Datatilsynet

avgradert 25/2-08

UNNTATT OFFENTLIGHET
I medhold av
Offl. § 6 nr. 5

Datatilsynet
2004/1636- 19
14 APR. 2005
AN. 325
Saksb. FBB Avskr.

Politiet i Helgeland
Pb. 570
8651 MOSJØEN

Deres ref	Vår ref (bes oppgitt ved svar)	Dato
8547967 626/05-45	2004/1636-19 FBB/-	// .04.2005

SVIKT I RUTINER VED INNSYNSRETT I PASIENTJOURNALER – BRUDD PÅ TAUSHETSPLIKT

Datatilsynet mottok henvendelse i brev av 10.11.2004, om en avdelingsleders antatt ulovlige innsyn i sykejournaler til sine ansatte, fra tillitsvalgt i Kommunalansattes Fellesorganisasjon (KFO) ved Helgelandssykehuset HF, avdeling Mosjøen.

Datatilsynet var på tilsyn ved Helgelandssykehuset HF, avdeling Mo i Rana 02.11.2004. Tilsynet var rettet mot hele helseforetaket, og hadde fokus på kommunikasjon med primærhelsetjenesten. På tross av annet fokus, ble det avdekket grunnleggende brudd knyttet til sykehusets behandling av personopplysninger. På bakgrunn av gjennomført tilsyn 02.11.2004, samt endelig rapport, ble det i brev av 05.01.2005 fattet vedtak om pålegg om utbedring, med hjemmel i helseregisterlovens § 32. Frist til å gjennomføre påleggene ble satt til 01.07.05.

Helgelandssykehuset HF orienterte ikke selv om de ulovlige innsynene, og Datatilsynet ble heller ikke på annen måte gjort kjent med hendelsen under tilsynet. På bakgrunn av de ulovlige innsynene har Datatilsynet valgt å foreta en ny vurdering av hvilke konsekvenser Helgelandssykehusets manglende overholdelse av personvernlovgivningens regelverk skal medføre. Datatilsynet har særlig vurdert spørsmålet om Helgelandssykehuset HF har behandlet helseopplysninger på en slik måte at det foreligger et straffbart brudd på helseregisterloven, og om omstendighetene rundt behandlingen er så alvorlig at tilsynet finner det nødvendig å politianmelde forholdet.

Datatilsynet har på bakgrunn av etterfølgende vurderinger konkludert med at bruddet på helseregisterloven § 16 må politianmeldes.

Tilsynet har fått oversendt Helgelandssykehuset HFs logg over avdelingsleders innsyn, samt dokumentasjon over informasjonssystemene og sikkerhetstiltak, skjema for tildeling av brukeridentitet (gammel og ny versjon) og rapporter på tilganger til de forskjellige journalgrupper. Med mindre Helgelandssykehuset HF, avdeling Mosjøen, har gitt uttrykk for en annen praksis er dokumentasjon fra tilsynet brukt ved utredningen av denne saken.

1 Sakens faktiske bakgrunn
Det er ikke bestridt av Helgelandssykehuset HF at det er foretatt ulovlige innsyn helt tilbake til 13.09.2002 i journalnotater som strekker seg tilbake til 1993-1994.

1.1 Kronologisk oversikt
De ulovlige innsynene ble ved en tilfeldighet oppdaget 31.08.2004. De ansatte gikk inn i loggene for sine egne journaler hvor det fremgikk at avdelingsleder hadde vært inne på forskjellige journalnotater. I følge det opplyste ble ulovlig innsyn foretatt i journalen til totalt tretten ansatte. Tillitsvalgte sendte 01.09.2004 brev til sykehusdirektøren. Det ble holdt en rekke møter ved Helgelandssykehuset HF i anledning saken.

I brev av 23.09.2004 varslet Datatilsynet Helgelandssykehuset ved foretaksledelsen, om at Datatilsynet ville gjennomføre stedlig tilsyn ved sykehuset.

Helgelandssykehuset HF konkluderte og holdt et avsluttende informasjonsmøte om de ulovlige innsynene 13.10.2004. Det ble sendt brev til de berørtes fagforeninger 01.11.2004 hvor sykehuset konkluderer, og hvor det ble orientert om at sykehuset vil utarbeide nye retningslinjer for tilgang.

Datatilsynet gjennomførte stedlig tilsyn ved Helgelandssykehuset HF, avdeling Mosjøen 02.11.2004. I brev av 08.03.2005 uttrykker Helgelandssykehuset HF at det i september 2004 ble foretatt telefonisk henvendelse til Datatilsynet. Datatilsynet er ikke kjent med noen slik henvendelse[1].

