skal forhåndsgodkjennes av REK og dette er et tilstrekkelig behandlingsgrunnlag for helseopplysningene. Prosjektet trenger da ikke tilleggsgodkjennelse, konsesjon e.l., f.eks. fra Datatilsynet, *personvernombud* eller andre.

I *virksomheter* som har *personvernombud* anbefales det at *prosjektleder* benytter denne kompetansen ved oppstart, gjennomføring og avslutning av forskningsprosjektet.

Vær oppmerksom på at ved legemiddelutprøving må det også søkes Statens legemiddelverk om godkjenning. Se bl.a. www.legemiddelverket.no. Forøvrig gjelder veilederen.

Ved klinisk utprøving av medisinsk utstyr skal det også sendes melding til Avdeling medisinsk utstyr og legemidler i Helsedirektoratet. Veileder for melding om klinisk utprøving av medisinsk utstyr finnes på www.helsedir.no.

Søknad om forhåndsgodkjenning av *forskningsbiobank* skal sendes REK. (Se www.etikkom.no.)

2.3 Forskning vs. alminnelig kvalitetssikring

Å skille mellom forskning i helseforskningslovens forstand og annen *behandling* av *helse- og personopplysninger*, f.eks. kvalitetssikring, er prinsipielt og praktisk viktig:

- For det første er skillet avgjørende for om *behandlingen* av *helse- og personopplysninger* trenger forhåndsgodkjenning fra REK
- For det andre vil kravet til behandlingsgrunnlag være ulikt. En forskningsaktivitet har behandlingsgrunnlag i og med en godkjennelse fra REK, mens annen *behandling* finner sitt grunnlag andre steder i lovverket, f.eks. i helselovgivningen
- For det tredje er skillet avgjørende for hvilken instans som er korrekt myndighet på området: Helsetilsynet vedr. hva som skal dokumenteres, Datatilsynet vedr. ikke-forskningsrelatert *behandling* av *helse- og personopplysninger* og REK vedr. forskningsaktiviteter

Grensegangen mellom forskning i helseforskningslovens forstand og annen *behandling* av *helse- og personopplysninger* (kvalitetssikring) vil bil gjort i forskrift med hjemmel i helseforskningsloven. Forskriften trer i kraft samtidig med den nye helseforskningsloven.

Endres et kvalitetssikringsprosjekt til et forskningsprosjekt skal det søkes REK som forhåndsgodkjenning.

Det er REK som med endelig virkning avgjør om en aktivitet som involverer *behandling* av *helse- og personopplysninger*, er å anse som forskning eller ikke.

Den nasjonale forskningsetiske komité for medisinsk forskning (NEM) er klageinstans for vedtak fattet av REK.

3 INFORMASJONSSIKKERHET I FORSKNINGSPROSJEKTER

I dette kapitlet beskrives informasjonssikkerhetskrav som må etableres for at forskningsprosjektet skal forhåndsgodkjennes av REK. For formelle krav til framstilling og dokumentasjon i søknaden henvises det til REK.

For alle tiltak gjelder prinsippet om forholdsmessig sikring, f.eks. ved uautorisert utlevering (se Normen kap. 4.4 Nivå for akseptabel risiko), basert på en risikovurdering og risikostyring. Med forholdsmessig sikring menes at tiltak som iverksettes skal stå i forhold til for eksempel: antall *forskningsdeltagere*, antall personer og *virksomheter* i forskningsprosjektet, om miljøet opplysningene lagres i er spesielt trusselutsatt og forskningsprosjektets varighet.

Kapitlene under omhandler krav til informasjonssikkerhet som *prosjektleder* skal ivareta. Vær oppmerksom på at *virksomheten* har ansvaret og i de fleste tilfeller allerede har ivaretatt flere av kravene og etablert nødvendige tiltak. Dette gjelder bl.a.: styringssystem for informasjonssikkerhet, avtalemaler, diverse prosedyrer, nivå for akseptabel risiko, risikovurdering, konfigurasjonskontroll, tekniske sikkerhetstiltak, *hendelsesregistrering*, innsynsrett og tilbaketrekking av *Prosjektleder* har likevel et selvstendig ansvar for å påse at kravene er ivaretatt.

3.1 Krav til informasjonssikkerhet ved oppstart av forskningsprosjekter

3.1.1 Søke REK om forhåndsgodkjennelse av forskningsprosjektet

Prosjektlederen skal utarbeide og sende søknad om godkjennelse av forskningsprosjektet til REK.

Før søknaden sendes REK anbefales det en intern behandling av søknaden som ivaretar tilgang til og bruk av interne ressurser slik at sentrale krav i *virksomheten* blir ivaretatt.

Resultater fra flere av punktene under (3.1.2 til 3.1.12) skal inngå i søknaden.

3.1.2 Bestemme formålet med bruken av forskningsdataene

Prosjektleder skal beskrive formålet med bruken av *forskningsdataene* slik at det er entydig for alle deltagere hva de kan benyttes til. *Forskningsdataene* kan kun benyttes til det angitte formålet.

Prosjektleder skal innhente godkjennelse av formålet fra *forskningsansvarlig*.

3.1.3 Etablere styringssystem for informasjonssikkerhet

Helseforskningsloven krever at det skal føres *internkontroll* i forskningsprosjekter. Det er *prosjektleders* ansvar å påse at det er etablert et system for *internkontroll* i prosjektet.

De fleste forskningsprosjekter vil være organisert under en *virksomhet* som i henhold til Normen skal ha etablert et styringssystem for informasjonssikkerhet. Styringssystemet er et verktøy for å sikre *internkontroll* slik at *virksomhetens data behandles* iht. gjeldende krav til informasjonssikkerhet. Det anbefales at det eksisterende styringssystemet gjøres gjeldende for det aktuelle forskningsprosjektet.

Dersom det er nødvendig å etablere et eget styringssystem for informasjonssikkerhet for det konkrete forskningsprosjektet, henvises det til Faktaark 2 - Styringssystem for informasjons-sikkerhet.

