

Tilsyn våren 2004:

Behandling av helseopplysninger i forskning

Funn og tendenser

Versjon 1.0 - 30.06.2004

Prosjektgruppe for tilsynene:
Juridisk rådgiver Hanne P. Gulbrandsen
Juridisk rådgiver Cecilie L. B. Rønnevik
Juridisk rådgiver Monica Fornes
Juridisk rådgiver Rune Vidar Bråthen
Senioringeniør Johan Braar Larsen
Avdelingsingeniør Helge Veum

Innholdsfortegnelse

1. Tilsyn i helsesektoren våren 2004.	5
1.1. <i>Prosjektgruppen</i>	5
1.2. <i>Prosjektmandatet</i>	5
1.2.1. <i>Mandat</i>	5
1.2.2. <i>Organisering</i>	5
1.2.3. <i>Om ressursbruk</i>	6
1.2.4. <i>Rapportering</i>	6
1.3. <i>Tilsynsobjektene</i>	6
1.4. <i>De behandlingsansvarlige</i>	8
2. Behandlingsansvar - funn og tendenser	9
2.1. <i>Er ansvaret plassert hos riktig virksomhet?</i>	9
2.2. <i>Er ansvaret plassert innad i virksomheten?</i>	10
2.2.1. <i>Det eksterne ansvaret påhviler ledelsen</i>	10
2.2.2. <i>Ansvaret kan delegeres internt</i>	10
2.2.3. <i>Kort om studentprosjekter</i>	11
2.3. <i>Konklusjoner</i>	12
3. Internkontroll – funn og tendenser.....	13
3.1. <i>Internkontrollsystemet brukt i praksis, med særlig vekt på forskning</i>	13
3.2. <i>Særlig om internkontroll i virksomheter som har inngått avtale med Norsk samfunnsvitenskaplig datatjeneste (NSD)</i>	13
3.3. <i>Konklusjoner</i>	14
4. Plikten til å sørge for et behandlingsgrunnlag – funn og tendenser	15
4.1. <i>Særlig om samtykke</i>	15
4.2. <i>Konklusjoner</i>	16
5. Konesjons- og meldeplikt – funn og tendenser	17
5.1. <i>Forståelse av konsesjons- og meldesystemet</i>	17
5.2. <i>Overholdelse av melde- og konsesjonsplikt</i>	17
5.3. <i>Konklusjoner</i>	18
6. Konesjonsvilkår – funn og tendenser.....	19
6.1. <i>Etterlevelse av konsesjonsvilkårene i praksis</i>	19
6.2. <i>Konklusjoner – funn og tendenser</i>	20

Innholdsfortegnelse

7. Den registrertes rettigheter – funn og tendenser.....	21
7.1. Ivaretagelsen av disse rettighetene i praksis.....	21
7.2. Konklusjon.....	21
8. Sletting eller anonymisering ved prosjektslutt – funn og tendenser.....	22
8.1. Generelt.....	22
8.2. Særlig om sletteplikten ved legemiddelutprøving.....	23
8.3. Konklusjon.....	23
9. Personvernombud for forskning – funn og tendenser	24
9.1. Virkningen på personvernet, målt i oppfyllelse av regelverk og konsesjonsvilkår.....	24
9.1.1. Ved prosjektets oppstart	24
9.1.2. Når prosjektet løper (forskningsperioden) og ved prosjektavslutning	25
9.2. Konklusjoner	25
10. Informasjonssikkerhet i forskning.....	26
10.1. Premisser.....	26
10.2. Sikkerhetsmessige aspekter ved tilsynsarbeidet	26
10.3. Forskning på aidentifiserte opplysninger.....	26
10.3.1. Generelt om aidentifisering.....	26
10.3.2. Konklusjoner basert på tilsynserfaringer.....	27
10.4. Sikkerhetsbehov.....	28
10.4.1. Valg av akseptabel risiko	28
10.4.2. Konklusjoner basert på tilsynserfaringer.....	28
10.5. Teknologiløsninger.....	28
10.5.1. Valg av teknologiløsninger	28
10.5.2. Konklusjoner basert på tilsynserfaringer.....	29
11. Faglig oppsummering.....	31
11.1. Konsesjonsplikt.....	31
11.2. Meldeplikt.....	31
11.3. Personvernombud.....	31
11.4. Internkontroll.....	32
11.5. Sletting.....	32
11.6. Ulike former for personopplysninger	32
11.7. Hovedanbefaling	32

Innholdsfortegnelse

Vedlegg A: Notat om krav etter personopplysningsloven og helseregisterloven til behandling av personopplysninger i forskning

Vedlegg B: Statistikk

1. Tilsyn i helsesektoren våren 2004.

Våren 2004 har Datatilsynet gjennomført tilsyn med fokus på bruk av helseopplysninger¹ og andre sensitive personopplysninger i forskning. Denne rapporten tar for seg statistikk, funn og tendenser fra tilsynene.

1.1. Prosjektgruppen

Prosjektgruppen fikk sitt mandat 9. februar 2004 og konstituerte seg 17. februar 2004. Prosjektet avsluttes med denne rapporten 30. juni 2004.

Deltagere i prosjektet har vært saksbehandlere knyttet til Datatilsynets faggruppe innen helse/forskning²:

- Juridisk rådgiver Cecilie L. B. Rønnevik
- Juridisk rådgiver Monica Fornes
- Juridisk rådgiver Rune Vidar Bråthen
- Juridisk rådgiver Hanne P. Gulbrandsen
- Senioringeniør Johan Braar Larsen
- Avdelingsingeniør Helge Veum

Rådgiver Hanne P. Gulbrandsen har vært gruppens prosjektleder. Rådgiver Monica Fornes har fungert som prosjektleder i prosjektleders fravær.

1.2. Prosjektmandatet

1.2.1. Mandat

Prosjektgruppen gis i oppdrag å planlegge, forberede, gjennomføre og ta ansvar for videre oppfølging av Datatilsynets tilsynsaktiviteter innen helsesektoren. Gruppen skal gjennomføre minst 40 tilsyn innen utgangen av juni 2004, hvorav en viss andel av disse kan være brevlige tilsyn. Gruppen skal levere en sluttrapport fra tilsynene hvor det redegjøres for funn innen sektoren. Gruppens leder skal rapportere om fremdrift etter milepæler angitt under avsnittet rapportering.

1.2.2. Organisering

Deltakere: Johan Braar Larsen, Helge Veum, Hanne Pernille Gulbrandsen, Monica Fornes, Cecilie L. B. Rønnevik, Rune Vidar Bråthen.

Gruppen konstituerer seg selv. Medlemmer i gruppen rapporterer til prosjektleder i forhold til alt som har med gjennomføring av ovennevnte mandat å gjøre. Prosjektleder rapporterer til leder for tilsyns- og sikkerhetsavdelingen i forbindelse med prosjektgjennomføringen. Prosjektleder må også koordinere med linjeledelse om uttak av ressurser fra linjen.

¹ Vil heretter bli benevnt som personopplysninger

² Med forskning menes forskning der bruk av helse- eller andre personopplysninger forekommer

Gruppen skal være selvstyrt og må selv finne plass og anledning til å gjennomføre tilsynene. Medlemmer i prosjektet vil ikke periodiseres til tilsynsarbeid, hvilket innebærer at gruppen selv må koordinere mot øvrige oppgaver.

1.2.3. Om ressursbruk

Datatilsynet anslår at tid brukt til tilsyn i gjennomsnitt vil være 12 timer pr. stedlig tilsyn/medarbeider (som deltar i tilsynet) eksklusiv reisetid. Når det gjelder brevlig tilsyn anslås det et gjennomsnitt på ca. 6-8 timer pr. tilsyn/medarbeider. Gruppen bes gi tilbakemelding i forhold til dette anslaget med hensyn til fremtidig organisering.

1.2.4. Rapportering

Det forventes at prosjektleder gir rapportering ved følgende milepæler:

- Planlegging er gjennomført
- Varsel er sendt ut
- Tilsyn er gjennomført
- Rapporter er sendt ut

Det gis ingen frister for ovennevnte (ut over endelig frist som er satt til utgangen av juni), da gruppen selv skal styre fremdriften. Gruppen bør imidlertid utarbeide en fremdriftsplan som sikrer tilfredsstillende fremdrift.

1.3. Tilsynsobjektene

Tilsynsobjekter ble valgt ut fra meldedatabasene hos Datatilsynet og Norsk samfunnsvitenskaplig datatjeneste³, og fra behandlede konsesjonssøknader. Det ble utført tilsyn i form av brevlige og stedlige tilsyn, i tillegg til en kombinasjon av disse.

Tilsynsobjektene var underlagt henholdsvis personopplysningsloven eller helseregisterloven. Helseregisterloven trådte i kraft 1. januar 2002, og er en særlov for behandling av helseopplysninger i helseforvaltningen og helsetjenesten⁴. Personopplysningsloven gjelder for behandling av personopplysninger generelt⁵. Personopplysningsloven og personopplysningsforskriften supplerer helseregisterloven der denne er taus jf. helseregisterlovens § 36.

Det ble initiert tilsyn med totalt 59 forskningsprosjekter. I seks tilfeller viste det seg at prosjektet likevel ikke var blitt iverksatt. I ett tilfelle viste det seg at behandlingsansvaret ikke ligger hos den som konsesjonen opprinnelig er utstedt til.

³ Heretter NSD

⁴ For mer om forholdet mellom personopplysningsloven og helseregisterloven og lovenes saklige virkeområde, se kommentarutgaven til helseregisterloven av Engelschiøn, Lie Ulrichsen og Nilsen

⁵ Se for øvrig personopplysningslovens §§ 1 og 3 og helseregisterlovens §§ 1 og 3 og kommentarutgaven til personopplysningsloven skrevet av Kaspersen, Bergsgeng Skullerud og Wiik Johansen

Ni prosjekter, som i henhold til Datatilsynets opplysninger skulle ha vært avsluttet, ble undersøkt utelukkende med tanke på å avdekke om personidentifiserbare data har blitt slettet eller anonymisert, i tråd med forutsetningene for prosjektet.

De øvrige prosjektene ble undersøkt med tanke på å avdekke blant annet om prosjektet har et gyldig behandlingsgrunnlag, om de registrertes rettigheter blir ivaretatt, om vilkår gitt i Datatilsynets konsesjoner etterleves, og om det finnes konsesjonspliktige prosjekter som ikke er meldt til Datatilsynet eller personvernombudene.

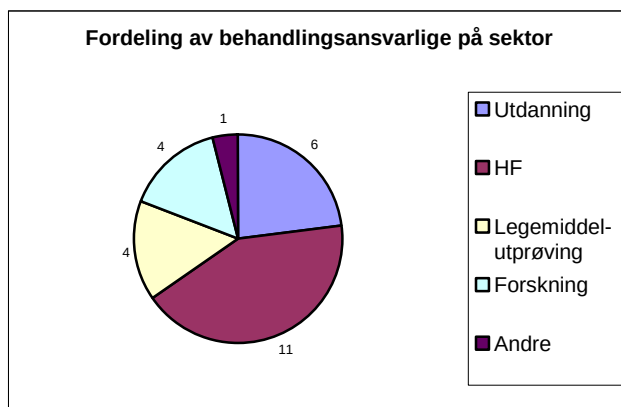
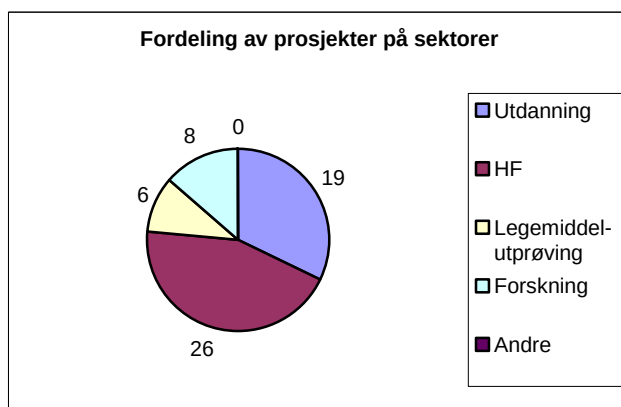
Det har vært vanskelig å få inn svar på brevkontrollene. Datatilsynets opprinnelige svarfrist ble i liten grad overholdt.

1.4. De behandlingsansvarlige

Det ble ført tilsyn med totalt 26 behandlingsansvarlige i fem ulike sektorer. Disse fordeler seg som følger:

- 11 helseforetak
- 6 læresteder
- 4 forskningsinstitusjoner
- 4 legemiddelprodusenter⁶
- 1 privat legesenter⁷

De behandlingsansvarlige for disse prosjektene har også blitt kontrollert i forhold til virksomhetens ansvarsstruktur og internkontroll knyttet til forskning som innebærer en eller annen form for bruk av personopplysninger⁸.