Den 10.11.2004 mottar Datatilsynet henvendelse fra tillitsvalgte om de ulovlige innsynene. I brev av 01.12.2004 ber Datatilsynet om en redegjørelse fra Helgelandssykehuset HF. Den 29.12.2004 mottar Datatilsynet svar fra Helgelandssykehuset HF. I brev av 13.01.2005 mottar tilsynet ytterligere informasjon fra tillitsvalgte. Tilsynet fant Helgelandssykehusets redegjørelse i brev av 29.12.2004 mangelfull. Det ble i brev av 21.01.2005 bedt om ytterligere dokumentasjon, samt en utdypende redegjørelse. Helgelandssykehuset svarte Datatilsynet i brev av 08.02.2005.

Samme dag sender Helgelandssykehuset anmeldelse til politiet for vurdering av om det foreligger brudd på taushetsplikten. På bakgrunn av anmeldelsen sendte Datatilsynet kopi av saken til Helsetilsynet i fylket[2]. Datatilsynet fortsatte sin saksbehandling knyttet til vurdering av sykehusets informasjonssikkerhet.

Da tilsynet hadde flere eksempler som kunne gi antydning om at sykehuset trenerte saksbehandlingen og holdt tilbake informasjon, purret tilsynet i brev av 23.02.2005 på Helgelandssykehuset HF. Helgelandssykehuset HF svarte, og vedla ytterligere dokumentasjon i brev av 08.03.2005. Tilsynet har også mottatt redegjørelse fra avdelingsleder i e-post fra hans advokat 10.03.2005.

---

[1] Tilsynet vil for ordens skyld orientere om at saker av en slik alvorlighet, heller ikke saksbehandles over telefon.
[2] Spørsmål om taushetsplikt ligger innenfor Helsetilsynets kompetanseområde, og Helgelandssykehuset HFs politianmeldelse tilsa en raskere oversendelse enn det som tidligere var avtalt mellom Helsetilsynet og Datatilsynet.

I brev av 10.03.2005 fra Helgeland Politidistrikt bes Datatilsynet om en uttalelse om hvorvidt Datatilsynet vurderer hendelsen som et straffbart brudd på gjeldende lover og forskrifter.

1.2 Ansvar
Det er virksomheten ved øverste leder som har ansvar for å etablere og opprettholde tilfredsstillende informasjonssikkerhet. Helgelanssykehuset HF har ikke dokumentert noen overordnede føringer for virksomhetens bruk av informasjonsteknologi, herunder hvilke sikkerhetsrisiko de aksepterer. Det vises til tidligere utarbeidet kontrollrapport.

På tidspunkt hvor de ulovlige innsyn ble foretatt forlå det ingen dokumentasjon om delegering av plikter som tilligger databehandlingsansvarlige i henhold til helseregisterloven og personopplysningsloven, se kontrollrapport.

1.3 Opplæring
Den tidligere avdelingsleder gir uttrykk for at han ikke har fått noe opplæring knyttet til bruk av pasientjournaler. I redegjørelse fra tidligere avdelingsleder av 01.03.2005 uttrykker han at fagfeltet (medisinsk dokumentasjon) var ukjent for han da han begynte i stillingen. Han ble bedt om å sette seg inn i virkemåten til programmene under den klare forutsetning at han var underlagt fullstendig taushetsplikt. Det ble ikke stilt noen spesielt oppnevnt instruktør/veileder til disposisjon. Han uttrykker at han ble henvist til gjeldende offentlige forskrifter vedrørende journaler. Det ble ikke lagt frem noen særskilt instruks eller bedriftsinterne retningslinjer i forbindelse med journalhåndtering. Han understreker at: "I etterpåklokskap blir det tydelig at jeg burde hatt en klar tilgang på veiledning i denne opplæringssituasjonen." Det er heller ikke dokumentert at det foreligger dokumentasjon som er tilgjengelig for medarbeiderne.

1.4 Autorisasjon
Datatilsynet har forsøkt å bringe klarhet i hvilke retningslinjer som sykehuset benytter for å finne frem til hvilken autorisasjon den enkelte medarbeider får til elektronisk pasientjournal (EPJ). Sykehuset dokumenterer ingen overordnede retningslinjer eller modeller for ulik autorisering. I internnotat av 01.02.2005 uttrykkes at en bruker ikke bygges opp av maler. Sykehuset har ikke innført et detaljert "bestillingsskjema" for brukertilgang i pasientdatasystemet fordi tilgangsmatrisen er så kompleks at det vil være meget uhensiktsmessig. Tilganger blir gitt og vurdert ut fra de arbeidsoppgaver som vedkommende har. Datatilsynet har fått lister over ulike grupper autorisasjoner som er i bruk. Av disse listene synes tilgangen stort sett å være lik for de forskjellige gruppene personell.

Opprinnelig fikk Datatilsynet oversendt en ny stillingsbeskrivelse som ikke eksisterte da aktuell tilgang ble gitt. For avdelingsleders autorisasjon er det senere lagt frem stillingsbeskrivelse, utgave 1.01. Stillingsbeskrivelsen gjaldt frem til 20.11.2004. Utover å delta i det daglige arbeid etter behov og tid, indikerer ikke stillingsbeskrivelsen at en slik vid tilgang til pasientjournaler er nødvendig.