Enkelte prosedyrer er imidlertid omtalt i kapitlene under samt at sjekklisten i kapittel 5.1 gir oversikt over hvilke prosedyrer som minimum skal etableres.

3.1.4 Etablere nødvendige avtaler

Prosjektleder skal påse at det opprettes nødvendige avtaler med ulike aktører. Avhengig av forskningsprosjektets omfang og karakter, vil det f.eks. kunne oppstå behov for å inngå databehandleravtale, avtale mellom forskningsprosjekt og oppdragsgiver (i oppdragsforskning) og avtaler med ulike underleverandører og informasjonsleverandører mv.

Oppdragsforskning
Når *virksomheten* inngår avtale med en oppdragsgiver om at *virksomheten* skal utføre nærmere bestemte forskningsoppgaver (avtale om oppdragsforskning), anbefales "Standardkontrakt for oppdragsforskning", utviklet av Kunnskapsdepartementet. Det er frivillig å bruke avtalen. Avtalen kan brukes overfor både offentlige og private oppdragsgivere. Det følger en egen veileder med til avtalen. Avtalen med veileder finnes her: http://www.regjeringen.no/nb/dep/kd/aktuelt/nyheter/2006/Ny-standardkontrakt-for-oppdragsforskning.html?id=100648.

Bruk av *databehandler*
Virksomheten/forskningsprosjektet kan ha behov for at et utenforstående miljø, en underleverandør, bearbeider eller drifter data på vegne av prosjektet. Den som bearbeider dataene i en slik sammenheng, er en *databehandler*. Hvis *virksomheten* inngår avtale med en *databehandler*, skal det utarbeides en databehandleravtale (se Faktaark 10 – Bruk av ekstern driftsenhet {*databehandler*}).

En *databehandler* kan ikke *behandle* data på annen måte enn det som er avtalt.

Informasjonsleverandører
En ekstern informasjonsleverandør, f.eks. Statistisk sentralbyrå, Folkehelseinstituttet m.fl., som sitter på demografiske data, opplysninger fra sentrale helseregistre som Medisinsk fødselsregister, Kreftregisteret og Dødsårsaksregisteret, og ulike helseundersøkelser, vil som regel stille vilkår eller inngå avtale med forskerne med tanke på formål, utlevering til

tredjemann og sletting. I så fall bør prosjektet legge leverandørens vilkår inn i prosedyrene for avslutning av prosjektet.

3.1.5 Utarbeide samtykkeerklæring og informasjonsskriv

Prosjektleder skal påse at det utarbeides samtykkeerklæring og informasjonsskriv til *forskningsdeltakerne* i forskningsprosjektet.

Det er krav om informasjonsskriv som setter forskningsdeltaker i stand til å gi et informert samtykke. Innholdet i skrivet vil normalt underlegges grundig kontroll under behandling av søknaden, for å sikre at lovens krav er oppfylt. Det tilrådes at forsker støtter seg på egnet veiledning om tema for å unngå problemer under søknadsbehandlingen hos REK.

Det finnes maler for deltakelse i legemiddelutprøving, og en generell mal for deltakelse i andre forskningsprosjekter.

REK, Den nasjonale forskningsetiske komité, Statens Legemiddelverk og Datatilsynet anbefaler at malene benyttes.

Malene finnes på: http://www.etikkom.no/REK/02012008/view

3.1.6 Sikre taushetsplikt

Prosjektleder skal påse at alle medarbeidere i forskningsprosjektet som har *taushetsplikt*, underskriver erklæring om dette. Dette skal gjøres selv om det tidligere er underskrevet på erklæring for *taushetsplikt* for eksempel i forbindelse med ansettelse i *virksomheten* og ved tildeling av *autorisasjon* til systemer med *helse- og personopplysninger*. Hensikten er å tydeliggjøre det individuelle ansvaret for den enkelte medarbeider i forskningsprosjektet.

Taushetsplikten er ikke til hinder for at *forskningsdata* gjøres kjent for *forskningsdeltageren*.

Det som opphever *taushetsplikten* er enten:

- Samtykke fra den personen opplysningene gjelder, helseforskningsloven §§ 13-17 og §§ 17-19; eller
- Dispensasjon fra *taushetsplikt*, helseforskningsloven §§ 28 og 35.

3.1.7 Etablere prosedyre for tilgangsstyring

Prosjektleder skal sørge for at det etableres prosedyrer for tilgangsstyring til *forskningsdataene* slik at kun *autoriserte* får *forskningstilgang.*

Prosedyrene må ta hensyn til om *forskningsdataene* er direkte identifiserbare eller *avidentifisert* i det kravet til forholdsmessig sikring kan være ulikt.

Ved eventuell bruk av lyd og bildeopptak må prosedyrene for tilgangsstyring omfatte dette.

Se Faktaark 14 – Tilgangsstyring, for ytterligere informasjon.

3.1.8 Fastsette nivå for akseptabel risiko (akseptkriterier)

Som grunnlag for gjennomføring av pålagt risikovurdering skal *prosjektleder* fastsette nivå for akseptabel risiko innenfor rammen av hva *databehandlingsansvarlig* har bestemt. Nivået for akseptabel risiko skal benyttes for å kontrollere at avdekket risiko ikke er større enn det fastsatte nivået. Se Normen kpt. 4.4 Nivå for akseptabel risiko.

Forskningsprosjektet skal som utgangspunkt benytte nivå for akseptabel risiko som gjelder for *virksomheten.*

Se Faktaark 5 - Fastsette akseptkriterier for tilgjengelighet, konfidensialitet og integritet.

3.1.9 Gjennomføre risikovurdering og etablere nødvendige tiltak

Prosjektleder skal sørge for gjennomføring av risikovurdering av *behandlingen* av *forskningsdataene*.

