Indenrigs- og Sundhedsministeriet
Dato: 15. januar 2007
Kontor: Forvaltningsjuridisk kt.
J.nr.: 2006-1640-17
Sagsbeh.: MER

Besvarelse af spørgsmål nr. 131 (L 50 B), som Folketingets Sundhedsudvalg har stillet til indenrigs- og sundhedsministeren den 9. januar 2007

Spørgsmål 131:

"Ministeren bedes kommentere henvendelsen af 21. november 2006 fra Chris von Ahnen, jf. L 50 B – bilag 45."

Svar:

Chris von Ahnen anfører i sin henvendelse af 21. november 2006, hvorledes han finder, at det vil være muligt at minimere risikoen for misbrug af de elektroniske patientjournaler (EPJ). Han finder, at der ved indførelse af stikprøvekontrol, indbyggede alarmer, der udløses ved et foruddefineret misbrug af EPJ, samt en elektronisk adgang for patienten til egne logoplysninger vil være tale om en betydelig sikring af EPJ.

Jeg kan oplyse, at reglerne vedrørende datasikkerhed er reguleret i den persondataretlige lovgivning. Lovgivningen om behandling af personoplysninger henhører under Justitsministeriets ressort. Datatilsynet administrerer reglerne og fører tilsyn med deres overholdelse.

Det følger af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Det følger af bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen) § 5, at den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af sikkerhedsbekendtgørelse. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for myndighedens tilsyn med overholdelse af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Det er således den enkelte dataansvarliges pligt at fastsætte en sikkerhedsorganisation.

De dataansvarlige kan således som led i fastsættelsen af deres sikkerhedsniveau, f.eks. i en sikkerhedsinstruks, regulere spørgsmålet omkring sikkerhedsalarmer og stikprøvekontrol. De dataansvarlige kan ligeledes egenhændigt indføre stikprøvekontrol som et led i en efterfølgende sikkerhedsforanstaltning. I øvrigt henvises til min besvarelse af spørgsmål nr. 44 (L 50) om den sikkerhedsmæssige forebyggelse af misbrug.

Endvidere kan jeg oplyse, at sikkerheds- og brugerstyringsproblematikker er et vedvarende tema i overvejelserne for den fremtidige EPJ-udvikling og vil blive adresseret i den nationale IT-strategi for sundhedsvæsenet.

Jeg kan endvidere oplyse, at Datatilsynet som et led i deres tilsyn foretager sygehusinspektioner. Der henvises til min besvarelse af spørgsmål nr. 13 herom.

I forhold til patientens elektroniske adgang til egne log-oplysninger kan jeg henvise til min besvarelse af spørgsmål nr. 24 og 53 (L 50).

Jeg kan supplerende hertil oplyse, at det indgår i mine overvejelser, hvorvidt der i ændringsforslaget vedrørende adgangen til at indhente elektroniske helbredsoplysninger skal indgå en bemyndigelsesbestemmelse, hvorefter indenrigs- og sundhedsministeren kan fastsætte nærmere regler om patientens elektroniske adgang til oplysninger hos offentlige og private dataansvarlige om, hvem der har foretaget opslag i patientens elektroniske patientjournal, og på hvilket tidspunkt opslagene er foretaget.