Den tidligere avdelingsleder hadde brukertilgang til alle somatiske pasientjournalnotater. Helgelandssykehuset HF, avdeling Mosjøen har et skjema for tildeling av brukeridentitet i DIPS, LHB.A.6.1.2. Skjemaet er for avdelingsleder ikke underskrevet, tiltross for at det fremgår av skjemaet at dette "*skal fylles ut, underskrives og leveres EDB-ansvarlig før tildeling av brukeridentitet*". Den

dagjeldende *Tildelingen av brukeridentitet DIPS* viser også til en taushetsbestemmelse og lov som ikke lenger var i kraft på det aktuelle tidspunktet. Det er på bakgrunn av tilgjengelig dokumentasjon ikke mulig å se at tildeling av tilgang er utført i henhold til faste og systematiske rutiner.

1.5 Kontroll med bruk av tilgang
I brev av 08.02.2005 uttrykker Helgelandssykehuset HF at den aktuelle avdelingsleder hadde den tilgang som var vurdert som nødvendig for å ivareta hans arbeidsoppgaver. I notat av 01.02.2005 gir Helgelandssykehuset HF uttrykk for at tilgang var nødvendig for skriving av journal og notater i perioder med stor belastning.

I *Redegjørelse overfor Helgeland Politidistrikt vedrørende Helgelandssykehusets anmeldelse 8.2.05* fra avdelingsleder, sies det under *Dokumentadministrasjon/økonomiske oppgjør* at innregistrering av innkommende post; prøvesvar, eksterne dokumenter, henvisninger, forespørsler fra forsikringsselskaper og rettsvesen, forespørsler fra kreftregister med videre, i normal rutine, ikke krever full journaltilgang. Ved avvik vil det imidlertid ofte være nødvendig med innsyn i dokumenter. Avdelingsleder gir for øvrig ikke uttrykk for at stillingen tilsa tilgang til pasientjournalene.

På vegne av de ansatte skriver tillitsvalgte i brev av 13.02.2005 at tidligere avdelingsleder "ikke skrev et eneste journalnotat, han var heller ikke opplært til å skrive slike dokument. Alle journaldokumenter som opprettes/skrives vises dessuten i dokumentlistene, med navn på sekretær, som til enhver tid er tilgjengelig for alle oss ansatte i skrivetjenesten. Tidl.avd.leder har altså hatt full tilgang til alle dokumenter i somatisk sykehus, dette bevis på logg, uten å delta i skriving av journaldokumenter".

Datatilsynet kan ikke se, av oversendte logger, at tidligere avdelingsleder har skrevet noe i pasientjournalene.

I *Redegjørelse overfor Helgeland Politidistrikt vedrørende Helgelandssykehusets anmeldelse 8.2.05*, datert 01.03.2005, fra avdelingsleder uttrykkes det på side 3 at "i forhold til enkelte av disse prosedyrene kan det tenkes at jeg, om fullstendig opplæring hadde vært gitt, kunne ha fått de samme opplysningene uten å gå inn på selve dokumentene."

Under tilsynet 02.11.2004 ved avdeling Mo i Rana ble det opplyst at loggene bare ble benyttet hvis sykehuset hadde konkret mistanke om brudd på sikkerhetsrutiner. Helgelandssykehuset HF avdeling Mosjøen utrykker i internnotat av 01.02.2005 at de ikke har rutiner for å sjekke hvorvidt autoriserte tilganger benyttes til andre ting enn arbeidsoppgaver. Av dette kan det sluttes at det ikke føres kontroll med de oppslag ansatte med tilgang foretar i pasientdatasystem.

Foretaket har heller ikke særskilte rutiner for å beskytte helseopplysninger om egne ansatte.

1.6 Sykehusets oppfølging av hendelsen - avviksbehandling
Vedkommende har i henhold til loggene også foretatt innsyn i journal til personer med samme etternavn. Det er antydet i notat datert 13.09.2004, utarbeidet av Helgelandssykehuset HF, at dette kan være avdelingsleders familie. Det uttales

imidlertid at det inntil videre ikke er valgt å gjøre ytterligere undersøkelser. Det er ikke dokumentert at sykehuset har foretatt noen videre undersøkelser for å avdekke hvorvidt dette er hans familie, og om det er i strid med hans tjenestelige behov.

I usignert brev levert 09.09.2004 som fremstår som skrevet av tidligere avdelingsleder uttrykkes det blant annet: *"Jeg har en følelse av at jeg neppe er den eneste som har beveget seg i grenseland mellom nødvendig innsyn, menneskelig nysgjerrighet og andre motiver. Dette bringes ikke inn som noen unnskyldning/bortforklaring, men jeg har hørt utsagn fra andre avdelingsledere som har referert til at ""det finner du i journalen til vedkommende" videre har det også vært snakket om journalinnsyn v. ansettelser. Jeg velger å tro at dette ikke er representativt for noen kultur i bedriften, men observasjonen kan være et grunnlag for å ta opp dette på generell basis."* .

