Datatilsynet

NTNU

7491 TRONDHEIM

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	09/01118-15 /CBR	23. april 2010

Oversendelse av endelig kontrollrapport og vedtak

Den 30. september 2009 gjennomførte Datatilsynet en kontroll hos NTNU. Kontrollen skjedde med hjemmel i lov om behandling av helseopplysninger av 18. mai 2001 nr. 24 (helseregisterloven) § 31. Kontrollen var knyttet særlig til bruk av pasientjournaler ved Norsk senter for elektronisk pasientjournal (NSEP).

Datatilsynets oversendte en foreløpig kontrollrapport til NTNU den 23. november 2009, og mottok virksomhetens tilsvar i brev av 7. desember og 14. desember 2009. Datatilsynet har også mottatt merknader til den foreløpige rapporten fra Anders Grimsmo og Carl Fredrik Bassøe.

1 NTNUs tilsvar og Datatilsynets merknader

1.1 Om det enkelte forskningsprosjekt, rapportens pkt 7.2

I sitt tilsvar anfører NTNU at Datatilsynet har misforstått, når det legger til grunn at de forskningsprosjektene som er fremlagt for tilsynet under kontrollen er meldt personvernombudet og gitt nødvendige konsesjoner[1].

NTNU opplyser at ingen av de prosjektene som ble fremlagt for Datatilsynet under kontrollen har benyttet opplysninger fra angjeldende pasientjournaler. Prosjektene er således ikke direkte relevante i denne forbindelse.

I e-post av 18. mars 2010 ba Datatilsynet om at NTNU fremla en oversikt over hvilke prosjekter som faktisk har benyttet angjeldende pasientjournaler, og opplyste om hvorvidt disse var meldt personvernombudet og eventuelt gitt konsesjon.

En slik oversikt ble sendt tilsynet 7. april 2010. Den viser at angjeldende opplysninger er brukt i forbindelse med 19 prosjekter. Ingen av disse er meldt til NSD, som er virksomhetens

[1] Jf rapportens pkt 7.2

Postadresse: Postboks 8177 Dep 0034 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

personvernombud. De er ikke lagt frem for forskningsetisk komité, og det er heller ikke søkt om dispensasjon fra taushetsplikten.

1.2 Om samarbeidet med Surnadal legesenter

NTNU har i samarbeid med Anders Grimsmo oversendt en intensjonsavtale inngått mellom virksomhetene i 1990. Datatilsynet har vurdert avtalen, men finner ikke at den medfører endringer i våre vurderinger. Avtalen tilfredsstiller ikke helseregisterlovens krav til en gyldig databehandleravtale.

NTNU har videresendt kommentarer fra Anders Grimsmo, og sier seg enig i Grimsmos vurdering om at det er vanskelig å skille mellom behandlinger som har forskningsformål og behandlinger som har kvalitetssikringsformål. Også Datatilsynet kan si seg enig i dette. Imidlertid har det liten innvirkning i foreliggende sak, da behandlingen etter tilsynets vurdering uansett strider mot krav som gjelder uavhengig av formål.

1.3 Feil i navn og begreper

Datatilsynet har endret alle påberopte feil i navn og begreper.

1.4 Informasjonsplikt

Datatilsynet har varslet NTNU om at det vil fatte vedtak om at virksomheten må informere de pasientene hvis journaler er omfattet av behandlingen, jf helseregisterlovens § 24.

I sitt tilsvar anførte NTNU at det er svært vanskelig å gjennomføre et slikt pålegg, da opplysningene om pasientene ble slettet i 2009. Opplysninger om de aktuelle pasientene er derfor ikke lenger er tilgjengelige for NTNU.

Datatilsynet vil bemerke at plikten til å gi informasjon står svært sterkt. Det vises til at kunnskap er en nødvendig forutsetning for at den registrerte skal kunne vareta sine rettigheter, for eksempel politianmelde lovstridige forhold eller sette frem krav om erstatning. At det å slette opplysningene skal medføre at informasjonsplikten bortfaller er derfor svært uheldig. Samtidig vil en slik praksis medføre at informasjonsplikten relativt lett kan omgås.

Datatilsynet ser at det å gi *individuell* informasjon er en betydelig praktisk utfordring for NTNU, da personopplysningene er slettet. Dette er allikevel ikke til hinder for at det gis *kollektiv* informasjon til pasientene, gjennom lokalpressen og ved oppslag på de aktuelle legekontorene.

Datatilsynet har derfor besluttet å treffe vedtak i tråd med sitt varsel av 4. november 2009.

1.5 Sletting

Datatilsynet har varslet at det vil fatte vedtak om at NTNU skal slette alle opplysninger som kan utledes fra pasientjournalene ved Surnadal legesenter og fra PROMED AS.

I sitt tilsvar bekrefter NTNU at opplysningene allerede er slettet, og at avviket derfor er håndtert og lukket på vedtakstidspunktet.

Datatilsynet legger redegjørelsen til grunn, og vil allikevel ikke treffe vedtak som varslet 4. november 2009.

1.6 Fremdriftsplan

Datatilsynet bekrefter at vedtakene treffes i tråd med fremlagte fremsdriftsplan[2], slik NTNU anmoder om i sitt tilsvar.

Oppsummering av lovstridige forhold

Datatilsynet har i vedlagte rapport redegjort for relevant regelverk, stadfestet funn og foretatt vurderinger av funn opp mot regelverket. Tilsynet konstaterer en rekke alvorlige brudd på regelverket. Disse omhandler etter tilsynets vurdering:

- Sannsynlig ulovlig erverv av elektroniske pasientjournaler for rundt 116.000 pasienter.
- Manglende informasjon til berørte pasienter
- Manglende rettslig grunnlag for behandlingen
- Mangelfull sikring av helseopplysningene, herunder plikt til å forestå forsvarlig innhenting av materiale
- Manglende tillatelser (konsesjoner)
- Mangelfull internkontroll hva gjelder implementering, minst i forhold til Nasjonalt Kompetansesenter for Elektroniske Pasientjournaler (NSEP).

Utover det nedtegnet tilsynet kritikkverdige forhold ved andre virksomheter som ikke var primærgjenstanden for kontroll:

- PROMED AS for å ha forestått datafangst av elektroniske pasientjournaler fra 21 legekontor uten databehandleravtale, gjennomført med metoder som strider mot krav til forsvarlig informasjonssikkerhet og stilt dette materiale til rådighet for annet enn helsehjelp, uten å ha informert eller innhentet samtykke fra pasient eller gyldige tillatelser.
- Surnadal Legesenter ved å ha stilt til rådighet elektroniske pasientjournaler for NSEP for andre formål enn helsehjelp, uten samtykke fra pasient eller gyldige tillatelser.

Forholdene som er avdekket representerer etter tilsynets oppfatning alvorlige brudd på regelverket. Bruddene har vedvart over tid, og kritiske innvendinger fra intern varsler har ikke blitt håndtert forsvarlig hos NSEP.

Hva gjelder NTNU konstaterer tilsynet at ledelsen reagerte raskt når forholdene først ble kjent. Tilsynet mener likevel at universitetet ikke har oppfylt sin plikt i forhold til implementering av internkontroll som beskrevet ovenfor.

