



Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
F +45 7226 9001
M im@im.dk
W www.im.dk

Folketingets Sundhedsudvalg

Dato: 6. maj 2011
Enhed: Kommunaljura
Sagsbeh.: SUMCVA
Sags nr.: 1104538
Dok nr.: 500133

Folketingets Sundhedsudvalg har den 8. april 2011 stillet følgende spørgsmål nr. 1 (L 171) til indenrigs- og sundhedsministeren, som hermed besvares. Spørgsmålet er stillet på udvalgets vegne af formand Preben Rudiengaard (V).

Spørgsmål nr. L 171, spørgsmål 1:

"Ministeren bedes oplyse, hvordan han vil sikre, at det ikke fører til øget misbrug af fortrolige oplysninger, når langt flere får adgang til disse oplysninger set i lyset af, at der er flere eksempler på misbrug i "Redegørelse om indhentning af elektroniske helbredsoplysninger i forbindelse med patientbehandling" fra 2010."

Svar:

I afsnit 3.4. i Indenrigs- og Sundhedsministeriets redegørelse af 21. september 2010 om indhentning af helbredsoplysninger i forbindelse med behandling, jf. SUU alm. del bilag 511 (Folketingsåret 2009-2010) er der omtalt følgende to eksempler på misbrug:

"Ministeriet har i forhold til spørgsmålet om uberettiget indhentning af elektroniske helbredsoplysninger i de øvrige tilfælde, hvor patienten ikke har afgivet negativt samtykke, noteret sig, at der har været enkelte konkrete eksempler herpå.

I februar 2009 blev en it-medarbejder ved et sygehus bortvist og politianmeldt for uberettiget at have indhentet og videregivet oplysninger om abort fra en kvindes patientjournal.

I oktober 2006 – det vil sige før vedtagelsen af sundhedslovens §§ 42 a-c – blev to læger politianmeldt for at have søgt oplysninger i den Personlige Elektroniske Medicinprofil om 15 andre læger, der alle havde tilknytning til professionelle fodboldklubber her i landet."

I redegørelsens afsnit 3.4. er endvidere anført følgende:

"På spørgsmålet om, hvorvidt indhentning af elektroniske helbredsoplysninger bliver logget i regionerne, og om der i givet fald foretages stikprøvekontroller af logningen, har Danske Regioner oplyst, at alle regioner i dag foretager logning af opslagene på de elektroniske patientjournaler, men at det ikke med sikkerhed kan siges, om stikprøvekontrol finder sted i samtlige regioner. Det er dog Danske Regioners formodning, at stikprøvekontrol er en fast del af regionernes sikkerhedsforanstaltninger, hvilket tillige fremgår af enkelte af regionernes bidrag, jf. ovenfor."

Sammenholdt med den omfattende og rutinemæssige brug af elektroniske patientjournaler gennem flere år må det på den baggrund formodes, at der kun i begrænset omfang foretages indhentning i strid med reglerne. Jeg har grund-

læggende tiltro til, at landets sundhedspersoner er deres ansvar bevidst og retter sig efter, hvad de må, i stedet for hvad de kan.

I den forbindelse er det vigtigt for mig at fremhæve, at lovforslaget har stort fokus på beskyttelse af oplysninger om patienternes privatliv. Det er min opfattelse, at der – også ved den foreslåede udvidelse af de grupper af sundhedspersoner, som kan indhente såvel aktuelle som historiske oplysninger om en patient – i det allerede eksisterende regelsæt er et gennemgående præventivt værn mod misbrug og uberettiget indhentning af oplysninger samt tilstrækkeligt alvorlige sanktionsmuligheder i eventuelle tilfælde heraf.

Den sundhedsretlige beskyttelse

De materielle krav til elektronisk indhentning af helbredsoplysninger m.v. i sundhedslovens § 42 a, stk. 1, hvorefter sundhedspersonen til enhver tid konkret skal vurdere, om opslaget – der kun må foretages i fornødent omfang – er nødvendigt for den pågældendes aktuelle behandling af patienten, foreslås således videreført. Det er med andre ord ikke tilladt at søge efter oplysninger om patienten, som ikke er relevante for den konkret omhandlede behandling.

I den forbindelse vil jeg minde om, at patienten grundlæggende har mulighed for selv at sikre sig mod elektronisk indhentning af den pågældendes helbredsoplysninger m.v. – såvel konkret i forhold til enkelte oplysninger eller sundhedspersoner som generelt – ved at udnytte sin ret til at frabede sig indhentning af elektroniske helbredsoplysninger, som nævnt i min besvarelse af spørgsmål nr. 4 (L 171).

Hertil kommer, at Sundhedsstyrelsen skal føre tilsyn med den sundhedsfaglige virksomhed, der udføres af personer inden for sundhedsvæsenet, jf. sundhedslovens § 215, stk. 1. Sundhedsstyrelsens tilsyn omfatter også sundhedspersoner på private behandlingssteder. Sundhedsstyrelsen kan iværksætte skærpet tilsyn med den nævnte personkreds, såfremt styrelsen har en begrundet formodning om, at den pågældende sundhedspersons virksomhedsudøvelse vil udgøre en forringet sikkerhed for patienter, jf. sundhedslovens § 215, stk. 2, 1. pkt.