⁶ Legemiddelprodusenter som driver klinisk utprøving av legemidler på mennesker

⁷ Omhandles ikke i denne rapporten da virksomheten viste seg å ikke bedrive forskning

⁸ Se for eksempel personopplysningslovens § 2 nr. 2 og helseregisterlovens § 2 nr. 5

2. Behandlingsansvar - funn og tendenser

Det er den behandlingsansvarlige og databehandlingsansvarlige⁹ som er pliktsubjektet etter henholdsvis personopplysningsloven og helseregisterloven. Plikten til å oppfylle regelverkets bestemmelser kalles *behandlingsansvaret/ databehandlingsansvaret*¹⁰.

Personopplysningslovens § 2 nr. 4 legger behandlingsansvaret på ”den som bestemmer formålet med behandlingen av personopplysningene og hvilke hjelpemidler som skal brukes”. Hvem som er behandlingsansvarlig for et forskningsprosjekt, vil derfor bero på en konkret vurdering i det enkelte tilfellet. Ved vurderingen vektlegges følgende momenter:

- hvem har initiert og finansiert prosjektet
- hvem har påtatt seg behandlingsansvaret overfor Datatilsynet i prosjektet i forbindelse med at det er sendt melding eller søkt om konsesjon.
- hvilken oppfatning fikk eventuelle deltagere i prosjektet, da de ble informert om prosjektet.¹¹

Det forekommer at det er uenighet mellom en institusjon og en tilknyttet forsker om *eierforholdene* rundt forskningsmaterialet og forskningsresultatene. Datatilsynet verken kan eller ønsker å ta stilling til spørsmål om eierskap. Det er bruksretten til personopplysningene som er fokus for Datatilsynet og det lovverket tilsynet forvalter.

Datatilsynet ser helst at behandlingsansvaret for behandling av personopplysninger legges hos en virksomhet, heller enn hos en privatperson, der det er mulig. Det er særlig hensynet til notoritet, kontinuitet og den sivilprosessuelle partsevne som begrunner dette.

2.1. Er ansvaret plassert hos riktig virksomhet?

En rekke forskningsprosjekter er samarbeidsprosjekter mellom ulike virksomheter, for eksempel mellom helseforetak og læresteder. Og det forekommer ofte at en forsker er ansatt i, eller på annen måte er tilknyttet to virksomheter. Dette viser seg å være en utfordring når behandlingsansvaret for et konkret forskningsprosjekt skal plasseres. Ofte vil det bero på tilfeldigheter hvorvidt det er i den ene eller den andre virksomhetens navn forsker søker om konsesjon for, eller melder prosjektet.

⁹ Heretter kalt behandlingsansvarlig(e)

¹⁰ Heretter kalt behandlingsansvaret

¹¹ Gjelder i de tilfeller hvor det oppstår tvil om behandlingsansvaret mens prosjektet løper. I nye prosjekter er dette i stedet et spørsmål om riktig informasjon. Det er svært vanlig at invitasjoner til å delta i forskningsprosjekter, samtykkeskriv med mer, føres på et brevpapir fra for eksempel et sykehus. I et slikt tilfelle vil Datatilsynet forholde seg til sykehuset som behandlingsansvarlig. Det vises her til at respondenten har tatt en beslutning om deltagelse blant annet med bakgrunn i den tillit vedkommende har til denne institusjonen, og at det er naturlig for respondenten å henvende seg til denne institusjonen for senere å ivareta sine rettigheter etter loven.

Datatilsynet har sjelden noen formening om hvorvidt behandlingsansvaret bør ligge hos den ene virksomheten eller hos den andre. Det tilsynet er opptatt av er at det utad må fremgå tydelig hvor behandlingsansvaret blir lagt, og særlig overfor eventuelle deltagere/respondenter.

I tre tilfeller ble det avdekket at det ikke er samsvar mellom de reelle ansvarsforholdene og de opplysninger som er gitt om behandlingsansvaret i forbindelse med at det ble søkt om konsesjon. I disse tilfellene vil Datatilsynet gi pålegg om at ansvarsforholdene klargjøres. I de tilfeller hvor respondenter er gitt uriktig informasjon, vil det i tillegg gis pålegg om at disse informeres om endringene i prosjektet.

2.2. Er ansvaret plassert innad i virksomheten?

Det har vært ført tilsyn med en rekke svært store og komplekse virksomheter med opptil flere tusen ansatte. I slike virksomheter er det spesielt viktig med klare ansvarsforhold, også hva angår ansvaret for etterlevelse av bestemmelsene i henholdsvis personopplysnings- og helseregisterloven.

2.2.1. Det eksterne ansvaret påhviler ledelsen

Datatilsynet vil forholde seg til virksomhetsledelsen som behandlingsansvarlig for de forskningsprosjektene som finner sted i virksomheten.

I forbindelse med de gjennomførte tilsynene ble det avdekket at *virksomhetsledelsen* ved tilsynsobjektene, med unntak av et lærested, ser på seg selv som behandlingsansvarlig utad for de forskningsprosjektene som finner sted i virksomheten¹². Hva gjelder studentprosjekter stilte dette seg noe annerledes, se punkt 2.2.3.

Kun hos syv av de behandlingsansvarlige var behandlingsansvaret dokumentert på et overordnet nivå.

I samtaler med *forskerne* ble det avdekket at de ofte ser på seg selv som behandlingsansvarlige for forskningsprosjektene utad, også i de tilfeller hvor ansvaret ikke formelt er delegert til dem. Behandlingsansvaret ble angitt til å ligge hos ledelsen i 10 av de 50 prosjektene. Dette gjelder selv om forskerne har store problemer med å forklare hvilket ansvar som etter loven er lagt til den behandlingsansvarlige.

Datatilsynet fikk forståelsen av at forskerne gjerne påtar seg behandlingsansvaret, med bakgrunn i deres nærhet til selve forskningsprosjektet og eventuelle respondenter. Videre fikk Datatilsynet forståelsen av at mange forskere i praksis opplever manglende styring fra ledelsen hva angår forskning, og derfor føler at ansvaret i realiteten påhviler dem.

2.2.2. Ansvaret kan delegeres internt

At ledelsen er behandlingsansvarlig utad er ikke til hinder for at ivaretagelsen av behandlingsansvaret delegeres internt i virksomheten.

¹² I praksis er det likevel lite som tyder på at ledelsen er sitt ansvar bevisst. Det vises her til pkt. 3 om internkontroll

Den interne ansvars plasseringen vil Datatilsynet sjelden ha synspunkter på. Det tilsynet er opptatt av er at det skal foreligge klare ansvarsforhold knyttet til forskningen. I dette ligger både at ledelsen har orientert seg om hvilke plikter som følger med ansvaret og at arbeidet med å ivareta disse pliktene tydelig er plassert/delegert i organisasjonen.

2.2.3. Kort om studentprosjekter

Tilsynene viste at ansvarsforholdet ved studentprosjekter var uklart. Ansvaret var på ulike steder plassert hos faglig veileder, studenten selv eller hos lærestedet. Manglende klarhet rundt ansvaret medførte i flere tilfeller manglende kontroll med de personopplysningene som var benyttet i studentprosjektet.

Dersom et lærested lar studentene legitimere seg utad som representanter for virksomheten¹³, for eksempel i sin kontakt med deltagere/respondenter og Datatilsynet, vil Datatilsynet forholde seg til virksomheten som behandlingsansvarlig.

Tre læresteder har problemer med å se at de har behandlingsansvaret for studentprosjekter. Det ble fra lærestedene anført at de har dårlige muligheter for faktisk kontroll med studentene og deres gjøremål. Blant annet vises det til at studentene ikke er underlagt virksomhetens instruksjonsmyndighet.

Studentene utfører forskningsprosjekter som et ledd i sin utdanning som lærestedene har det overordnede ansvaret for, herunder oppstilling av hvilke krav som må oppfylles for å oppnå ulike utdannelsesgrader. Gjennomføring av mer eller mindre omfattende prosjektarbeid omfattes ofte av slike krav, hvilket hentyder at lærestedene har et ansvar også her.

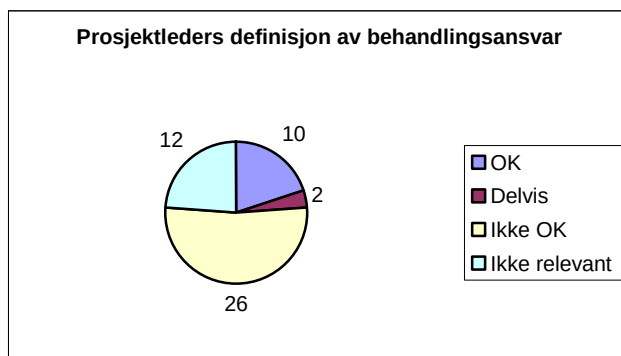
¹³ For eksempel ved bruk av brevpapir fra virksomheten eller kosignatur fra faglig veileder med tilknytning til virksomheten

2.3. Konklusjoner

Datatilsynets generelle inntrykk er at ansvarsforholdene rundt forskningsprosjektene er uklare, internt i de kontrollerte virksomhetene. Selv om ledelsen hevder å ha ansvaret, er forskerne normalt av den oppfatning at ansvaret påhviler dem.

Virksomhetsledelsen må definere en ansvarsstruktur, hvor det interne ansvaret for forskningsvirksomheten plasseres. Det må gis klare føringer for det forskningsarbeidet som skal finne sted i virksomheten, for eksempel gjennom et internkontrollsystem.

Lærestedene og andre må se nærmere på deres muligheter for kontroll med studentprosjekter. I den utstrekning man finner at det ikke er mulig å holde tilfredsstillende kontroll med studentprosjektene, må det i større grad vurderes hvilke prosjekter som kan aksepteres gjennomført av studenter i virksomhetens regi. Uavhengig av dette må det klargjøres hvem som er faglig ansvarlig for prosjektet og hvem som er behandlingsansvarlig, herunder om dette ønskes plassert på samme sted i virksomheten.



3. Internkontroll – funn og tendenser

Det påhviler den behandlingsansvarlige å ha et system for internkontroll for å sikre at pliktene etter personopplysningsloven og helseregisterloven blir overholdt¹⁴.

Kravet til at det skal foreligge et internkontrollsystem er absolutt. Men internkontrollsystemet skal være individuelt tilpasset til den enkelte virksomhetens art og størrelse, og må i tillegg ta hensyn til hvilke behandlinger av personopplysninger som finner sted.

3.1. Internkontrollsystemet brukt i praksis, med særlig vekt på forskning

Bare en av 29 behandlingsansvarlige kunne dokumentere et tilnærmet fullstendig implementert internkontrollsystem som også regulerer virksomhetens behandlinger av person- og helseopplysninger både i forskning og på andre områder. I et annet tilfelle er internkontrollsystemet tilrettelagt med henblikk på behandling av opplysningene også i forskningsøyemed, men systemet var ikke tilfredstillende implementert.

De fleste av virksomhetene forklarer fravær av internkontroll med mangel på nødvendige ressurser, herunder mangel på kunnskap om personopplysningslovens og helseregisterlovens krav til internkontroll.

Et lærested mente at det ville bli vanskelig å få implementert et internkontrollsystem knyttet til forskning. De anførte at prinsippet om fri forskning står så sterkt blant forskerne at de ikke vil la seg underordne virksomhetens rutiner. Under Datatilsynets intervjuer med forskerne fremkom det likevel at de har behov for, og et sterkt ønske om, rutiner knyttet til blant annet informasjonssikkerhet.

3.2. Særlig om internkontroll i virksomheter som har inngått avtale med Norsk samfunnsvitenskaplig datatjeneste (NSD)

En rekke behandlingsansvarlige forklarte manglende internkontroll for forskning med at de har inngått avtale med NSD som personvernombud for forskning. Ledelsen synes å ha den oppfatningen at de gjennom sin avtale med NSD har delegert bort ivaretagelsen av alle de plikter som påhviler den behandlingsansvarlige knyttet til forskning.

Det skal her bemerkes at NSD sin standardkontrakt om personvernombud for forskning, etter Datatilsynets vurdering, ikke innebærer at det fulle ansvaret for kontroll med forskningsprosjekter delegeres til ombudet. Det påhviler virksomhetens ledelse å ivareta hoveddelen av dette ansvaret gjennom sitt øvrige internkontrollsystem¹⁵.

¹⁴ Innholdet i plikten er nærmere beskrevet i vedlegg A, pkt. 2.2.

¹⁵ Jf. pkt. 9 om virkningen av at det er opprettet personvernombud for forskning

En virksomhet bekrefter overfor NSD at de har implementert et internkontrollsystem, idet de inngår avtale med NSD som personvernombud for forskning. Virksomheten må i tillegg bekrefte dette overfor Datatilsynet før tilsynet kan gjøre vedtak om fritak fra meldeplikten basert på opprettelsen av et personvernombud. Vårens tilsyn viser at den egenerklærte internkontroll i de langt fleste tilfeller likevel ikke finnes. Dette innebærer at både Datatilsynets vedtak om fritak fra meldeplikten ved opprettelse av personvernombud og avtalen mellom virksomheten og NSD er basert på uriktige opplysninger fra den behandlingsansvarlige. Datatilsynet ser alvorlig på dette.