---

[2] Jf NTNUs brev av 14. desember 2009

Datatilsynets reaksjon

Datatilsynet har ut fra en samlet vurdering valgt å ikke anmelde NTNU for foreliggende forhold. I vurderingen er det lagt avgjørende vekt på at forholdene som er avdekket langt på vei har skjedd uten universitetsledelsens kunnskap, og i strid med interne retningslinjer. Universitetet kan kritiseres for manglende internkontroll, men ikke i en slik grad at det anses å være grovt uaktsomt, hvilket vil være kriterium for at straffebestemmelsene i regelverket kommer til anvendelse.

Hva gjelder øvrige virksomheter, herunder eventuelle brudd på lovbestemt taushetsplikt, oversendes foreliggende rapport i gjenpart til helsemyndighetene for vurdering av adekvat oppfølging.

Vedtak

Med hjemmel i helseregisterlovens § 32, vil Datatilsynet fatte følgende vedtak overfor NTNU:

1. Virksomheten må snarest, og senest *innen 31. juli 2010*, informere pasientene som er omfattet av behandlingen, slik at disse settes i stand til å ivareta egne rettigheter, jf. helseregisterlovens § 24. Informasjonen kan gis kollektivt, gjennom lokal presse og oppslag på aktuelle legekontorer.
2. Virksomheten må snarest, og senest *innen 31. desember 2011* stadfeste og implementere intern-kontroll i samsvar med personopplysningsloven § 14. I implementeringen må det legges spesiell vekt på å integrere instituttene og tilsluttede sentra. Det vises til tilsynsrapportens kapittel 8.
3. Virksomheten må snarest, og senest *innen 31. desember 2011* foreta en gjennomgang av system for håndtering av avvik og/eller sikkerhetsbrudd og verifisere at disse fungerer etter hensikten, jf. personopplysningsloven § 13, jf. personopplysningsforskriften §§ 2-6.

Klageadgang

Dette er et forvaltningsvedtak som kan påklages i henhold til forvaltningslovens kap VII om klage på enkeltvedtak. En eventuell klage må fremsettes overfor Datatilsynet, innen tre uker etter mottak av dette brev.

Kort om forhold i andre virksomheter

Datatilsynet har mottatt skriftlige redegjørelser fra både Andres Grimsmo, ved Surnadal legesenter, og fra Carl Fredrik Bassøe ved PROMED AS. Disse har ikke medført endringer i tilsynets vurderinger knyttet til forhold ved NTNU, som er tilsynsobjektet i denne saken.

Tilsynet videresender deres kommentarer til Helsetilsynet, sammen med foreliggende kontrollrapport og vedtak. Tilsynet vil be om at Helsetilsynet vurderer hensiktsmessig oppfølgning av nevnte virksomheter.

Med hilsen

Leif T. Aanensen
Avdelingsdirektør

Cecilie L. B. Rønnevik
seniorrådgiver

Vedlegg: endelig
kontrollrapport
Kopi: Statens helsetilsyn

Datatilsynet

Endelig kontrollrapport		
Saksnummer: 09/01118 Dato for kontroll: 30.09.2009 Rapportdato: 20.04.2010	Kontrollobjekt: NTNU/NSEP Sted: Trondheim	Utarbeidet av: Leif T. Aanensen Cecilie Rønnevik

1 Innledning

1.1 Sakens bakgrunn

Den 27. mai 2009 mottok Datatilsynet en henvendelse fra Helsedirektoratet[1], hvor tilsynet bes vurdere å gjennomføre kontroll med et konkret forhold ved NTNU. Henvendelsens bakgrunn var at direktoratet mottok en søknad fra NTNU om dispensasjon fra helsepersonellovens bestemmelser om taushetsplikt, i forbindelse med forskning. Under behandlingen fremkom opplysninger som gjorde at direktoratet stilte NTNU spørsmål om hvorvidt behandlingen hadde startet opp før de nødvendige tillatelser var innhentet. NTNU valgte da å trekke søknaden tilbake.

Datatilsynet fikk oversendt en kopi av dokumentene fra direktoratets saksbehandling. Tilsynet besluttet på bakgrunn av dokumentasjonen å gjennomføre en stedlig kontroll ved virksomheten den 30. september 2009.

Formålet med kontrollen var å klarlegge omstendighetene rundt innhenting og bruk av elektroniske pasientjournal ved NTNU, Norsk senter for elektroniske pasientjournalers (NSEP). Herunder belyse hvordan journalene er skaffet til veie, og i hvilke grad det er gjennomført lovstridig behandling av materialet.

1.2 Det rettslige grunnlaget for kontrollen

Kontrollen ble gjennomført med hjemmel i lov om behandling av helseopplysninger av 18. mai 2001 nr 24 (helseregisterloven). Det vises spesifikt til helseregisterlovens § 31 annet ledd, hvoretter Datatilsynet kan kreve de opplysningene som trengs for at tilsynet kan gjennomføre sine oppgaver, samt § 31 første ledd som bestemmer at Datatilsynet skal føre kontrollen med at helseregisterloven med forskrifter blir fulgt, og at feil eller mangler blir rettet.

Den 1. juli 2009 trådte helseforskningsloven i kraft. Loven regulerer behandling av helseopplysninger i forbindelse med helseforskning, og er å anse som en særlov i forhold til helseregisterloven. De forholdene som kontrollen omfatter ligger tilbake i tid, før helseforskningslovens ikrafttredelse. Det innebærer at det, uansett formål, er helseregisterlovens bestemmelser som regulerer den aktuelle virksomheten, og som regulerer hvilken kompetanse Datatilsynet har i forbindelse med kontrollen.

[1] Datatilsynets saksnr 09/00503-2

1.3 Kontrollobjektet

Kontrollen er i utgangspunktet begrenset til å omfatte forhold som NTNU svarer for, som behandlingsansvarlig i henhold til helseregisterlovens bestemmelser og som eventuell databehandler for andre virksomheter.

For å belyse dette på en tilfredsstillende måte har det vært nødvendig for tilsynet å belyse og vurdere forhold hos virksomhetene PROMED AS og Surnadal legesenter, som behandlingsansvarlig for behandlinger hvor NTNU eventuelt har vært å anse som databehandler. En kopi av kontrollrapporten vil oversendes Helsetilsynet, for eventuell oppfølgning i henhold til helsepersonellovens bestemmelser.

I det følgende vil Datatilsynet beskrive de faktiske forhold som ble avdekket under kontrollen. Kontrollrapporten danner grunnlag for Datatilsynets vurderinger, eventuelle pålegg og reaksjoner.

2 Kontrollgjennomføringen

Kontrollen ble gjennomført som en stedlig kontroll hos virksomheten. Det ble gjennomført både plenumssamtaler og individuelle samtaler med ansatte ved NTNU. De individuelle samtalene ble gjennomført med representanter fra virksomhetens ledelse tilstede. Det ble foretatt lydopptak, etter samtykke fra de involverte.

Forutfor den stedlige kontrollen gjennomførte Datatilsynet et telefonintervju med en ansatt ved NTNU, som tidligere var involvert i den aktuelle forskningen. Vedkommende har over tid tatt opp problemet rundt datasettene, internt ved Norsk senter for elektroniske pasientjournaler (NSEP). Flere kilder ved NTNU bekrefter også at de har mottatt bekymringsmeldinger fra stipendiaten. Han var bekymret over at det ble behandlet identifiserbare helseopplysninger, uten at det var innhentet nødvendige godkjenninger fra REK og Datatilsynet. Tidligere leder ved senteret kunne fortelle at stipendiaten flere ganger hadde tatt opp spørsmålet med han, og at drøftelsene hadde intensivert seg medio 2007. Stipendiaten kontaktet etter hvert administrasjonen ved NTNU som satte i gang egne undersøkelser i saken.

