tienter til at se log-oplysninger, hvor ofte der skal foretages kontrol osv.

Sikkerheds- og brugerstyringsproblematikker er endvidere et vedvarende tema i overvejelserne for den fremtidige EPJ-udvikling og vil blive adresseret i den nationale IT-strategi for sundhedsvæsenet. Indenrigs- og Sundhedsministeriet er opmærksomt på, at kravene til EPJ-løsningens samlede IT-sikkerhed, særligt i form af systemtekniske adgangsbegrænsninger, øges med målsætningen om styrkelsen af en elektronisk patientjournal, der fuldt ud understøtter et sammenhængende patientforløb på tværs af sundhedsvæsenets sektorer baseret på pålidelige og opdaterede patientdata. Det er imidlertid den nye centrale EPJ-organisation, der i første omgang skal behandle problemstillingens tekniske begrænsninger og muligheder på sundhedsområdet, og det vil ligeledes være op til EPJ-bestyrelsen at drøfte behovet for en central sikkerheds- og brugerstyringsløsning. Indenrigs- og sundhedsministeren kan fastsætte krav til sundhedsvæsenets IT-anvendelse, herunder IT-sikkerhed, samt til godkendelsen heraf, eksempelvis i form af en certificeringsprocedure som styringsredskab, såfremt der er behov herfor for f.eks. at sikre effektiv gennemførelse af den nationale IT-strategi, jf. lovforslagets § 193 a.

Det følger af artikel 17, stk. 1, 2. pkt., i *persondatadirektivet* (Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 2005 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger), at sikkerhedsforanstaltninger skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, under hensyn til det aktuelle tekniske niveau og de omkostninger, der er forbundet med deres iværksættelse. Det forudsættes således i direktivet, at de tekniske sikkerhedsløsninger kan udvikle sig over tid. Der er i persondatalovens kapitel 11 fastsat nærmere regler om behandlingssikkerhed.

Datasikkerhed henhører under Datatilsynets kompetence. Spørgsmålet om, i hvilket omfang en bestemt teknisk adgangskontrol og efterfølgende kontrol udgør et tilstrækkeligt sikkerhedsniveau på et givent tidspunkt – i forhold til konkrete elektroniske systemer eller i forhold til en sikkerhedsbekendtgørelse udstedt af Sundhedsstyrelsen – vil således skulle afklares af Datatilsynet efter en dialog med de relevante sundhedsmyndigheder.

Det er af væsentlig betydning, at spørgsmålet om tekniske adgangsbegrænsende foranstaltninger for konkrete systemer indtænkes af den dataansvarlige (for eksempel regionen eller en privatpraktiserende læge) på et tidligt tidspunkt, f.eks. i forbindelse med formuleringen af kravspecifikationer. De dataansvarlige opfordres derfor til at kontakte Datatilsynet så tidligt som muligt, så der ikke senere skal bruges ressourcer på at tilpasse systemerne til de gældende datasikkerhedskrav. Derudover vil Indenrigs- og Sundhedsministeriet drage omsorg for, at EPJ-bestyrelsen drøfter, på hvilket tidspunkt det vil være hensigtsmæssigt at kontakte Datatilsynet, hvis organisationen beskæftiger sig med en central sikkerheds- og brugerstyringsløsning eller andre datasikkerhedsrelaterede emner.

4.2.1.3. Klage og straf

Klager over indhentning af oplysninger efter den foreslåede § 42 a, stk. 1-5, kan indbringes for Sundhedsvæsenets Patientklagenævn. Det kan f.eks. være en klage over, om det har været nødvendigt at indhente helbredsoplysninger mv. i forbindelse med en aktuel patientbehandling.

Der henvises til den affattelse af § 2, stk. 1, i lov om klage- og erstatningsadgang inden for sundhedsvæsenet, som foreslås med lovforslagets § 2, nr. 1.

Det er en væsentlig offentlig interesse at sikre en stor tillid til fortroligheden af oplysninger i elektroniske patientjournaler. Indenrigs- og Sundhedsministeriet finder derfor, at den, der indhenter oplysninger i strid med den foreslåede § 42 a, stk. 1-5, bør kunne straffes.

Der findes straffebestemmelser i lov om behandling af personoplysninger, men disse bestemmelser finder ikke anvendelse, når der – som i dette tilfælde – sker overtrædelse af materielle behandlingsregler i anden lovgivning.

Der findes i straffeloven forskellige bestemmelser, hvorefter uberettiget videregivelse eller udnyttelse af oplysninger i forskellige sammenhænge kan straffes. Det drejer sig om straffelovens §§ 152-152 f om tavshedspligt samt straffelovens § 155 om misbrug af offentlig stilling. Sundhedsloven henviser i § 267 til disse bestemmelser.

Hverken efter de nævnte regler i straffeloven eller efter andre regler er det muligt at straffe den, der indhenter oplysninger ved opslag i elektroniske patientjournaler i strid med den foreslåede bestemmelse i § 42 a.

Det foreslås derfor, at der ved en ændring af sundhedslovens § 271 fastsættes regler om, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde eller fængsel indtil 4 måneder den, der indhenter oplysninger i strid med § 42 a, stk. 1-5. Dette svarer til strafferammen efter persondataloven.