3.3. Konklusjoner

Det er, med få unntak, svært dårlig internkontroll med de forskningsprosjektene som gjennomføres hos de behandlingsansvarlige som det er ført tilsyn med.

Det interne ansvaret legges i stor grad til den enkelte forskeren. Dette gjøres uten at det er tydeliggjort overfor vedkommende gjennom formell delegasjon, uten at forsker gis nødvendige retningslinjer for hvordan ansvaret skal ivaretas og uten at det fra ledelsens side føres noen form for kontroll med at ansvaret faktisk blir ivaretatt på en tilfredsstillende måte.

Dette medfører samtidig store muligheter for tilfeldig oppstart av forskningsprosjekter der personopplysninger benyttes i stor utstrekning uten at dette er innenfor ledelsens kontroll.

Hva angår forskning spesielt er det særlig uheldig at det ikke finnes rutiner for å fange opp hvilke vilkår som gjelder for det enkelte forskningsprosjektet, og for å påse at vilkårene faktisk blir fulgt. Det er også uheldig at det ikke foreligger rutiner for å sikre at de registrertes rettigheter i prosjektet blir ivaretatt.

For de virksomheter som ikke har et internkontrollsystem, men som likevel har inngått avtale med NSD om personvernombud for forskning, vil Datatilsynet måtte vurdere å oppheve sitt vedtak om fritak fra meldeplikt. Det vises her til at vedtaket er basert på den uriktige forutsetningen om at virksomheten har et internkontrollsystem.

4. Plikten til å sørge for et behandlingsgrunnlag – funn og tendenser

Personopplysningslovens og helseregisterlovens utgangspunkt er at det er forbudt å behandle helse- og andre personopplysninger. Slik behandling er bare tillatt dersom man har et behandlingsgrunnlag¹⁶.

Der er særlig to grunnlag som er brukt i forbindelse med forskning:

- At det foreligger et informert og aktivt samtykke fra den det behandles opplysninger om (respondenten eller deltageren).
- At det foreligger samfunnsinteresser som nødvendiggjør behandlingen, og som klart overstiger de ulempene behandlingen medfører for den enkelte (respondenten eller deltageren).

4.1. Særlig om samtykke¹⁷

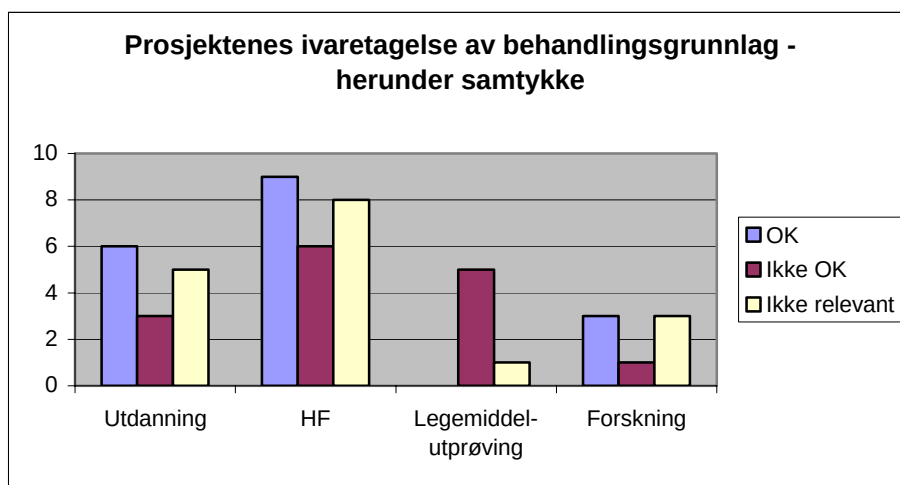
For at et samtykke skal være gyldig oppstiller loven som vilkår blant annet at den som samtykker skal være informert om alle sider ved behandlingen. Datatilsynet stiller ofte konsesjonsvilkår om den konkrete utformingen av informasjonsskriv for å sikre at alle relevante opplysninger kommer frem.

I praksis viser det seg at det ofte skjer endringer underveis i prosjektet, som for eksempel forsinkelser eller andre forlengelser. For at samtykket fremdeles skal være gyldig, må deltageren som hovedregel informeres om disse endringene. Hvorvidt informasjonsplikt utløses, må ses i sammenheng med den aktuelle endringens omfang. Samtykke kan derfor sies å være et behandlingsgrunnlag som krever en viss omsorg fra den behandlingsansvarlige, også underveis i et forskningsprosjekt.

¹⁶ Jf. personopplysningslovens § 11 jf. §§ 8 og 9 og helseregisterlovens § 5

¹⁷ Datatilsynet har ikke vurdert gyldigheten av andre behandlingsgrunnlag enn samtykke i denne tilsynsomgangen

Av de 50 prosjektene hadde 18 et tilfredstillende behandlingsgrunnlag på plass, mens 15 prosjekter manglet behandlingsgrunnlag for sin forskning¹⁸. Dette innebærer at nær halvparten av alle de prosjektene som ble kontrollert mangler et gyldig behandlingsgrunnlag.



I tre samtykkebaserte prosjekter viste det seg å ha skjedd så store endringer etter at samtykket ble innhentet, at det kan stilles spørsmål ved om det opprinnelige samtykket fremdeles er gyldig som behandlingsgrunnlag. I disse tilfellene vil Datatilsynet gi pålegg om at respondentene informeres om endringene, samtidig som de gjøres oppmerksom på at de har rett til å trekke seg fra prosjektet.

4.2. Konklusjoner

Datatilsynets erfaring er at man ved oppstart er opptatt av å tilfredsstille alle kravene til et gyldig behandlingsgrunnlag. Dersom behandlingen baseres på samtykke er forskere derimot ikke oppmerksomme på at endringer i prosjektet ofte medfører krav om ny informasjon til respondenter for at det avgitte samtykket fortsatt skal ha status som et gyldig behandlingsgrunnlag. Manglende innsikt medførte at flere av de kontrollerte prosjekter per i dag i realiteten er uten et gyldig behandlingsgrunnlag, hvilket er i strid med personopplysningslovens § 11 bokstav a.

¹⁸ De resterende 17 er ikke målbare i denne sammenheng

5. Konsesjons- og meldeplikt – funn og tendenser

Forskningsprosjekter hvor det gjøres bruk av personopplysninger er som hovedregel melde- eller konsesjonspliktige. Datatilsynets konsesjonsbehandling er en forhåndskontroll av om forskningsprosjektet kan gjennomføres som forutsatt i henhold til gjeldende regelverk. Ofte settes det vilkår for gjennomføringen for å bringe prosjektet innenfor lovverkets rammer. Prosjekter som meldes underlegges ingen behandling eller godkjenning, men registreres direkte i en offentlig database over behandlinger av personopplysninger.¹⁹

5.1. Forståelse av konsesjons- og meldesystemet

En rekke av de behandlingsansvarlige var av den oppfatning at Datatilsynet saksbehandler de meldingene som kommer inn, slik at meldte behandlinger er godkjente av Datatilsynet.

5.2. Overholdelse av melde- og konsesjonsplikt

Datatilsynet har ved tilsynene konsentrert seg om forskningsprosjekter som er gitt konsesjon eller er meldt til oss eller personvernombudet.

Det er i liten grad gjort forsøk på å avdekke hvorvidt det finnes forskningsprosjekter ved virksomhetene som ikke er lagt frem for oss eller personvernombudet. Ved en tilfældighet ble det likevel avdekket to konsesjonspliktige forskningsprosjekt som det ikke er søkt om konsesjon for etter helseregisterloven og personopplysningsloven. En forsker ga også inntrykk av at prosjekter som de anser å være kvalitetssikring ble vurdert til å falle utenfor personopplysningslovens og helseregisterlovens saklige virkeområde.

Datatilsynet har under tilsynet sett på meldte prosjekter og vurdert om disse i stedet skulle ha vært underlagt konsesjonsbehandling. Det er ikke funnet noen meldte prosjekter som har vist seg å være konsesjonspliktig på meldetidspunktet.

At det skal foreligge et samtykke er et absolutt vilkår for fritak fra konsesjonsplikt for forskningsprosjekter etter personopplysningsforskriftens § 7-27. I tre konkrete prosjekter viste det seg at det opprinnelige samtykket ikke lenger er gyldig, som følge av senere endringer i prosjektet²⁰. Rent formelt oppstår det konsesjonsplikt for prosjektet idet samtykket faller bort. Men i stedet for å pålegge den behandlingsansvarlige å søke konsesjon, velger Datatilsynet å gi pålegg om at respondentene skal få informasjon om endringene og minnes om muligheten til å trekke seg fra prosjektet.

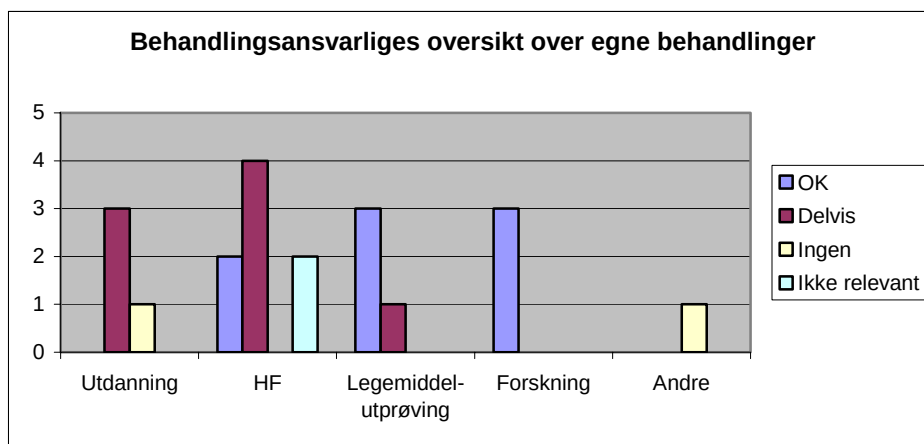
¹⁹ For en nærmere redegjørelse av konsesjons- og meldeplikten vises det til vedlegg A, pkt. 2.8.

²⁰ Jf. pkt. 4

5.3. Konklusjoner

Datatilsynet har gjennom vårens tilsyn ikke fått et dokumentert grunnlag for å kunne si noe om i hvilken grad eksisterende forskningsprosjekter faktisk meldes eller legges frem for konsesjonsbehandling. Med bakgrunn i den gjennomgående mangel på internkontroll som er avdekket på dette området, er det likevel grunn til å tro at det foreligger en viss grad av underrapportering. Flere behandlingsansvarlige ga også selv uttrykk for at det trolig fantes forskningsdata/registre fra eldre og nyere tid, herunder personopplysninger, lagret i virksomhetens system. Dette er opplysninger som ledelsen ikke har kontroll over eller på annen måte kjenner til eksistensen av.

Av 18 relevante behandlingsansvarlige, har to oppgitt at oversikt mangler, åtte har oppgitt delvis oversikt og åtte at de har fullstendig oversikt.



Når et forskningsprosjekt først legges frem for Datatilsynet eller personvernombudet, viser resultatene fra tilsynene at prosjektene behandles riktig, med tanke på melde- og konsesjonsplikt. Datatilsynet antar at dette har sammenheng med en utstrakt bruk av personvernombud for forskning som bistår forskeren i å vurdere prosjektet også med tanke på melding og konsesjon.

6. Konesesjonsvilkår – funn og tendenser

Det finnes to ulike typer konsesjonsvilkår.

Den ene typen er vilkår som i utgangspunktet følger direkte av loven, men som Datatilsynet har sett seg nødt til å presisere i konsesjonsvedtaket (uegentlige konsesjonsvilkår). Som eksempel på et uegentlig konsesjonsvilkår nevnes at det settes vilkår om at det må foreligge et samtykke²¹. Slike vilkår er svært mye brukt i Datatilsynets praksis.

Den andre typen er vilkår som ikke følger av loven, men som Datatilsynet har satt etter en skjønnsmessig vurdering for å begrense ulempene behandlingen ellers ville medføre for den enkelte (egentlige konsesjonsvilkår), jf. personopplysningslovens § 35 jf. helseregisterlovens § 36. Som eksempel nevnes at det stilles vilkår om at respondentene informeres i større grad enn det som følger direkte av loven, og at den behandlingsansvarlige pålegges en plikt til å bekrefte skriftlig overfor Datatilsynet hvert tredje år at behandlingen foretas i samsvar med lov og konsesjonsvilkår. Datatilsynet bruker få vilkår av denne typen, men de vilkår som benyttes, går ofte igjen i de utstedte konsesjonene.