Datatilsynet kreditterte NTNU for å ha reagert adekvat etter at de mottok varsel fra stipendiaten om forholdene. Universitets undersøkelser ble stilt i bero etter at varsel om kontroll ble mottatt. Universitetet har likevel iverksatt arbeider som tar sikte på å forhindre tilsvarende hendelser i fremtiden.

Under kontrollen stilte virksomheten med et bredt panel som på en fyldestgjørende måte belyste de problemstillinger kontrollen omhandlet. Tilsynet vil uttrykke tilfredshet med den åpenhet universitet viste, hvilket bidro til en god og effektiv kontroll. Det er tydelig at virksomheten har hatt en grundig intern gjennomgang av saken, i forkant av kontrollen.

Følgende personer deltok under kontrollen:

2.1 Fra virksomheten

- Helge Klungland (prodekanus, Det Medisinske Fakultet)
- Kari Håland (rådgiver , DMF)
- Anne Marie Snekvik (juridisk rådgiver, NTNU)
- Anders Grimsmo (Professor ISM/daglig leder NSEP)
- Carl-Fredrik Bassøe (Professor, NSEP)
- Arild Faxsvaag (fungerende daglig leder NSEP)
- Trond Stillaug Johansen (rådgiver NSEP)
- Terje Røsand (overingeniør NSEP/ISI)
- Guttorm Sindre (Instituttleder IDI/NTNU)
- Øystein Nytrø (1. amanuensis IDI)
- Rune Nordbø Skillingstad (IT-sikkerhetsansvarlig DMF)
- Lars Jacob Stovner (Instituttleder INM)

I tillegg til å være ansatt ved NTNU er Anders Grimsmo og Carl-Fredrik Bassøe engasjerte i andre virksomheter. Grimsmo er kommuneoverlege i Surnadal, og ansatt i Surnadal legesenter. Bassøe har vært daglig leder i virksomheten PROMED AS. Det presiseres her at Grimsmo og Bassøe primært deltok i kontrollen som representanter for NTNU/NSEP, ikke som representanter for henholdsvis Surnadal legesenter og PROMED AS.

2.2 Fra Datatilsynet

- Leif T. Aanensen
- Cecilie Rønnevik

3 Generelt om NTNU og NSEP

NTNU er et av Norges største universiteter med rundt 20.000 studenter og uteksaminering av rundt 3.000 studenter årlig. Universitetet er tildelt hovedansvaret for den høyere teknologiutdannelsen i Norge. Det er totalt ca 4.500 ansatte i virksomheten, hvorav ca 2.700 er knyttet til undervisning og forskning. Årlig budsjett er på rundt 4,4 milliarder kroner.

Universitetet er organisert med syv fakultet. De syv fakultet er henholdsvis:

- Det humanistiske fakultet (HF)
- Det Medisinske fakultet (DMF)
- Fakultet for arkitektur og billedkunst (AB)
- Fakultet for informasjonsteknologi, mattematikk og elektroteknikk (IME)
- Fakultet for ingeniørvitenskap og teknologi (IVT)
- Fakultet for naturvitenskap og teknologi (NT)
- Fakultet for samfunnsvitenskap og teknologiledelse (SVT)

Under disse fakultetene sorterer 53 institutter. I forbindelse med denne kontrollen er følgende institutter sentrale:

- Institutt for nevromedisin (INM) som sorterer under DMF
- Institutt for datateknikk og informasjonsvitenskap (IDI) som sorterer under IME

Under enkelte institutter er det organisert kompetansesentre. Norsk senter for elektroniske pasientjournaler (NSEP) er eksempel på et slikt senter. Senteret er tverrfaglig og henter primært kompetanse fra de to ovennevnte institutter. Senteret har en egen faglig leder og tilrettelegger, men har denne ikke personalansvar. Det ligger til de respektive instituttlederne.

Uavhengig av ovennevnte organisering, er alle ledd administrativt underlagt den internkontroll som skal fastlegges av universitets ledelse. Under kontrollen var universitets øverste ledelse representert ved prodekanus Helge Klungeland (DMF).

NSEP er formelt organisert inn under institutt for nevromedisin (som igjen ligger under det medisinske fakultet), men har et vesentlig innslag av medarbeidere fra institutt for datateknikk og informasjonsvitenskap. Kompetansesentrene synes opprettet for å bygge bro mellom ulike disipliner i universitetsmiljøet. Gjennom slike sentre kan det trekkes veksler på kompetanse som normalt forvaltes av instituttleder, men som for kortere eller lengre periode kan stilles til senterets rådighet.

Ved NTNU skjer det utstrakt forskning på helseopplysninger, for eksempel ved det medisinske fakultetet. Opplysningene hentes normalt fra St. Olav sykehus HF, som NTNU har et naturlig og tett forskningssamarbeid med. I tillegg benyttes opplysninger fra Helseundersøkelsen i Nord-Trøndelag (HUNT), som NTNU har databehandlingsansvaret for.

NSEPs kjernevirksomhet er forskning på bruk av elektroniske pasientjournaler, hvilket fordrer kompetanse innen både medisin og informatikk. Under kontrollen fremkom at det ikke har blitt behandlet helseopplysninger ved NSEP, utover i de tilfellene som kontrollen omfatter.

I den videre rapport vil det være omstendighetene rundt NSEP som er i hovedfokus. Databehandlingsansvaret ligger imidlertid formelt sett hos rektor ved universitetet. Hva gjelder ansvar og virksomhetsintern delegering og oppfølging vil dette bringes inn hvor det faller naturlig.

4 Nærmere om opplysningenes opprinnelse, karakter og omfang

Det er identifisert to kilder til pasientjournalene ved NSEP:

Surnadal legesenter
Kommuneoverlege i Surnadal kommune, Anders Grimsmo, er ansatt i et professorat ved NSEP. Han har en perioden mellom 2004 og 2008 fungert som daglig leder ved senteret. Grimsmo har for tiden permisjon fra denne funksjonen.

I 2004 brakte han med seg en kopi av pasientjournalene ved Surnadal legesenter til NSEP. Dette er journaler som han hadde tilgang til som ansatt ved Surnadal legesenter og kommuneoverlege i Surnadal. Datasettet er en ren kopi av elektroniske pasientjournaler for rundt 6.000 pasienter ved legesenteret.

Journalene ble tatt med til NSEP med det formål å trekke veksler på kompetansemiljøet ved senteret. Datasettet ble lagret på en frittstående maskin i NSEPs lokaler.

PROMED AS
Daglig leder ved PROMED AS, Carl-Fredrik Bassøe, har utviklet elektroniske pasientjournalsystemer som har vært i bruk ved minst 21 legekontor. Bassøe opplyser å ha hatt faktisk tilgang til journalene som driftsansvarlig for sine kunder.

Fra medio 2007 gikk Bassøe inn i et professorat ved NSEP, frem til juli 2009. Bassøe gikk da inn i en 20% stilling, med varighet frem til 31.13.2009.

Kort tid etter tiltredelse brakte han med seg en kopi av sine kunders elektroniske pasientjournalsystemer. Datasettet omfatter fullverdige elektroniske pasientjournaler for rundt 110.000 pasienter ved nevnte legekontorer. Datasettet ble lagret på en frittstående maskin i NSEPs lokaler.

PROMED AS er etter det opplyste under avvikling.

