DRI3001: Bacheloroppgave - vår 2007

- Sikkerhetsorganisering ved et mindre legekontor

Av

Erik Hornnes

Asbjørn Korsbakken

Øivind Langeland

Leif Uwe Vogelsang

Avdeling for forvaltningsinformatikk
Juridisk fakultet, Universitetet i Oslo

1. juni 2007

1. Innholdsfortegnelse

1. Innholdsfortegnelse 2
2. Forord 4
3. Problemstilling 5
4. Oppdragsgiver 6
5. Rettslig utgangspunkt 8
5.1 Klinikkens behandling av helseopplysninger 8
5.2 Forholdet mellom sentrale lover 9
5.3 Grunnkrav til informasjonssikkerhet 10
5.3.1 Nærmere om konfidensialitet, tilgjengelighet og integritet 11
5.4 Annen helselovgivning 13
6. Aktørene databehandlingsansvarlig og databehandler 14
6.1 Databehandlingsansvarlig 14
6.2 Databehandlere 16
6.2.1 Medisiniske partnere 17
6.2.2 IT-konsulenten 18
7. Roller og oppgaver hos databehandlingsansvarlig 19
7.1 Daglig leder (DL) 20
7.1.1 Sikkerhetsledelse (pof. § 2-3) 21
7.1.2 Risikovurdering (pof. § 2-4) 21
7.1.3 Organisering (pof. § 2-7) 22
7.1.4 Personell (pof. § 2-8) 23
7.1.5 Taushetsplikt (pof. § 2-9) 24
7.1.6 Sikkerhetstiltak (pof. § 2-14) 24
7.1.7 Sikkerhet hos andre virksomheter (pof. § 2-15) 24
7.1.8 Dokumentasjon (pof. § 2-16) 24
7.2 Daglig ansvarlig (DA) 24
7.2.1 Avviksbehandling (pof. § 2-6) 26
7.2.2 Fysisk sikring (pof. § 2-10) 26
7.2.3 Sikring av konfidensialitet (pof. § 2-11) 26
7.2.4 Sikring av tilgjengelighet (pof. § 2-12) 26
7.2.5 Sikring av integritet (pof. § 2-13) 27
7.3 Sikkerhetsrevisor (SR) 27
7.4 Personell 28

7.5 Personvernombud 30
8. Etterord 31
9. Om gruppearbeidet 32
10. Kilder 33
10.1 Litteraturliste 33
10.2 Benyttede lover og forskrifter 33
10.3 Intervjuer og dokumentasjon 34

2. Forord

I denne oppgaven tar vi for oss sikkerhetsorganiseringen og relaterte spørsmål ved et mindre legekontor. Nærmere bestemt ser vi på hvilke krav som stilles til organiseringen av sikkerhetsarbeidet i relevant lovverk, vurderer hvordan situasjonen er hos oppdragsgiver og gir våre forslag til forbedringer av den eksisterende situasjonen. Selv om oppgaven er skrevet for en konkret virksomhet, kan det tenkes at den også har en viss overføringsverdi for tilsvarende virksomheter.

Vårt valg av oppdragsgiver baserer seg på at klinikken er en liten og oversiktlig organisasjon, med i overkant av ti faste ansatte. Dette er en størrelse gruppen ser på som hensiktsmessig for en praktisk gjennomføring av prosjektarbeidet. Siden oppgaven fokuserer på organisering, er det en fordel at organisasjonen ikke blir for kompleks å forholde seg til.

Den innsikten vi i løpet av prosjektets gang har opparbeidet oss om klinikken, bygger på intervjuer med ansatte og eier, samt oversendt dokumentasjon og informasjon fra klinikkens nettsider.

Oppgaven er lagt opp slik at vi begynner med en generell del om oppdragsgiver, der vi presenterer virksomhetens arbeidsområder og organisering. Deretter går vi inn på de regelverk som har relevans for oppdragsgiver i forbindelse med organiseringen av sikkerhetsarbeidet. Dernest gir vi våre vurderinger av i hvilken grad oppdragsgiver kan sies å være i tråd med lovverket, for så å gi våre anbefalinger til endringer som kan lukke de avvik som foreligger mellom oppdragsgivers situasjon og lovgivningens krav pr. mai 2007. For de enkelte ting som tas opp, vurderes og konkluderes det fortløpende, samt at det gis en overordnet oppsummering i etterordet.

Løsningsforslagene er ikke uttømmende, fokuset er i utgangspunktet sikkerhetsorganisasjonen, og i noen grad tilgrensende organisatoriske tiltak. Gruppen er også opptatt av at oppdragsgiver skal være mest mulig komfortabel med de forslag til endringer vi legger fram. Herunder at endringsforslagene skal være mulige å gjennomføre uten for store kostnader, både i form av tid og penger.

3. Problemstilling

Alle virksomheter som behandler personopplysninger med elektroniske hjelpemidler er underlagt et omfattende lovverk hva angår bestemmelser vedrørende informasjonssikkerhet. Lovverket, i det minste personopplysningsforskriften, bærer preg av å være dimensjonert for forholdsvis store virksomheter. Det blir derfor en utfordring for mindre virksomheter å tilpasse lovverkets krav til sine behov. For å gjøre dette, kreves det antakeligvis både en viss juridisk og informatisk kompetanse. Det kan tenkes at mindre virksomheter ikke har ressurser til å besitte denne type kompetanse. Dermed blir det vanskelig å forstå lovverkets betydning for egen situasjon, og derfor vil også etterlevelsen av kravene kunne bli vanskelig.

I denne oppgaven vil vi tolke lovverket i lys av en mindre virksomhets situasjon. På denne måten ønsker vi å gjøre det mer tilgjengelig og forståelig for oppdragsgiver. For å oppnå dette har vi gått frem på følgende måte;

A) Kartlegge hvorledes legekontoret har organisert sitt arbeid med informasjonssikkerhet, avgrenset til helseopplysninger.

B) Vurdere funnene gjort under punkt A i lys av lovgivningens krav til slik organisering.

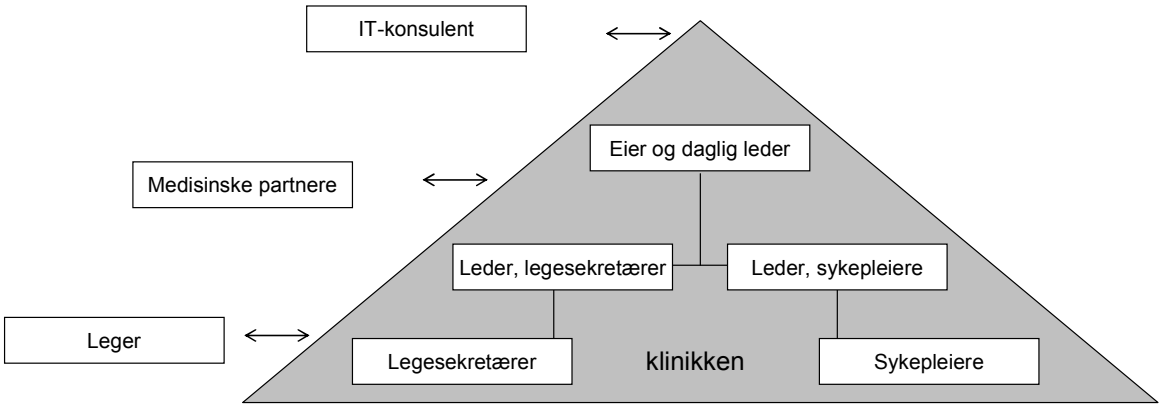
C) Foreslå nødvendige endringer i organiseringen, for å komme i tråd med lovgivningens krav.

4. Oppdragsgiver

Gruppens oppdragsgiver i prosjektarbeidet er en mindre klinikk, nærmere bestemt et enkeltpersonforetak som diagnostiserer og behandler hudsykdommer. Klinikken er helt privat finansiert uten kommunal driftsavtale eller trygderefusjon. Pasienter trenger ikke henvisning, men oppsøker spesialist direkte. Klinikken består av syv hudleger, hvorav seks av dem er innleid gjennom egne virksomheter, jf. straks under. I tillegg er det ansatt seks legesekretærer og fem sykepleiere.

Av legene er det kun eieren som har fast tilhold ved klinikken. De andre legene jobber der ved behov, men er ikke i noe ansettelsesforhold. Det fungerer slik at disse legene leier kontorplass og infrastruktur hos klinikken, og har separate regnskap gjennom sine egne virksomheter. Forholdet mellom klinikken og disse legene reguleres i egne avtaler. Det er også klinikken som mottar timebestillinger for de enkelte legene, slik at det utad virker som om legene er en del av legekontoret. Begrunnelsen for å organisere virksomheten på denne måten er primært skattemessig. Ordningen er godkjent av Riksskattestyret. Fleksibilitet og kontroll over virksomheten har også vært viktige faktorer i valget av organisasjonsform..

Klinikken har også knyttet til seg en ekstern IT-konsulent, som bidrar med teknisk assistanse på informasjonssystemet når dette er nødvendig. For mer informasjon om denne konsulentens arbeid, se avsnitt 6.2.



Figur 1, hele bildet

Figur 1 viser hvordan klinikken er organisert pr. mai 2007. I tillegg fremkommer hvilket forholdet klinikken har til eksterne samarbeidspartnere. Organisasjonskartet i trekanten viser virksomhetens hierarkiske organisasjon. Piler er brukt mellom eksterne samarbeidspartnere og klinikken, fordi det er tale om kontraktbaserte forhold under avtalefrihet.

