RÅD FOR IT & PERSONDATASIKKERHED

Råd for IT- og Persondatasikkerhed
V/Dansk IT
Store Kongensgade 59A,
1264 København K.
Tlf.: Tlf. 33 11 15 60

Råd for IT- og Persondatasikkerheds kommentarer til lov om ændring af sundhedsloven

Generelt:

1. Den dataansvarlige efter persondataloven og overholdelse af DS484.

Der mangler en helt overordnet fastsættelse af, hvem der er dataansvarlig og for hvilke systemer, og som således er ansvarlig overfor persondataloven, herunder ikke mindst for det rent sikkerhedsmæssige.
Dog har §157, stk. 7 bestemt, at Lægemiddelstyrelsen er den dataansvarlige i forhold til Medicinprofilen, men det er det eneste sted i loven, hvor den dataansvarlige specifikt angives.
Dataansvarlighed vil automatisk medføre ansvar for sikkerheden i systemerne.
På side 16 i baggrundsmaterialet redegøres for dette, men der skabes stadig ikke klarhed over, hvem der reelt har ansvaret for de forskellige registre.
Hvis registrene bliver centrale, så bør dataansvaret ligge centralt, og ikke helt ude hos de praktiserende læger. Et decentralt dataansvar er uhensigtsmæssigt i situationer, hvor flere dataansvarlige tilgår samme databaser og systemer, idet Persondataloven foreskriver, at det er den dataansvarlige, der stiller de nødvendige krav til databehandler. I det omfang systemerne er regionalt udviklet og implementeret, vil det dog naturligvis i en overgangsfase være acceptabelt, at de regionale myndigheder er dataansvarlige.
Hvis der bliver flere dataansvarlige myndigheder, bør der i loven indføjes en bestemmelse om, at Indenrigs- og Sundhedsministeren kan fastsætte regler om system-, data- og driftssikkerheden, som de dataansvarlige skal tilslutte sig ved brug af systemerne. En lignende praksis findes i Finanssektoren, hvor de finansielle institutioner i praksis tilslutter sig de sikkerhedsbestemmelser, der udstedes af fælles datacentraler.

Generelt er området alt for ringe beskrevet i loven, hvilket åbner en klar risiko for manglende opmærksomhed på IT-sikkerheden, hvilket desværre understøttes af det faktum, at sikkerhed ikke nævnes som et væsentligt element hverken i loven eller baggrundsmaterialet.
Et krav både i loven og baggrundsmaterialet kunne være overholdelse af DS484.

2. IT-Sikkerhed er andet end blot hvem der har formelt adgang til hvad.

En bekymrende rød tråd i lovarbejdet, er det faktum, at der udelukkende adresseres problemstillinger omkring, hvilke sundhedsmyndigheder, der har adgang til hvad, og de tekniske adgangskontroller, der etableres i den sammenhæng.
Der sigtes således ikke mod de mindst ligeså væsentlige udfordringer omkring datakvalitet, datatilgængelighed og eller den helt uautoriserede adgang (hackning eller systemlækager).
Hvis datakvaliteten er ringe (hvis f.eks. databaserne, som indeholder konkret patientdata ikke har en høj integritet ved f.eks. backup og restore), så kan det betyde fejl-data, og dermed fejl-behandlinger.
Tilsvarende alvorlige problemstillinger vil opstå ved manglende tilgængelighed til systemerne eller de relevante data. Eksempelvis kan et banalt driftsnedbrud eller dataødelæggelse betyde

Råd for IT- og Persondatasikkerhed
V/Dansk IT
Store Kongensgade 59A,
1264 København K.
Tlf.: Tlf. 33 11 15 60

utilgængelighed i forhold til livsvigtige patientdata og dermed standse eller farliggøre behandlingsprocessen. Disse ting er ikke nævnt med ét ord i hverken loven eller baggrundsmaterialet.

3. Borgerens ret til at frabede sig registrering eller ubegrænset adgang.

Der findes i § 42a, stk. 4 en ret for borgeren til at frabede sig lægers og sygeplejerskers adgang til sine sundhedsdata, men kun efter §42, stk. 1. Dette betyder således ikke, at der dermed også hindres adgang jf. §157, stk. 4, 6 og 7, hvor tandlæger, sundhedsstyrelsen og lægemiddelstyrelsen gives dataadgang til medicinprofilen. En borgers mulighed for ønske om begrænsning må være gældende overalt, også i relation til Medicinprofilen overfor tandlæger, Sundhedsstyrelsen og Lægemiddelstyrelsen.