Felles for de aktuelle journalopplysningene er at de i sin helhet er produsert i primærhelsetjenesten, hvilket innebærer at opplysningene:

- Ofte beskriver pasientens helhetlige helsesituasjon over tid
- Kan innbefatte både somatiske og psykiatriske helseopplysninger
- Inneholder tilbakemeldinger fra spesialisthelsetjenesten
- Kan omtale forhold om tredjeperson, dvs. pasientens nære relasjoner

Det betyr at materialet om den enkelte pasient vil kunne være omfattende og svært sensitiv karakter.

5 Identifisering av formålet med behandlingen ved NTNU

En behandling etter helseregisterloven defineres ut fra behandlingens konkrete formål. Behandlingsformålet vil være bestemmende for hvilke krav lovverket oppstiller til den aktuelle behandlingen. For eksempel er det vesentlige forskjeller i regelverket knyttet til forskning og regelverket knyttet til helsehjelp.

Representantene fra NSEP og PROMED AS hevdet at materialet egentlig ikke var stilt til rådighet for NSEP, men at man kun oppbevarte datasettene der. Videre ble det hevdet, minst fra en av kildene, at i den grad medarbeidere i NSEP arbeidet på med opplysningene, så var det på oppdrag fra den behandlingsansvarlige. Prodekanus avviste en slik mulighet. Alle som

hadde hatt befatning med materialet, mens det ble oppbevart i NSEPs lokaler, måtte anses som ansatt ved NTNU og gjennomførte sitt arbeide med materialet som ansatt ved NTNU. Både representanten fra *PROMED AS* og representanten fra *Surnadal legesenter* hevdet videre at journalopplysningene ble behandlet ved NSEP som et ledd i systemutvikling og/eller kvalitetsikring av virksomheten ved Surnadal legesenter og hos PROMEDs kunder. De bestrider at formålet med oppbevaring og bruk av pasientopplysningene ved NSEP var forskning.

Det ble anført, også fra *NTNU*, at systemutvikling, kvalitessikring og forskning i praksis er to sider av samme sak, og at formålene vanskelig kan skilles fra hverandre. Det fremstår derfor også som uklart når man går fra kvalitetssikringsformål over til forskningsformål. NTNU bestred imidlertid ikke at det arbeidet som har funnet sted også har dannet grunnlag for flere forskningsprosjekter ved NSEP.

Datatilsynet er enig i at grensen mellom kvalitetssikring, systemutvikling og forskning kan oppleves uklar. Datatilsynet vil derfor vurdere om helseregisterlovens bestemmelser er ivaretatt, ut fra alle de påberopte formål, jf kapittel 6 flg.

6 Funn og avvik fra krav om behandlingsgrunnlag

I henhold til helseregisterlovens § 5 kan helseopplysninger behandles elektronisk bare når det er basert på samtykke, følger direkte av lov eller er tillatt etter personopplysningslovens § 9. Dette er gjerne formulert som et krav om at det skal foreligge et behandlingsgrunnlag.

6.1 Helsehjelpsformål

Elektroniske pasientjournaler er å anse som behandlingsrettede registre, jf helseregisterlovens § 6. Det primære formålet med pasientjournaler er å gi helsehjelp, dvs å gi grunnlag for handlinger som har forebyggende, diagnostiske, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient, samt administrasjon av slike handlinger, jf helseregisterlovens § 2 nr 7.

Representanten fra *Surnadal legesenter* anfører at den behandlingen som har funnet sted ved NTNU er å anse som en del av den helsehjelpen som blir gitt pasientene ved Surnadal legesenter.

6.1.1 Databehandlingsansvarlig

Den databehandlingsansvarlige er det primære pliktssubjektet i helseregisterlovens bestemmelser, og har således hovedansvaret for at loven etterleves. Helseregisterlovens § 6 annet ledd fastslår at behandlingsansvaret for behandlingsrettede registre ligger hos den virksomhet som tar i bruk registeret. I dette tilfellet er registeret oppstått ved Surnadal legesenter.

Videre følger det av helseregisterlovens § 11 at formålet med den aktuelle behandlingen av helseopplysningene må være saklig begrunnet i den behandlingsansvarliges virksomhet.

Datatilsynet vil bemerke at det fremstår som åpenbart at helsehjelp ikke er et formål som er saklig begrunnet i NTNUs virksomhet, jf rapportens kapittel 3. Det er Surnadal legesenter som har gitt og gir helsehjelp til de aktuelle pasientene, og som således er behandlingsansvarlig for behandling av egne pasienters helseopplysninger til helsehjelpsformål.

6.1.2 Krav om rettslig grunnlag

I henhold til helseregisterloven § 5 er det et vilkår for behandling av helseopplysninger at det foreligger et rettslig grunnlag for behandlingen, jf personopplysningslovens § 9.
Når Surnadal legesenter behandler helseopplysningene i egne pasientjournaler for helsehjelpsformål, skjer dette med hjemmel i helsepersonellovens bestemmelser om pasientjournal. Det rettslige grunnlaget for behandlingen er lovhjemmel, jf personopplysningslovens § 9 litra b.

6.1.3 NTNUs rolle i behandlingen – databehandler?

Den behandlingsansvarlige kan sette bort hele eller deler av sin behandling av helseopplysninger til en annen virksomhet. Behandlingen gjennomføres da i den andre virksomheten på vegne av den behandlingsansvarlige, i en databehandlerrelasjon, jf helseregisterlovens § 2 nr 9 jf § 18.

For at det skal foreligge en gyldig databehandlerrelasjon mellom å legesenteret og NTNU, må det inngås en databehandleravtale, hvor legesenteret delegerer sin kompetanse til NTNU og samtidig etablerer instruksjonsmyndighet overfor NTNU i forbindelse med den aktuelle behandlingen.

Datatilsynet har fått seg forelagt en databehandleravtale som var inngått mellom Surnadal legesenter og NTNU/NSEP. Formålet med avtalen var å delegere ansvar for blant annet å utvikle og teste ut løsninger som kan forbedre informasjonssikkerheten og gi beslutningsstøtte i diagnostikk og behandling, fra Surnadal legesenter til NTNU.

Avtalen ble inngått den 15. desember 2008. Pasientjournalene var imidlertid stilt til disposisjon ved NTNU allerede i 2004. Dette medfører at den behandlingen som har funnet sted ved NTNU i perioden mellom 2004 og 2008 ikke under noen omstendighet kan anses å være hjemlet i en databehandlerrelasjon knyttet til helsehjelpen ved Surnadal legesenter.

Avtalen var signert av daværende daglig leder ved NSEP, Andres Grimsmo, på vegne av NTNU. For Surnadal legesenter har Agnete Halgunset signert avtalen. Da Andres Grimsmo både var ansatt ved Surnadal legesenter og var daglig leder for NSEP, kan det stilles spørsmål ved hans habilitet og derfor også avtalens gyldighet.

Fra NTNU ble det uansett presisert under kontrollen at stillingen som daglig leder ved NSEP ikke gir fullmakt til å inngå denne type avtaler på vegne av NTNU. Det kan derfor stilles spørsmål ved om avtalen er inngått med bindelde virkning for NTNU.

Datatilsynet finner det etter dette ikke dokumentert at NTNUs behandling av pasientjournaler fra Surnadal legesenter har vært hjemlet i helseregisterlovens § 6 jf helsepersonellovens

bestemmelser om journal, delegert til NTNU i en databehandleravtale i henhold til helseregisterlovens § 18.