I det følgende omhandles begge typer konsesjonsvilkår.

6.1. Etterlevelse av konsesjonsvilkårene i praksis

Datatilsynet har i sin praksis valgt å stille konsesjonsvilkår knyttet til gjennomføringen av et prosjekt for å få det innenfor lovverkets rammer, snarere enn å avslå konsesjonssøknaden fullstendig. Således er konsesjonsvilkår ansett å være et smidig verktøy i konsesjonsbehandlingen, hvilket også kommer forskerne til gode.

I 17 prosjekter kontrollerte Datatilsynet etterlevelsen av konsesjonsvilkår. I 11 av disse ble vilkårene ikke fulgt, uten at forsker kunne gi noen god forklaring på dette.

At konsesjonsvilkårene synes å etterleves i bare 6 av 17 tilfeller er et nedslående resultat. Datatilsynet har fått forståelsen av at manglende etterlevelse stort sett skyldes manglende oppmerksomhet rundt vilkårene, altså glemsomhet eller slurv.

I to tilfeller hevdet forskerne at de ikke forstod vilkåret. Forskerne kunne ikke gi noen god forklaring på hvorfor de ikke har tatt kontakt med Datatilsynet for å få vilkåret forklart.

I to andre tilfeller ble det innrømmet at forskerne ikke etterlevde vilkåret fordi de var uenige i Datatilsynets vurdering. Forskerne kunne ikke gi noen god forklaring på hvorfor de ikke har benyttet sin adgang til å klage på konsesjonsvedtaket. Slike forhold ser Datatilsynet alvorlig på.

²¹ For eksempel at det må hentes inn samtykke fra deltagerne

6.2. Konklusjoner – funn og tendenser

De tilsynene som ble foretatt viser at konsesjonsvilkårene i liten grad følges når forskningsprosjektene skal iverksettes. Dette kan tvinge Datatilsynet til å vurdere sin praksis, slik at prosjekter som (i henhold til innsendte dokumentasjon) ikke ligger innenfor lovens grenser blir avslått. Det er dermed opp til den behandlingsansvarlige å beskrive et prosjekt som kan gjennomføres innenfor lovens rammer, ikke Datatilsynet.

Datatilsynet ser en klar sammenheng mellom manglende internkontrollsystem og dårlig ivaretagelse av konsesjonsvilkår. Når det ikke er etablert rutiner for kontroll med hvilke vilkår som stilles for et prosjekt, og for å påse at konsesjonsvilkårene faktisk etterleves, vil etterlevelsen derfor bero på den enkelte forskers ryddighet eller respekt for regelverket.

Datatilsynet kan ikke se at konsesjonsvilkårene overholdes i større grad, i de tilfeller hvor det er oppnevnt et *eksternt* personvernombud for forskning. Tvert imot har Datatilsynet inntrykk av at det fremstår som uklart for disse virksomhetene om ansvaret for slik oppfølging er delegert til personvernombudet eller om det må ivaretas av virksomheten selv. Den virksomheten hvor det er opprettet et *internt* personvernombud for forskning skilte seg imidlertid positivt ut i denne forbindelse²².

²² Se for øvrig pkt. 9 om bruk av personvernombud for forskning

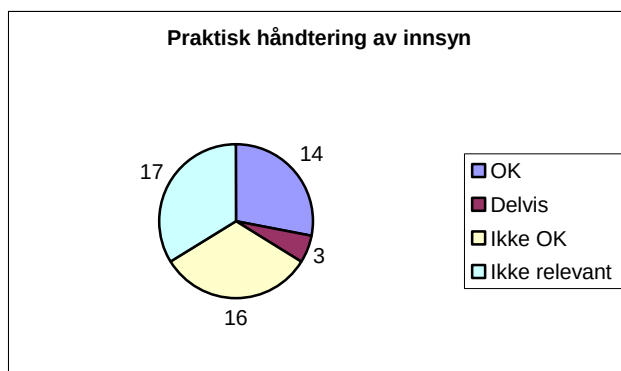
7. Den registrertes rettigheter – funn og tendenser

Personopplysningsloven og helseregisterloven gir den registrerte en rekke rettigheter, herunder rett til informasjon, innsyn, retting og rett til å få opplysningene slettet. Den behandlingsansvarlige har plikt til å ivareta disse rettighetene.

7.1. Ivaretagelsen av disse rettighetene i praksis

Bare unntaksvis forelå det dokumenterte rutiner i virksomheten knyttet til ivaretagelse av den registrertes rettigheter etter loven. Det vises her til kapittel 3 om internkontroll.

På Datatilsynets spørsmål om hvordan henvendelser vedrørende innsyn, retting og sletting har blitt, eller ville ha blitt håndtert, gav omtrent halvparten av prosjektlederne tilfredsstillende svar. Som eksempel kan nevnes at det i 14 av 33 relevante prosjekter ble besvart tilfredsstillende på spørsmål om hvordan innsyn har blitt, ble eller vil bli håndtert.



Forskere som er utdannet helsepersonell synes gjennomgående å ha større kunnskap om den registrertes rettigheter enn andre forskere. Dette henger trolig sammen med at innsyn, retting og sletting også er pasientrettigheter som vedkommende kjenner til fra sitt arbeid med pasientbehandling.

Dersom tilsynsobjektet er omfattet av personopplysningslovens saklige virkeområde, vil det være unntak fra retten til innsyn dersom personopplysningene utelukkende behandles til vitenskaplige formål og behandlingen ikke får noen direkte betydning for den registrerte, se personopplysningslovens § 18, siste ledd.

7.2. Konklusjon

Datatilsynet har avdekket en gjennomgående mangel på dokumenterte rutiner for oppfyllelse av deltageres rettigheter. Den daglige håndteringen av disse pliktene oppleves dog som tilfredsstillende, med unntak av forholdet til sletting²³.

²³ Det vises her til pkt. 8 i denne rapporten

8. Sletting eller anonymisering ved prosjektslutt – funn og tendenser

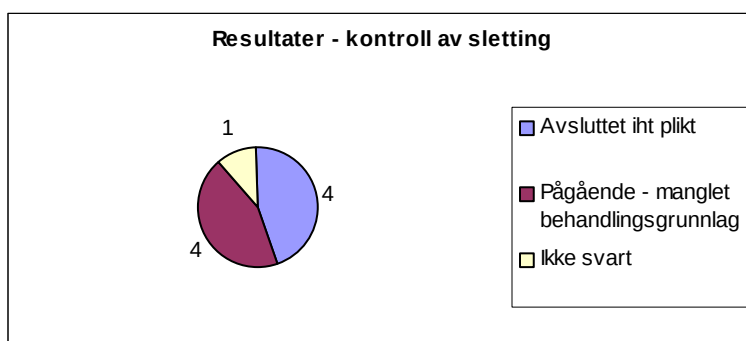
8.1. Generelt

Personopplysningsloven og helseopplysningsloven oppstiller et forbud mot å oppbevare personopplysninger lengre enn det som er nødvendig for å gjennomføre formålet med behandlingen²⁴. Sletteplikten gjelder likevel ikke dersom det foreligger oppbevaringsplikt i henhold til annen lovgivning²⁵.

Personopplysninger som inngår i et forskningsprosjekt skal normalt slettes eller anonymiseres senest når prosjektet er avsluttet dersom respondentene ikke har samtykket til videre lagring²⁶.

Datatilsynet har gjennomført ni tilsyn som bare tok for seg overholdelse av sletteplikten. Dette er prosjekter som i henhold til Datatilsynets opplysninger skal være avsluttet, og hvor det ikke er søkt om forlenget konsesjon eller gitt informasjon til personvernombudet om at prosjektet ønskes forlenget.

Fire av ni behandlingsansvarlige opplyste at personopplysningene som inngikk i angjeldende forskningsprosjekt er slettet. For fire prosjekter ble opplysningene fremdeles oppbevart uten at behandlingsgrunnlaget var på plass²⁷. I hovedsak skyldes dette at prosjektene ikke er ferdigstilt innen den opprinnelige tidsrammen. Tilsynene ble gjennomført ved en skriftlig forespørsel til den behandlingsansvarlige. Resultatene er ikke søkt verifisert gjennom et stedlig tilsyn.



Utover de egne slettetilsynene har Datatilsynet i liten grad gjort undersøkelser med tanke på overholdelse av sletteplikten.

²⁴ Personopplysningslovens § 11 bokstav e jf. § 28, og helseregisterlovens § 11 jf. § 27

²⁵ For eksempel forskrift om klinisk utprøving av legemidler og journalforskriften

²⁶ For eksempel i påvente av en oppfølgingsundersøkelse. Her stilles det ofte vilkår om at opplysningene skal aidentifiseres for forsker, og at personidentifiserbare data skal oppbevares ved en arkivinstitusjon (for eksempel NSD).

²⁷ Den siste brevkontrollen er foreløpig ikke blitt besvart

8.2. Særlig om sletteplikten ved legemiddelutprøving

I henhold til forskrift om klinisk utprøving av legemidler til mennesker foreligger det en oppbevaringsplikt som gjelder i 15 år fra behandlingen avsluttes. Idet oppbevaringsplikten opphører inntreffer imidlertid sletteplikten i henhold til personopplysningsloven og helseregisterloven.

Koblingsnøkkelen som gjør dataene identifiserbare befinner seg hos deltagerens behandlende lege. Det er likevel utprøver, som behandlingsansvarlig, som må påse at koblingsnøkkelen makuleres. Dette gjøres praktisk ved at det for eksempel inntas en instruks om sletting i databehandleravtalen mellom utprøver og den behandlende lege.

I forbindelse med tilsyn hos fire virksomheter som bedriver klinisk utprøving av legemidler fremstod det uklart hvorvidt disse var klar over sletteplikten. Deres fokus var på oppbevaringsplikten.

I bare ett tilfelle var sletteplikten omhandlet i virksomhetens internkontrollsystem.

8.3. Konklusjon

Tilsynene viser at de behandlingsansvarlige har problemer med å overholde den opprinnelige dato for prosjektavslutning, og at de har et lite bevisst forhold til hvilke krav som stilles når det er aktuelt å utvide prosjektperioden.

Tilsynene viser en gjennomgående dårlig ivaretagelse av sletteplikten, også i de tilfeller hvor prosjektet faktisk er avsluttet innen den opprinnelige fristen. Med en gjennomgående mangel på internkontroll hos de behandlingsansvarlige er det grunn til å tro at det foreligger store mørketall på dette området.

9. Personvernombud for forskning²⁸ – funn og tendenser

Behandlingsansvarlige som oppretter personvernombud vil kunne få fritak for meldeplikten etter personopplysningslovens § 31²⁹, jf. bestemmelsens siste ledd. Det blir opp til personvernombudet å føre oversikt over hvilke behandlinger den behandlingsansvarlige gjør. Personvernombudet skal videre ivareta personvernet til de som virksomheten registrerer opplysninger om, herunder for eksempel å bistå ved begjæringer om innsyn, retting og sletting.

Et personvernombud kan være et internt ombud, ansatt i den behandlingsansvarliges virksomhet, eller en ekstern aktør som den behandlingsansvarlige har inngått avtale med. Hvilke oppgaver personvernombudet har reguleres av vedkommendes stillingsbeskrivelse, eller avtale om personvernombud.

Med unntak av legemiddelfirmaene, den privatpraktiserende legen og et helseforetak, har alle de behandlingsansvarlige som er kontrollert i dette tilsynsprosjektet inngått avtale med NSD som personvernombud for forskning. I bare ett tilfelle er personvernombudet ansatt i virksomheten. Kun en av de behandlingsansvarlige hadde opprettet internt personvernombud med forskning som ansvarsområde.

9.1. *Virkningen på personvernet, målt i oppfyllelse av regelverk og konsesjonsvilkår*

9.1.1. Ved prosjektets oppstart

Det er Datatilsynets erfaring fra den løpende konsesjonsbehandlingen at personvernombudene påser at konsesjonssøknader som oversendes er godt gjennomarbeidet, blant annet med tanke på behandlingsgrunnlag, ivaretagelse av den registrertes rettigheter og konsesjons- / meldeplikt. Det er stor forskjell på disse søknadene og de som ikke har vært gjennomarbeidet av et personvernombud

Det er sjelden Datatilsynet gir rene avslag på konsesjonssøknader som er forberedt av et personvernombud. I denne forbindelse spiller det liten rolle om personvernombudet er eksternt eller internt.

Datatilsynet har imidlertid inntrykk av at et internt personvernombud i større grad enn et eksternt klarer å orientere seg om hva som skjer i virksomheten. Slik kan vedkommende av eget initiativ plukke opp forskningsprosjekter som ”flyter” i systemet, og som ikke er meldt eller søkt om konsesjon for. Her spiller det naturligvis en stor rolle at et internt personvernombud har helt andre faktiske muligheter for å ha oversikt over og føre kontroll med forskningsaktiviteten, enn et eksternt personvernombudet har.