Relevante momenter å risikovurdere er:
- Bruk av teknisk utstyr (f.eks. lagring i nettverk, sikring av bærbart utstyr, nettverk for overføring av data, opptaksutstyr for bilde og lyd)
- Metode for *autorisasjon* og tilgangsstyring til *forskningsdata* for medarbeidere i det enkelte forskingsprosjektet
- Om *forskningsfilen* er tilfredsstillende *avidentifisert*
- Bruk av *koblingsnøkkel* med vekt på samtidighet mellom *koblingsnøkkel* og *forskningsfil*
- 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

Identifiseres det *avvik* fra nivå for akseptabel risiko skal det iverksettes tiltak for å bringe informasjonssikkerheten innefor akseptabelt nivå.

Har *virksomheten* etablert en generell teknisk løsning for forskning er det ikke nødvendig å risikovurdere løsningen for hvert enkelt forskningsprosjekt. Det skal gjennomføres ny risikovurdering hvis forskningsprosjektet har et strengere nivå for akseptabel risiko enn det som er benyttet for den gjennomførte risikovurderingen.

Se Faktaark 7 – Risikovurdering, for metode for gjennomføring av risikovurdering.

Det kan være nødvendig å gjennomføre ny risikovurdering ved:
- Alvorlig *avvik* eller sikkerhetsbrudd, for eksempel:
  - Uautorisert utlevering av forskingsdata
  - Brudd på *integriteten* i *forskningsdata* ved *multisenterstudier*
  - Feil lagring eller uautorisert bruk av *koblingsnøkkelen*
  - Bruk av *forskningsdata* utover hva samtykket fra *forskningsdeltager* tillater
- Vesentlige endringer i forskningsprosjektets formål
- Vesentlige endringer i den tekniske løsningen

3.1.10 Etablere konfigurasjonskontroll

Det tekniske utstyret som benyttes skal ikke endres uten at endringen godkjennes av *prosjektleder*. *Prosjektleder* skal påse at det etableres, eller at *virksomhetens* eksisterende, konfigurasjonskontroll benyttes i forskningsprosjektet. Se Normen kapittel 5.5.1 – Konfigurasjonskontroll.

Prosjektleder skal føre oversikt over utstyr som benyttes til *behandling* av *forskningsdata* og *forskningsfilen* i forskningsprosjektet. Oversikten bør inneholde:
- Type utstyr: Server, stasjonær PC, bærbar PC, annet mobilt utstyr (se også tekniske sikkerhetstiltak under)
- Nettverk med konfigurasjonskart
- Laboratorieinstrumenter
- Hvor utstyret er plassert
- Hvem som eier utstyret
- Hvem som eier informasjonssystemet
- Hvem som er sluttbrukeren: Ansatt i *virksomheten* eller eksterne
- Oversikt over bruksmønsteret: Om utstyret brukes til annet enn forskning, f.eks. til vanlig kliniske eller administrative oppgaver, om utstyret brukes i eller utenfor arbeidstiden

3.1.11 Etablere tekniske sikkerhetstiltak

Prosjektleder skal sørge for at det etableres *tekniske tiltak* for å sikre *konfidensialitet, integritet, tilgjengelighet* og *kvalitet*. *Tiltakene* bør omfatte:
- Beskyttelse av data/*register*, herunder bruk av administratorrettigheter til *forskningsdata*, *forskningsfil* og *koblingsnøkkel*
- Beskyttelse av kataloger og filområder
- Beskyttelse mot ødeleggende programvare
- Kryptering av *forskningsdata/-fil* og datakommunikasjon (f.eks. ved overføring til annen *virksomhet*)
- Forholdsmessig fysisk sikring av rom og områder (låsing og adgangskontroll til rom, brannvarsling og slokking, temperaturregulering, strømforsyning)
- *Tekniske tiltak* ved bruk av mobilt utstyr
- Tilkobling til andre nett (internt i organisasjonen og eksterne nett) og sikring av dette

3.1.12 Etablere hendelsesregistrering

Prosjektleder skal påse at det etableres *hendelsesregistrering* i informasjonssystemene. Siktemålet med *hendelsesregistreringen* er bl.a. å forebygge, avdekke og hindre gjentakelse av sikkerhetsbrudd. Spesielt viktig er det å *hendelsesregistrere forskningstilgang* og bruk av *forskningsfilen* og *koblingsnøkkelen*.

Følgende skal *hendelsesregistreres*:
- *Forskningsdata*: All *forskningstilgang*, registrering, retting og sletting, *autorisert* og forsøk på uautorisert bruk og kopiering / duplisering
- *Forskningsfilen:* All *forskningstilgang*, registrering, retting og sletting, *autorisert* og forsøk på uautorisert bruk og kopiering / duplisering
- *Koblingsnøkkelen*: *Autorisert* og forsøk på uautorisert bruk og kopiering / duplisering
- Fil med *koblingsnøkler*: *Autorisert* og forsøk på uautorisert bruk og kopiering / duplisering

Både manuell og elektronisk *hendelsesregistrering* kan benyttes. Med manuell *hendelsesregistrering* menes fortløpende føring av protokoll. Med elektronisk *hendelsesregistrering* menes at IT-systemet automatisk genererer *hendelsesregistre*.

Forskingsprosjektet må ha prosedyrer for gjennomgang av *hendelsesregistre*. Dersom omfanget av *hendelsesregistreringen* er stort bør det benyttes et IT-verktøy for analyse av *hendelsesregistre*.

Se Faktaark 15 – Hendelsesregistrering og oppfølging.

3.2 Krav til informasjonssikkerhet ved gjennomføring av forskningsprosjekter

I dette kapitelet beskrives krav og anbefalinger som *prosjektleder* skal ivareta så lenge forskningsprosjektet varer.