5. Rettslig utgangspunkt

5.1 Klinikkens behandling av helseopplysninger

De rettslige krav som stilles til arbeidet med informasjonssikkerhet i virksomheter som behandler helseopplysninger, fremgår primært av helseregisterloven[1], personopplysningsloven[2] og personopplysningsforskriften[3]. Forholdet mellom disse lovene omtales nærmere i oppgavens avsnitt 5.2. Vi vil i det følgende redegjøre for helseregisterlovens anvendelse i forhold til oppdragsgiver, og gå nærmere inn på hva det menes med å behandle helseopplysninger.

I henhold til helseregisterloven (hrl.) § 3 nr. 1, gjelder loven for "behandling av helseopplysninger i helseforvaltningen og helsetjenesten som skjer helt eller delvis med elektroniske hjelpemidler for å fremme formål som beskrevet i § 1". Med helseopplysninger menes 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. hrl. § 2 nr. 1. Med behandling menes enhver formålsbestemt bruk av helseopplysninger, eksempelvis innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. hrl. § 2 nr. 5. En behandling kan bestå av en eller flere operasjoner (Schartum og Bygrave 2004: 123). Gjennom medisinsk behandling av pasienter ved klinikken, oppstår det nødvendigvis opplysninger om den enkelte pasients helseforhold, altså helseopplysninger. Helseopplysninger samles inn, lagres og aksesseres; det vil si at de "behandles". Det er derfor på det rene at klinikken behandler helseopplysninger.

Schartum og Bygrave (2004: 196) argumenterer for at begrepet "helsetjenesten" trolig omfatter "alle de institusjoner som gir helsehjelp som utføres av helsepersonale, jf. helsepersonelloven § 3". Dermed må vilkåret i § 3 første ledd om "helseforvaltningen og helsetjenesten" også anses oppfylt for klinikken. Hrl. § 3 annet ledd fastsetter i tillegg at loven gjelder både for offentlig og privat virksomhet, dette understreker at loven gjelder for vår oppdragsgiver. Vi anser at vilkåret om helt eller delvis elektronisk behandling er oppfylt, tatt i

[1] Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) 18. mai 2001 nr. 24
[2] Lov om behandling av personopplysninger (personopplysningsloven) 14. april 2000 nr. 31
[3] Forskrift om behandling av personopplysninger (personopplysningsforskriften) 15. desember 2000 nr. 1265

betraktning at klinikken benytter seg av journalsystemet Infodoc i sin behandling av helseopplysninger.

Infodoc er et datamaskinbasert system som består av flere moduler. For eksempel finnes det en egen modul for føring av journaler, og en egen modul for økonomi. Den ene modulen, journalsystemet, brukes med det formål å yte helsehjelp. Økonomimodulen benyttes for å fakturere pasientene. Således understøtter de to modulene to ulike formål, selv om de inngår i det samme datamaskinsystemet. Schartum og Bygrave (2004: 123) viser til at én behandling ofte tilsvarer det som skjer innenfor rammene av et edb-system eller en modul av et slikt system. Vi mener derfor at det foreligger to ulike behandlinger av helseopplysninger ved klinikken.

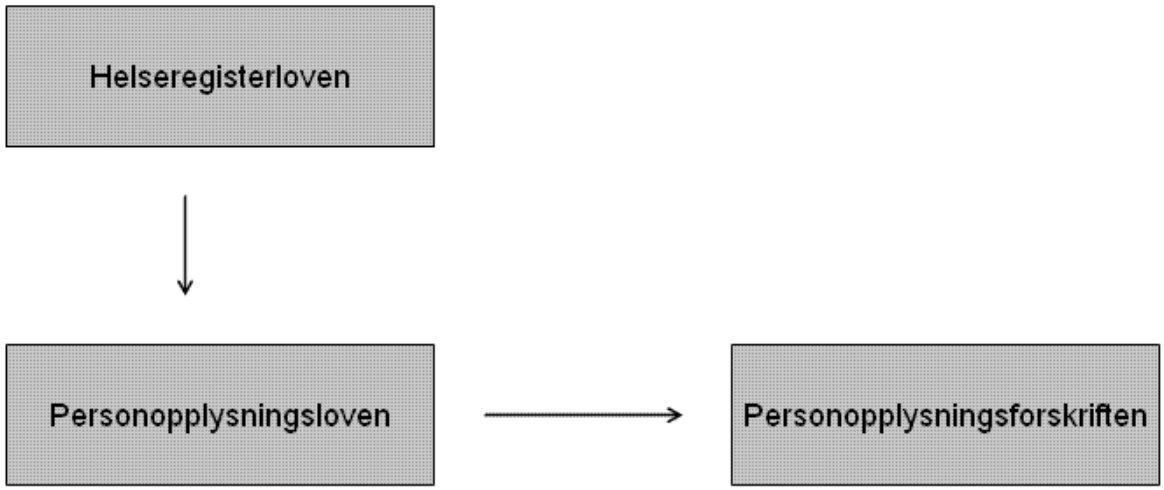
Vi går ikke nærmere inn på de grunnkrav[4] helseregisterloven § 5 krever oppfylt for å behandle helseopplysninger, da dette faller utenfor oppgavens rekkevidde. Vi vil fokusere på bestemmelser knyttet til informasjonssikkerhet, med utgangspunkt i hrl § 16 og kapittel 2 i personopplysningsforskriften.

5.2 Forholdet mellom sentrale lover

Personopplysningsloven er den generelle loven på området for behandling av personopplysninger, mens helseregisterloven er særlov for behandling av en særskilt type personopplysning; helseopplysninger. Forholdet mellom de to lovene er eksplisitt regulert i helseregisterloven § 36 som fastsetter at "i den utstrekning ikke annet følger av denne lov, gjelder personopplysningsloven med forskrifter som utfyllende bestemmelser".

Selv om vi fokuserer på de regelverk som gjelder for virksomheter som behandler helseopplysninger, vil antakeligvis oppgavens innhold i stor grad også være relevant for virksomheter som behandler andre typer personopplysninger. Dette fordi kravene til organisering etter helseregisterloven i stor grad er sammenfallende med personopplysningslovens krav, og fordi forskriften til personopplysningsloven også får anvendelse i forhold til helseregisterloven. Vel å merke får forskriften bare anvendelse når det er tale om helt eller delvis elektronisk behandling av opplysninger.

[4] For nærmere om grunnkrav vises det til Schartum og Bygrave 2004 side 198.



Figur 2, lovenes ordningsforhold

5.3 Grunnkrav til informasjonssikkerhet

Vi vil i det følgende gjennomgå noen grunnkrav som stilles til informasjonssikkerhet etter helseregisterloven og personopplysningsforskriften. Selv om de teknisk sett faller utenfor det rent organisatoriske, mener vi likevel det er viktig å redegjøre for dem. Dette fordi sikkerhetsorganiseringen også skal bidra til å oppfylle de grunnkravene som presenteres i det følgende, samtidig med å være selvstendige krav som følger av lovverket.

Helseregisterloven § 16 er utgangspunktet for de krav virksomheter stilles overfor når det gjelder ivaretakelse av informasjonssikkerhet. Av første ledd fremgår det at arbeidet med informasjonssikkerhet, gjennom planlagte, systematiske og dokumenterte tiltak, skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet.

Med ”planlagt” menes det at man skal møte informasjonssikkerhetsarbeidet med en helhetlig oppfatning av hvilke sikkerhetstruende situasjoner som kan oppstå, samt at man skal ha en plan for hva som skal gjøres når slike situasjoner inntreffer. Dette arbeidet skal være gjort før behandlingen starter, og det skal vedlikeholdes så lenge behandlingen pågår. Med ”systematisk” menes det at arbeidet med informasjonssikkerhet ikke skal gjennomføres på en tilfeldig måte, men i tråd med planer og prosedyrer. Således henger det nøye sammen med planlegging. Det er ikke gitt fra lovgiver hvilken systematikk og hvilke prosedyrer som skal følges, men de må nok i det minste være utformet slik at man gjennom å følge dem evner å

belyse hovedspørsmålene hrl. § 16 første ledd er satt til å verne (Schartum 2005: 120). Sikkerhetstiltakene skal også dokumenteres, og være tilgjengelig for medarbeidere i organisasjonen, samt for tilsynsmyndigheter.

Tilfredsstillende informasjonssikkerhet, som er rammen for hva slags tiltak som skal settes i verk, er ingen absolutt størrelse. Hva som er tilfredsstillende informasjonssikkerhet for en type behandling, er ikke nødvendigvis tilfredsstillende for en annen. Årsaken er at ulike behandlinger kan generere ulik risiko for personvernskade. For å vurdere den antatte risikoen for personvernskade, må man for det første se på hvorvidt det er trusler knyttet til den enkelte behandlingen som kan virke inn på realiseringen av lovens formål, jf. hrl. § 1. Videre må man se på formålet med den konkrete behandlingen for å fastslå hva som er tilfredsstillende informasjonssikkerhet (Schartum 2005: 117). Tilfredsstillende informasjonssikkerhet oppnås således når antatt risiko er innenfor hva man mener er akseptabel risiko. Det må derfor gjennom risikovurderinger vurderes hva som er akseptabel risiko og hva som er antatt risiko for den konkrete behandlingen jf. pof § 2-4. For mer om risikovurderingen, se oppgavens avsnitt 7.1.2.