Det er ikke dokumentert at sykehuset har foretatt noen videre undersøkelser for å avdekke hvorvidt dette medfører riktighet.

2 Datatilsynet vurderinger
Tilsynet vil jf. ovenfor vurdere hvorvidt Helgelandssykehuset HF behandler helseopplysninger i strid med helseregisterloven § 16.

2.1 Brudd på helseregisterloven § 16 ?

2.1.1 Helseregisterloven § 16 første ledd
I henhold til helseregisterlovens *§ 16 første ledd* skal den databehandlingsansvarlige "gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger".

Spørsmålet er om Helgelandssykehuset HF gjennom planlagte og systematiske tiltak har sørget for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialiteten.

Med beskyttelse av helseopplysningenes konfidensialitet menes at den databehandlingsansvarlige må hindre at uvedkommende får innsyn, se Helseregisterloven Kommentarutgave, Sverre Engelschiøn mfl. side 120. Uvedkommende vil være alle som ikke har rett til å lese helseopplysningene. Konfidensialiteten vil kunne sikres selv om det gis tilgang til helseopplysningene. Konfidensialiteten må i disse tilfellene beskyttes ved sikkerhetstiltak som består av tilgangsstyring, og andre forholdsmessige tiltak som iverksettes i samsvar med en risikovurdering. Hvorvidt tilgangen samsvarer med taushetspliktbestemmelsene, samt er nødvendig for forsvarlig medisinsk behandling, ligger innenfor Helsetilsynets kompetanseområde. Dette vil derfor ikke bli nærmere drøftet.

Kravet om informasjonssikkerhet, herunder konfidensialitet, er nærmere utdypet i forarbeidene. I merknadene til Ot.prp. nr. 5 (1999-2000) om lov om helseregistre og behandling av helseopplysninger uttrykkes at krav "om tilstrekkelig konfidensialitet innebærer at bestemmelsene om taushetsplikt og de alminnelige bestemmelsene om tilgang til og utlevering eller overføring av helseopplysninger [må] overholdes". Informasjonssikkerheten, må i henhold til forarbeidene, som et minimum legges på et slikt nivå at sikkerheten ivaretar sykehusets taushetsplikt.

Hensynene bak loven tilsier også at det stilles strenge krav til informasjonssikkerhet ved behandling av journalopplysninger. Brudd på konfidensialiteten ved journalopplysninger vil, som i dette tilfellet, kunne medføre et stort inngrep i den enkeltes integritet, noe som også presiseres i forarbeidene. Ved et helseforetak må kravene være av en slik kvalitet at pasienter, ansatte og andre, kan føle seg trygge på at helseopplysningene ikke blir gjort kjent for andre enn de som har et tjenestelig behov.

Etter helseregisterloven § 16 første ledd synes sikkerheten som et minimum å måtte legges på et slikt nivå at den vil ivareta taushetsplikten. Å ivareta taushetsplikten, ved bare å regulere tilgang, vil som utgangspunkt kunne medføre en for dårlig tilgjengelighet til opplysningene for helsepersonell, og annet personell med lovhjemlet behov for innsyn. Det er ikke omstridt at avdelingsleder har hatt tilgang til mer helseopplysninger i pasientjournalene ved Helgelandssykehuset HF, enn hva han har rett til etter helsepersonelloven. Når det gis vid tilgang i forhold til det tjenestelige behovet må risikoen for brudd på konfidensialiteten, begrenses med andre sikkerhetstiltak som beskytter konfidensialiteten.

Ot.prp. nr. 5 (1999-2000) om lov om helseregistre og behandling av helseopplysninger forutsetter at det både etableres organisatoriske og tekniske sikkerhetstiltak.

Kompetansesenteret for IT i helsevesenet AS (KITH) ferdigstilte og publiserte sommeren 2001 en standard for elektronisk pasientjournaler. Sosial- og helsedirektoratet orienterte om standarden i rundskriv IS-1/2002. Rundskrivet ble blant annet sendt til landets helseforetak. Direktoratet uttrykker at "standarden konkretiserer krav og funksjoner som må ivaretas i journalsystemene for å etterleve forutsetningene i regelverket". Standarden oppstiller strengere krav til tilgang og kontroll enn kravene på Helgelandssykehuset HF. Det vises også til høringsutkast til Norm for informasjonssikkerhet i helsesektoren, som ligger vedlagt. Sistnevnte norm er utarbeidet for representanter i sektoren, herunder fra Den norske legeforening, representanter fra de regionale helseforetak, Norsk Sykepleierforbund, Norges Apotekerforening og Kommunenes Sentralforbund. Det må tillegges betydning hva slags planlagt og systematiske rutiner som eksisterer ved andre helseforetak. Det vises til Ullevål universitetssykehus HFs praksis, jf. vedlagte instrukser Pasientjournalen – Tilgang til journalen, tilgangsmatrise og aktualiseringsrett, Pasientjournalen – Retting, sletting og sperring og Pasientjournalen – Føring, tilgang, behandling, pasientens innsynsrett, forskning og oppbevaring, særlig 7.5.3, samt prosedyren Pasientansvarlig lege, journalansvarlig person m.m..