3.2.1 Innhente forskningsdata

Forskere kan få tilrettelagt *forskningsdata* på flere måter:

- Innsamling direkte fra *forskningsdeltager* ifm. selve forskningsprosjektet
- Uttrekk og utlevering av *forskningsdata* fra *virksomheten* til forskningsprosjektet (EPJ, laboratoriesystem, sentrale helseregistre)
- Anskaffelse av data fra andre kilder, dvs. andre helseregistre eller helseundersøkelser

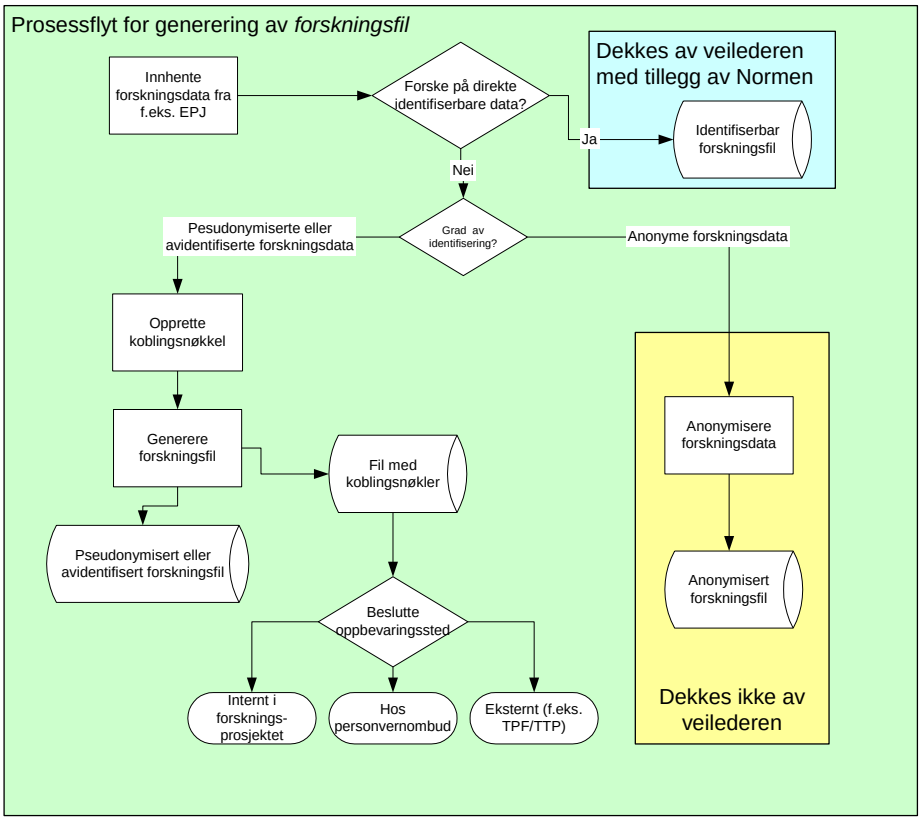
Det er alltid avgivende *virksomhet* som skal bestemme hvordan opplysningene skal gjøres tilgjengelig for forskeren.

Der det er mulig anbefales det en løsning hvor *forskningsdata* gjøres tilgjengelige for forskeren ved at andre enn forskeren klargjør *forskningsdataene*, fortrinnsvis den institusjonen som har ansvaret for dataene. Fordelene med dette er: en service for forskeren som får ferdig bearbeidede data, ansvaret for dataene ligger på klargjører og det er bedre kontroll med at *forskningstilgangen* til dataene er i samsvar med gjeldende regler.

Prosjektleder må påse at innhenting av *forskningsdata* skjer i samsvar med Normen, samtykkeerklæringen og godkjenningen fra REK.

3.2.2 Opprette koblingsnøkkel og generere forskningsfil

Prosjektleder skal sørge for å generere en *forskningsfil* som har samme grad av personidentifisering som godkjenningen fra REK gir (se figur under).



Ved generering av *forskningsfilen* benyttes det en *koblingsnøkkel* som gir riktig grad av personidentifisering. Gjennom opprettelse av *forskningsfilen* skal den enkelte *koblingsnøkkel*, tilhørende hver forekomst av *forskningsdata*, lagres i en fil med *koblingsnøkler*. Se illustrasjon under.

Prosjektleder skal påse at både *forskningsfilen* og filen med *koblingsnøkler* sikres.

3.2.3 Sikre forskningsdata, forskningsfil og koblingsnøkkel

Prosjektleder skal påse at oppbevaring, *forskningstilgang*, bruk og sletting av *forskningsfil*, *koblingsnøkkel*, *forskningsdata* og fil med *koblingsnøkler* skjer iht. etablerte prosedyrer.

Valg av oppbevaringssted og metode må gjøres etter prinsippet om forholdsmessig sikring (se kapittel 3), gjennom risikovurderingen som er beskrevet i kapittel 3.1.9.

All bruk av de ulike kategoriene skal *hendelsesregistreres* iht. prosedyre fastsatt i kapittel 3.1.12.

Spesielle forhold som må ivaretas

- *Forskningsdata:*
  - *Prosjektleder* skal påse at forskningsprosjektets *forskningsdata* oppbevares og sikres iht. kravene i Normen
  - Eksempel på sikring er kryptering. Krypteringsnøkkelen må sikres mot uautorisert *tilgang* (for eksempel oppbevaring i safe) og sletting (vha backup)
- *Koblingsnøkkel:*