5.3.1 Nærmere om konfidensialitet, tilgjengelighet og integritet

Vi vil i det følgende gå nærmere inn på hovedspørsmålene i hrl. § 16, slik de fremkommer i første ledd. Personopplysningsforskriften §§ 2-11 – 2-13 vil danne utgangspunktet for gjennomgangen, fordi denne, med unntak av spørsmålet om kvalitet, utdyper nærmere hva hovedspørsmålene går ut på.

Det første av hovedspørsmålene angår sikring av konfidensialitet. Med konfidensialitet menes at uautoriserte skal hindres tilgang til helseopplysninger, og annen informasjon med betydning for informasjonssikkerheten, der dette er nødvendig. Hjelpestørrelsen ”nødvendig” kan være forvirrende når det er tale om sikring av konfidensialitet, fordi det kun unntaksvis er unødvendig å sikre konfidensialitet til opplysninger (Schartum 2005: 129). Styrken i konfidensialitetskravet kan imidlertid variere, fra tilfeller der man behandler sensitive personopplysninger til tilfeller der det gis samtykke til vid spredning av opplysninger. Både uautorisert tilgang til faktiske opplysninger, og annen informasjon som kan ha betydning for konfidensialiteten, skal hindres. ”Annen informasjon” betegner informasjon som kan være nyttig for personer som ønsker å begå sikkerhetsbrudd, for eksempel beskrivelser av svakheter

ved informasjonssystemet (Schartum 2005). Det understrekes at det kun er informasjon som er egnet til å svekke sikkerheten som skal vernes.

Det andre hovedspørsmålet angår sikring av tilgjengelighet. Med tilgjengelighet menes at helseopplysningene skal være tilgjengelig når det er nødvendig. Dette må vurderes i forhold til ønsket om å unngå personvernskade (Schartum 2005: 131). Nødvendighet er i dette tilfellet et relativt krav. Hvis manglende tilgjengelighet til opplysningene ikke har direkte betydning for integritet eller privatliv, kan det ikke kreves at databehandlingsansvarlig iverksetter tiltak for å sikre tilgjengelighet, og vice versa. Schartum (ibid.) anfører følgende; ”som en tommelfingerregel tilsier personvern at tilgjengeligheten blir sikret når personopplysninger skal være:

- tilgjengelig for den registerte selv,
- tilgjengelig for andre som handler på den registrertes vegne,
- tilgjengelig for andre som treffer avgjørelser med innvirkning på den registrertes privatliv/integritet.”

Det tredje hovedspørsmålet angår sikring av integritet. Med integritet menes at helseopplysninger skal sikres mot uautorisert endring i de tilfeller dette er nødvendig. Igjen er det tale om et relativt krav til nødvendighet. Også her kan nevnte tommelfingerregel gi veiledning. Det er dog større sjanse for at integritetsbrudd kan føre til personvernskade, og man bør derfor være strengere når behov for integritetssikrende tiltak vurderes (Schartum 2005).

Det må nødvendigvis foreligge en autorisasjon for de som skal ha tilgang til å endre helseopplysninger, jf. ”uautorisert endring”. Schartum (2005) argumenterer for at dette trolig må forstås som en positiv beslutning om hvem som kan gjøre endringer i opplysninger og annen informasjon som kan ha betydning for informasjonssikkerheten.

Med ”annen informasjon”, jf. pof. § 2-13 andre ledd, menes eksempelvis programkode, rutinebeskrivelser og øvrig informasjon som kan forårsake personvernskade hvis den blir endret.

Det er viktig å se sammenhengen mellom sikring av konfidensialitet og integritet, da autorisasjon er et nøkkelelement i begge sammenhenger. Derfor bør det helst også være sammenheng mellom de to typene autorisasjon (Schartum 2005: 133).

Det siste hovedspørsmålet som fremgår av hrl. § 16, men ikke av personopplysningsforskriften, gjelder spørsmålet om kvalitet ved behandling av helseopplysninger. Schartum & Bygrave (2004: 200) fremholder at "dette er et vidtrekkende krav som ikke i særlig grad blir utdypet i andre bestemmelser i loven". Forfatterne påpeker imidlertid at hrl. § 11 første ledd inneholder et krav om at opplysningene skal være "nødvendige" og "relevante" i forhold til formålet med databehandlingen. I tillegg påpekes det at hrl. § 16 inneholder forskriftshjemmel til å gi forskrifter om standard kodeverk, eksempelvis sykdomsklassifikasjon, samt andre forhold av betydning for sikring av kvalitet konfidensialitet, tilgjengelighet og integritet.

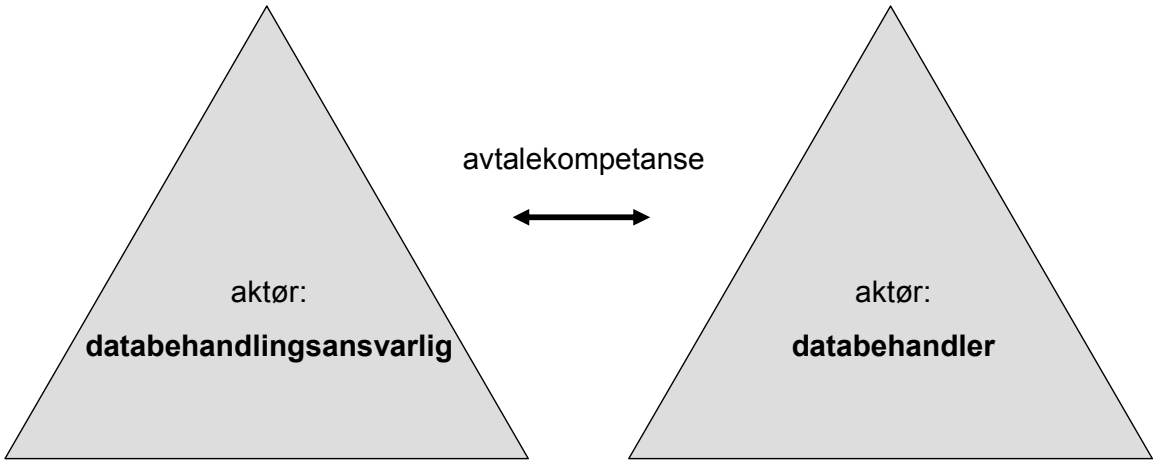
5.4 Annen helselovgivning

Gruppen har i prosjektarbeidet tatt for seg andre helselover og forskrifter for å se etter organisatoriske bestemmelser som kan være gjeldende for oppdragsgiver. Dette for å forsøke å kartlegge eventuelle konflikter i forhold til de sentrale lovene oppgaven tar utgangspunkt i. Gruppen tok utgangspunkt i kategorien helse i Lovdatas systematiske register[5], og foretok en vurdering av relevans hovedsakelig på bakgrunn av navn, formålsparagrafer, saklig virkeområde og forarbeider. Dette innebar at mange lover kunne avskrives ganske raskt, mens andre krevde nærmere ettersyn, blant annet helsepersonelloven[6], spesialisthelsetjenesteloven[7], journalforskriften[8] og forskrift om pasientansvarlig lege[9]. Etter denne gjennomgangen, har ikke gruppen funnet bestemmelser som kommer i konflikt med de forslag til endringer som legges frem i oppgaven.

[5] http://www.lovdata.no/all/syste.html
[6] Lov om helsepersonell mv. 2. juli 1999 nr. 64
[7] Lov om spesialisthelsetjenesteloven m.m. 2. juli 1999 nr. 61
[8] Forskrift om pasientjournal 21. desember 2000 nr. 1385
[9] Forskrift om pasientansvarleg lege 1. desember 2000 nr. 1218

6. Aktørene databehandlingsansvarlig og databehandler

Vi gjør i denne oppgaven et skille mellom aktører og roller, jf Schartum & Bygrave (2006: 34). Aktører betegner de primære rettssubjektene oppgaven beskjeftiger seg med; databehandlingsansvarlig og databehandler. Disse har begge plikter og rettigheter knyttet til seg etter helseregisterloven og personopplysningsforskriften. Med roller sikter vi til de funksjoner som etter gjeldende lovverk må være tilstede i de to aktørenes virksomheter. I dette kapittelet går vi nærmere inn på de to aktørene databehandlingsansvarlig og databehandler, og gir en vurdering av hvem som bekler disse. Figur 3 illustrerer forhold mellom de to aktørene.



Figur 3, forholdet mellom aktørene

6.1 Databehandlingsansvarlig

Den tyngste og mest sentrale aktøren i helseregisterloven, er databehandlingsansvarlig. Man kan si at den databehandlingsansvarlige er helseregisterlovens "hovedperson", med en rekke plikter og rettigheter knyttet til seg. Databehandlingsansvarlig[10] er i hrl. § 2 nr 8 definert som "den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven". Formålet omhandler hva helseopplysningene skal brukes til, og er obligatorisk for den databehandlingsansvarlige å fastsette etter hrl. § 11. Hjelpemidler henspiller på det tekniske og teknologiske utstyret som benyttes i behandlingen

[10] Det er grunn til å understreke at "databehandlingsansvarlig" etter helseregisterloven har den samme betydningen som "behandlingsansvarlig" etter personopplysningsloven. Grunnen til at begrepet databehandlingsansvarlig brukes i helseregisterloven, er den innarbeidete bruken av begrepet behandlingsansvarlig lege i betydningen pasientansvarlig lege (Ot.prp. nr. 5(1999-2000): 252)

av helseopplysningene. Verktøy for å ivareta informasjonssikkerhet er også regnet som hjelpemidler.