6.2 Kvalitetssikringsformål

Både representanten fra Surnadal legesenter og fra PROMED AS anførte at den behandlingen som har skjedd ved NTNU har skjedd som ledd i kvalitetssikring av helsehjelpen i henholdsvis Surnadal legesenter og de legekontorene som er kunder av PROMED AS.

6.2.1 Databehandlingsansvarlig

Helsepersonellovens § 26 gir hjemmel for kvalitetssikring innen helsetjenesten. Den gir helsepersonell adgang til å gi opplysninger til ledelsen i den virksomheten man er ansatt, blant annet når dette er nødvendig for kvalitetssikring av tjenesten. Bestemmelsen gir føringer for hvordan kvalitetssikringen skal gjennomføres. Blant annet heter det at opplysningene så langt det er mulig skal gis uten individualiserende kjennetegn.

Bestemmelsen regulerer *intern* kvalitetssikring i den enkelte virksomhet, og gir ikke hjemmel for *utlevering* av helseopplysninger til andre virksomheter for dette formålet.
Det er ikke tvilsomt at det er det enkelte legekontoret som er behandlingsansvarlig for kvalitetssikring av egen tjeneste.

6.2.2 Rettslig grunnlag

I henhold til helseregisterloven § 5 er det et vilkår for behandling av helseopplysninger at det foreligger et rettslig grunnlag for behandlingen, jf personopplysningslovens § 9.

Når et legekontor behandler helseopplysningene i egne pasientjournaler for kvalitetssikringsformål, skjer dette med hjemmel i helsepersonellovens § 26. Det rettslige grunnlaget for behandlingen er lovhjemmel, jf personopplysningslovens § 9 litra b.

6.2.3 NTNUs rolle i behandlingen – databehandler?

Den behandlingsansvarlige kan sette bort hele eller deler av sin behandling til en annen virksomhet. Behandlingen gjennomføres da i den andre virksomheten på vegne av den behandlingsansvarlige, i en databehandlerrelasjon iht helseregisterlovens § 2 nr 9 jf § 18.

Surnadal legesenter

Datatilsynet fikk seg forelagt en databehandleravtale, inngått mellom Surnadal legsenter og NSEP. Denne er omtalt under pkt 4.3. Datatilsynet finner ikke at NTNUs behandling av pasientjournaler fra Surnadal legesenter har vært hjemlet i helsepersonellovens § 26, delegert til NTNU i en databehandleravtale i henhold til helseregisterlovens § 18.

PROMED AS

For at NTNU skal kunne påberope seg kvalitetssikringsformål for sin behandling av opplysninger fra PROMED AS sine kunder, må det være etablert en databehandlerrelasjon direkte mellom de aktuelle legekontorene og NTNU. Noen slik avtale foreligger ikke.

Alternativt kan det etableres en databehandlerrelasjon mellom legekontorene og PROMED AS, og videre mellom PROMED AS og NTNU hvor kvalitetssikringsarbeidet delegeres ytterligere. En slik videre delegasjon skal på forhånd være avklart med den behandlingsansvarlige, i dette tilfellet legekontorene.

For at PROMED AS skal kunne delegere arbeidet med kvalitetssikringen til NTNU, må det først foreligge en avtale *mellom PROMED AS og de ulike legekontorene*. Representanten fra PROMED AS hevder å ha innhentet skriftlig samtykke fra flere legekontorer til kvalitetssikringsformål, innhentet i 2007. Videre presiseres det under kontrollen at de ulike legekontorene uansett har vært inneforstått med PROMED AS sin praksis.

Datatilsynet har fått seg forelagt en rekke tillatelser, gitt fra ulike legekontorer. Ordlyden i tillatelsen er standardisert og lyder som følger:

> *"Undertegnede gir PROMED AS tillatelse til å bruke mine anonymiserte data i databasen PROMED.MDB til forskningsformål. Det er en forutsetning at data ikke skal kunne tilbakeføres til noen av pasientene eller til meg og andre PROMED-brukere."*

Da det etter erklæringens ordlyd er en klar forutsetning at opplysningene skal være anonymiserte før PROMEDs behandling tar til, kan ikke dette ses som en tillatelse til å behandle identifiserbare opplysninger til kvalitetssikrings- eller utviklingsøyemed. Tilsynet vil uansett bemerke at en slik ensidig erklæring ikke på noen måte tilfredsstiller helseregisterlovens krav til en databehandleravtale.

Datatilsynet finner det etter dette ikke dokumentert at PROMEDs behandling av pasientjournaler fra de aktuelle legekontorene har vært hjemlet i helsepersonellovens § 26 om kvalitetssikring, delegert til virksomheten i en databehandleravtale i henhold til helseregisterlovens § 18.

Datatilsynet har ikke fått seg forelagt noen databehandleravtale mellom NTNU og PROMED AS. Da PROMED AS selv ikke har hatt tillatelse til selv å behandle de aktuelle opplysningene for kvalitetssikringsformål, ville en eventuell avtale *mellom PROMED AS og NTNU* uansett ikke ha vært gyldig.

6.3 Systemutviklingsformål

Både PROMED AS og Surnadal legesenter anførte at behandlingen kunne ses som systemutvikling, som kvalitetssikring og utvikling av de elektroniske journalsystemene som ble brukt i virksomheten.

Systemutvikling, utover det som faller inn under helsehjelps- og kvalitetssikringsbegrepet i helsepersonelloven, er ikke hjemlet direkte i lov. Behandlingen kan eventuelt hjemles i andre rettslig grunnlag i henhold til helseregisterlovens § 5 jf personopplysningslovens § 9.

6.3.1 Samtykke

Et frivillig, uttrykkelig og informert samtykke fra den registrerte selv er normalt et relevant behandlingsgrunnlag for systemutviklingsformål, jf helseregisterlovens § 5 jf personopplysningslovens § 9 litra a.

Det er ikke dokumentert at *PROMED AS* har hentet inn samtykke fra pasientene til den behandlingen som har skjedd ved PROMED AS eller ved NTNU, eller at slik samtykke er hentet inn av PROMEDs kunder.

Heller ikke *Surnadal legesenter* har dokumentert å ha hentet inn samtykke fra sine pasienter til egen eller NTNUs behandling for systemutviklingsformål. Representanten fra virksomheten opplyste at det var hengt opp en plakat i venteværelset på legesenteret, hvor pasienten ble gitt noe informasjon om samarbeidet med NTNU. Datatilsynet har ikke sett den aktuelle informasjonen, men finner uansett at ensidig informasjon fra behandlende lege vanskelig kan oppfylle helseregisterlovens krav til et uttrykkelig, frivillig og informert samtykke.

Det følger av dette at den aktuelle systemutviklingen, ikke har vært basert på samtykke fra de registrerte.

6.3.2 Alternative behandlingsgrunnlag

Personopplysningslovens § 9 h fastslår at sensitive personopplysninger kan behandles når det er nødvendig for vitenskaplige formål og samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den medfører for den enkelte.

Systemutviklingsformål, utover det som er å anse som forskning, kan vanskelig sies å være vitenskaplig arbeid. Normalt skjer systemutvikling i regi av en leverandør av programvare, som en del av dennes produktutvikling. Behandlingen skjer som en del av forretningsvirksomheten, og er ikke å anse som å ha et vitenskaplig formål.

6.4 Forskningsformål

I denne saken er det på det rene at NTNU har brukt opplysningene i forbindelse med forskning, som virksomheten er behandlingsansvarlig for. Det vises til at opplysningene er brukt i flere løpende og avsluttede forskningsprosjekter.