  - *Prosjektleder* skal avgjøre om *koblingsnøkkel* skal oppbevares i forskningsprosjektet, innenfor rammen av REKs forhåndsgodkjenning, av *virksomheten* (*personvernombud*) eller eksternt hos en tiltrodd pseudonymforvalter (TPF) / tiltrodd tredjepart (TTP). Beslutningen skal være basert på akseptkriterier (for eksempel omfanget av *forskningsdeltagere* {100 vs 100.000}, spesielle personvernutfordringer og spesielle utfordringer ved *multisenterstudier*)
  - Ved *pseudonymisering* av en *forskningsfil* kan det være hensiktsmessig å benytte en TPF. Det skal opprettes databehandleravtale med TPF
  - Ut fra risikovurderingen kan *virksomheten* velge å oppbevare *koblingsnøkkelen* på en egen forskingsserver eller forskningsområde i *virksomhetens* nettverk. Ved bruk av nettverkslagring er det viktig et det er på plass gode prosedyrer for tilgangsstyring. Som et sikkerhetstiltak bør filen med *koblingsnøkkelen* krypteres. Krypteringsnøkkelen må sikres mot uautorisert *tilgang* (for eksempel oppbevaring i safe) og kopiering (av både *autorisert* og uautorisert bruker)
  - Om *koblingsnøkkelen* oppbevares på en minnepinne bør denne krypteres
- Fil med *koblingsnøkler:*
  - Når filen med *koblingsnøkler* ikke er i bruk skal den oppbevares sikret og adskilt fra forskingsfilen. Se strekpunkt over vedrørende prinsipper for oppbevaring av *koblingsnøkkel*

3.2.4 Ivareta forskingsfilens kvalitet og integritet

Prosjektleder skal påse at prosedyrer vedrørende sikring av *kvalitet* og *integritet* av forskningsfilen ved registrering, endring og sletting av data blir etablert og fulgt.

Prosjektleder skal sørge for å rette uriktige opplysinger, oppdatere foreldete opplysinger og supplere ufullstendige opplysninger.

Prosjektleder skal påse at all registrering, endring og sletting av data i *forskningsfilen hendelsesregistreres* og kontrolleres iht prosedyre fastsatt i kapittel 3.1.12.

Ved *multisenterstudier* må det avtales gjensidige forpliktelser mellom partene slik at *kvalitet* og *integritet* til *forskingsfilen* ivaretas.

3.2.5 Gjennomføre opplæring i informasjonssikkerhet

Prosjektleder skal påse at det gjennomføres opplæring i informasjonssikkerhet. Opplæringen skal fokusere på *virksomhetens* eventuelle sikkerhetsinstruks og områder risikovurderingen peker ut som sentrale for den enkelte medarbeider.

Opplæring skal gis når:
- Forskningsprosjektet starter
- Det kommer nye medarbeidere i forskingsprosjektet
- Det er påkrevet som følge av endringer i styringssystemet for informasjonssikkerhet
- Det er påkrevet som følge av gjennomført risikovurdering
- Det innføres nye regulatoriske krav innen informasjonssikkerhet
- *Avvik* avdekker behov for opplæring

For ytterligere informasjon om opplæring se Faktaark 9 – Opplæring av ledere og medarbeidere.

3.2.6 Identifisere og håndtere sikkerhetshendelser (avvik)

Prosjektleder skal påse at *avvik* behandles fortløpende iht. etablert avviksprosedyre. *Avvik* bør løses på det nivået i organisasjonen det oppstår. Korrigerende tiltak skal dokumenteres.

Om *avviket* har medført uautorisert utlevering med betydning for *konfidensialiteten* skal Datatilsynet varsles.

Se Faktaark 8 – Avviksbehandling, for nærmere informasjon.

3.2.7 Gjennomføre sikkerhetsrevisjon

Prosjektleder skal sørge for at det jevnlig gjennomføres sikkerhetsrevisjon av forskningsprosjektet. Spesielt er dette viktig ved langvarige forskingsprosjekter. Frekvensen for sikkerhetsrevisjon vurderes etter forskningsprosjektets størrelse, omfang, antall *forskningsdeltagere*, varighet og graden av personvernutfordringer i prosjektet.

For å ivareta en uhildet sikkerhetsrevisjon bør denne gjennomføres av andre enn de som til daglig arbeider i forskingsprosjektet. Alle sikkerhetsrevisjoner skal dokumenteres.

Se Faktaark 6 - Sikkerhetsrevisjon, for nærmere informasjon.

3.2.8 Påse at forskningsdata kan spores til opprinnelse

Prosjektleder ivaretar kravet til sporbarhet gjennom oppbevaring og sikring av: *forskningsdata, forskningsfil,* fil med *koblingsnøkler* og *hendelsesregistrene*.

3.2.9 Overføring av forskningsdata til utlandet

Ved overføring av *forskningsdata* til utlandet skal *prosjektleder* påse at reglene for dette følges.

Forskningsdata kan overføres til land innen EØS-området.

Overføring av *forskningsdata* til land utenfor EØS-området er som hovedregel ikke tillatt.

Slik overføring er likevel tillatt:

- Hvis den utenlandske *databehandlingsansvarlige* skriftlig forsikrer overfor den *forskningsansvarlige* at opplysningene vil bli behandlet i samsvar med EUs regelverk (se også reglene om Safe Harbour på www.datatilsynet.no) og *forskningsdeltageren* har gitt samtykke, eller
- Det er gitt informasjon til *forskningsdeltager* om overføring til utlandet og *forskningsdeltager* ikke har reservert seg

Overføring av *avidentifiserte* og *pseudonymiserte* opplysninger er tillatt dersom opplysningene fremstår som *anonyme* for mottakeren, og at denne ikke har mulighet til å re-identifisere opplysningene.

Hvis *forskningsdata* er overført til utlandet i forbindelse med forskningen, skal *prosjektleder* vite hvordan opplysningene blir håndtert etter at prosjektet er avsluttet. Sluttmeldingen til REK må inneholde en redegjørelse for hvilke *forskningsdata* som på avslutningstidspunktet befinner seg i utlandet og hvem som er *databehandlingsansvarlig* for opplysningene.

3.2.10 Ivareta innsynsretten

Forskningsdeltageren har, med enkelte lovbestemte unntak, rett til innsyn i identifiserbare og pseudonyme *forskningsdata* om seg selv.