Databehandlingsansvaret ligger vanligvis hos den øverste ledelsen i en virksomhet, men det kan likevel være vanskelig å plassere ansvaret konkret. En rettesnor kan være å identifisere den som har den øverste beslutningsmyndigheten i saker som gjelder behandling av helseopplysninger. En annen rettesnor er at databehandlingsansvaret kan legges til den instansen i en virksomhet som har sivilprosessuell kompetanse, dvs. den som kan saksøke eller bli saksøkt (Schartum 2005: 111). Databehandlingsansvaret må være klart plassert, fordi den registrerte må kunne håndheve sine rettigheter overfor databehandlingsansvarlig (Ot.prp. nr. 5(1999-2000: 252)). Med den "registrerte" menes den som helseopplysninger kan knyttes til.

Siden databehandlingsansvaret vanligvis vil være plassert hos ledelsen, er det ledelsens ansvar å sørge for at databehandlingsansvarliges oppgaver gjennomføres. Som et ledd i dette arbeidet kan det være aktuelt å foreta en intern arbeidsdeling, slik at det er klart hvilken stilling det tilligger å sørge for etterlevelse av loven i praksis (Ot.prp. nr. 5(1999-2000: 253)). I mindre virksomheter, med færre personer å fordele ansvar på, er det imidlertid rimelig å anta at en slik arbeidsdeling vil være av mindre betydning.

Klinikken er et enkeltpersonforetak, hvor eier står personlig ansvarlig for hele virksomheten. I kraft av sin posisjon bestemmer eier og daglig leder alt (Spør OSS 2007), og har full instruksjons- og organisasjonsmyndighet over de ansatte. Således kan han styre og organisere virksomheten på den måten han ønsker. I praksis er det også eier og daglig leder som håndterer arbeidet med informasjonssikkerhet. Dette arbeidet kan sies å bære preg av en ad-hoc tilnærming, der tiltak hovedsakelig treffes på bakgrunn av uønskede hendelser i forbindelse med informasjonssikkerhet. Det fremgår av klinikkens dokumentasjonen at eier og daglig leder har databehandlingsansvaret. Dokumentasjonen skiller imidlertid ikke mellom roller og aktører.

Det er vår vurdering at plasseringen av databehandlingsansvaret hos klinikken, er i samsvar med lovens krav. For det første understreker organisasjonsformen, et enkeltpersonforetak, at eier må anses å være databehandlingsansvarlig, da det er han som faktisk utgjør virksomheten. Videre er det slik at i tilfelle virksomheten skulle bli saksøkt, eller ønske å

saksøke noen, vil klinikken ved eieren være adressat eller avsender. Det har også fremkommet i intervjuer med eier at det er han som bestemmer formål for behandlingen av helseopplysninger, samt de hjelpemidler som skal nyttes i behandlingen, jf. hrl. § 2 nr. 8.

Det finnes ikke, etter gruppens oppfatning, noen alternativer hva angår plassering av databehandlingsansvaret. Likevel ser vi grunn til å stille spørsmål om bevisstheten rundt dette ansvaret. Dette fordi dokumentasjonen som fastsetter at eier er databehandlingsansvarlig, bærer preg av å være en direkte respons på tilsynsvirksomhet fra Datatilsynet, og ikke som et resultat av et pågående sikkerhetsarbeid. Gjennom intervjuer med oppdragsgiver har denne antakelsen blitt bekreftet. Av den grunn at databehandlingsansvarlig er helseregisterlovens hovedperson, og således pålegges en rekke plikter, er det viktig at man har et bevisst forhold til ansvaret dette innebærer. I motsatt fall kan det tenkes vanskelig å etterleve de plikter som følger av dette ansvaret.

6.2 Databehandlere

Databehandler defineres i hrl. § 2 nr 9, og er ”den som behandler personopplysninger på vegne av den databehandlingsansvarlige”. Databehandleren er en aktør som ikke er en del av den databehandlingsansvarliges egen organisasjon, noe som innebærer at den databehandlingsansvarlige ikke har noen instruksjons- og organisasjonsmyndighet overfor databehandleren. I følge Ot.prp. nr. 5 (1999-2000: 253) favner begrepet databehandler svært vidt. Her sies det at ”databehandler kan være en som bearbeider opplysninger for den databehandlingsansvarlige, eller det kan være en som kommer i kontakt med opplysningene på en mer passiv måte, som for eksempel ved oppbevaring av opplysninger når dette er nødvendig for å kunne utføre service på datasystemer etc.” Det åpnes dermed for at en reparatør av datamaskiner kan være en databehandler, forutsatt at det er nødvendig for vedkommende å behandle, for eksempel lagre helseopplysninger.

Siden databehandleren er utenfor den databehandlingsansvarliges instruksjons- og organisasjonsmyndighet, stiller hrl. § 18 et krav om at forholdet mellom databehandlingsansvarlig og databehandler skal reguleres i en skriftlig avtale, der databehandlers oppgaver er spesifisert. Dette kommer frem av pilen mellom de to aktørene i figur 3. Hrl. § 18 andre ledd stiller også krav om at databehandlers plikt til å gjennomføre sikkerhetstiltak skal fremgå av avtalen. Det er også viktig å nevne at databehandler har et

selvstendig ansvar for informasjonssikkerhet etter hrl. § 16, samt personopplysningsforskriften kapittel 2 (ved elektronisk behandling), selv om forskriften etter ordlyden primært retter seg mot den databehandlingsansvarlige som setter bort behandlingen av opplysninger.

6.2.1 Medisiniske partnere

Virksomheten benytter diverse laboratorier for analysering av ulike former for humant biologisk materiale, for eksempel vevsprøver. Det humane biologiske materiale oversendes laboratoriene pr. tradisjonell post. Materialet som oversendes til analyse er merket med navnet på pasienten. Dersom det er tale om kjente personer i samfunnslivet brukes gjerne improviserte pseudonymer, for eksempel Hans Hansen. Interaksjonen med de ulike laboratoriene når det gjelder formidling av analyseresultatene varierer noe, men i ett av tilfellene formidles resultatet av analysen ved hjelp av en elektronisk løsning. I de øvrige tilfellene sendes resultatet pr. tradisjonell post. Det mottatte analyseresultatet blir så lagt inn i klinikkens journalsystem, enten automatisk eller manuelt.

I følge Personvernnemndas behandling av KLAGESAK 2002/08 blir humant biologisk materiale å regne som personopplysninger, dersom det er assosiert med identifiserende elementer, for eksempel navn og analysedata. Det synes dermed på det rene at materialet som oversendes laboratoriene er å regne som helseopplysninger. Det synes også klart at behandling av henholdsvis det humant biologiske materiale og analyseresultatet helt eller delvis skjer ved bruk av elektroniske virkemidler. Riktignok i større eller mindre grad, avhengig av hvilket av laboratoriene man vurderer. På bakgrunn av dette mener vi at laboratoriene blir å regne som databehandlere etter hrl. § 2 nr. 9.

Det er brudd på hrl. § 18 at det ikke foreligger avtaler mellom virksomheten og de ulike laboratoriene som eksplisitt regulerer behandlingen av personopplysningene. Slike avtaler bør derfor utformes, signeres og arkiveres. I dette spesielle tilfellet finner vi det rimelig å anbefale at jobben med å utforme slike avtaler utføres av databehandlerne, det vil si laboratoriene. Dette begrunner vi med at databehandlerne det gjelder, er forholdsvis store virksomheter. Det er sannsynlig å anta at disse aktørene vil ønske å utforme en standardavtale som kan benyttes overfor samtlige av sine oppdragsgivere, det vil si databehandlingsansvarlige. I så måte ser vi det ikke som særlig sannsynlig at de uten videre vil akseptere en avtale utarbeidet og fremmet av en enkelt oppdragsgiver. Et alternativ til dette kunne kanskje vært at en

interesseorganisasjon for de databehandlingsansvarlige, for eksempel Lægeforeningen, påtok seg arbeidet med å koordinere og utforme en slik avtale. Uansett er det grunn til å understreke at ansvaret i seg selv for at avtalene kommer på plass, ikke lar seg delegere. Således vil dette ansvaret fortsatt hvile på databehandlingsansvarlig, uavhengig av hvordan man fordeler selve arbeidet med avtalen. Det understrekes at databehandlingsansvarlig har en plikt til å følge opp at databehandler etterlever de sikkerhetskrav som oppstilles i hrl. § 16.

6.2.2 IT-konsulenten

Virksomheten har etablert et samarbeid med en IT-konsulent, som leies inn gjennom sitt enkeltpersonforetak. Vedkommende konsulent bistår med teknisk kompetanse ved akutte hendelser, for eksempel svikt i maskin- eller programvare. I tillegg har konsulenten et løpende ansvar for å vedlikeholde datamaskinsystemet. Arbeidet innebefatter både maskin- og programvare, derunder journalsystemet. Ved arbeid i journalsystemet benyttes eiers brukeridentitet, det vil si at IT-konsulenten har full tilgang til systemet. Arbeidet konsulenten utfører blir ikke systematisk dokumentert. I den grad tilbakemeldinger gis er det i en uformell og knapp form. Typisk i form av beskjeder som ”ok” skrevet på frittstående papirer. Det foreligger en avtale mellom IT-konsulenten og klinikken, som hovedsakelig gjelder forhold vedrørende taushetsplikt. Denne avtalen er imidlertid ikke signert av noen av partene.