Forskning er et behandlingsformål som ikke direkte er hjemlet i lov. Behandlingen kan eventuelt hjemles i andre rettslig grunnlag, i henhold til helseregisterlovens § 5 jf personopplysningslovens § 9.

6.4.1 Samtykke

Et frivillig, uttrykkelig og informert samtykke fra den registrerte selv er normalt et relevant behandlingsgrunnlag for forskningsformål, jf helseregisterlovens § 5 jf personopplysningslovens § 9 litra a.

Det er imidlertid ubestridt at NTNU ikke selv har hentet inn samtykke fra noen av pasientene til forskning ved NSEP, eller har påsett at et slikt samtykke er gitt til Surnadal legesenter eller PROMED AS. Det vises til at søknaden som ble sendt Helsedirektoratet gjaldt dispensasjon fra taushetsplikten i henhold til helsepersonellovens bestemmelser. Det er ikke nødvendig med dispensasjon i de tilfeller hvor pasienten selv har samtykket til behandlingen.

6.4.2 Alternative behandlingsgrunnlag

Personopplysningslovens § 9 h fastslår at sensitive personopplysninger kan behandles når det er nødvendig for vitenskaplige formål og samfunnets interesse i at behandlingen finner sted klart overstigerulempene den medfører for den enkelte. Dette er en svært relevant bestemmelse for behandling som skjer til forskningsformål.

Datatilsynet kan imidlertid ikke se at NTNU har foretatt en interesseavveining, før behandlingen tok til for nevnte formål. Det anses derfor ikke dokumentert at en forsvarlig interesseavveining ligger til grunn for behandlingen.

Datatilsynet har uansett tolket bestemmelsen nokså strengt i sin praksis, blant annet knyttet til konsesjonsbehandling. Det blir normalt stilt som vilkår for behandlingen at opplysningene behandles avidentifisert, og at de registrerte gis anledning til å reservere seg. Dette er tiltak som minsker personvernulempen ved behandlingen.

Da behandlingen i dette tilfellet har skjedd uten at pasientene har er gitt anledning til å reservere seg, og opplysningene er behandlet ved NTNU med direkte identifiserende kjennetegn, kan Datatilsynet vanskelig se at samfunnets interesse ved behandlingen klart overstiger personvernulempen for den enkelte.

6.5 Konklusjon om behandlingsgrunnlag

Datatilsynet kan ikke se at NTNU har hatt rettslig grunnlag for sin behandling av de aktuelle opplysningene, verken som behandlingsansvarlig eller som databehandler for PROMED AS og/eller Surnadal legesenter. Dette gjelder uavhengig av hvilket formål opplysningene ble behandlet for. Dette er klart i strid med helseregisterlovens § 5 og § 18.

7 Funn og avvik fra krav om konsesjonsplikt

I henhold til helseregisterlovens § 5 plikter den behandlingsansvarlige å innhente konsesjon i henhold til personopplysningslovens § 33, ved behandling av helseopplysninger. Konsesjonen er en forhåndstillatelse gitt av Datatilsynet til den aktuelle behandlingen.

NTNU har inngått avtale med NSD som personvernombud for virksomheten. Det innebærer at konsesjonsplikten for visse forskningsprosjekter er erstattet med en meldeplikt til NSD, jf personopplysningsforskriftens § 7-27. For at konsesjonsplikten skal bortfalle er det et vilkår at NSD finner at behandlingen skjer i henhold til gjeldende regelverk, og derved tilrår behandlingen. NSD er retteslig å anse som den behandlingsansvarliges medhjelper, slik at den behandlingsansvarlige også hefter for eventuelle feil som NSD gjør.

7.1 Forskningsmaterialet - grunnregisteret

Det samlede materialet, bestående av de to basene fra Surnadal legesenter og PROMED AS, er ikke samlet inn i tilknytning til et bestemt prosjekt. Materialet kan etter tilsynets vurdering ses som et slags grunnregister, tilgjengelig for bruk i enkeltstående forskningsprosjekter.

Datatilsynet vil presisere at lovens bestemmelser om konsesjons- og meldeplikt like fullt gjelder for grunnregisteret, som for de konkrete forskningsprosjektene. Tilsynet vil videre presisere at unntaket i § 7-27 ikke vil komme til anvendelse på dette materialet. Unntaket gjelder kun for definerte og avgrensede forskningsprosjekter.

Datatilsynet har ikke registrert å ha mottatt noen søknad om konsesjon for materialet. Hvorvidt dette beror på mangelfull oppfølgning i NSEP, NTNU eller NSD er uten betydning.

Dette er å anse som et klart brudd på helseregisterlovens § 5 jf personopplysningslovens § 33.

Under kontrollen ble det opplyst at det samlede materialet, eller grunnregisteret, er slettet hos NSEP. Datatilsynet tar det til etterretning.

7.2 De enkeltstående forskningsprosjektene – bygger på grunnregisteret

Datatilsynet legger til grunn at NSD er koblet inn i forbindelse med de fleste forskningsprosjektene, og at de enten er tilrådd i henhold til personopplysningsforskriftens § 7-27 eller oversendt Datatilsynet for konsesjonsbehandling.

Da selve grunnregisteret ikke har hatt konsesjon, og opplysningene i grunnregisteret er behandlet i strid med regelverket, kan det stilles spørsmål ved om eventuelle tillatelser gitt til de ulike prosjektene som bygger på registeret er gyldige. Det vises til at tilsynets konsesjoner er gitt i tillit til, og under den klare forutsetningen av, at opplysningene behandles i henhold til gjeldende regelverk, herunder at opplysningene hentes inn på en lovlig måte.

De funn som er gjort i forbindelse med denne kontrollen har avdekket alvorlige brudd på regelverket knyttet til behandling av helseopplysninger. Det innebærer at konsesjonene er gitt på uriktige eller bristende forutsetninger, og må anses å være ugyldige.

Eventuell videre behandling av opplysningene i de ulike prosjektene må derfor bero på nye tillatelser, enten etter helseregisterloven eller helseforskningsloven, jf helseforskningslovens § 2.

8 Funn og avvik fra krav om internkontroll

Datatilsynet legger til grunn at NTNU er å anse som behandlingsansvarlig for den forskningsvirksomheten som har skjedd ved NSEP, jf pkt 6.4.

Helseregisterlovens § 17 stiller krav om at databehandlingsansvarlig skal iverksette systematiske tiltak som sikrer virksomhetens etterlevelse av regelverket. Tilsvarende har personopplysningslovens § 14 krav for de behandlinger som faller innen denne lovens virkeområde.

NTNU er en kompleks og sammensatt organisasjon. Det er dermed nødvendig å presisere avgrensningen som ble lagt til grunn ved kontrollen. Det var omstendighetene rundt innhenting av opplysninger og bruk av elektroniske pasientjournalsystemer ved NSEP som var kontrollens hovedfokus. Datatilsynet vil likevel berøre universitetets internkontroll som helhet, så langt det er relevant i saken.

Prodekanus opplyste at rektor ved universitetet er å anse som databehandlingsansvarlig for egen forskningsvirksomhet. Utover det er det fastlagt virksomhetsinternt ansvar i forhold til ordnær linjeledelse. Formelt følges denne myndighetsstruktur:

1. Rektor
2. Dekanus
3. Instituttledere

Hva gjelder denne saken er følgelig instituttledere databehandlingsansvarliges nærmeste representant og beslutningstaker ovenfor NSEP. Leder ved NSEP har ikke administrativt og personalmessig ansvar.