Vedkommende har også rett til innsyn i sikkerhetstiltakene som omgir opplysningene. Dette gjelder likevel bare dersom innsyn kan skje uten fare for at sikkerheten blir svekket. Avgjørelsen om innsyn skal nektes ut fra sikkerhetshensyn, tas av *prosjektleder*. For *virksomheter* som har laget felles tekniske løsninger, er det den sentrale sikkerhetsledelsen i *virksomheten* som avgjør dette.

Prosjektleder skal påse at forespørsel om innsyn er besvart uten ugrunnet opphold og senest innen 30 dager.

3.2.11 Behandle tilbaketrekking av samtykke

Om *forskingsdeltager* trekker tilbake samtykket til å delta i et forskningsprosjekt skal *prosjektleder* sørge for at forskningen på vedkommendes biologiske materiale eller *forskningsdata* opphører.

Den som har trukket samtykket kan kreve at materialet destrueres og forekomsten om vedkommende i *forskningsdataene* og *forskningsfilen* slettes innen 30 dager.

Retten til å kreve sletting eller destruksjon gjelder ikke:

- Hvis materialet etter bearbeidelse inngår i et annet biologisk produkt
- Hvis *forskningsdata* allerede har inngått i utførte analyser
- I legemiddelutprøving

Avgjørelser om sletting skal tas av *prosjektleder*, men avgjørelsen kan klages inn for REK. Alle slettinger skal dokumenteres og skal være sporbare. Dersom sterke samfunns- eller forskningshensyn tilsier det, kan REK etter søknad fra forskningsprosjektet likevel tillate fortsatt forskning på materialet / *forskningsdataene.*

3.2.12 Bruk av e-post og Internett i forskningsprosjekter

Prosjektleder skal påse at e-postløsninger ikke benyttes ved overføring av direkte identifiserbare og *avidentifiserte forskningsdata*.

Forsendelse av *forskningsfil* (identifiserbare og *avidentifiserte* data) og *koblingsnøkkel* via e-post skal sikres med *PKI* og sikker identifikasjon av mottaker.

For ytterligere informasjon se Faktaark 33 – Bruk av e-post ifm helseopplysninger.

3.3 Krav til informasjonssikkerhet ved avslutning av forskningsprosjekter

3.3.1 Påse at forskningsdata arkiveres

Det vil fremgå av forhåndsgodkjenningen fra REK at *forskningsdata* kan lagres i sammenheng med den forskningen som skal utføres. Godkjennelsen fra REK bygger på prosjektbeskrivelsen og vil derfor normalt angi hvor lenge opplysningene kan beholdes.

Når forskningen/forskningsprosjektet er avsluttet, skal *prosjektleder* sørge for at opplysninger som kan identifisere *forskningsdeltagerne* ikke oppbevares lenger enn nødvendig og ikke lenger enn det er gitt samtykke til.

Hvis *forskningsdata* skal oppbevares lenger enn det opprinnelige samtykket gir rett til, må det innhentes nytt samtykke fra *forskningsdeltager*. *Prosjektleder* kan søke REK om dispensasjon for videre oppbevaring uten samtykke.

Prosjektleder skal avklare med REK om hvor lenge *forskningsdata* skal oppbevares for å kunne avdekke forskningsjuks. REK kan pålegge at forskningsprosjektet, av hensyn til etterkontroll, oppbevarer *forskningsfil* og *forskningsresultat* i fem år etter at sluttmelding er sendt.

3.3.2 Sikre sletting av forskningsdata

Ofte er både *anonymisering* og sletting av dataene akseptert. I så fall kan en *anonymisert* versjon av datasettet beholdes.

Hvis noen har stilt krav om sletting, f.eks. REK, informasjonsleverandøren, eller det er gitt informasjon om dette i forbindelse med innhentingen av samtykke, skal *prosjektleder* sørge for at sletting av *forskningsdata* skjer på en hensiktsmessig, fullstendig og sikker måte. En full *anonymisering* er likestilt med sletting.

Prosjektleder skal sørge for at det føres et *register* over hvilke lagringsmedia som benyttes. I samsvar med etablerte prosedyrer skal lagringsmedia merkes med ”Inneholder *forskningsdata*” eller ”Inneholder pasientjournal” e.l. Merkingen plasseres på et godt synlig sted. Se Faktaark 34 – Håndtering av lagringsmedia.

Når *forskningsdata* skal slettes, er det viktig at slettingen skjer fullstendig, dvs. på en måte som ikke gjør det mulig å reversere prosessen. Slettingen skal utføres iht. etablert prosedyre.

Slettingen skjer ved at lagringsmedia destrueres eller overskrives, *koblingsnøkler* destrueres mv. Med lagringsmedia menes f.eks. håndskrevne notater, opplysninger på papir, bilder, film/video, CD-ROM, ZIP-disk, magnetbånd og minnepinner. Vær oppmerksom på at sikkerhetskopier, *forskningsfilen* og *koblingsnøkler* også må slettes. Slettes kun *nøkkelfilen* er *forskningsfilen anonym*.

Hvis det blir aktuelt å avhende lagringsmedia som har vært brukt i forskningsprosjekt (server eller PC, mobilt utstyr, magnetbånd, osv.) skal dette behandles slik at det ikke er fare for brudd på kravene til *konfidensialitet*. Lagringsmediene må derfor slettes for informasjon slik at det ikke er mulig å gjenskape *forskningsfil* og *forskningsdata*.

Forskningsprosjektet (eventuelt med hjelp fra egen IT-funksjon) kan utføre slettingen selv eller arbeidet kan utføres av en ekstern leverandør som sletter lagringsmedia. Enkelte eksterne leverandører tilbyr sletteløsninger som er godkjent av Nasjonal Sikkerhetsmyndighet (NSM). Det anbefales å bruke disse.

Et alternativ til sletting er at lagringsmedia fysisk demonteres og ødelegges (f.eks. å brenne eller makulere minneplatene/-enhetene i lagringsmediet). Se Faktaark 25 - Lagringstid og sletting av helse- og personopplysninger.