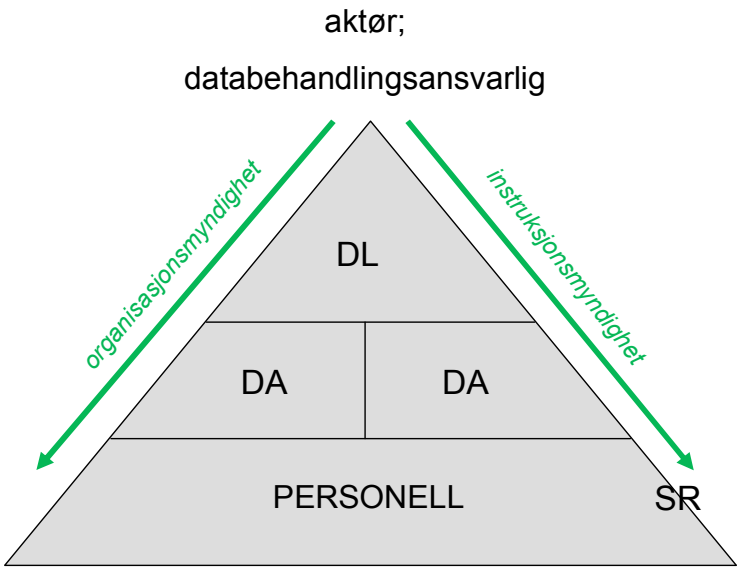
Vi synes det er mest nærliggende å betrakte IT-konsulenten som databehandler. Dette fordi han kommer i kontakt med helseopplysninger på en passiv måte, slik forarbeidene gir anvisning på. Som et eksempel kan det nevnes at konsulenten logger seg inn i Infodoc for å utføre oppdateringer av programvaren, og således har muligheten til å behandle helseopplysninger. På den annen side, hvis man ser på ordlyden i hrl. § 2 nr. 9, virker det ikke helt åpenbart at konsulenten er å regne som en databehandler, da formålet med vedkommendes oppgaver ikke er å behandle helseopplysninger på vegne av databehandlingsansvarlig. Men tatt de nevnte forarbeidene i betraktning finner vi det allikevel rimelig å anse konsulenten som en databehandler.

Det er gruppens oppfatning at kontrakten som foreligger mellom IT-konsulenten og klinikken, må utvides for å ta høyde for de krav hrl. § 18 stiller. Den må også signeres av partene. Det er grunn til å understreke at selv om kontrakten i seg selv er viktig som et formelt dokument, vil det også være avgjørende med bevissthet rundt kontraktens innhold slik at det er klart

hvilke plikter og ansvar det pålegges konsulenten i kraft av å være databehandler. Også her nevnes databehandlingsansvarliges plikter etter hrl. § 16 tredje ledd.

7. Roller og oppgaver hos databehandlingsansvarlig

Vi vil i dette kapitelet gå nærmere inn på aktøren databehandlingsansvarlig, og dens tilhørende roller og oppgaver. Selv om vi fokuserer på databehandlingsansvarlig, vil vurderingene trolig være parallelle også for databehandler. Figur 4 fremstiller hvilke roller som tilhører aktøren.



Figur 4, databehandlingsansvarliges sikkerhetsorganisasjon, tilnærming hentet fra Schartum & Bygrave (2006: 34)

Modellen bygger på en hierarkisk tankegang, der instruksjons- og organisasjonsmyndighet spiller en viktig funksjon. Med instruksjonsmyndighet menes den myndighet et overordnet organ eller en person har til å gi direktiver eller retningslinjer om hvordan underordnede skal forholde seg i forskjellige sammenhenger (Eckhoff & Smith 2003: 114). Eksempelvis hvordan arbeidsoppgaver skal utføres, enten på et generelt eller individuelt plan. Med organisasjonsmyndighet menes de bestemmelser som sier noe om hvilke organer man skal ha og hvordan disse skal stå i forhold til hverandre (Eckhoff & Smith 2003: 113). Det gjelder også hvordan avgjørelser skal treffes, hvor stort personalet skal være, samt hvorvidt det er adgang til delegering av oppgaver. Instruksjons- og organisasjonsmyndighet er viktige instrumenter i de fleste sammenhenger hvor det eksisterer over- og underordningsforhold. Dette gjelder selvsagt også når virksomhetens ledelse skal utforme en sikkerhetsorganisasjon

bestående av de roller lovverket legger opp til. Vi har brukt en forvaltningsrettslig tilnærming til instruksjons- og organisasjonsmyndighet, men vi anser at denne også er anvendelig for en privat virksomhet, slik som vår oppdragsgiver.

Pof. § 2-7 er utgangspunktet for plikten til organiseringen av sikkerhetsarbeidet i virksomheter som behandler personopplysninger, herunder helseopplysninger. Det fremgår av pof. § 2-7 at det skal etableres klare myndighets- og ansvarsforhold for bruk av informasjonssystemet, slik at organiseringen av arbeidet med informasjonssystemet bidrar til å oppnå tilfredsstillende informasjonssikkerhet (Datatilsynet 2000). Ansvars- og myndighetsforholdene skal dokumenteres og ikke endres uten autorisasjon fra den databehandlingsansvarliges daglige leder.

7.1 Daglig leder (DL)

Rollen daglig leder følger av pof. § 2-3. Rollen er ikke nærmere definert, men henspiller eksempelvis på posisjonen som direktør, administrerende direktør, departementsråd, rådmann osv. (Schartum & Bygrave 2006: 34). Innehaveren av denne rollen er ansvarlig for at bestemmelsene i pof. kapittel 2 om informasjonssikkerhet blir overholdt, og fungerer således som en knagg for databehandlingsansvarliges plikter i denne sammenhengen.

Eier av klinikken er daglig leder av virksomheten. Dette har fremkommet i intervjuer med eieren, og understrekes dessuten av organisasjonsformen enkeltpersonforetak. Arbeidet med informasjonssikkerhet blir utført av daglig leder, og stopper opp ved hans fravær. Imidlertid er arbeidet med backup delegert til to av legesekretærene, for å sikre at det alltid blir tatt sikkerhetskopier.

Det er på det rene at en rekke av oppgavene som følger av pof. kapittel 2, ikke ivaretas pr. mai 2007. Dette gjelder spesielt de bestemmelsene som har et strategisk preg. Det siktes her til sikkerhetsledelse (pof. § 2-3), risikovurdering (pof. § 2-4), organisering, (pof. § 2-7), personell (pof. § 2-8), taushetsplikt (pof. § 2-9), sikkerhetstiltak (pof. § 2-14), sikkerhet hos andre virksomheter (pof. § 2-15) og dokumentasjon (pof. § 2-16).

Gruppen mener det bør skje en bevisstgjøring rundt de oppgaver som påligger daglig leder i forhold til ivaretakelse av informasjonssikkerhet etter personopplysningsforskriften kapittel

2. Det kunne også tenkes at det ville vært hensiktsmessig at enkelte av oppgavene gjennomføres av rollen daglig ansvarlig. Vi mener det er hensiktsmessig at de oppgavene som har et strategisk preg, gjennomføres av rollen daglig leder. De oppgaver som har et operativt preg, for eksempel backup, avviksmeldinger og fysisk sikring, ser vi for oss gjennomført av rollen daglig ansvarlig. Vi ønsker med dette å få frem forskjellen mellom de oppgaver som må gjennomføres daglig og de oppgaver som er mer langsiktige.

I det følgende redegjør vi for de oppgaver som etter gruppens syn bør gjennomføres av daglig leder.

7.1.1 Sikkerhetsledelse (pof. § 2-3)

Formålet med behandlingen av helseopplysninger og de overordnede føringene for bruk informasjonsteknologi skal beskrives i sikkerhetsmål. Det vil si at virksomheten må beskrive hva informasjonssystemet skal brukes til. Hvilke typer behandlinger skal foretas ved elektroniske hjelpemidler. Hvordan informasjonssystemet skal benyttes. Hva som er akseptabelt av privat bruk, for eksempel privat bruk av e-post. Det må også klarlegges hvordan virksomheten skal forholde seg til opplysninger som vil trenge sikring for å oppnå tilfredsstillende informasjonssikkerhet. Målene skal gjelde for hele informasjonssystemet, ikke bare de automatiserte delene, men også de manuelle.

Det skal utarbeides en sikkerhetsstrategi med utgangspunkt i sikkerhetsmålene. Strategien skal dekke alle sikkerhetsmålene og inneholde beslutninger for hvordan disse skal nås. Sikkerhetsstrategien vil inneholde konkrete planer for organisering og gjennomføring av sikkerhetsarbeidet på et grunnleggende nivå. Detaljeringsgraden vil avhenge av resultatet av risikovurderingen. Eksempelvis kan sikkerhetsstrategien kreve at all behandling av helseopplysninger skjer på utstyr som ikke er tilkoblet eksterne nett. Sikkerhetsmål og sikkerhetsstrategi skal gjennomgås jevnlig av ledelsen, eksempelvis årlig, for å avdekke om virksomhetens beslutninger er i samsvar med behovet for informasjonssikkerhet. Gjennomgangen vil danne grunnlag for eventuelle endringer som er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet.