NTNU hadde i følge virksomheten etablert et system for internkontroll i tråd med regelverkets krav. Systemet har kontinuerlig vært under utvikling i siden medio 2004. Gjennomgang av systemet indikerte at de viktigste komponentene var tilstede. Det kunne identifiseres styrende, gjennomførende og kontrollerende elementer.

På forespørsel om avvik og avvikshåndtering opplyste virksomhetene at det var meldt svært få avvik. Tilsynet viste til at dette var en vanlig indikasjon på at systemet ikke var tilstrekkelig implementert og aktiv i virksomheten. Fravær av avviksmeldinger svekker virksomhetens muligheter for å korrigere avvik, men gir også svekkede muligheter til å utvikle systemet i en konstruktiv retning.

NTNU var usikker på hvor langt man var kommet med implementering av internkontroll på fakultets og instituttnivå. Systemet som sådan var fastsatt og det var etablert gode kanaler for å gjøre regelsettet tilgjenglig. Universitetet hadde valgt intranett som viktigste kanal.

Internkontrollsystemet ble ikke underlagt grundige vurderinger, men fungerte mer som en innfallsvinkel til de omtalte problemstillinger. Datatilsynet tar med det universitetets redegjørelse til etterretning.

Datatilsynet observerte at selv om dokumentasjonen syntes å foreligge, var det flere faktor som pekte i retning av mangler med systemet. Tilsynet sikter spesielt til håndheving av de regelsett systemet foreskriver. I sine vurderinger har tilsynet lagt vekt på:

- Tilsynelatende uklare rammer for håndhevelse av system i ytre enheter, her spesifikt i forhold til NSEP.
- Tilsynelatende uklart system for avvik og avvikshåndtering, særlig hva gjelder NSEP.
- Tilsynelatende uklare rammer for å ivareta myndighetspålagte rammer hva gjelder tillatelser og konsesjoner, særlig hva gjelder NSEP

8.1 Konklusjon vedrørende internkontroll

Datatilsynet begrenser seg i dette tilfellet til å påpeke NTNUs plikter etter nevnte bestemmelse.

Det presiseres at plikten ikke bare gjelder etablering av et system, men også å håndheve det i organisasjonen. Avvikshåndtering er et avgjørende redskap for ledelsen i et slikt arbeidet. Datatilsynet rådet universitet til å vitalisere betydningen av å melde avvik, etablere et godt mottaksapparat og sørge for handling på rett nivå for å sette i verk korrigerende tiltak ved behov.

Videre tilråder tilsynet at det skapes klarere rammer rundt ansvar og myndighet i relasjon til internkontroll. Det sentrale er å stadfeste hvem det er som håndhever pliktene nedover i organisasjonen. I prinsippet trenger ikke dette å stoppe ved instituttleder, men det bør uansett være samsvar mellom tiltenkt ansvar og myndighet.

9 Funn og avvik fra plikten til å gi informasjon

I henhold til helseregisterlovens § 24 plikter den behandlingsansvarlige å på eget tiltak å informere pasienten, når det samles inn opplysninger fra andre enn pasienten selv. Blant annet skal det gis informasjon om formålet med behandlingen, om det er frivillig å delta og annet som gjør vedkommende i stand til å ivareta egne rettigheter etter loven. Informasjonen skal gis så snart opplysningene er hentet inn.

Det er i dette tilfellet på det rene at NTNU, som behandlingsansvarlig for forskningen, ikke selv har informert pasientene om den aktuelle bruken eller har påsett at slik informasjon er gitt av Surnadal legesenter og PROMED AS.

Dette er å anse som et klart brudd på helseregisterlovens § 24.

10 Krav til forsvarlig sikring av helseopplysninger

I henhold til helseregisterlovens § 16 plikter den behandlingsansvarlige å iverksette systematiske tiltak for å sikre at helseopplysninger behandles på en forsvarlig måte. Bestemmelsen krever at det iverksettes systematiske tiltak som sikrer tilfredstillende ivaretakelse av konfidensialitet, integritet og tilgjengelighet. Utdypende bestemmelser finnes i personopplysningsforskriftens kapittel 2.

Grimsmo og Bassøe forklarte muntlig at grunnregisteret ble lagret på frittstående datamaskiner, som ikke var knyttet til nettverk ved NTNU. Disse datamaskinene var etter det opplyste spesielt bestilt for formålet. De to hadde ifølge egne vurderinger god fysisk kontroll over maskinene og styrte restriktivt hvem som fikk tilgang til dataene.

Bassøe kunne berette at i hans virke for PROMED AS, hadde det vært nødvendig å ha kopier av legenes journaler. Det ble pekt på at uten slik tilgang ville kvaliteten i videreutvikling av

journalsystemet bli mangelfull. Nye versjoner av produktet måtte, ifølge Bassøe, testes ut på reelle data før produktet ble installert hos de lokale legekontor. Utover det pekte Bassøe på nødvendigheten av sikkerhetskopi, i fall systemet hos legekontoret sviktet. De omtalte data ble lagret på en bærbar, usikret hardisk. Det var innholdet på denne harddisken som, kort tid etter Bassøe's tiltredelse som professor ved NTNU, ble lastet inn på omtalte datamaskin.

Hva gjelder Grimsmo kunne han berette at de aktuelle elektroniske journalene var brakt til NSEP ved at en utransjert server fra legesenteret med det aktuelle innhold ble transporter til NSEP's lokaler. Disse data ble senere lastet over på omtalt datamaskin. Tilsynet vil også i dette tilfellet påpeke risiko helseopplysningene utsettes for under transport, med mindre innholdet var beskyttet i form av for eksempel kryptering.

Datatilsynet vil anføre at ovennevnte praksis vitner om utilfredstillende sikkerhetskultur i et forskningsmiljø hvor bevisstheten rundt taushetsplikt og forsvarlig håndtering av helseopplysninger burde vært fremtredende. Hva tittelen til senteret indikerer, "Nasjonalt Senter for Elektroniske Pasientjournaler", skaper en forventning om hvordan slike opplysninger skal håndteres og sikres.

Etter tilsynets vurdering representerer praksisen som ble beskrevet hos PROMED AS alvorlige brudd helseregisterlovens § 16 om forsvarlig informasjonssikkerhet. Leverandøren henter i dette tilfellet systematisk ut sensitive helseopplysninger fra legenes journaler, uten at dette er eksplisitt avtalt med legen. Virksomheten kan uavhengig av hva som påstås ikke fremlegge noen dokumentasjon som underbygger en databehandlerrelasjon. Uavhengig av dette svarer en databehandler uansett for forsvarlig behandling etter nevnte bestemmelse. Datatilsynet stiller seg tvilende til om legene fullt ut har vært klar over omfanget av virksomhetens praksis. Nevnte forhold vil Datatilsynet henstille helsemyndighetene om å bringe klarhet i. Datatilsynet vil ikke forfølge nevnte forhold ovenfor NTNU, da disse har skjedd utenfor universitets kontroll og medvirking.

Datatilsynet reagerer imidlertid på at det ikke er klarere rutiner rundt etablering av grunnregisteret som universitets ansatte og studenter senere har til hensikt å forske på. Etter tilsynets vurdering må universitetet ha en tilfredstillende kontroll på at personopplysninger som samles inn, herunder helseopplysninger, er lovlig ervervet og sikres på en forsvarlig måte.