4. National it-sikkerhedsløsning.

Der er behov for en samlet national it-sikkerhedsløsning og gerne et koncept, som kunne bringes til anvendelse for alle statslige og kommunale/regionale IT-systemer, hvor der registreres og i visse situationer endda videregives personfølsomme data efter persondatalovens definitioner.
Det bør fremgå, om ikke andet så af baggrundsmaterialet, at en sådan national it-sikkerhedsløsning søges etableret og anvendt. Man kunne på det praktiske plan eventuelt overveje OCES' rolle i den sammenhæng.

5. Revision.

Et væsentligt element i kvalitetsudviklingen i sundhedssektoren bliver ved indførelse af elektroniske journal- og ordinationssystemer, at de anvendte systemer til stadighed er på et sikkerhedsmæssigt betryggende niveau, herunder at systemerne til stadighed er tilgængelige og pålidelige og giver den persondatabeskyttelse, der er beskrevet i lov og bekendtgørelser. Lignende overvejelser har for længst ført til at der stilles skærpede krav til andre sektorer, hvor kravene til pålidelighed og tilgængelighed og data fra samfundets side er høje.

Det anbefales derfor, at system-, data- og driftssikkerheden bør være underlagt årlige tilsyn af en ekstern revisor. Lignende bestemmelser findes i lovgivningen om elektroniske signaturer, bekendtgørelse om systemrevisionens gennemførelse i værdipapircentraler og bekendtgørelse om systemrevisionens gennemførelse i fælles datacentraler."

Hvis ikke en sådan revision finder sted, vil det være vanskeligt at opretholde en reel respekt for følsomheden af de data, som systemerne indeholder. En manglende opmærksomhed på f.eks. system-sårbarhedstilstanden, vil skabe risiko for, at systemerne kan kompromitteres, således at uautoriserede kan have adgang til systemerne ad bagdøre eller såkaldte "remote agents". En sådan sårbarhed kan være særdeles kritisk i forhold til følsomheden af de data der lagres.

RÅD FOR IT & PERSONDATASIKKERHED

Råd for IT- og Persondatasikkerhed
V/Dansk IT
Store Kongensgade 59A,
1264 København K.
Tlf.: Tlf. 33 11 15 60

Selve lovforslaget:

§42a, stk. 4:

I baggrundsmaterialet til lovforslaget anføres det, at der grundet patientens adgang til at frabede sig sundhedspersonalets adgang, "er taget fuldt ud hensyn til patientens retssikkerhed og selvbestemmelsesret". Dette er også korrekt på det teoretiske plan, men da data kommer til at ligge elektronisk, er der behov for lovmæssigt direkte at regulere det it-sikkerhedsmæssige. En patient kan frabede sig nok så meget, men hvis der uden det store besvær kan skaffes adgang til systemerne, er denne frabedelses-beskyttelse både akademisk og illusorisk.

§42b:

Det er problematisk, at mundtligt samtykke alene er tilstrækkeligt, idet dette er helt umuligt at dokumentere efterfølgende. Hvis en sundhedsmedarbejder i en klagesituation siger, at der er givet mundtligt samtykke, mens patienten afviser det, vil det være umuligt at fastslå sandheden, og det efterlader de involverede i en uheldig bevismæssig situation. Det er derfor vigtigt, at den sundhedsfaglige dokumenterer det modtagne mundtlige samtykke i journal eller it-system, og at patienten på en eller anden vis bekræfter dette. Det kunne evt. håndteres via Internettet med et OCES-certifikat eller ved en bekræftende e-mail. Hermed gives en rimelig beskyttelse af medarbejderen, hvis der senere opstår uenighed om samtykket.

§157, stk. 4, stk. 6 og 7:

Tandlægers, sundhedsstyrelsen og lægemiddelstyrelsens adgang bør fastsættes med samme fasthed i loven, og ikke overlades til efterfølgende ministerielle bekendtgørelser, der reelt kunne ende med at være løsere fastsat end for lægerne.

§157, stk. 7:

Det fremgår af denne paragraf at Lægemiddelstyrelsen er dataansvarlig for lægemiddelregistret. Dette mangler for de andre registre, og afgrænsningen kunne være klarere.

§193a:

Efter denne paragraf kan Sundhedsministeren fastsætte regler for it-anvendelsen i sundhedsvæsenet. Det vil imidlertid være hensigtsmæssigt om det fremgik af selv loven, at dette også gælder it-sikkerheden.

/Kim Aarenstrup, formand.