7.1.2 Risikovurdering (pof. § 2-4)

En risikovurdering inneholder flere hovedtrinn:

- Klargjøre og identifisere hvilke opplysninger som skal behandles.
- Hva er akseptabel risiko for opplysningene
- Hvilke sikkerhetsbrudd kan opplysningene bli utsatt for
- Hva er sannsynligheten for at sikkerhetsbrudd oppstår

Før en virksomhet starter behandling av personopplysninger eller helseopplysninger skal den ha oversikt over hvilke opplysninger som vil bli behandlet med elektroniske hjelpemidler. Det skal også føres oversikt over de opplysningene hvor det er behov for sikring av konfidensialitet, tilgjengelighet eller integritet. For hver av disse opplysningene skal det avgjøres hva som er akseptabel risiko. Hva som er å anse som akseptabel risiko vil avhenge av de personvernkonsekvensene uautorisert innsyn i opplysningene vil føre til. Videre må en kartlegge de trusler og farer en antar kan redusere sikkerheten gjennom avvik og sikkerhetsbrudd. Sannsynligheten for at disse inntreffer må vurderes. Er risikoen for høy må den reduseres gjennom sikkerhetstiltak. Når det oppstår endringer som har betydning for informasjonssikkerheten, endringene kan både være interne (økt privat bruk) og eksterne (virus, hackerangrep), må det gjennomføres en ny sikkerhetsvurdering (Datatilsynet 2000).

Risikovurderingen danner grunnlaget for utarbeidelsen av de tiltakene som er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet. Risikovurderingen bør ikke være mer omfattende og formalisert enn det som er nødvendig. I de situasjonene hvor det er risiko for betydelig skade på personvernet bør de risikovurderingene som skjer være tilstrekkelig grundige.

7.1.3 Organisering (pof. § 2-7)

Bruk av informasjonssystemet som har betydning for informasjonssikkerheten, skal utføres i henhold til fastlagte rutiner etter pof. § 2-7 siste ledd. Dette innebærer at det skal lages rutiner som resulterer i tilfredsstillende informasjonssikkerhet ved utførelse av arbeidsoppgaver, samt at like oppgaver alltid utføres likt. Rutinene skal dokumenteres og gjøres kjent for virksomhetens medarbeidere. Dette kan gjøres ved hjelp av en databrukerinstruks som beskriver tillatt og ikke tillatt bruk av informasjonssystemet.

Informasjonssystemet skal utformes og settes opp på en måte som gjør at man oppnår tilfredsstillende informasjonssikkerhet. Dette arbeidet skal dokumenteres og gjøres kjent for virksomhetens ledelse. Informasjonssystemet skal utformes for å oppnå tilfredsstillende informasjonssikkerhet. Dette kan gjøres ved hjelp av brannmur for skjerming mot eksterne nett (f. eks Internett) og installasjon av antivirusprogramvare. I enkelte tilfeller hvor konsekvensene av sikkerhetsbrudd er spesielt store, kan man velge å kun gjennomføre behandlingen på utstyr som ikke er tilknyttet eksterne nett.

7.1.4 Personell (pof. § 2-8)

All bruk av informasjonssystemet medfører risiko. Derfor er den databehandlingsansvarlige pålagt å begrense bruken til det som tjenestelig nødvendig. Privat bruk er ikke absolutt forbudt, men må være kjent for den behandlingsansvarlige, og må kunne gjennomføres uten at behandlingen av personopplysninger utsettes for ytterligere trusler.

Avvik kan avdekkes ved at sikkerhetsbrudd oppdages ved gjennomgang av informasjonssystemets logger. I denne sammenhengen kan det være nødvendig at også autorisert bruk bli registrert.

Det er et krav at medarbeiderne har tilstrekkelig kompetanse for forsvarlig bruk av informasjonssystemet, dvs. at de kjenner informasjonssystemet og er i stand til å følge rutinene som er fastlagt for sikker bruk. Den databehandlingsansvarlige har også ansvar for at kompetansen holdes ved like og heves, da den digitale verden utvikler seg raskt. Databehandlingsansvarlig vil også ha behov for å kjenne til de ansattes kunnskap om IKT og informasjonssikkerhet i forhold til krav som stilles for den enkelte funksjon eller stilling (Datatilsynet 2000).

All bruk av informasjonssystemet medfører risiko. Informasjonssystemet skal kun benyttes til å utføre pålagte oppgaver. Databehandlingsansvarlig pålegges å begrense bruken av informasjonssystemet til det som er tjenestelig nødvendig. Begrensning av bruken reduserer eksponeringen av opplysningene i informasjonssystemet (Datatilsynet 2000).

7.1.5 Taushetsplikt (pof. § 2-9)

For de opplysningene hvor konfidensialitet er nødvendig skal medarbeiderne hos den behandlingsansvarlige pålegges taushetsplikt. Taushetsplikten gjelder også for informasjon som har betydning for informasjonssikkerheten. Taushetsplikten skal ikke hindre den databehandlingsansvarlige i å informere om sikkerhetstiltak ved begjæringer om innsyn, jf. helseregisterloven § 22. Den databehandlingsansvarlige skal informere de ansatte om de situasjoner hvor det er behov for konfidensialitet og hvilke konsekvenser brudd vil medføre.

7.1.6 Sikkerhetstiltak (pof. § 2-14)

De sikkerhetstiltakene som er satt i verk for å sikre konfidensialitet, tilgjengelighet og integritet kan ikke bare være avhengige av at den enkelte medarbeider følger fastlagte rutiner og som dermed er enkle å omgå. Sikkerhetstiltakene må også fungere uavhengig av den enkeltes handlinger. Dette gjøres gjennom gradering av tilgang i informasjonssystemet, eksempelvis ved at man bare har tilgang til journalene til de pasientene man behandler, og ikke alle journalene i journalsystemet.

7.1.7 Sikkerhet hos andre virksomheter (pof. § 2-15)

Databehandler er utenfor den databehandlingsansvarliges instruksjonsmyndighet. Etter pol § 15 er det derfor krav om skriftlig avtale mellom partene hvor databehandlers oppgaver er spesifisert. Ansvars- og myndighetsforhold skal også beskrives. Databehandlingsansvarlig skal være kjent med sikkerhetsarbeidet hos databehandler og jevnlig forsikre seg om at arbeidet gir tilfredsstillende informasjonssikkerhet.

7.1.8 Dokumentasjon (pof. § 2-16)

Alle tiltak med betydning for informasjonssikkerheten skal dokumenteres og dokumentasjonen skal oppbevares i fem år.

7.2 Daglig ansvarlig (DA)

Databehandlingsansvarlig er ofte et kollegialt organ, for eksempel et virksomhetsstyre, og kan således være distansert fra den behandlingen av helseopplysninger som finner sted i virksomheten. Hrl. § 30 nr. 3 stiller derfor krav til at det alltid skal være en daglig ansvarlig person som skal oppfylle den databehandlingsansvarliges plikter, herunder pliktene forbundet med informasjonssikkerhet. Avhengig av virksomhetens størrelse og antall behandlinger, kan

det være flere daglige ansvarlige å forholde seg til for den daglige lederen nevnt ovenfor. En person kan for eksempel være daglig ansvarlig for behandling av opplysninger knyttet til administrative systemer, mens en annen kan være ansvarlig for behandling av opplysninger knyttet til forskning. Dette vil være to separate behandlingsopplegg, som begge krever melding til Datatilsynet, og således må ha daglig ansvarlige personer som oppfyller databehandlingsansvarliges plikter. Det er dog ikke noe krav om at det må være forskjellige personer som er daglig ansvarlige for forskjellige behandlinger, én person kan med andre ord være daglig ansvarlig for flere forskjellige behandlinger. I mindre virksomheter er det ofte slik at den som er daglig leder også er daglig ansvarlig (Schartum 2005: 112).

Klinikken foretar to behandlinger, jf. oppgavens avsnitt 5.1. Meldinger om disse behandlingene har blitt sendt til Datatilsynet, og blitt registrert. Eier er oppgitt som daglig ansvarlig.

Det er altså på det rene at rollen daglig ansvarlig er plassert og at melding om behandling har blitt sendt til Datatilsynet. Dermed oppfyller klinikken lovgivningens krav hva gjelder plasseringen av rollen daglig ansvarlig. Imidlertid, ettersom eier både er daglig leder og daglig ansvarlig, er det grunn til å tro at de betraktninger som gjaldt for daglig leder, også gjelder for daglig ansvarlig, jf. oppgavens avsnitt 7.1.

Gruppen ser ikke noen grunn til å plassere rollen som daglig ansvarlig på noen andre enn eier. Det anbefales imidlertid at det legges større vekt på de operative oppgaver gruppen mener bør ligge på rollen, det vil si avviksbehandling (pof. § 2-6), fysisk sikring (pof. §2-10), og sikring av konfidensialitet (pof. § 2-11), integritet (pof. § 2-12) og tilgjengelighet (pof. § 2-13). Siden eier både har rollen daglig leder og daglig ansvarlig, vil ikke skillet ha stor betydning i en normal driftssituasjon. Likevel ønsker vi å opprettholde et skille mellom disse to rollene. Dette henger sammen med at de operative oppgavene må gjennomføres kontinuerlig, også i eiers fravær. Skillet mellom rollene daglig leder og daglig ansvarlig vil kunne underbygge dette, ved at det vil være enklere å identifisere oppgavene, og delegere dem midlertidig til annet personell. Det er viktig å understreke at det kun er den praktiske gjennomføringen av oppgavene som lar seg delegere[11], ikke ansvaret som sådan.