Datatilsynet velger å tro at foreliggende situasjon ikke er representativt for universitetet, men skyldes at NSEP ikke har vært tilstrekkelig integrert i universitets Internkontroll for informasjonssikkerhet. Tilfredstillende sikkerhet under datafangst, transport, overføring, uttrekk, bearbeiding og eventuell sletting må være på plass. Datatilsynet mener det er påvist utover rimelig tvil at så synes ikke å være tilfelle i denne konkrete sak.

Av ovennevnte fremgår at universitet ikke har hatt tilfredstillende informasjonssikkerhet, særlig hva gjelder NSEP's håndtering av helseopplysninger.

11 Oppsummering

Datatilsynet finner det dokumentert at det foreligger til dels grove brudd på regelverket knyttet til behandling av helseopplysninger. Dette gjelder både forhold som NTNU er ansvarlig for, og forhold som de virksomhetene NTNU har samarbeidet med har ansvaret for i henhold til helsepersonellovens bestemmelser.

Lovbruddene har i praksis medført at helseopplysninger som pasienter har avgitt i tillit til helsepersonellets taushetsplikt, i forbindelse med helsehjelp gitt ved minst 22 legekontorer, i sin helhet har blitt stilt til rådighet for forskning på NTNU, uten at de nødvendige tillatelser er hentet inn og uten at det forelå et rettslig grunnlag for behandlingen.

Det anses skjerpende at NTNU ikke kan dokumentere å ha hatt nødvendig kontroll med behandlingen av opplysningene ved NSEP. Det kan derfor reises alvorlig innvendinger i forhold til om informasjonssikkerhet har blitt tilfredsstillende ivaretatt ved behandlingen, herunder kravet til konfidensialitet.

Datatilsynet vil kreditere den stipendiaten som har reagert på praksisen og tatt forholdene opp med ledelsen, med Helsedirektoratet og med Datatilsynet. Tilsynet anser at de funn som er gjort fullt ut understøtter stipendiatens vurderinger, slik de fremkom både overfor tilsynet og overfor ledelsen ved NTNU.

Datatilsynet vil videre kreditere ledelsen ved NTNU som tok stipendiatens bekymringer på alvor, og iverksatte interne undersøkelser av påstandene. Tilsynet understreker betydningen av at de ansatte skal stå fritt til å melde fra om forhold som kan innebære brudd på virksomhetens egne retningslinjer og i verste fall brudd på norsk lov. På den annen side kan universitetet kritiseres for selv å ha brakt seg i situasjonen ved mangelfull implementering av Internkontroll.

12 Merknader om forhold i andre virksomheter

Som det er presisert tidligere er denne kontrollen rettet mot virksomheten NTNU. Datatilsynet finner det allikevel nødvendig å knytte enkelte merknader til de funn som er gjort vedrørende Surnadal legesenter, virksomheten PROMED AS, og dennes kunder.

Datatilsynet anser at lovbruddene er grove, og ber derfor om at Helsetilsynet vurderer nødvendige tiltak, i henhold til helselovgivningen.

PROMED AS
Av det skriftlige materialet fremgår at PROMED AS har samlet pasientjournaler over en lang tidsperiode. Virksomhetens representant opplyste at under kontrollen at opplysningene ble hentet inn ved at han jevnlig kopierte pasientjournalene lokalt på det enkelte legekontoret, for blant annet å ha en back-up for legekontorene. Journalene ble kopiert inn på en usikret harddisk, som ble oppbevart i vedkommendes bil og bolig. Det ble opplyst at han fremdeles har en kopi av det samlede materialet i sin bolig, som er tilkoblet et alarmselskap.

Virksomhetens representant fremstilte det som en rimelig og vanlig praksis at leverandør av et elektronisk pasientjournalsystem kunne ha kopi av legenes journaler. Tilsynet vil hevde at det strider mot enhver rimelig betraktning at en leverandør av pasientjournalsystemer skal råde over en kopi av pasientjournalene, uten at det er regulert i en databehandleravtale. Under gitte forutsetninger kan en leverandør gis tilgang til datasett for å kunne konvertere, oppgradere eller på annen måte tilpasse system. Også dette må skje under databehandlingsansvarliges kontroll.

Datatilsynet anser det sannsynliggjort at PROMED AS har disponert over materialet i strid med

- helseregisterlovens § 18, hvoretter en databehandler ikke har adgang til å behandle helseopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige (her: legekontorene),

- helseregisterlovens § 15, hvoretter den som behandler helseopplysninger etter denne lov har taushetsplikt etter forvaltningslovens og helsepersonellovens bestemmelser, og

- helseregisterlovens § 16, jf personopplysningsforskriftens kapittel 2, hvoretter en den behandlingsansvarlige og en databehandler plikter å sørge for tilfredsstillende informasjonssikkerhet. Oppbevaring av elektroniske pasientjournalene på en bærbar, usikret hardisk anses å være et alvorlig brudd på nevnte bestemmelse. Sensitive personopplysninger skal alltid være sikret med kryptering eller likende tiltak i det øyeblikk opplysningene befinner seg utenfor databehandlingsansvarliges kontroll.

PROMEDs kunder
I den grad legesentrene *har samtykket* til PROMEDs behandling kan det stilles spørsmål ved om det foreligger brudd på blant annet

- helsepersonellovens § 21, hvoretter helsepersonell har taushetsplikt om helseopplysninger,

- helseregisterlovens § 13, hvoretter den behandlingsansvarlige ikke kan gi tilgang til helseopplysninger til andre personer enn de som virksomheten har instruksjonsmyndighet over, jf helseregisterlovens § 15.

I den grad legesentrene *ikke har samtykket* til PROMEDs behandling, kan det stilles spørsmål ved om det foreligger brudd på blant annet

- helseregisterlovens § 13, hvoretter den behandlingsansvarlige ikke kan gi tilgang til helseopplysninger til andre personer enn de som virksomheten har instruksjonsmyndighet over, jf helseregisterlovens § 15, og

- helseregisterlovens § 16, jf personopplysningsforskriftens kapittel 2, hvoretter en den behandlingsansvarlige og en databehandler plikter å sørge for tilfredsstillende informasjonssikkerhet.

Surnadal legesenter
Datatilsynet finner det dokumentert at Anders Grimsmo har utlevert helseopplysninger fra Surnadal til ansatte ved NTNU. Dette er gjort uten at pasientene har samtykket til det, eller er tilfredsstillende informert om det.

I den grad Surnadal legesenter *samtykket til* at Grimsmo leverte ut opplysningene, anser tilsynet det sannsynliggjort at Surnadal legesenter har brutt følgende bestemmelser:

- helsepersonellovens § 21, hvoretter helsepersonell har taushetsplikt om helseopplysninger, og

- helseregisterlovens § 13, hvoretter den behandlingsansvarlige ikke kan gi tilgang til helseopplysninger til andre personer enn de som virksomheten har instruksjonsmyndighet over, jf helseregisterlovens § 15.

I den grad legesenteret *ikke samtykket* til utleveringen, anser tilsynet det sannsynliggjort at virksomheten har brutt følgende bestemmelser:

- helseregisterlovens § 16, jf personopplysningsforskriftens kapittel 2, hvoretter en den behandlingsansvarlige og en databehandler plikter å sørge for tilfredsstillende informasjonssikkerhet.

Andres Grimsmo personlig anses i begge tilfeller å ha brutt helsepersonellovens bestemmelser om taushetsplikt.