²⁸ Med forskning forstås her forskning som inkluderer behandling av helse- og andre personopplysninger

²⁹ Jf. helseregisterlovens § 36

9.1.2. Når prosjektet løper (forskningsperioden) og ved prosjektavslutning

Datatilsynet har erfart at det jevnt over føres mangelfull kontroll med om konsesjonsvilkårene etterleves, og hvorvidt behandlingen ellers skjer i henhold til fremlagt prosjektbeskrivelse og gjeldende regelverk. Datatilsynet kan ikke se at den løpende oppfølgingen av pågående forskningsprosjekter er bedre i virksomheter som har utnevnt personvernombud for forskning.

I hvilken grad personvernombudet fører kontroll med at lovverket etterleves vil bero på vedkommendes stillingsbeskrivelse (internt ombud) og avtalen (ekstent ombud).

Det skal her bemerkes at NSD sin standardkontrakt om personvernombud for forskning, etter Datatilsynets vurdering, ikke medfører at ansvaret for slik løpende kontroll delegeres til ombudet. Det påhviler den behandlingsansvarlige å ivareta dette ansvaret, gjennom sitt internkontrollsystem, på vanlig måte.

Den faktiske muligheten til å følge opp forskningsprosjekter vil trolig variere etter hvorvidt personvernombudet er plassert internt i virksomheten eller om det er en ekstern samarbeidspartner. Til tross for etableringen av et internt personvernombud, var konsesjonsvilkårene heller ikke etterlevd i to av de tre kontrollerte prosjektene også i denne virksomheten,

9.2. Konklusjoner

Datatilsynet er av den oppfatning at personvernombudsordningen synes å fungere svært godt i forbindelse med oppstart av nye prosjekter.

I prosjektperioden og ved prosjektavslutning har ombudsordningen liten eller ingen betydning, spesielt ved benyttelse av et eksternt personvernombud. Dette har trolig å gjøre med at det mest brukte personvernombudet for forskning, NSD, normalt ikke påtar seg å føre løpende kontroll med forskningsprosjekter.

Eksterne personvernombud innehar en oversikt over forskningsprosjektene ved virksomheten. Utover dette kan Datatilsynet ikke se at opprettelsen av eksterne personvernombud har noen effekt for virksomhetens internkontroll.

10. Informasjonssikkerhet i forskning

10.1. Premisser

Hovedspørsmålet for vurdering av sikkerheten ved vårens tilsyn har vært forholdet til forskning på aidentifiserte³⁰ personopplysninger. Forskning på direkte identifiserbare opplysninger forekommer som hovedregel kun i særskilte situasjoner, mens bruk av aidentifiserte data er det normale. Utgangspunktet i det følgende er derfor forskning på aidentifiserte personopplysninger.

Informasjonssikkerhet i forskning er i praksis et samspill mellom ledelsens sentrale valg og føringer i form av internkontroll og teknologiske sikkerhetstiltak, og den enkelte forskers kunnskap om disse føringene og regelverket ellers.

10.2. Sikkerhetsmessige aspekter ved tilsynsarbeidet

Tilsynsprosjektet har hatt fokus på følgende problemstillinger vedrørende informasjonssikkerhet:

- Virksomhetens generelle kunnskap om sikkerhetsregelverket, herunder tilfredsstillende oppfyllelse av regelverkets dokumentasjonskrav.
- Verifikasjon av virksomhetens implementering av de planlagte styrende, gjennomførende og kontrollerende tiltak.
- Virksomhetens akseptkriterier for behandling av ulike opplysninger i forskning.
- Virksomhetens gjennomføring av aidentifisering.
- Virksomhetens konfigurasjon og konfigurasjonskontroll .
- Virksomhetens kontroll med datalagring og sletting i forskning.

10.3. Forskning på aidentifiserte opplysninger

10.3.1. Generelt om aidentifisering

For forskning på aidentifiserte personopplysninger kan sikkerhetsfokuset flyttes fra selve datasettet til koblingsnøkkelen.

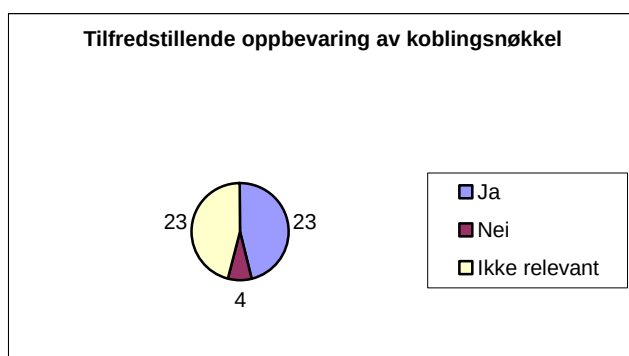
³⁰ For mer om aidentifiserte opplysninger, se Vedlegg A pkt. 1 og pkt. 2.7.

De to viktige elementene i denne sammenheng er:

- hvorvidt koblingsnøkkelen oppbevares tilstrekkelig atskilt fra datasettet. Manuelle koblingsnøkler som er nedlåst separat vil normalt oppfylle kravet om tilfredstillende atskillelse fra det resterende datamaterialet. Oppbevares derimot koblingsnøkkelen på samme lagringsmedium som datasettet, vil dette sjelden anses tilfredstillende.
- hvorvidt avidentifiseringen er reell. Dersom opplysningene ikke kan regnes som avidentifiserte, vil opplysningene fremdeles ha et høyt beskyttelsesbehov.

10.3.2. Konklusjoner basert på tilsynserfaringer

Koblingsnøkkelen oppbevares ofte manuelt i form av en liste, tilstrekkelig atskilt fra datasettet. Av 27 relevante prosjekt betraktet Datatilsynet håndteringen av koblingsnøkler til å være forsvarlig i 23 av prosjektene.



Det er dog avdekket enkelte graverende unntak:

- I minst tre tilfeller var koblingsnøkkelen skrevet i en datafil som ble lagret på samme området som forskningsdataene.
- I et tilfelle inneholdt datasettet direkte identifiserende opplysninger. Disse ble først fjernet ved oversendelse av de samme data til det nordiske hovedprosjektet.

Håndtering av koblingsnøkler har så stor betydning for informasjonssikkerheten at det må holdes et stadig fokus på dette spørsmålet.

Det er generelt lav kunnskap om hva som anses som avidentifiserte til forskjell fra anonyme opplysninger. Dette er erfart gjennom stedlige tilsyn hvor det ofte har vært nødvendig å forklare begrepene. Av 27 relevante prosjekt betrakter Datatilsynet avidentifiseringen til å være ikke tilfredstillende i 10 av prosjektene. Dette anses som alvorlig, ikke minst fordi sikringen av det antatt avidentifiserte datasettet ofte ikke vil være tilfredstillende når dataene i realiteten er identifiserbare.

10.4. Sikkerhetsbehov

10.4.1. Valg av akseptabel risiko

Personopplysningsforskriftens kapittel 2 stiller krav om et styringssystem for informasjonssikkerhet med systematisk bruk av risikovurderinger hvor resultatet måles opp mot fastlagte kriterier (akseptkriterier). Ledelsens dokumenterte sikkerhetsvalg er en del av virksomhetens internkontrollsystem.

Det var i tilsynene et mål å se hvilke valg virksomhetens ledelse hadde tatt for forskningsaktivitet spesielt, herunder hvordan aidentifisering skal utføres og hvordan aidentifiserte data og koblingsnøkkelen skal håndteres.

Når det gjelder ledelsens akseptkriterier var ønsket å se hvilket beskyttelsesbehov de ulike delene av forskningsdataene var tillagt. Det nevnes at Datatilsynet har hjemmel til å overprøve virksomhetens akseptkriterier dersom de finnes utilstrekkelige.

10.4.2. Konklusjoner basert på tilsynserfaringer

Virksomheten hadde med få unntak ikke gjort selvstendige vurderinger av akseptkriterier for forskningsaktiviteten. Videre har tilsynene gitt oss følgende erfaringer:

- Helseforetakene har kommet langt med å fastsette akseptkriterier for elektronisk pasientjournal. I de fleste tilfeller var disse imidlertid ikke tilpasset forskningsaktivitet. Denne manglende tilpasningen medfører at forskerne ikke har et relevant regelverk å følge internt, og at det eksisterende interne regelverket brytes.
- Innen legemiddelutprøving er det i stor grad internasjonale virksomheter som benytter risikovurdering som et sentralt element i virksomhetens faglige arbeidsmåte. Dette medfører praktiske løsninger / akseptkriterier som kan godtas uten at grunnlaget var personopplysningsforskriftens kapittel 2.
- Innen andre virksomheter enn helseforetak og legemiddelutprøving har man kommet kort med utviklingen av internkontrollsystem, og følgelig mangler akseptkriterier. Dette har medført mange pålegg.

10.5. Teknologiløsninger.

10.5.1. Valg av teknologiløsninger

Systemløsninger og programvare for forskning har en spesiell karakter med særegne tekniske behov, slik at det ikke er en selvfølge at virksomhetens generelle konfigurasjon er tilfredstillende for forskningsaktiviteten. Ofte har disse behovene vært løst ved at det benyttes dedikert utstyr til forskningsaktiviteten fremfor virksomhetens ordinære informasjonssystem.

Datatilsynet har dessuten gjennom mange år stilt vilkår om at forskning skal skje i "fysisk isolert system". Dette vilkåret har også vært brukt i den senere tid der det har manglet en tilfredstillende sikkerhetsløsning / sikkerhetsdokumentasjon av informasjonssystemet. Med

fysisk isolert system menes et informasjonssystem som ikke er tilknyttet andre systemer, eksempelvis virksomhetens administrative nettverk eller Internett.

Med denne bakgrunn er det nødvendig at virksomhetene gjør selvstendige valg vedrørende konfigurasjon, og sørger for å tilrettelegge slik at valgene gir tilfredstillende informasjonssikkerhet.

10.5.2. Konklusjoner basert på tilsynserfaringer

Innledningsvis må det presiseres at begrepet ”fysisk isolert system” ofte ikke forstås i sin rette forstand av forskere.

Det er høyst variabelt om virksomheten har gjort overordnede teknologivalg, om valgene er kjent i organisasjonen, og om man på ansvarlig hold har kontroll med om valgene blir fulgt.

Følgende erfaringer er gjort etter tilsynene:

- Innen legemiddelutprøving er det i stor grad internasjonale virksomheter som benytter kontrollert overføring av opplysningene. Tilsynene har ikke avdekket konkrete problemer med teknologiløsningen
- For læresteder er det generelt gitt få føringer om hvordan forskningsdata skal håndteres. Uten at man har oversikt over hvor i informasjonssystemet forskningsdata oppbevares er det vanskelig å sørge for tilfredstillende informasjonssikkerhet.
- I noen forskningsinstitusjoner eksisterer tilrettelagte områder for lagring av ulike dokumenter. Dette kan gi tilfredstillende sikkerhet, men det er ikke tatt generell stilling til hvordan aidentifiserte personopplysninger skal lagres.
- Et av helseforetakene har et tilpasset fastsatt teknologimiljø for forskning. For øvrig er spredningen stor på bruk av privat utstyr, forskningsutstyr, og i et tilfelle lagring i andre virksomheters datasystemer.
- En forskningsinstitusjon tilkjenner at det ikke fantes rutiner for sletting av sikkerhetskopier som inneholder forskningsdata.

Av 31 relevante prosjekt betraktet Datatilsynet 17 til å være utført praktisk forsvarlig, åtte prosjekt var utført delvis forsvarlig, og seks var etter Datatilsyntes oppfatning ikke forsvarlig utført.



Funnene er alvorlige, men kunne ha vært verre med tanke på virksomhetenes manglende tilrettelegging. Konservativ bruk av manuelle koblingsnøkler gjør at mange av datasettene har et lavt sikkerhetsbehov slik at de i denne sammenheng faller innefor betegnelsen ”praktisk forsvarlig”.

11. Faglig oppsummering

Forskning er en spesiell form for behandling av personopplysninger. Ofte forskes det på sensitive personopplysninger innefor tema som enkeltpersonen betrakter som svært følsomme. For å ivareta personvernet kontrolleres forskningsaktiviteter i stor grad gjennom konsesjonspliktens forhåndskontroll.

11.1. Konsesjonsplikt

Tilsynene har vist at det er en rekke avvik også i de behandlinger som har vært gjenstand for en forhåndskontroll. Avvikene fremtrer i form av brudd både mot vilkår stilt i konsesjoner og mot regelverket generelt. Datatilsynet må på bakgrunn av dette vurdere hvorvidt det er hensiktsmessig å fortsatt benytte vilkår i konsesjoner for å korrigere søkeren til å oppfylle sine lovpålagte plikter. Alternativet er at konsesjonssøknaden avslås inntil prosjektet er innenfor regelverket på alle områder³¹. Dette underbygger behovet for fortsatt forhåndskontroll, men også en økt etterkontroll innen forskning, for eksempel i form av brevlige kontroller.