[11] Det vil i siste instans være databehandlingsansvarlig som står ansvarlig i de tilfeller gjennomføringen av oppgavene ikke finner sted eller er mangelfull.

I det følgende redegjør vi for de oppgaver som etter gruppens syn bør gjennomføres av daglig ansvarlig.

7.2.1 Avviksbehandling (pof. § 2-6)

Bruk av virksomhetens informasjonssystem som er i strid med fastlagte rutiner og sikkerhetsbrudd, skal behandles som avvik. Formålet med avviksbehandlingen er å gjenopprette normal tilstand, fjerne årsaken og hindre gjentakelse. Har avviket ført til utlevering av personopplysninger hvor konfidensialitet er nødvendig skal Datatilsynet varsles.

7.2.2 Fysisk sikring (pof. § 2-10)

For å hindre at uvedkommende får tilgang, skal utstyr som brukes i behandling av personopplysninger sikres fysisk.

7.2.3 Sikring av konfidensialitet (pof. § 2-11)

Uautorisert innsyn i helseopplysninger, samt opplysninger om informasjonssystemets sikkerhetstiltak, skal hindres. Nødvendige tiltak skal også treffes for å sikre konfidensialitet når helseopplysninger overføres. Konfidensialiteten kan sikres ved å bruke kryptering. De lagringsmedia (cd-rom, disketter, backup-taper) som inneholder konfidensielle personopplysninger skal merkes. Lagringsmedia som tas ut av bruk skal slettes fullstendig og permanent, så det ikke er mulig å få tilgang til opplysningene igjen.

7.2.4 Sikring av tilgjengelighet (pof. § 2-12)

Det må sikres tilgang til de opplysningene hvor tilgjengelighet er nødvendig. Hvilke opplysninger dette gjelder følger av risikovurderingen. For de situasjoner hvor informasjonssystemet er utilgjengelig, må det forberedes opplegg for alternativ behandling av person- og helseopplysninger. Det stilles også krav til at annen informasjon med betydning for informasjonssikkerheten skal være tilgjengelig, eksempelvis informasjon som er nødvendig for å få tilgang til reservekopier av opplysninger og etablering av alternative rutiner for behandling. Det skal tas sikkerhetskopier av personopplysninger og informasjon som er nødvendig for å gjenopprette normal drift.

7.2.5 Sikring av integritet (pof. § 2-13)

Informasjonssystemet skal sikres mot utilsiktede og uautoriserte endringer av helseopplysninger og informasjon som har betydning for arbeidet med informasjonssikkerhet. Dette omfatter også sikring mot ødeleggende programvare, det vil si både programvare som kan endre opplysninger direkte og programvare som kan endre den programvaren som behandler opplysninger (Schartum 2005: 133).

7.3 Sikkerhetsrevisor (SR)

En rolle som ikke nevnes eksplisitt i personopplysningsforskriften, er sikkerhetsrevisoren, jf pof. § 2-5. Bestemmelsen stiller krav til jevnlige sikkerhetsrevisjoner av informasjonssystemet hos virksomheten. Ved sikkerhetsrevisjonen skal det kontrolleres at vedtatte sikkerhetstiltak er satt i gang og fungerer. Ved revisjonen skal den faktiske bruken av informasjonssystemet sammenlignes med virksomhetens retningslinjer for bruk (Datatilsynet 2000). Det er her viktig å se informasjonssystemet som noe mer enn det tekniske systemet. Informasjonssystemer defineres gjerne som et system som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker (Jansen og Skagestein 2005: 62). Dette gjenspeiles også i pof. § 2-5 andre ledd, da sikkerhetsrevisjonen blant annet skal omfatte organisatoriske forhold, ved siden av sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører.

Selv om sikkerhetsrevisoren ikke nevnes eksplisitt som en rolle, er det vanskelig å tenke seg at en sikkerhetsrevisjon skal kunne gjennomføres uten at en person står for den. Forskriften gir ingen veiledning på hvorvidt sikkerhetsrevisoren skal være en ekstern eller intern person, men det må nok være en forutsetning at personen har en slik integritet at revisjonsarbeidet får tilstrekkelig kvalitet (Schartum 2005: 113).

Det eksisterer en rutine for sikkerhetsrevisjon hos oppdragsgiver. Sikkerhetsrevisjonen gir anvisning på en bestemt person i virksomheten som skal utføre den, og at den skal utføres en gang i året. Personen det gjelder er å regne som personell. Videre nevner den at eksterne leverandører skal benyttes ved gjennomgang. Den lister dessuten opp en rekke aktiviteter som inngår i sikkerhetsrevisjonen, for eksempel innkalling av ledelse og gjennomgang av referat fra forrige sikkerhetsrevisjon. Avslutningsvis oppstiller den krav til dokumentasjon av selve

prosessen, samt revidering av øvrig dokumentasjon, for eksempel sikkerhetsstrategien dersom det er nødvendig.

Rutinen for sikkerhetsrevisjon eksisterer og rollen er plassert. Rutinen later imidlertid ikke til å være i bruk. Vi anser at oppdragsgiver i praksis ikke er i samsvar med lovgivningen.

Gruppen er av den oppfatning at rutinen som finnes for sikkerhetsrevisjon bør bekreftes og tas i bruk. Selve rutinen virker fornuftig, idet den blant annet fordrer at klinikken benytter seg av eksternt personell. Det kan også være gunstig at en annen person enn eier bekler rollen som sikkerhetsrevisor. Dette kan føre til en avlastning for eier, samt en økt grad av integritet.

7.4 Personell

Personopplysningsforskriften § 2-8 omtaler personell. Benevnelsen sikter både til personer som er involvert i drift av informasjonssystemet, eksempelvis for ivaretakelse av informasjonssikkerhet, samt personer som har tilgang til opplysningene for å behandle dem til de angitte formålene (Schartum 2005: 113). Slikt personell skal etter pof. § 2-8 være autorisert for bruk. Det er irrelevant hvor personellet fysisk oppholder seg, men det er en forutsetning at de ligger under databehandlingsansvarligs fulle instruksjons- og organisasjonsmyndighet i forhold til bruken av de informasjonssystemene de er autorisert for å bruke, jf. pof. § 2-7. I denne sammenhengen er en viktig bestemmelse helseregisterloven § 13. Det fremgår her at det bare er den databehandlingsansvarlige eller dens databehandler(e) som kan gis tilgang til helseopplysninger. Med andre ord må de personene som får tilgang til helseopplysningene være underlagt deres instruksjonsmyndighet.

Det finnes en rekke personer som bruker klinikkens informasjonssystem; legesekretærer, sykepleiere og leger. Av disser er sykepleierne og legesekretærene ansatt hos klinikken, og er underlagt daglig leders instruksjons- og organisasjonsmyndighet i henhold til bruken av informasjonssystemet. De andre legene er egne enkeltpersonforetak, og klinikkens samarbeid med disse reguleres gjennom avtale. Informasjonssystemet blir brukt til føring av timelister, utskrift av resepter, legge til og oppdatere journaler mv. Med unntak av legene og to av sykepleierne, har ikke personellet egne brukeridentiteter for pålogging til journalsystemet. Dette til tross for at de har et berettiget behov for tilgang. De aktuelle personene bruker eiers brukeridentitet ved pålogging til journalsystemet.

Det faktum at det brukes en felles og lånt brukeridentitet kan være problematisk i forhold til pof. § 2-8 tredje ledd om registrering av autorisert bruk. Men antageligvis vil dagens praksis først kunne regnes som et brudd dersom det umuliggjør gjennomføring av avviksbehandlingen. Uansett er det nok klart at det ikke er en optimal løsning å ha delte brukeridentiteter, nettopp fordi det vanskeliggjør blant annet sporing av avvik. Det kan også stilles spørsmålstegn ved om § 2-8 første ledd er brutt i denne sammenhengen. Dette beror imidlertid på om man skal se på "autorisert for slik bruk" som tekniske autorisasjoner, dvs. egne brukeridentiteter, eller om det kan være nok at man har godkjenning til å bruke systemet via en felles identitet.

Etter pof. § 2-8 første ledd skal personellet som nevnt være autorisert for bruk av informasjonssystemet, samt kun nytte det til pålagte oppgaver. Dette er tilfelle for legenes bruk av informasjonssystemet ved klinikken. På bakgrunn av dette kan det utledes at legene kan sies å være underlagt den databehandlingsansvarliges instruksjonsmyndighet med hensyn til bruken av informasjonssystemet, derunder helseopplysningene. Dessuten inneholder kontrakten mellom legene og klinikken, bestemmelser om føring av journal. Instruksjonsmyndighet i forhold til bruken av informasjonssystemet og helseopplysningene kan således også utledes av denne kontrakten. På bakgrunn av dette finner gruppen det rimelig anse de tilknyttede legene som personell. Det er liten tvil om at de øvrige ansatte, det vil si eieren, sykepleierne og legesekretærene, er å regne som personell etter pof. § 2-8. Således later klinikken også til å være i overensstemmelse med hrl. § 13, selv om legene ikke er en del av virksomheten.

