**Indenrigs- og Sundhedsministeriet**
Dato: 4. december 2006
Kontor: Forvaltningsjuridisk kt.
J.nr.: 2006-1640-17
Sagsbeh.: sdy
Fil-navn: FT-spg/SUU nr. 15 L50 besvarelse

# Besvarelse af spørgsmål nr. 15 (L 50), som Folketingets Sundhedsudvalg har stillet til indenrigs- og sundhedsministeren den 13. november 2006

## Spørgsmål 15:

"Hvordan agter ministeren at sikre, at uberettiget brug af EPJ kan kontrolleres og undgås?"

## Svar:

Der findes allerede i dag elektroniske patientjournaler i sundhedsvæsenet.

Lovgivningen om behandling af personoplysninger henhører under Justitsministeriets ressort. Datatilsynet administrerer reglerne og fører tilsyn med deres overholdelse.

Efter lov om behandling af personoplysninger § 41, stk. 3, skal den dataansvarlige træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer eller i øvrigt behandles i strid med persondataloven.

Det følger blandt andet af den gældende bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelse) § 11, at kun autoriserede personer må have adgang til de personoplysninger, som behandles, og der må kun autoriseres personer, som er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Det vil sige, at også i forhold til eksisterende elektroniske patientjournaler er der behov for, at den dataansvarlige foretager en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til. Desuden skal der efter sikkerhedsbekendtgørelsens § 12 træffes foranstaltninger som sikrer, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelse, som de er autoriserede til. Endvidere følger det af sikkerhedsbekendtgørelsens § 17, at der mindst hvert halve år foretages kontrol af, om de autoriserede brugere fortsat har behov for den fastlagte adgang.

Det følger endvidere af sikkerhedsbekendtgørelsen § 18, at der ved behandling af følsomme oplysninger/anmeldelsespligtige behandlinger skal foretages registrering af alle afviste adgangsforsøg. Der skal desuden blo-

keres for yderligere forsøg, hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, og der skal ske løbende opfølgning i myndigheden. Endvidere følger det af sikkerhedsbekendtgørelsens § 19, stk. 1, at der ved behandling af følsomme personoplysninger/anmeldelsespligtige behandlinger skal foretages maskinel registrering (logning). Registreringen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Desuden skal den dataansvarlige myndighed efter sikkerhedsbekendtgørelsens § 5 fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af sikkerhedsbekendtgørelsen. Jeg vil i den forbindelse henvise til besvarelse af spørgsmål nr. 16.

Der er således i den gældende lovgivning en række krav om forudgående og efterfølgende kontrol.

Sikkerheds- og brugerstyringsproblematikker er endvidere et vedvarende tema i overvejelserne for den fremtidige EPJ-udvikling. Det er imidlertid den nye centrale EPJ-organisation, der i første omgang skal behandle denne problemstilling, herunder spørgsmålet om de tekniske muligheder og begrænsninger. Ligeledes vil det også i første omgang være op til den centrale EPJ-organisation at drøfte behovet for en central sikkerheds- og brugerstyringsløsning.

Når den centrale EPJ-organisation har færdiggjort sine overvejelser, vil der blive taget stilling til, hvorvidt der er behov for, at indenrigs- og sundhedsministeren som foreslået i lovforslagets § 1, nr. 31 (§ 193 a) fastsætter krav til sundhedsvæsenets IT-anvendelse, herunder IT-sikkerhed, samt til godkendelse heraf, eksempelvis i form af en certificeringsprocedure som styringsredskab, såfremt der er behov herfor for f.eks. at sikre effektiv gennemførelse.