Datatilsynet kan, på bakgrunn av tilgjengelig dokumentasjon, *generelt* ikke se at Helgelandssykehuset HF gjennom planlagte og systematiske tiltak har sørget for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialiteten til helseopplysninger i pasientjournalen.

I henhold til merknadene i Ot. prp. nr. 5, svarer bestemmelsen til forslag til lov om behandling av personopplysninger, bortsett fra at begrepet sikker behandling av helseopplysninger også omfatter opplysningenes kvalitet. Personopplysningsloven § 13 har i det vesentligste samme ordlyd og betydning som helseregisterloven, med unntak av helseregisterlovens krav om kvalitet, se Ot. prp. nr. 5 (1999-2000) til helseregisterloven. Kravene skal også tillegges betydning i den utstrekning ikke annet følger av helseregisterloven, jf. helseregisterloven § 36. Brudd på

personopplysningsloven § 13 kan også sanksjoneres med straff, jf. personopplysningsloven § 48. Personopplysningsforskriften § 2-11 omhandler sikring av personopplysningers konfidensialitet. Det vil i det følgende bli vist til bestemmelser i personopplysningsforskriftens kapittel 2 om informasjonssikkerhet for presisering av hvordan helseregisterloven § 16 er blitt tolket i praksis.

Kravene til informasjonssikkerhet er nærmere uttredet på side 126 flg. i Ot.prp. nr. 5 (1999-2000) om lov om helseregistre og behandling av helseopplysninger. De mer konkrete krav vil bli nærmere drøftet nedenfor.

2.1.2 Sikkerhetsledelse
Det er Helgelandssykehuset HFs direktør som er databehandlingsansvarlig. Datatilsynets tilsynsrapport legger til grunn at ansvaret ikke er dokumentert. Det er heller ikke dokumentert noen delegering av ansvar. Manglene kan ha hatt betydning for den manglende informasjonssikkerheten ved Helgelandssykehuset HF. Det vises til tilsvarende bestemmelser i personopplysningsforskriftens § 2-3, samt til Ullevål universitetssykehus HFs praksis, jf. vedlagte instrukser og prosedyrer.

2.1.3 Planlagte og systematiske tiltak
Helseregisterloven § 16 første ledd krever at tiltakene skal være "planlagte og systematiske". Ot.prp. nr. 5 (1999-2000) gir uttrykk for at det skal foreligge en strategi for hvordan sikkerhetsmålene skal kunne nås.

I følge merknadene til personopplysningsloven § 13, Ot. prp. nr. 92 (1998-99) skal den behandlingsansvarlige, "på bakgrunn av behandlingens formål, personopplysningenes omfang og art (herunder om de er sensitive eller ikke), samt utføre risikoanalyser, utarbeide mål og strategi for etablering av tilfredsstillende informasjonssikkerhet. Ved risikoanalyse skal personopplysningenes antall og art vurderes mot trusler mot informasjonssikkerheten – for eksempel faren for menneskelig feil".

Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om sikkerhetsstrategien er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat. Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuelle endringer av sikkerhetsmål og strategi. I KITHs norm under punkt *7.3 Tiltak* foreslås et tiltak (*Besluttet tiltak*) som hindrer at personell går inn i journaler som sykehuset ikke aktivt arbeider med. Det var bare en av de ansatte som var under behandling når det ulovlige innsynet ble foretatt. Et slikt tiltak i den konkrete sak ville dermed hindret innsyn for alle ansatte, med unntak av denne ene.

Datatilsynet kan ikke se at Helgelandssykehuset HF på det aktuelle tidspunkt har utført risikoanalyser, eller utarbeidet mål og strategi for tilfredsstillende informasjonssikkerhet. Praksisen strider således mot helseregisterloven § 16.

2.1.4 Tilgangsstyring
I samsvar med vurderingene ovenfor, ligger det innenfor Helsetilsynets tilsynsområde å vurdere spørsmål knyttet til taushetsplikt og forsvarlig medisinsk behandling.

Tilgangsstyringen vil imidlertid også være et sikkerhetstiltak som må være "planlagt[e] og systematisk[e]", jf. helseregisterloven § 16.