Det bør videre vurderes hvorvidt samtykkebaserte prosjekter der kun aidentifiserte opplysninger gjøres tilgjengelig for forsker, for eksempel via et sentralt helseregister, kan unntas fra konsesjonsplikten. Dette fordi personverntrusselen her vil være liten.

11.2. Meldeplikt³²

Tilsynene har vist at det er en rekke brudd på forutsetningene der meldeplikten trer inn ved unntak fra hovedregelen om konsesjonsplikt. Prosjekt starter som et meldepliktig prosjekt, og kommer siden i konflikt med vilkårene uten at reparerende tiltak iverksettes. Datatilsynet bør avklare hvordan slike situasjoner skal håndteres på en forutsigbar måte. Meldepliktige prosjekter har tydelig et oppfølgingsbehov.

11.3. Personvernombud

Generelt ser man at oppfyllelse av meldeplikten overfor personvernombudet medfører en større grad av kontroll med grunnlaget for behandlingen enn hva en melding til Datatilsynet gjør. Bruken av personvernombud betraktes generelt som personvernforebyggende. Bruk av interne personvernombud hvor dette er hensiktsmessig, gir personvernet ytterligere fordeler, som bedre kontroll med den løpende oppfølgingen av forskningsprosjekter. Datatilsynet bør med denne bakgrunn fortsette arbeidet for å utbrede bruken av personvernombud³³. Ordningen med personvernombud bør videreutvikles og påskyndes.

³¹ Se pkt. 6.2.

³² Se pkt. 5.2 og vedlegg A pkt. 2.8.2.

³³ Se pkt. 9

11.4. Internkontroll

Under tilsynene kontrollerte Datatilsynet hvorvidt virksomhetenes internkontroll kunne sies å være tilpasset forskningsaktivitet. Kun to av de kontrollerte virksomhetene hadde etter Datatilsynets forståelse et internkontrollsystem som tok høyde for forskning. Tilsynene avdekket at bruken av eksternt personvernombud tilsynelatende resulterer i at virksomhetene selv ikke ivaretar sine plikter etter regelverket i form av å ha et etablert internkontrollsystem. Generelt ser Datatilsynet et behov for informasjon på området internkontroll.

11.5. Sletting

Forskningsetikken påberopes som grunnlag for å oppbevare forskningsdata lenger enn det som er nødvendig for å kunne gjennomføre forskningsprosjektet. Oppbevaringen anses blant annet nødvendig for å kunne forsvare det faglige innholdet i forskningsresultatet³⁴. Datatilsynet vil se nærmere på dette i forhold til krav om behandlingsgrunnlag for videre oppbevaring, herunder praktiske løsninger på dette problemet.

11.6. Ulike former for personopplysninger

Definisjonene og forskjellene på indirekte identifiserbare data, aidentifiserte data og anonyme data er gjennomgående misforstått hos de behandlingsansvarlige. Dette er grunnleggende definisjoner i Datatilsynets arbeid, og enkelt informasjonsmateriale bør utformes på dette området.

Innen legemiddelutprøving er det uttrykt et faglig behov for å ta med parametre i forskningsmaterialet som samlet sett kan være indirekte identifiserende. Det er et behov for å komme til akseptable normer for hvilke parametre som kan følge datasettene slik at de fremdeles kan betraktes som aidentifiserte, for eksempel gjennom dialog med legemiddelindustrien.

11.7. Hovedanbefaling

Overordnet viser tilsynene at det generelt er et stort behov for informasjon og kompetanseheving i forhold til personvernlovgivningens krav. Dette gjelder både i de behandlingsansvarlige virksomheter generelt og for de som arbeider konkret med forskning.

³⁴ Det henvises i den sammenheng til Vancouver-traktaten.

Vedlegg A:

Behandling av helseopplysninger i forskning – Generelt om regelverket

Versjon 1.02 - 30.06.2004

Prosjektgruppe for tilsyn innen helsesektoren:

Juridisk rådgiver Hanne P. Gulbrandsen

Juridisk rådgiver Cecilie L. B. Rønnevik

Juridisk rådgiver Monica Fornes

Juridisk rådgiver Rune Vidar Bråthen

Senioringeniør Johan Braar Larsen

Avdelingsingeniør Helge Veum

Innholdsfortegnelse

1. Innledning	3
1.1. Lovverket	3
1.2. Anvendelsesområde	3
2. Lovbestemte krav for behandling av personopplysninger	5
2.1. Hvem er behandlingsansvarlig?.....	5
2.2. Internkontroll.....	5
2.3. Krav om hjemmelsgrunnlag for å kunne behandle sensitive personopplysninger.	6
2.4. Øvrige grunnkrav	7
2.5. Informasjonsplikt.....	7
2.6. Sletting.....	9
2.7. Informasjonssikkerhet	9
2.7.1. Metoder for håndtering personopplysninger i forskning.....	10
2.8. Forhåndskontroll eller etterhåndskontroll?.....	11
2.8.1. Konesjonsplikt	11
2.8.2. Meldeplikt	12

1. Innledning

I det følgende gis en kort redegjørelse for hvilke krav helseregisterloven og personopplysningsloven oppstiller for forskning på helseopplysninger¹.

Datatilsynet har satt ned en prosjektgruppe som skal skrive en veileder rettet mot forskning. Denne er ventet å bli ferdig i løpet av høsten 2004.

1.1. Lovverket

Personopplysningsloven trådte i kraft 1. januar 2001, og avløste den tidligere personregisterloven. Det ble vedtatt overgangsregler for behandlinger som hadde konsesjon etter personregisterloven, slik at personopplysningsloven gjaldt fullt ut fra 1. januar 2003. Personopplysningsloven er en generell lov for behandling av personopplysninger som skjer helt eller delvis med elektroniske hjelpemidler, eller personopplysninger som skal inngå i et manuelt personregister. Loven gjelder i den utstrekning den aktuelle behandlingen ikke er regulert i egen særlovgivning.

Helseregisterloven trådte i kraft 1. januar 2002, og er en særlov for behandling av helseopplysninger i helseforvaltningen og helsetjenesten. Personopplysningsloven og personopplysningsforskriften supplerer helseregisterloven der denne er taus².

1.2. Anvendelsesområde

Avgjørende for om ovennevnte lover kommer til anvendelse er hvorvidt det behandles personopplysninger. Med personopplysninger menes *"opplysninger og vurderinger som direkte eller indirekte kan knyttes til en enkeltperson"*, jf personopplysningslovens § 2 nr 1. Helseopplysninger er definert i helseregisterlovens § 2 nr. 1 som *"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"*. Lovene gjelder også aidentifiserte personopplysninger. Helseregisterloven definerer aidentifiserte opplysninger slik: *"helseopplysninger 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"*³. Dette betyr at det ikke alltid vil være tilfredsstillende å bare fjerne de direkte identifiserbare personopplysningene for å kunne anse det resterende datasettet som aidentifisert etter lovens definisjon. Nivået på aidentifiseringen skal være slik at datasettet er anonymt ved makulering av koblingsnøkkelen.

Lovene gjelder også personopplysninger som fremstår å være anonyme, men likevel er knyttet til en så liten gruppe eller satt sammen på en slik måte at identiteten indirekte kan fremkomme. Muligheten for identifikasjon av enkeltpersoner må derfor vurderes nøye ved

¹ Betegnelsen personopplysninger vil bli benyttet i det følgende

² Jf. helseregisterlovens § 36

³ Jf. helseregisterlovens § 2 nr. 2

oppstart av forskningsprosjekter der det benyttes antatt anonyme opplysninger. Kan enkeltpersoners identitet fremkomme gjennom sammenstilling av slike opplysninger, vil disse anses å være indirekte identifiserbare personopplysninger og omfattes av lovverket.

Etter personopplysningsloven / helseregisterloven anses opplysninger for anonyme først når det ikke lenger er mulig å knytte opplysningene tilbake til enkeltpersoner. Slike opplysninger omfattes ikke av lovenes saklige virkeområde.

2. Lovbestemte krav for behandling av personopplysninger

Ansvar for at behandlingen av personopplysninger oppfyller kravene i lovverket ligger til den behandlingsansvarlige⁴. Siden alle pliktene i loven retter seg mot behandlingsansvarlig er det et viktig å finne ut hvem dette ansvaret påhviler etter loven. Ansvar må være klart plassert slik at den registrerte skal kunne få håndhevet sine rettigheter overfor rett behandlingsansvarlig.

Lovens krav gjelder uavhengig av om behandlingen er konsesjons- eller meldepliktig.

2.1. Hvem er behandlingsansvarlig?

Den behandlingsansvarlige er definert i loven som *”den som bestemmer formålet med behandlingen av opplysningene og hvilke hjelpemidler som skal brukes”*⁵. Tilsvarende følger av helseregisterlovens § 2 nr. 8. Behandlingsansvarlig har bestemmelsesrett over opplysningene og den elektroniske behandlingen. Det er den behandlingsansvarlige som står ansvarlig utad for at behandlingen er lovlig, og vil være den som kan saksøkes og pådrar seg straffeansvar for eventuell overtredelse av lovens bestemmelser. Den behandlingsansvarlige må derfor være en som har søksmålskompetanse / sivilprosessuell partsevne. Både fysiske og juridiske personer kan ha partsevne. Den daglige gjennomføringen av behandlingsansvaret kan delegeres.

Følgende momenter er av betydning når det skal avgjøres hvem som er ansvarlig: Hvem som initierer prosjektet, hva respondentene informeres om, om forskerens befatning med behandlingen skjer i egenskap av å være ansatt eller ikke, og hvem som finansierer prosjektet.

Det er viktig å presiseres at personopplysningsloven og helseregisterloven ikke regulerer eiendomsretten til datamaterialet. Behandlingsansvarlig er ikke nødvendigvis den som har eiendomsretten, slik at det blir viktig å skille eierbegrepet fra behandlingsansvaret. Datatilsynet verken kan eller ønsker å ta stilling til spørsmål om eierskap. Det er bruksretten til personopplysningene som er fokus for Datatilsynet og det lovverket tilsynet forvalter.

Deltagerne skal informeres om navn og adresse på behandlingsansvarlig slik at det er klart hvem man skal ta kontakt med for å bruke sine rettigheter, blant annet til innsyn, retting og sletting med mer.

2.2. Internkontroll

Personopplysningslovens § 14, helseregisterlovens § 17 og supplerende bestemmelser i personopplysningsforskriftens kapittel 3 stiller krav om at den behandlingsansvarlige skal

⁴ Databehandlingsansvarlig dersom prosjektet reguleres av helseregisterloven. Heretter behandlingsansvarlig

⁵ Jf. personopplysningslovens § 2 nr. 4 og helseregisterlovens § 2 nr. 8

etablere og holde ved like planlagte, systematiske og dokumenterte tiltak som er nødvendige for å oppfylle kravene i personopplysningsloven og helseregisterloven.

Regelverket oppstiller ingen formelle strukturkrav til hvordan internkontrollsystemet skal utformes, men det er et krav om at tiltakene skal kunne dokumenteres.

Internkontrollsystemet skal tradisjonelt bestå av en styrende, gjennomførende og kontrollerende del. Det er viktig å påpeke at mange virksomheter har et ensidig fokus på rutiner for informasjonssikkerhet, mens kravet til internkontroll også omfatter rutiner knyttet til juridiske forhold som eksempelvis oppfyllelse av innsyn, retting, sletting, innhenting av samtykke, samt ivaretagelse av informasjonsplikt og melde- og konsesjonsplikt.

Virksomheten må ha et system som sikrer at forskningsprosjekter blant annet har nødvendig konsesjon eller er meldt til Datatilsynet⁶, og at vilkår i konsesjon følges. Systemet må videre sikre at opplysningene anonymiseres / slettes senest ved prosjektslutt, at henvendelser fra registrerte håndteres i henhold til personopplysnings- og helseregisterlovens krav, og at de registrerte gis de rettighetene de har med hensyn til blant annet innsyn, retting og sletting.

Det vises til ytterligere informasjon om krav til etablering av internkontroll, sjekkliste for internkontroll og faktaark om internkontroll på Datatilsynets hjemmeside (www.datatilsynet.no) under pekeren temasider og tema internkontroll.

