Elektronisk pasientjournal og taushetsplikt

Tilsyn med to store helseforetak i 2006 avdekket at taushetsbelagte opplysninger i de elektroniske pasientjournalsystemene ikke var forsvarlig vernet mot innsyn fra ansatte som ikke hadde legitime behov for opplysningene. Dette skyldtes delvis at datasystemene var utformet slik at det ikke var lagt til rette for slik tilgangsstyring som lovgivningen krever og delvis at de eksisterende mulighetene for tilgangsstyring ikke var fullt ut utnyttet. Mangler ved kontrollsystemene gjorde at det var lav risiko for å bli avslørt dersom ansatte ved kliniske avdelinger snoket i de elektroniske pasientjournalene.

Lovgivningen stiller krav om at helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell. Taushetsplikten er altså ikke bare en passiv plikt til å tie, men også en aktiv plikt til å hindre uvedkommende i å få tilgang til taushetsbelagt informasjon.

Journalforskriften inneholder bestemmelser om at virksomhet som yter helsehjelp må opprette pasientjournalsystem. Journalsystemet må organiseres slik at det både sikrer nødvendig tilgang til og utlevering av journal og verner opplysningene mot innsyn fra uvedkommende.

Utveksling av taushetsbelagt informasjon mellom helsepersonell kan kun skje når det er nødvendig for behandling og oppfølging av pasienten, eller hvor det foreligger annet rettslig grunnlag for å gi slik informasjon.

Helsetilsynet og Datatilsynet gjennomførte i fellesskap i mai 2006 tilsyn med hvordan Helse Bergen HF Haukeland Universitetssykehus ivaretok taushetsplikten og tilgjengeligheten ved bruk av pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS. Tilsynet omfattet både innhenting og utlevering av pasientinformasjon fra elektronisk pasientjournal og tilgangsstyring i forhold til elektronisk pasientjournal og det pasientadministrative systemet PIMS.

I juni 2006 gjennomførte Helsetilsynet og Datatilsynet et lignende tilsyn ved Akershus Universitetssykehus HF. Temaet ved dette tilsynet var sikring av taushetsplikten og tilgjengeligheten ved bruk av det elektroniske pasientjournalsystemet DIPS.

Tilsynene ble gjennomført som systemrevisjoner og var av to dagers varighet. En systemrevisjon gjennomføres ved granskning av dokumenter, ved intervjuer og andre undersøkelser. Ved tilsynene ble tiltak og praksis ved helseforetakene vurdert opp mot aktuelle krav i helselovgivningen, helseregisterloven og personopplysningsloven.

Det ble konstatert avvik ved begge tilsynene. Avvik defineres som mangel på oppfyllelse av krav gitt i eller i medhold av lov eller forskrift. Avvikene dreide seg om at helseforetakene ikke sikret at taushetsbelagte personopplysninger i de elektroniske pasientjournalsystemene var forsvarlig vernet mot innsyn fra ansatte som ikke hadde legitimt behov for opplysningene. Avvikene bygde i hovedsak på at store grupper helsepersonell var gitt tilgang til hele eller deler av de elektroniske pasientjournalene uavhengig av om de var involvert i pasientbehandlingen eller ei. Dette skyldtes delvis at journalsystemene ikke var laget slik at det var mulig å etterleve kravene til taushetsplikt og tilgangsstyring og delvis at helseforetakene ikke fullt ut hadde utnyttet de mulighetene for tilgangsstyring som lå i systemene.

Hvert år gjør helsepersonell millioner av oppslag i pasientjournalene ved disse sykehusene. Alle oppslag loggføres automatisk. Det store antallet oppslag, små kontrollressurser og svake kontrollrutiner gjør at ansatte ved kliniske avdelinger som kikker i pasientjournaler uten å ha tjenstlige behov, har lav risiko for å bli avslørt. Loggkontroll ble derfor vurdert til å være et lite egnet hjelpemiddel til å avdekke misbruk.

Oppfølgingen av tilsynene er ikke avsluttet og det er derfor ikke klart hvordan helseforetakene vil løse de utfordringene som disse tilsynene avdekket.