Datatilsynet vil bemerke at rutinene for tildeling ikke fremstår som tilstrekkelig gode til å ivareta en tilstrekkelig informasjonssikkerhet jf. helseregisterloven § 16. De dokumenterte rutiner har heller ikke blitt fulgt for den aktuelle avdelingsleder. Det vises blant annet til at avdelingsleder ikke har underskrevet avtale om brukertilgang, se kapittel 1.5, samt at sykehuset ikke har dokumentert hvorvidt tilgangen er revurdert etter første gangs tildeling av tilgang, se eksempelvis 1.6 tredje til sjette avsnitt.

Av vedlagte logger kan også enkelte tilgangene som er gitt fremstå som generelle, se eksempelvis D-2030 – Liste over brukere med valgt brukertype, særlig side 2 hvor arbeidssted *Med. avdeling* ikke inneholder stilling eller personalkategori. Se også samme dokument side 1 hvor stilingsbetegnelsene fysioterapeut, server og sykepleier kirpol ikke inneholder personellkategori eller arbeidssted. Det samme gjelder for stillingsbetegnelsene student, vikar arkiv, legesekretær student, Daglig leder psykiatri på side 2. Generell tilgang er klart i strid med helseregisterloven § 16.

2.1.5 Avvik
Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd skal behandles som avvik. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse. Det vises til personopplysningsforskriften § 2-6 som omhandler avvik.

Helgelandssykehuset har ikke fremlagt dokumentasjon som viser at sykehuset har utført tilstrekkelige undersøkelser, og foretatt tilstrekkelige tiltak for å hindre gjentagelse. Det vises til at Helgelandssykehuset HF ikke har undersøkt nærmere om hvorvidt andre avdelingsledere har foretatt tilsvarende ulovlig innsyn, eller hvorvidt avdelingslederen også har foretatt ulovlige innsyn hos andre enn egne ansatte.

Datatilsynet kan på bakgrunn av den konkrete sak og tidligere tilsyn ikke se at virksomheten har en dokumentert avviksrutine knyttet til behandlingen av helseopplysninger. Slik Helgelandssykehuset HF har fulgt opp den konkrete sak, kan Datatilsynet heller ikke se at Helgelandssykehuset HF har udokumenterte, men tilstrekkelige avviksrutiner som følges i praksis. Helgelandssykehuset HFs praksis fremstår som markert avvikende fra kravene til informasjonssikkerhet, jf. helseregisterloven § 16.

2.1.6 Personell
Medarbeidere må ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt. Bruk av vide tilgangsrettigheter krever god opplæring og oppfølging. Det vises for øvrig til personopplysningsforskriften § 2-8 som omhandler personell.

På bakgrunn av avdelingsleders egen forklaring, og øvrig dokumentasjon fremstår det for Datatilsynet som at avdelingsleder hadde mangelfull kunnskap. Dette kan også indikere at Helgelandssykehuset HF har for dårlige rutiner knyttet til opplæring av sitt personell i behandling av helseopplysninger. Det er ikke fremlagt annen dokumentasjon som tilsier at den utilstrekkelige opplæringen av avdelingsleder var et unntakstilfelle.

2.1.7 Sikkerhetstiltak
Helseregisterloven § 16 uttrykker at informasjonssikkerheten må være "tilfredsstillende". Ot.prp. nr. 5 (1999-2000) om lov om helseregistre og behandling av helseopplysninger side 127 andre spalte stiller krav til sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet.

Sikkerhetstiltak skal gjøre det mulig å oppdage forsøk på uautorisert bruk. Forsøk på uautorisert bruk skal registreres. Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne. Det vises til personopplysningsforskriften § 2-14 som omhandler sikkerhetstiltak, og tidligere nevnt norm utarbeidet av KITH. Normen foreslår at tilgang skjer på grunnlag av *Besluttede tiltak.* Besluttede tiltak gir meget begrenset tilgang, og således et mindre behov for etterfølgende kontroll. Til tross for dette krever normen at det "regelmessig kjøres rapport som lister ut registrerte *Tjenesteutførelser* som bør kontrolleres nærmere. I denne standarden stilles det krav om to slike kontrollrapporter". For det første skal det finnes en rapport som lister ut alle Tjenesteutførelser av typen nødhjelp registrert i angitt tidsrom. For det andre skal det finnes en rapport som lister ut alle Tjenesteutførelser registrert i angitt tidsrom som oppfyller nærmere kriterier.

Helseforetaket har logger knyttet til pasientjournalene. Effekten av loggene uten nærmere gjennomgang vil være svært liten. Helgelandssykehuset HF har ingen kontrollerende tiltak som er med på å ivareta konfidensialiteten, herunder tiltak som kan oppdage ulovlig innsyn. De manglende kontrolltiltak, må når Helgelandssykehuset HF tildeler så vid tilgang, anses som et markert avvik fra helseregisterloven § 16 krav om konfidensialitet.