Selv om det kan utledes en instruksjonsmyndighet fra det faktum at legene benytter klinikkens informasjonssystem, er ikke denne instruksjonsmyndigheten eksplisitt forankret noe sted, bortsett fra punktet om journalføring i kontrakten. Kontraktene mellom eier og legene bør derfor revideres. Dette slik at databehandlinganSvarliges instruksjonsmyndighet overfor de tilknyttede legene, hva angår bruken av informasjonssystemet, blir presisert.

Optimalt sett bør også alle medarbeidere som skal bruke informasjonssystemet ha sine egne brukeridentiteter, slik at arbeidet med avviksbehandling blir lettere. Ordningen med brukeridentiteter er for øvrig i strid med virksomhetens egen datainstruks om unike

brukerkontorer og hemmelighold av passord, noe som også trekker i retning av at alle bør ha egne identiteter.

7.5 Personvernombud

Personvernombudet følger ikke direkte av helseregisterloven, men av personopplysningsforskriften § 7-12. I henhold til hrl. § 36 kan imidlertid denne ordningen være aktuell også for virksomheter som behandler helseopplysninger, da helseregisterloven er taus hva angår muligheten for å innføre ordningen. Vi vil her kun beskrive hva ordningen med personvernombud innebærer, men ikke komme med løsningsforslag i forhold til plassering i oppdragsgivers organisasjon. Dette begrunnes med at rollen er frivillig, samt at vi mener de øvrige løsningsforslagene bør prioriteres før man går nærmere inn på en vurdering om hvorvidt personvernombud bør benyttes.

Ombudet skal sørge for at den databehandlingsansvarlige følger personopplysningsloven med forskrift. Personvernombudet har nok også en rolle i forhold til det mer alminnelige sikringsarbeidet som følger av internkontrollbestemmelsen i hrl. § 17, jf. pol. § 14. Ombudet er en del av den databehandlingsansvarliges organisasjon, men forutsetter også en meldeplikt til Datatilsynet, noe som ligger implisitt i at ombudet skal være ”uavhengig”. Både databehandlingsansvarlig og Datatilsynet skal varsles om brister i informasjonssystemet. Ved å innføre personvernombud, kan virksomheter bli unntatt meldeplikt til Datatilsynet, men det ligger ingen automatikk i dette (Schartum & Bygrave 2006). Ett ombud kan være felles for flere behandlingsansvarlige.

8. Etterord

På bakgrunn av de foregående kapiteler, synes det rimelig å konstatere at klinikken i stor grad oppfyller lovens krav når det gjelder organisering av arbeidet med informasjonssikkerhet. Det vil si at de aktørene og rollene lovverket gir anvisning på er avklart og plassert. Det er imidlertid grunn til å fremheve at det later til å være et ganske betydelig avvik mellom den organiseringen dokumentasjonen gir anvisning på, og slik virksomheten i praksis forholder seg til dette. Det fører blant annet til at det er svært liten bevissthet rundt de oppgavene som følger av de ulike rollene, og at mange av disse oppgavene således ikke ivaretaes tilfredsstillende. Det gjelder spesielt strategiske oppgaver, som for eksempel arbeid med sikkerhetsstrategi. Samtidig understrekes det at man ikke uten videre kan konkludere med at arbeidet med informasjonssikkerhet i virksomheten i praksis er fraværende, til tross for at en rekke oppgaver ikke blir utført. Både dagens praksis og intervjuer med de ansatte, vitner om at det eksisterer en bevissthet rundt informasjonssikkerhet i virksomheten. Klinikken later imidlertid til å ha inntatt en mer pragmatisk holdning, hvor praktiske løsninger inngår som et viktig element. De formelle aspektene, derunder lovens krav, blir tilsvarende mindre vektlagt.

Det er gruppens vurdering at det ikke nødvendigvis vil bli spesielt kostbart å bringe virksomheten betydelig nærmere de krav lovverket stiller til arbeidet med informasjonssikkerhet. Mye av arbeidet vil oppdragsgiver kunne gjøre selv. Men enkelte oppgaver vil antakeligvis fordre bruk av eksterne konsulenter, for eksempel risikovurdering. Det er i seg selv ikke et mål at alle avvik skal utbedres umiddelbart. Det er av større viktighet at arbeidet foregår systematisk og kontinuerlig, og ikke minst at klinikken får et eierskap til arbeidet og den dokumentasjon det avstedkommer. Det er dessuten et poeng at arbeidet med informasjonssikkerhet fortsetter som en kontinuerlig prosess, og ikke stopper opp idet avvikene er utbedret.

Det vil åpenbart være å regne som en fordel i seg selv at virksomheten opererer innen rammene av gjeldende lovverk når det gjelder informasjonssikkerhet. Men en kan også se for seg at dette arbeidet vil gi andre fordeler. For eksempel kan en tenke seg at virksomheten vil stille langt sterkere i en situasjon hvor et brudd på personvernet skulle oppstå. Virksomheten vil antakeligvis også være bedre rustet til å håndtere uønskede situasjoner som er av en mer driftsmessig karakter, for eksempel svikt i maskin- eller programvare.

9. Om gruppearbeidet

Gruppen består av Asbjørn Korsbakken, Erik Hornnes, Leif Uwe Vogelsang og Øivind Langeland. Dag Wiese Schartum har fungert som gruppens veileder.

Gruppen har avholdt gruppemøter ukentlig. Intensiteten og lengden på disse møtene har typisk økt foran spesielle hendelser. For eksempel møter med veileder eller oppdragsgiver, eller i anledning innsending av utkast. Møtenes form har variert etter formålet. Innledningsvis ble mye tid brukt til diskusjon om oppgavens innhold. I forkant av intervjuene har møtene fungert som rollespill, for å forberede gruppen til intervjusituasjonen. Mot slutten av oppgaven har møtene gått med til diskusjon om de ulike bidragene gruppens medlemmer har produsert, så vel som oppgaven under ett.

Vi har vært opptatte av at alle skal delta i lik grad, og at ingen skal gjøre for mye eller for lite. Det har dessuten vært et poeng for gruppen at intense og engasjerte diskusjoner kan være et gode, så lenge de forblir konstruktive og saklige. Dette synes vi at vi har lykkes med.

Gruppen har jevnlig vært i kontakt med veileder, både for korte avklaringer og lengre diskusjoner. Kontakten har funnet sted både gjennom møter og e-post. Uansett har alltid gruppen i sin helhet vært en del av denne dialogen, selv om kun et utvalgt gruppemedlem har fungert som kontaktpunkt mot veileder.

For å sørge for passende progresjon har gruppen benyttet seg av regnearkmodulen som tilbyes gjennom Google Docs[12]. For å lagre og distribuere dokumenter, samt for å holde rede på ulike dokumentversjoner mv., har gruppen benyttet en form for Wikipedia[13]. Denne har imidlertid kun vært åpen for gruppens medlemmer. Endelig har gruppen benyttet en e-postliste[14] for å koordinere arbeidet.

[12] http://docs.google.com
[13] http://wiki.forvaltningsinformatikk.no
[14] bachelor@forvaltningsinformatikk.no

10. Kilder

10.1 Litteraturliste

Datatilsynet (2000): *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.* Oslo: Datatilsynet

Jansen, Arild og Gerhard Skagestein (2005): "Sikkerhet i informasjonssystemer og infrastrukturer." I: *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT.* Jansen, Arild og Dag Wiese Schartum (red.). Bergen: Fagbokforlaget Vigmostad og Bjørke AS

Eckhoff, Torstein og Eivind Smith (2003): *Forvaltningsrett.* Oslo: Universitetsforlaget

Personvernnemda (2002): *KLAGESAK 2002/08. Klage på Datatilsynets vedtak om overføring av biologisk materiale fra Ullevål sykehus til forskeren.*

Schartum, Dag Wiese (2005): "Krav til sikring av personopplysninger." I: *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT.* Jansen, Arild og Dag Wiese Schartum (red.) Bergen: Fagbokforlaget Vigmostad og Bjørke AS

Schartum, Dag Wiese og Lee Bygrave (2004): *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger.* Bergen: Fagbokforlaget Vigmostad og Bjørke AS

Schartum, Dag Wiese og Lee Bygrave (2006): *Rapport 2006. Utredning av behov for endringer i personopplysningsloven* Oslo: Justis- og politidepartementet

Sosial- og helsedepartementet (1999): *Ot.prp.nr. 5 (1999-2000). Om lov om helseregistre og behandling av helseopplysninger (helseregisterloven)* Oslo: Sosial- og helsedepartementet.

10.2 Benyttede lover og forskrifter

Lov om helseregistre og behandling av helseopplysninger av 18. mai 2001 nr. 24

Lov om behandling av personopplysninger av 14. april 2000 nr. 31

Forskrift om behandling av personopplysninger 15. desember 2000 nr. 1265

10.3 Intervjuer og dokumentasjon

- 29. januar 2007: oppstartsmøte med eier og daglig leder
- 5. mars 2007: intervju med eier og daglig leder
- 21. mars 2007: intervju med leder for sykepleiere
- 21. mars 2007: intervju med leder for legesekretærer
- 25. april 2007: oppfølgingsmøte med eier og daglig leder
- Dokumentasjon fra Datatilsynets stedlige tilsyn