3.3.3 Sende sluttmelding til REK

Prosjektleder skal sende sluttmelding til REK når forskningsprosjektet er avsluttet.

Register over lagringsmedia, inkludert sletting av *forskningsfilen* og *forskningsdata* skal være med i sluttmeldingen.

En nærmere beskrivelse av sluttmeldingen vil gå frem av forhåndsgodkjenning fra REK, evt. i veiledningen på REK/NEM hjemmeside.

4 REFERANSER MELLOM FAKTAARK OG VEILEDEREN

Tabellen under viser faktaark og infoark som er særlig relevante for forskningsprosjekter.

Faktaark	Betydning i forskningsprosjektet
2 – Styringssystem for informasjonssikkerhet	• Oppbygging og innhold i styringssystemet • Vanligvis har *virksomheten* dette på plass, ellers må det utarbeides
5 – Fastsette akseptkriterier for *tilgjengelighet*, *konfidensialitet* og *integritet* og *kvalitet*	• Fastsettes for forskningsprosjektet uavhengig av hva som er fastsatt av *virksomheten* (fordi dette kan avvike)
6 – Sikkerhetsrevisjon	• Etablere plan for sikkerhetsrevisjoner • Sikkerhetsrevisjon skal gjennomføres jevnlig
7 – Risikovurderinger	• Risikovurdering skal gjøres for enhver *behandling* av *forskningsdata* • *Avidentifisering* og *anonymisering* er en ny *behandling*
8 – Avviksbehandling	• Prosedyrer og dokumentasjon skal etableres
9 – Opplæring av ledere og medarbeidere	• Opplæring av prosjektmedarbeidere
10 – Bruk av ekstern driftsenhet (*databehandler*)	• Krav som skal ivaretas hvis *databehandler* benyttes (bl.a. for ekstern bearbeiding) • Databehandleravtale skal opprettes
14 – Tilgangsstyring	• Krav som skal ivaretas i forskningsprosjektet • Sikring av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel*

Faktaark	Betydning i forskningsprosjektet
15 – Hendelsesregistrering og oppfølging (Se definisjon av *hendelsesregistrering*)	• Sporing av *forskningstilgang*, bruk, opprinnelse, sammenstillinger og endringer • Kontroll og oppfølging i ettertid
17 – Fysisk sikring av områder og utstyr	• Hindre uautorisert adgang til forskningslokaler og utstyr som benyttes i forskningsprosjektet
18 – Bruk av bærbart utstyr	• Lagring av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel* på bærbart utstyr • Kryptering av lagringsmedia
21 – Sikkerhetskopi	• Sikkerhetskopiering av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel* • Sikre kopi av versjoner av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel* • Ekstern oppbevaring av sikkerhetskopi
23 – Avtaler og tillatelser vedrørende forskning	• Forslag til innhold i avtaler
25 – Lagringstid og sletting av *helse- og personopplysninger*	• Lagring av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel* etter avsluttet forskning • Sletting av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel* etter avsluttet forskning
33 – Bruk av e-post	• Elektronisk forsendelse av *forskningsdata*, *forskningsfil*, fil med *koblingsnøkler* og *koblingsnøkkel*
34 – Håndtering av lagringsmedia	• *Register* over lagringsmedia
37 – Sikkerhetskrav og sikkerhetsdokumentasjon i prosjekter	• Dokumentasjon som skal utarbeides i forskningsprosjektet hvis det anskaffes eller utvikles systemer ifm forskningen
40 – Informasjonssikkerhet i forskningsprosjekter	• Ansvar og oppgaver for den enkelte forsker

5 VEDLEGG

5.1 Sjekkliste for prosjektleder

Oppgaver under markert med **fet skrift** må vanligvis ivaretas av *prosjektleder*. Øvrige oppgaver er oftest et virksomhetsansvar og kan allerede være etablert eller ivaretatt. *Prosjektleder* skal uavhengig av dette forsikre seg om at alle oppgavene er ivaretatt.

Nr	Oppgave	Utført
	Oppstart	
1.	**Søke REK om forhåndsgodkjennelse av forskningsprosjektet**	

Nr	Oppgave	Utført
2.	**Bestemme formålet med bruken av forskningsdataene**	
3.	Etablere styringssystem for informasjonssikkerhet	
4.	Etablere nødvendige avtaler	
5.	**Utarbeide samtykkeerklæring og informasjonsskriv**	
6.	Sikre taushetsplikt	
7.	Etablere prosedyre for tilgangsstyring	
8.	Fastsette nivå for akseptabel risiko (akseptkriterier)	
9.	Gjennomføre risikovurdering og etablere nødvendige tiltak	
10.	Etablere konfigurasjonskontroll	
11.	Etablere tekniske sikkerhetstiltak	
12.	Etablere hendelsesregistrering	
13.	Etablere prosedyre for informasjonssikkerhet for forskning: ☐ Samtykke (se kapittel 3.1.5) ☐ Tilgangsstyring (se kapittel 3.1.7) ☐ Fysisk sikring av områder og utstyr (se Faktaark 17) ☐ Bruk av bærbart utstyr (se Faktaark 18) ☐ Sikkerhetskopiering (se Faktaark 21) ☐ Håndtering av lagringsmedia (se Faktaark 34) ☐ Avviksbehandling (se Faktaark 8) ☐ Bruk av e-post (se Faktaark 33) ☐ Sikkerhetsrevisjon (se Faktaark 6) ☐ Oppbevaring og sikring av forskningsdata (se kapittel 3.2.3) ☐ Oppbevaring og sikring av forskningsfil (se kapittel 3.2.3) ☐ Oppbevaring og sikring av forskningsresultat (se kapittel 3.2.3) ☐ Oppbevaring og sikring av koblingsnøkkel (se kapittel 3.2.3) ☐ Oppbevaring og sikring av fil med koblingsnøkkel (se kapittel 3.2.3) ☐ Sletting av alle forskningsdata (se kapittel 3.3.2) ☐ Sikring av kvalitet og integritet i forskningsfil (se kapittel 3.2.4) ☐ Forskningsdeltagers rett til innsyn (se kapittel 3.2.10)	
	Gjennomføring	
14.	**Innhente forskningsdata**	
15.	**Opprette koblingsnøkkel og generere forskningsfil**	
16.	**Sikre forskningsdata, forskningsfil og koblingsnøkkel**	
17.	**Ivareta forskningsfilens kvalitet og integritet**	
18.	**Gjennomføre opplæring i informasjonssikkerhet**	
19.	**Identifisere og håndtere sikkerhetshendelser (avvik)**	
20.	**Gjennomføre sikkerhetsrevisjon**	
21.	**Påse at forskningsdata kan spores til opprinnelse**	
22.	**Overføring av forskningsdata til utlandet**	
23.	**Ivareta innsynsretten**	
24.	**Behandle tilbaketrekking av samtykke**	
25.	**Bruk av e-post og Internett i forskningsprosjekter**	
	Avslutning	
26.	**Påse at forskningsdata arkiveres (i samsvar med forhåndsgodkjennelsen fra REK)**	
27.	**Sikre sletting av forskningsdata**	