2.2 Helseregisterloven § 16 andre ledd
I henhold til helseregisterloven *§ 16 andre ledd* skal den databehandlingsansvarlige for å oppnå tilfredsstillende informasjonssikkerhet "dokumentere informasjonssystemet og sikkerhetstiltakene". Dokumentasjonen skal være tilgjengelig for tilsynsmyndighetene. I den grad det er planlagt og etablert tilstrekkelige tiltak rundt tilgangsstyring, har Helgelandssykehuset HF uansett ikke gjort denne dokumentasjonen tilgjengelig for Datatilsynet. Dette innebærer således et brudd på helseregisterloven § 16 andre ledd.

2.3 Anmeldelse?
I henhold til helseregisterloven § 34 nummer 1. "straffes den som forsettlig eller grovt uaktsomt" behandler helseopplysninger i strid med § 16.

Tilsynet legger, i henhold til dets vurderinger ovenfor i kapittel 2.1 til og med 2.2, til grunn at Helgelandssykehuset HF har behandlet helseopplysninger i strid med § 16.

Spørsmålet er om databehandlingsansvarlig må sies å ha opptrådt grovt uaktsomt ved behandlingen av helseopplysningene. Foreligger det et markert avvik fra det forsvarlige?

Aktsomhetsvurderingen må knyttes til hva som kan forventes at databehandlingsansvarlige, Helgelandssykehuset HF ved øverste leder, måtte skjønne. Ved fastleggelsen av aktsomhetsnormen må det tillegges betydning at en direktør ved et helseforetak er en profesjonell part som det må forventes setter seg inn i det

regelverk som er nødvendig for å drive sykehusvirksomhet. Ulovlig innsyn kan innebære et stort inngrep i den enkeltes integritet. Disse momentene tilsier en streng aktsomhetsnorm.

Ved vurderingen av aktsomhetsnormen må det også tillegges betydning at helseregisterloven § 16 er skjønnsmessig. I utgangspunktet tilsier dette at det skal mer til for å anse skyldkravet oppfylt. Helseregisterloven § 16 gir imidlertid klart uttrykk for at databehandlingsansvarlig skal "sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet". Da konfidensialiteten ikke kan sies å være nevneverdig beskyttet mot ulovlig innsyn fra ansatte foreligger det imidlertid klare brudd på helseregisterloven § 16.

For å kunne stadfeste uaktsomhet må det ha foreligget en alternativ handlemåte. Helgelandssykehuset HF, ved øverste leder, må kunne ha handlet på en alternativ, effektiv og praktisk gjennomførbar måte. Helgelandssykehuset HF ved øverste leder har ikke dokumentert noen overordnede føringer for virksomhetens bruk av informasjonsteknologi, se punkt 1.2. Den konkrete sak viser også at de faktiske rutinene var svært mangelfulle. Dette kan i stor grad skyldes manglende tildeling av oppgaver nedover i organisasjonen. Det burde vært foretatt risikovurderinger av hvorvidt personells tildelte tilgang, samt kontrollerende tiltak, ga en tilfredsstillende beskyttelse av konfidensialitet. Risikovurderinger ville avdekket at informasjonssikkerheten ikke var tilstrekkelig. For å sikre kravet til konfidensialitet kunne databehandlingsansvarlig ha snevret inn tilgang og/eller hatt strengere rutiner for opplæring, tildeling, samt kontroll med hvorvidt tilgangen ble misbrukt. Dette ville i større grad hindret brudd på kravet om konfidensialitet. For alternativ handlemåte vises det for øvrig til KITHs norm.

I den konkrete sak synes det forebyggende arbeid svært begrenset, samtidig med at det ikke foreligger systematiske måter sykehuset kan avdekke ulovlig innsyn fra egne ansatte. Helgelandssykehuset HF har dårlige rutiner for tildeling av tilgang, opplæring og avvikshåndtering, samt ingen kontrollerende tiltak. Datatilsynet vurderer det slik at databehandlingsansvarlig måtte forstå at sykehusets informasjonssikkerhet knyttet til journalopplysninger ikke i tilstrekkelig grad ivaretok hensynet til konfidensialiteten. Databehandlingsansvarlig måtte forstå at sykehusets praksis er markert avvikende fra forsvarlig praksis.

Risikoen for brudd på kravet om konfidensialitet ved utro ansatte er kjent. Det vises eksempelvis til daværende Haukeland Sykehus høringsuttalelse i Ot. prp. nr. 5 (1999-2000) side 129 hvor sykehuset uttaler "at det vesentligste potensialet for misbruk sannsynligvis er at ansatte i registrene, som i og for seg har legitim adgang til opplysningene, kan komme til å bryte taushetsplikt uaktsomt eller forsettlig". Videre uttaler Sosial- og helsedepartementet at en av de tre største sikkerhetsrisikoene ved behandling av helseopplysninger er utro tjenere. Det vises også til vedlagte avisartikler, hvor det fremgår at denne risikoen er kjent. I Aftenposten.no uttaler sjeflege ved Ullevål at "Nysgjerrighet er en sterk kraft, og det er veldig viktig at sykehusene er strenge med å kjøre tilsyn.".