Sundhedsstyrelsen kan endvidere indbringe en sag for Sundhedsvæsenets Disciplinærnævn, hvis der findes at være grundlag for kritik af eller sanktion over for en sundhedsperson, jf. § 2 a i lov om klage- og erstatningsadgang inden for sundhedsvæsenet (lovbekendtgørelse nr. 24 af 21. januar 2009 som ændret ved lov nr. 706 af 25. juni 2010)(klage- og erstatningsloven). Disciplinærnævnet behandler endvidere klager fra patienter over autoriserede sundhedspersoners forhold omfattet af sundhedslovens kapitel 4 – 7 og 9 om patienters retsstilling. Disciplinærnævnet afgiver i de nævnte sager en udtalelse om, hvorvidt sundhedspersonen har handlet i strid med sundhedspersonens forpligtelser efter sundhedslovens kapitel 4 – 7 og 9 om patienters retsstilling, jf. klage- og erstatningslovens § 3, herunder hvorvidt sundhedspersonen har foretaget opslag i elektroniske systemer i strid med reglerne i sundhedslovens § 42 a. Disciplinærnævnet kan herunder udtale kritik med indskærpelse eller i meget alvorlige tilfælde indbringe sagen for anklagemyndigheden. Dette følger af klage- og erstatningslovens § 3.

Sundhedsstyrelsen har efter kapitel 3 i lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed (autorisationsloven) (lovbekendtgørelse nr. 1350 af 17. december 2008 som ændret ved lov nr. 140 af 9. februar 2010, lov nr. 706 af 25. juni 2010 og lov nr. 155 af 26. februar 2011) forskellige reaktionsmuligheder overfor konkrete autoriserede sundhedspersoner, hvis virksomhedsudøvelse efter Sundhedsstyrelsens vurdering udgør en forringet sikkerhed for patienterne.

Den mest vidtgående sanktionsmulighed er permanent autorisationsfratagelse, som helt afskærer den pågældende fra at udføre det hverv, som autorisationen vedrører. Sundhedsstyrelsen kan også tage initiativ til permanent virksomhedsindskrænkning, iværksættelse af midlertidig autorisationsfratagelse eller virksomhedsindskrænkning, give en sundhedsperson fagligt påbud eller sætte vedkommende under skærpet tilsyn.

Såfremt en sundhedsperson – som jo er undergivet en lovbestemt tavshedspligt, jf. sundhedslovens § 40, stk. 1 – uberettiget indhenter helbredsoplysninger m.v. i strid med sundhedslovens § 42 a, vil den pågældende desuden, medmindre højere straf er forskyldt efter anden lovgivning, kunne ifalde straf i form af bøde eller fængsel indtil 4 måneder i medfør af sundhedslovens § 271, stk. 1, nr. 2.

Der henvises i det hele til lovforslagets afsnit 2.1.1. om gældende regler i sundhedsloven samt afsnit 2.1.3.2. om datasikkerhed.

Den dataretlige beskyttelse

Hertil kommer den dataretlige beskyttelse af oplysninger om patienters privatliv. Offentlige og private dataansvarlige skal – under ansvar over for Datatilsynet – 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, jf. persondatalovens § 41, stk. 3.

For offentlige dataansvarlige gælder ydermere kravene i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen). Kun de personer, der er autoriseret hertil, må have adgang til de personoplysninger, der behandles for den offentlige forvaltning, jf. sikkerhedsbekendtgørelsens § 11, stk. 1. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, jf. sikkerhedsbekendtgørelsens § 11, stk. 2. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for, jf. ligeledes sikkerhedsbekendtgørelsens § 11, stk. 2. Det er den dataansvarlige myndighed, der udsteder autorisationerne, og som sikrer overholdelsen af de nævnte autorisationskrav, jf. herved sikkerhedsbekendtgørelsens §§ 5 og 6. Ud over, at betingelserne i sundhedslovens § 42 a skal være opfyldt for lovligt at foretage opslag, skal den dataansvarlige myndighed således altid have tildelt en brugerautorisation til den pågældende sundhedsperson for, at vedkommende kan få teknisk adgang til et elektronisk system, som benyttes af flere. Og en sådan brugerautorisation må kun gives sundhedspersoner, der er beskæftiget med de formål, hvortil personoplysninger behandles, og omfatte opslag, vedkommende har behov for.

Ydermere er der for offentlige dataansvarlige en logningspligt. Der skal som udgangspunkt foretages maskinel registrering (logning) af alle anvendelser af en række fortrolige personoplysninger og følsomme oplysninger i den offentlige forvaltning. Registreringen skal mindst indeholde oplysning 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 dog opbevare loggen i op til 5 år. Der henvises nærmere til sikkerhedsbekendtgørelsens § 19. Der skal således foretages en registrering af, hvem der inden for de sidste 6 måneder har foretaget opslag i en patientjournal, og på hvilket tidspunkt opslaget foretages. Den dataansvarlige myndighed er forpligtet til ved forskellige kontrolforanstaltninger, herunder ved logning af, hvem der har foretaget opslag, at sikre, at disse ikke uberettiget har gjort brug af den adgang, som de er autoriserede til, og kan som følge heraf foretage stikprøvekontroller.

Med venlig hilsen

Bertel Haarder / Carlo V. Andersen