Nr	Oppgave	Utført
28.	**Sende sluttmelding til REK**	

5.2 Eksempel på risikovurdering av forskningsprosjektet

Nedenfor vises et eksempel på en forenklet risikovurdering.

RISIKOVURDERING		
Virksomhet:	**Avdeling:**	
Kontaktperson:	**Telefon:**	
Vurdert av: **Dato:**	**Avdeling:**	**Telefon:**

Formålet med denne risiko-vurderingen:	

Forhold som er vurdert (uønsket hendelse) **<eksempel>**		**Konsekvens for**	**Risikonivå**	**Nødvendig med tiltak** **Alltid Ja på Høy og Meget høy**
1.	Avidentifisering er ikke fullstendig for alle forekomster i forskningsdataene.	☒Konfidensialitet ☐Integritet ☐Tilgjengelighet ☐Kvalitet	☐Lavt ☒Middels ☐Høy ☐Meget høy	☐Ja ☒Nei
2.	Koblingsnøkkel er ikke forsvarlig sikret.	☒Konfidensialitet ☒Integritet ☐Tilgjengelighet ☒Kvalitet	☐Lavt ☐Middels ☒Høy ☐Meget høy	☒Ja ☐Nei
3.	Tap eller tyveri av forskningsfil lagret på bærbart utstyr.	☒Konfidensialitet ☐Integritet ☒Tilgjengelighet ☐Kvalitet	☐Lavt ☐Middels ☒Høy ☐Meget høy	☒Ja ☐Nei
4.	Tyveri av forskningsserver.	☒Konfidensialitet ☐Integritet ☒Tilgjengelighet ☐Kvalitet	☐Lavt ☐Middels ☒Høy ☐Meget høy	☒Ja ☐Nei
5.	Hendelsesregistrering dekker ikke forskningstilgang, bruk, opprinnelse, sammenstillinger og endringer.	☒Konfidensialitet ☒Integritet ☐Tilgjengelighet ☒Kvalitet	☒Lavt ☐Middels ☐Høy ☐Meget høy	☐Ja ☒Nei
6.	Kopi av forskningsdata lagres ikke eksternt.	☐Konfidensialitet ☐Integritet ☒Tilgjengelighet ☐Kvalitet	☐Lavt ☐Middels ☐Høy ☒Meget høy	☒Ja ☐Nei

Beskrivelse av tiltak *(Nr 1 har høyest prioritet)*		**Betydning/ Kommentar**	**Ref linje nr over**
1.	Koblingsnøkkel skal oppbevares hos Personvernombud.		2
2.	Lagringsmedia på bærbart utstyr krypteres.		3
3.	Server med forskningsdata skal sikres i avlåst datarom med alarm.		4

Beskrivelse av tiltak *(Nr 1 har høyest prioritet)*		**Betydning/ Kommentar**	**Ref linje nr over**
4.	Etablere prosedyre med ekstern oppbevaring av sikkerhetskopi. Frekvens: Ukentlig.		6

5.3 Avtaler og tillatelser vedrørende forskning

Se Faktaark 23 – Avtaler og tillatelser vedrørende forskning.

5.4 Deltagere i referansegruppen for utarbeidelse av veilederen

Nr	Navn	Virksomhet
1.	Ellef Mørk	Akershus universitetssykehus
2.	Braar Larsen	Datatilsynet
3.	Nils J. Langtvedt	Den nasjonale forskningsetiske komité for medisin og helsefag (NEM)
4.	Riccarda Pfeiffer	Forskerforbundet
5.	Eline Monstad	Helse Bergen HF
6.	Arnstein Leonardsen	Helse Midt-Norge IT (HEMIT)
7.	Arild Hals	REK Midt-Norge [1]
8.	May Britt Rossvoll	REK Nord
9.	Jørgen Hardang	REK Sør
10.	Arne Salbu	REK Vest
11.	Ingrid Middelthon	REK Øst
12.	Tor Ottersen	Helsedirektoratet
13.	Jan Gunnar Broch	Sykehuset Innlandet
14.	Andreas Moan	Ullevål universitetssykehus
15.	Heidi Thorstensen	Ullevål universitetssykehus
16.	Per Bruvold	Universitetssykehuset for Nord-Norge

6 REFERANSER

Øvrig relevant og nyttig informasjon finnes i disse dokumentene / nettstedene:

- Helseforskningsloven - se www.lovdata.no
- Norm for informasjonssikkerhet - se www.normen.no
- Forskningshåndboken – se www.helsebiblioteket.no
- Den nasjonale forskningsetiske komité for medisin og helsefag (NEM) og De regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK) – se www.etikkom.no

[1] REK = De regionale komiteer for medisinsk og helsefaglig forskningsetikk