2.3. Krav om hjemmelsgrunnlag for å kunne behandle sensitive personopplysninger

Sensitive personopplysninger kan bare behandles i forskningsøyemed dersom det finnes hjemmel i personopplysningslovens §§ 8 og 9, jf § 11 og helseregisterlovens §§ 5, 7 og 8. Det følger av bestemmelsene at behandling bare kan finne sted dersom den registrerte har samtykket til behandlingen, hvis behandlingen er fastsatt ved lov, eller dersom ett eller flere av vilkårene i bokstav a til f er oppfylt. Felles for disse vilkårene er at behandling av personopplysninger bare er tillatt i den utstrekning behandlingen er nødvendig for å ivareta de der nærmere definerte interesser. Vilårene er skjønnsmessige og det kreves en konkret vurdering i hvert enkelt tilfelle.

Det følger av lovens systematikk og forarbeider at behandling av personopplysninger i hovedsak skal basere seg på den registrertes samtykke eller hjemmel i lov. Dette fremgår også ved at det er oppstilt et nødvendighetskrav for vilkårene i bokstav a til f. Det er uttalt i forarbeidene til personopplysningsloven⁷ at behandling av personopplysninger i størst mulig grad bør baseres på samtykke fra den registrerte, da dette vil styrke den registrertes muligheter til å råde over opplysninger om seg selv, jf. Ot. prp. nr. 92 (1998-99) side 108.

⁶ Eller personvernombudet dersom slik avtale er inngått.

⁷ Disse forarbeidene er også relevante ved tolkning av bestemmelser i helseregisterloven da helseregisterlovens § 5 viser nettopp til personopplysningslovens § 9 og indirekte til §8.

2.4. Øvrige grunnkrav

Lovene oppstiller også krav om blant annet formålsbestemthet, saklighet og relevans. Behandlingen skal ha et uttrykkelig angitt formål som er saklig begrunnet i den behandlingsansvarliges virksomhet. Videre skal opplysningene som behandles være relevante og nødvendige for formålet. Angivelse av ”forskning” som et formål vil generelt ikke oppfylle kravet om uttrykkelighet.

Formålet med behandlingene av opplysningene er sentralt for vurdering av øvrige krav i loven. Den registrerte må derfor informeres også om dette. For samtykkebaserte prosjekter vil den informasjonen som er gitt være styrende for omfanget av behandlingen. Skal opplysningene brukes til nye forskningsformål må den enkelte som regel informeres på nytt.

2.5. Informasjonsplikt

Det behandlingsansvarlige har en plikt til, av eget tiltak, å informere den registrerte om visse forhold både når det samles inn opplysninger fra den registrerte selv og når det samles inn opplysninger fra andre.

Retten til informasjon er en grunnleggende personvernrettighet for den registrerte. Informasjon om hvilke personopplysninger som behandles, av hvem, og hva som er formålet med behandlingen, er nødvendig for at man skal kunne utøve kontroll over egne opplysninger. Retten til innsyn, retting og sletting blir illusorisk dersom den registrerte ikke engang har kunnskap om at behandlingen av personopplysninger finner sted. Det er gjort enkelte unntak fra informasjonsplikten⁸.

Det er utarbeidet en mal for hva som bør inngå i et informasjonsskriv. Denne veiledningen for et informasjonsskriv er utarbeidet i fellesskap av de enhetene⁹ som vurderer kvaliteten av utarbeidede informasjonsskriv og samtykkeerklæringer. Hensikten med malen er å gi forskere et hjelpemiddel som gjør at de enkelt skal kunne utforme informasjonsskriv som inneholder de opplysninger som etterspørres.

Den følgende liste av momenter er veiledende. Den er ikke uttømmende, men kan benyttes som en huskeliste. Anvendelsen må tilpasses og vurderes i forhold til hvert enkelt prosjekt.

- Innledning med forespørsel om deltakelse.
- Prosjektets formål / prosjektets tittel.
- Navn og kontaktopplysninger til den behandlingsansvarlige.
- De metoder som skal benyttes og hva disse innebærer for den registrerte.
- Praktiske følger av deltakelse.
- Hvor opplysninger innhentes fra og hvilke opplysninger som innhentes (fra pasientjournalen, annet helseregister, SSB etc.)

⁸ se personopplysningslovens §§ 19, 20 og 23 og helseregisterlovens §§ 23, 24 og 25

⁹ Herunder Den nasjonale forskningsetiske komité for medisin, Sosial- og helsedirektoratet, Helsedepartementet og Datatilsynet.

- Hvilke kriterier som gjelder for deltakelse.
- Om prosjektet kan være direkte til gagn for den enkelte registrerte eller ikke.
- Omtale av risiko, bivirkninger og eventuelle ubehag.
- Opplysning om hvilken alternativ behandling som tilbys, hvis den registrerte ikke ønsker å delta i forskningsprosjektet eller ønsker å trekke seg fra deltakelse.
- Eventuell avslutning av nåværende behandling som forutsetning for å delta.
- Eventuell oppfølgingsbehandling.
- Informasjon om den registrertes rett til å kreve innsyn og rett til å kreve retting og sletting av opplysninger.
- Eventuelle muligheter for tilbakemelding om eller tilgang til resultater etter at prosjektet er avsluttet.
- Når eventuelle lydbåndopptak vil slettes.
- Konfidensialitet, oppbevaring, eventuell gjenbruk av data. Det skal opplyses om i hvilken form opplysningene lagres (direkte personidentifiserbare eller aidentifiserte). Dersom det indirekte er mulig å spore opplysningene tilbake til vedkommende, for eksempel ved hjelp av et kodenummer, skal begrepet aidentifisert brukes, ikke anonymisert.
- Hvem har tilgang til personidentifiserbare data?
- Dersom opplysningene skal utleveres, skal mottaker angis. Dersom opplysningene skal utleveres til land utenfor EU, skal det gis informasjon dersom landet ikke har personvernlovgivning som anses tilfredsstillende i europeisk sammenheng.
- Angivelse av prosjektets varighet, samt hva skjer med personopplysningene etter prosjektets avslutning, sletting, anonymisering eller lagring i påvente av eventuell oppfølging.
- Forskeres taushetsplikt og dens eventuelle begrensninger.
- Understrekning av at deltakelse er frivillig og at et samtykke kan trekkes tilbake på et hvilket som helst tidspunkt uten at man må oppgi grunn. For pasienter og andre i avhengighetsforhold må det opplyses om at det ikke får innvirkning på deres forhold til behandlere eller andre, dersom de ikke vil delta i studien.
- Det skal opplyses om eventuelle konsekvenser av at samtykket trekkes tilbake, for eksempel begrensninger i rekkevidden av hvilke opplysninger og materiale som kan trekkes tilbake etter at de har inngått i vitenskapelige analyser.
- Navn og adresse for behandlingsansvarlig for prosjektet. Opplysninger om hvem som er kontaktperson for prosjektet og hvordan denne kan kontaktes.
- Opplysninger om hvem som finansierer prosjektet og om prosjektleders økonomiske interesser (særlig honorar per pasient) og eventuelle interessekonflikter.
- Til slutt skal det opplyses om forsikringsdekning, hvem som står bak studien (oppdragsgiver) og hvem som er ansvarlig for å gjennomføre den (prosjektleder, utprøver).
- Dersom det opprettes en biobank, må det informeres om dette, herunder hvem som er ansvarshavende.
- Dersom biobankmaterialet skal føres ut av landet skal det opplyses om dette, og til hvilket land overføringen vil skje.
- Dersom prosjektet innebærer bruk av genetiske undersøkelser må informasjonsskrivet opplyse om dette.

Praktiske opplysninger om fremmøte, hva som skal gjøres ved hvert enkelt besøk, osv, bør ikke stå i selve informasjonsskrivet, men kan utformes i form av en separat bruksanvisning.

Samtykket skal følge i teksten etter informasjonen, f.eks. slik: "Jeg har mottatt skriftlig og muntlig informasjon og er villig til å delta i studien," med plass for signatur og dato.

2.6. Sletting

Den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis opplysningene ikke er oppbevaringspliktig i henhold til arkivlov eller annen lovgivning, skal de slettes eller anonymiseres når formålet er oppfylt.

Med "anonymiseres" menes at identifiserbare kjennetegn slettes slik at det ikke lenger er mulig å knytte opplysningene tilbake til enkeltpersoner. Når det gjelder behandling av personopplysninger for forskningsformål finnes det krav om at opplysningene skal lagres i lengre tid enn forskningsstudien pågår, eksempelvis krav om å ha kilde data tilgjengelig i 15 år etter sluttrapport¹⁰.

Sentralt i denne sammenheng er at de registrerte er informert om prosjektets varighet, hva som skjer med opplysningene etter prosjektslutt og når opplysningene slettes/anonymiseres. Dersom det i ettertid viser seg å være ønskelig å oppbevare opplysningene lenger enn det respondentene er informert om og således har samtykket til, må det informeres på nytt slik at man ikke behandler opplysningene i strid med respondentenes allerede avgitte samtykke.

I konsesjoner til forskningsprosjekter gis det ofte vilkår med tidsfrist for sletting / anonymisering senest ved prosjektslutt, eksempelvis at koblingsnøkkel skal slettes straks koblingen er gjennomført. Dersom et forskningsprosjekt skal være omfattet av unntaket fra konsesjonsplikt i personopplysningsforskriftens § 7-27, er det et vilkår at opplysningene skal slettes / anonymiseres ved prosjektslutt.

2.7. Informasjonssikkerhet

I personopplysningslovens § 13 og helseregisterlovens § 16 stilles det krav om at virksomheten gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet. Personopplysningsforskriftens kapittel 2 gir utfyllende bestemmelser. Dokumentasjon av tiltakene for tilfredsstillende informasjonssikkerhet vil være en del av virksomhetens internkontrollsystem.

Generelt er forskning en form for behandling som avviker vesentlig fra de andre, mer ordinære, behandlinger av personopplysninger virksomheter forestår. I ordinær behandling velger virksomheten en felles programvare og drift, der alle ansatte med tjenestelig behov autoriseres til å bruke fellessystemet og dets felles databaser (lønn- og personal, kunde eller pasientssystem). I forskning opprettes det normalt en egen database for hvert enkelt prosjekt. Databasene inneholder prosjektspesifikke opplysninger. Ofte benyttes generelle

¹⁰ I henhold til forskrift om klinisk utprøving av legemidler på mennesker § 5-3.

analyseverktøy som gir virksomheten liten kontroll med hvilke delbehandlinger som iverksettes.

Forskningsens særegenhet medfører at virksomheten må gjøre særskilte vurderinger for sikkerhetstiltak i forhold til sin forskningsvirksomhet, og at virksomhetens valg for øvrige behandlinger av personopplysninger ikke direkte kan overføres til forskningsaktiviteten. De konkrete valgene for forskningsaktiviteten skal finnes i virksomhetens internkontroll sammen med de øvrige valg for informasjonssikkerhet.

2.7.1. Metoder for håndtering personopplysninger i forskning

1) Forskning på identifiserbare opplysninger.

Det foretas relativt sjelden forskning på direkte identifiserbare opplysninger, og det skal være et særskilt behov for å håndtere opplysningen i identifiserbar form før Datatilsynet betrakter denne fremgangsmåten som akseptabel.

2) Forskning på aidentifiserte opplysninger.

De identifiserende opplysningene er fjernet fra datasettet og erstattet med en kode. Opplysningen kan kun føres tilbake til enkeltpersoner ved å gå via en koblingsnøkkel hvor koden referer til de identifiserende opplysningene. Sikkerhetsfokuset kan her flyttes fra datasettet til koblingsnøkkelen.

3) Forskning på aidentifiserte opplysninger hvor koblingsnøkkelen lagres hos tredjepart i perioder det ikke er behov for den i prosjektsammenheng.

I enkelte prosjekter er det av Datatilsynet stilt krav om at koblingsnøkkelen oppbevares i en annen virksomhet for å sikre at datasettet og koblingsnøkkelen er tilfredstillende atskilt. Praktiske eksempler på tredjeparter er NSD og SSB.

4) Forskning på aidentifiserte opplysninger hvor virksomheten som forestår forskningen aldri har hatt tilgang til koblingsnøkkelen.

Dette er en aktuell situasjon hvor det forskes på datasett hentet fra de større nasjonale registrene, hvor datasettet blir aidentifisert ved uttak fra registeret.

5) Forskning på anonyme opplysninger.

Anonyme opplysninger faller ikke under regelverkets definisjon av personopplysninger, og har heller ikke et sikkerhetsbehov sett med henblikk på personvernet. Imidlertid ligger utfordringen her i hvorvidt datainnsamlingen er anonym. Dersom man går via identifiserende opplysninger for å generere det anonyme datasettet, vil dette være en behandling av personopplysninger, som kommer inn under regelverkets virkeområde.