Det vil også kunne tillegges betydning hva slags praksis andre helseforetak har, og eventuelt hvor betydelig avviket fra andre Helseforetaks praksis er. Det vises til KITHs norm, samt høringsutkast til Norm for informasjonssikkerhet i helsesektoren,

som ligger vedlagt. Helgelandssykehuset HFs praksis knyttet til behandling av helseopplysninger er på flertallet av punktene ikke i samsvar med normene.

Det vises også til Ullevål universitetssykehus HFs (UUS) rutiner, som ligger vedlagt. Ullevål universitetssykehus HF har avdekket ansatte som har foretatt ulovlige innsyn i pasientjournaler. Sykehusets rutiner er betydelig bedre. Eksempelvis gjennomgås loggene jevnlig for å avdekke misbruk. Rutinene står i sterk kontrast til Helgelandssykehuset HFs manglende rutiner.

Helgelandssykehuset HFs praksis avviker markert fra KITHs norm. Andre sykehus' (UUS) praksis er mer i overensstemmelse med kravet til tilstrekkelig informasjonssikkerhet. Avviket fra normen taler for at Helgelandssykehuset HF, ved øverste leder, måtte forstå at deres praksis ikke var i samsvar med kravene til konfidensialitet, jf. helseregisterloven § 16. Det vises også til personopplysningsforskriften kapittel 2.

Helgelandssykehusets HFs praksis er avvikende på svært mange områder knyttet til informasjonssikkerhet. Tilsynet finner etter en helhetsvurdering at Helgelandssykehuset HF har opptrådt grovt uaktsomt. Det foreligger en kvalifisert klanderverdig opptreden som foranlediger sterke bebreidelser for mangel på aktsomhet.

Datatilsynet finner at Helgelandssykehuset HFs behandlingen av personopplysninger oppfyller vilkårene for straff, jf. lov av 18.05.01 nr. 24 om helseregistre og behandling av helseopplysninger § 36 første ledd, nummer 1, jf. § 16.

Datatilsynet ber også om at det vurderes hvorvidt det er grunn til å ilegge foretakstraff, jf. straffeloven §§ 48 a. Tilsynet vil her påpeke at det er brudd på helseregisterloven § 16 som vil være grunnlag for foretaksstraff. Hvorvidt avdelingslederen har handlet på vegne av foretaket når han foretok de ulovlige innsynene er således uten betydning. Denne sak ligger i kjernen av formålet med foretaksstraff. Foretaket kan ha hatt økonomiske fordeler av å ikke legge tilstrekkelige ressurser i informasjonssikkerhet jf. helseregisterloven § 16. Det er da viktig, i samsvar med formålet bak straffelovens § 48 a og § 48 b, å reagere på brudd.

3 Konklusjon

Tilsynet finner på bakgrunn av ovennevnte gjennomgang at sikkerheten i så liten grad er knyttet til rutiner og overordnede prioriteringer at Helgelandssykehuset HF bør straffes. Denne saken har fått stor publisitet i mediene. Det vil være viktig for allmennhetens tillit til at pasientopplysninger blir oppbevart forsvarlig, at saken forfølges rettslig.

Strenge rutiner ved et helseforetak er svært viktig. Det er en viktig samfunnsinteresse at borgerne har tillit til at journalopplysninger oppbevares og benyttes på en forsvarlig måte. Som i den konkrete sak kan ulovlig innsyn i pasientjournal få store konsekvenser, og gi den enkelte store psykiske og fysiske problemer. En straffeforfølging av Helgelandssykehuset HF vil gi preventive virkninger, ved at sykehus vil øke prioriteringen av beskyttelse av journalopplysninger. Dette vil gjøre det mer risikabelt for den enkelte ansatte å foreta ulovlig innsyn i pasientjournaler. Ansatte med tilgang skal ikke kunne ulovlig lese pasientjournaler uten fare for å bli

oppdaget. Det bør også tillegges betydning at Helgelandssykehuset HF selv ønsker en etterforskning for å vurdere hvorvidt sykehuset har opptrådt i strid med loven.

Med hilsen

Georg Apenes
direktør

Frode Bergland Bjørnstad
rådgiver
(saksbehandler,
telefon 22 39 69 00)

Vedlegg: Kopi dokument 2005/1-16 med vedlegg
Kopi dokument 2004/1278-8 med vedlegg (vedtak om pålegg og kontrollrapport)
Rundskriv IS-1/2002 fra Sosial- og helsedirektoratet
KITHs EPJ standard kapittel 7. tilgangsstyring
Ullevål universitetssykehus HFs rutiner med e-post

Kopi: Helsetilsynet i Nordland, Moloveien 10, 8002 BODØ (saksnr. 05/3903)