Det bemerkes at forventningen til aidentifisering i regelverkets forstand er store. Generelt kan man si at et tilfredstillende aidentifisert datasett blir anonymt dersom man tilintetgjør koblingsnøkkelen. Imidlertid er det ofte at bare de direkte identifiserende opplysningene, som navn og personnummer, som er fjernet, mens det gjenværende datasettet likevel er indirekte identifiserbart. En slik situasjon kan sees som en mellomting mellom metode 1) og metode 2). Selv om datasettet ikke er aidentifisert etter regelverkets definisjon, må en slik fremgangsmåte betraktes som mindre personverntruende enn forskning på direkte

identifiserbare opplysninger. Likefullt må man være oppmerksom på at datasettet fremdeles vil ha et relativt høyt beskyttelsesbehov, og at all fokus ikke kan rettes mot koblingsnøkkelen alene.

Personopplysningsforskriftens § 2-1 stiller krav om forholdsmessig sikring av personopplysninger. Hvilken av de ovennevnte metoder som benyttes, vil klart påvirke hvilket beskyttelsesnivå de ulike delene av forskningsdataene har behov for. Nivået skal fastlegges på grunnlag av hvilken type personopplysninger som behandles, herunder hvorvidt det behandles sensitive personopplysninger i informasjonssystemet. Nivået (akseptkriteriene) skal fastsettes av virksomhetens ledelse, i tillegg har Datatilsynet i § 2-2 anledning til å fastsette akseptabel risiko. Ofte gis akseptkriteriet for atskillelse av koblingsnøkkel og aidentifisert datasett som konsesjonsvilkår. Datatilsynet krever her separat atskilt medium for koblingsnøkkelen, men det overlates til virksomheten å definere kriteriet for det øvrige materialet da personverntrusselen nå er beskjedent. Dersom det mot formodning skulle foretas forskning på identifiserbare sensitive opplysninger, må akseptkriteriene her vurderes særskilt.

2.8. Forhåndskontroll eller etterhåndskontroll?

Forskningsprosjekter der sensitive personopplysninger behandles elektronisk, er som hovedregel underlagt konsesjonsplikt etter personopplysningsloven eller helseregisterloven. Personopplysningsforskriften har imidlertid en unntaksbestemmelse som gjør at forskningsprosjekter som oppfyller noen spesifikke vilkår i stedet kan forholde seg til den langt enklere meldeplikten.

2.8.1. Konsesjonsplikt

Dersom et forskningsprosjekt er konsesjonspliktig, anbefales det at eget konsesjonssøknadsskjema fylles ut. Søknaden oversendes Datatilsynet sammen med prosjektbeskrivelse og annen dokumentasjon som er nødvendig for å belyse søknaden.¹¹ Dersom forsker er tilknyttet en virksomhet som har inngått avtale med Norsk Samfunnsvitenskaplig Datatjeneste¹² som personvernombud, skal det samme materialet oversendes dit. Personvernombudet vil skrive en innstilling til Datatilsynet.

Dersom det ikke legges opp til at respondentene skal samtykke til deltakelse i prosjektet, må man begrunne hvorfor et av de alternative behandlingsgrunnlagene er oppfylt, herunder må det belyses hvorfor nødvendighetsvilkåret anses oppfylt. Det må videre opplyses om hvordan informasjonsplikten skal oppfylles. Om den behandlingsansvarlige mener at undersøkelsen faller inn under et unntak fra informasjonsplikten, må dette standpunktet også begrunnes.

Uansett om søknaden sendes direkte fra forsker eller via et personvernombud, er søknaden og vedleggene gjenstand for saksbehandling hos Datatilsynet. Når konsesjon gis, har Datatilsynet foretatt en forhåndskontroll av prosjektet og funnet at dersom det gjennomføres i henhold til søknaden, er det i overensstemmelse med personopplysningslovens / helseregisterlovens krav. Konsesjoner gis med vilkår dersom Datatilsynet etter en vurdering har kommet til at det er nødvendig for å begrense ulempene behandlingen ellers ville

¹¹ Blant annet kopi av samtykkeerklæring / informasjonsskriv, kopi av eventuell uttalelse fra en etisk komité, kopi av eventuell nødvendig dispensasjon fra taushetsplikt.

¹² NSD

medføre for den registrerte. Det kan også gjøres presiseringer av personopplysningslovens / helseregisterlovens krav i merknader til konsesjon. Konsesjonen gis da med forutsetning om at vedlagte merknader følges.

2.8.2. Meldeplikt

Personopplysningsforskriften gjør unntak fra konsesjonsplikt for forskningsprosjekter som oppfyller noen nærmere fastsatte vilkår, jf forskriftens § 7-27. Les bestemmelsen under for en utfyllende liste.

Unntak fra konsesjonsplikten gjelder bare dersom vilkårene i punktene a) – e) alle er oppfylt:

- a) Førstegangskontakt opprettes på grunnlag av offentlig tilgjengelig informasjon eller gjennom en faglig ansvarlig person ved virksomheten der respondenten er registrert, eller respondenten selv tar kontakt med prosjektleder eller dennes representant,*
- b) respondenten har samtykket i alle deler av undersøkelsen. Dersom respondenten er umyndig, kan en annen med samtykkekompetanse for respondenten avgi slikt samtykke.*
- c) prosjektet skal avsluttes på et tidspunkt som er fastsatt før prosjektet settes i gang,*
- d) det innsamlede materialet anonymiseres eller slettes ved prosjektavslutning, og*
- e) prosjektet ikke gjør bruk av elektronisk sammenstilling av personregistre.*

Dersom behandlingen oppfyller forskriftens § 7-27, skal behandlingen meldes til Datatilsynet¹³. Meldingen skal i følge personopplysningslovens § 31, 2. ledd, sendes til Datatilsynet senest 30 dager før behandlingen starter. Den kan sendes elektronisk på Datatilsynets hjemmeside (www.datatilsynet.no/melding) .

Ved melding godkjennes ikke behandlingen av Datatilsynet før den tar til. Meldingen registreres direkte i en offentlig database. Den behandlingsansvarlige får en kvittering fra Datatilsynet på at meldingen er mottatt. Meldingen har ikke vært gjenstand for saksbehandling hos Datatilsynet, og behandlingsansvarlig må selv sørge for at prosjektet skjer i overensstemmelse med personopplysningsloven / helseregisterloven. Dette er en endring etter overgangen fra personregisterloven til personopplysningslov/ helseregisterlov.

Flere behandlinger av personopplysninger er gjort meldepliktig i stedet for konsesjonspliktig, nettopp fordi Datatilsynet skal fokusere mer på etterkontroll og mindre på forhåndskontroll.

¹³ Dersom det er inngått avtale om personvernombud, sendes tilsvarende melding direkte til personvernombudet som er forpliktet til å føre en offentlig oversikt over disse meldingene.

Vedlegg B

Statistikkgrunnlag

Definisjoner

HF	Bransje Helseforetak
Utdanning	Bransje Lærested
Klinisk	Bransje Klinisk utprøving av legemidler på mennesker
Forskning	Bransje Forskningsinstitusjon
BH-ANSV	Behandlingsansvarlig
Prosjekt	Forskningsprosjekt
TOTAL	Summering av kolonne / eller rad
Antall	Delutvalgets størrelse
IR	Ikke relevant
BHGRL	Behandlingsgrunnlag

Overordnet statistikk

Totalt antall utførte tilsyn, ordinære og sletting

	BH-ANSV	PROSJEKT
Utdanning	6	19
HF	11	26
Klinisk	4	6
Forskning	4	8
Andre	1	0
TOTAL	26	59

Mrk. En BH-ANSV innen utdanning er felles for ordinære og sletting

Totalt antall utførte kontroller av ulik art

	Ordinære	Sletting	TOTAL
Brevlige K	18	9	27
Brev + sted	23	0	23
Stedlige	9	0	9
TOTAL	50	9	59

Tilsyn rettet mot slettepliktige prosjekter

Fordeling av behandlingsansvarlige og prosjekt

	BH-ANSV	PROSJEKT
Utdanning	3	5
HF	3	3
Forskning	1	1
TOTAL	7	9

Samtlige (9) tilsyn er brevkontroller

Overholdelse av sletteplikt

Prosjektets status	Antall
Avsluttet iht plikt	4
Pågående - manglet BHGRL	4
IR (Ikke svart)	1

Tilsyn mot ordinære prosjekt

Fordeling av behandlingsansvarlige og prosjekt

	BH-ANSV	PROSJEKT
Utdanning	4	14
HF	8	23
Klinisk	4	6
Forskning	3	7
Andre	1	0
TOTAL	20	50

Mrk. Andre er et objekt i primærhelse

Behandlingsansvarlig - fordeling brevlige og stedlige tilsyn

	Brev	Stedlig	Brev+stedlig	TOTAL
Utdanning	1	0	3	4
HF	5	1	2	8
Klinisk	3	0	1	4
Forskning	0	2	1	3
Andre	0	0	1	1
TOTAL	9	3	8	20

Prosjekt - fordeling brevlige og stedlige tilsyn

	Brev	Stedlig	Brev+stedlig	TOTAL
Utdanning	5	0	9	14
HF	9	4	10	23
Klinisk	4	0	2	6
Forskning	0	5	2	7
TOTAL	18	9	23	50

Prosjekt - Brudd på vilkår gitt i konsesjon

Prosjekt med konsesjon	22
Ikke relevante	5
Relevante prosjekt	17
Brudd på vilkår gitt i konsesjon	11

Behandlingsansvarlig - Varsel om pålegg generelt på den behandlingsansvarlige

	Pålegg § 13	Pålegg § 14
Utdanning	4	4
HF	2	5
Klinisk	0	4
Forskning	2	2
Andre	1	1
TOTAL	9	16

Mrk. Det ble ikke gitt pålegg etter andre §§ på overordnet nivå

Behandlingsansvarlig - Definert behandlingsansvar i styrende dok

	OK	Delvis	Ingen	IR	TOTAL
Utdanning	0	1	3	0	4
HF	6	0	0	2	8
Klinisk	0	1	3	0	4
Forskning	1	2	0	0	3
Andre	0	0	1	0	1
TOTAL	7	4	7	2	20

Behandlingsansvarlig - Oversikt over egne behandlinger

	OK	Delvis	Ingen	IR	TOTAL
Utdanning	0	3	1	0	4
HF	2	4	0	2	8
Klinisk	3	1	0	0	4
Forskning	3	0	0	0	3
Andre	0	0	1	0	1
TOTAL	8	8	2	2	20

Behandlingsansvarlig - Internkontroll egnet for forskning

	Ja	Delvis	Nei	IR	TOTAL
Utdanning	0	0	4	0	4
HF	1	1	3	3	8
Klinisk	0	0	4	0	4
Forskning	0	0	2	1	3
TOTAL	1	1	13	4	19

Prosjekt - Status og varsel om pålegg

	Antall	Aktive	Avsluttede	Ikke startet	IR	PÅLEGG
Utdanning	14	8	3	2	1	2
HF	23	16	2	4	1	15
Klinisk	6	5	0	1	0	4
Forskning	7	4	2	0	1	3
TOTAL	50	33	7	6	3	24

Prosjekt - Tilfredstillende aidentifisering

	Ja	Nei	IR	TOTAL
Utdanning	2	4	8	14
HF	9	4	10	23
Klinisk	3	2	1	6
Forskning	1	0	6	7
TOT	15	10	25	50

Prosjekt - Tilfredstillende oppbevaring av kryssliste

	Ja	Nei	IR	TOTAL
Utdanning	5	1	8	14
HF	11	2	10	23
Klinisk	5	0	1	6
Forskning	2	1	4	7
TOT	23	4	23	50

Prosjekt - Praktisk utførelse sikkerhetsmessig forsvarlig

	OK	Ikke OK	Delvis	IR	TOTAL
Utdanning	2	1	1	10	14
HF	9	5	4	5	23
Klinisk	4	0	1	1	6
Forskning	2	0	2	3	7
TOT	17	6	8	19	50

Prosjekt - Forsvarlige føringer fra ledelsen til forsker

	OK	Ikke OK	Delvis	IR	TOT
Utdanning	0	8	0	6	14
HF	5	9	1	8	23
Klinisk	0	1	4	1	6
Forskning	0	4	0	3	7
TOT	5	22	5	18	50

Prosjekt - Ivaretagelse av plikt om behandlingsgrunnlag (også samtykke OK)

	OK	Ikke OK	IR	TOT
Utdanning	6	3	5	14
HF	9	6	8	23
Klinisk	0	5	1	6
Forskning	3	1	3	7
TOT	18	15	17	50

Prosjekt - Prosjektleders forståelse av behandlingsansvarlig

	OK	Delvis	Ikke OK	IR	TOT
Utdanning	0	1	9	4	14
HF	8	1	9	5	23
Klinisk	0	0	5	1	6
Forskning	2	0	3	2	7
TOT	10	2	26	12	50

Prosjekt - Praktisk håndtering av innsyn i prosjektet

	OK	Delvis	Ikke OK	IR	TOT
Utdanning	2	1	5	6	14
HF	8	1	8	6	23
Klinisk	2	0	3	1	6
Forskning	2	1	0	4	7
TOT	14	3	16	17	50