DATATILSYNET

Region Midtjylland
Skottenborg 26
Postboks 21
8800 Viborg

Att.: Regionsrådet
v. regionsrådsformand Bent Hansen

Sendt til: kontakt@regionmidtjylland.dk

30. januar 2015

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2012-622-0004
2014-632-0075
Sagsbehandler
Maiken Christensen
Direkte 3319 3224

Vedrørende Region Midtjyllands fælles elektroniske patientjournal (MidtEPJ)

1. Datatilsynet har gennem længere tid korresponderet med Region Midtjylland om brugeradgangen i MidtEPJ til elektroniske patientoplysninger og om opfølgningen på en inspektion, som tilsynet tidligere har gennemført på Regionshospitalet Randers.

Datatilsynet skal – efter at sagen har været behandlet i Datarådet – sammenfattende udtale følgende:

1.1 Region Midtjylland har bevidst valgt at indrette MidtEPJ sådan, at samtlige autoriserede personalegrupper, inden for de "roller" de er blevet tildelt, har adgang til oplysninger om alle patienter, der er eller har været i behandling i Region Midtjylland. Der er således ikke etableret tekniske foranstaltninger for nogen brugerroller, som begrænser adgangen til patientoplysninger på tværs af regionens forskellige behandlingsenheder eller som på anden måde teknisk hindrer, at der kan ske uberettigede opslag i systemet.

En sådan indretning af EPJ-systemet er efter Datatilsynets opfattelse kritisabel og ikke i overensstemmelse med persondatalovens regler om saglighed, proportionalitet og behandlingssikkerhed, jf. § 5 og § 41, ligesom kravene i sikkerhedsbekendtgørelsens § 11, stk. 2, ikke kan anses for opfyldt. Efter de oplysninger, som Datatilsynet har kunnet få fra regionen, er det således tilsynets vurdering, at i hvert fald nogle autoriserede personalegrupper har adgang til oplysninger, som de må antages ikke at have behov for i deres opgaveløsning.

Datatilsynet skal i den forbindelse også pege på sundhedslovens § 42 a, stk. 2, som omhandler adgangen for andre sundhedspersoner end de, der er omfattet af § 42 a, stk. 1[1], til at indhente oplysninger ved "opslag i elektroniske systemer, hvori adgangen for den pågældende sundhedsperson teknisk er begrænset til de patienter, der er i behand-

[1] § 42 a, stk. 1, omfatter læger, tandlæger, jordemødre, sygeplejersker, sundhedsplejersker, social- og sundhedsassistenter, radiografer og ambulancebehandlere med særlig kompetence.

ling på samme behandlingsenhed, som den pågældende sundhedsperson er tilknyttet […]."

Bestemmelsen bygger således efter sin ordlyd på en forudsætning om, at disse kategorier af sundhedspersoner kun skal have adgang til oplysninger efter bestemmelsen, hvis der er en teknisk adgangsbegrænsning i relation til organisatorisk tilknytning. Det fremgår af bemærkningerne til bestemmelsen, at der ved udtrykket behandlingsenhed forstås sygehus, sygehusafdeling, afsnit, klinik el.lign., og at kravet om organisatorisk tilknytning datasikkerhedsmæssigt skal administreres så snævert, som det teknisk er muligt.

Det er efter Datatilsynets opfattelse endvidere et krav, at det personale, der *ikke* er sundhedspersoner, *kun* har systemteknisk adgang til oplysninger om patienter i aktuel behandling i samme behandlingsenhed, som vedkommende er tilknyttet, jf. hertil sundhedslovens § 42 a, stk. 11.

Datatilsynet anmoder regionen om at oplyse, hvad man agter at foretage sig i anledning af tilsynets udtalelse.

Hvad angår sundhedspersoner omfattet af sundhedslovens § 42 a, stk. 1, synes forarbejderne til bestemmelse at forudsætte, at der også for disse kategorier af sundhedspersoner skal være en teknisk adgangsbegrænsning under en eller anden form, se herved lovforslag nr. L 50 af 25. oktober 2006, bemærkningerne til § 42 a, stk. 1.

Efter de oplysninger, som Datatilsynet har modtaget fra Region Midtjylland, er dette imidlertid ikke tilfældet med hensyn til MidtEPJ. Datatilsynet har derfor samtidig hermed over for Ministeriet for Sundhed og Forebyggelse rejst spørgsmål om, hvorvidt dette er i overensstemmelse med § 42 a, stk. 1.

1.2 Datatilsynet finder det ligeledes kritisabelt, at Region Midtjylland som dataansvarlig myndighed ikke har kunnet redegøre for hjemlen/hjemlerne til personalets opslag og baggrunden for oprettelsen af de enkelte "roller" med adgang til oplysninger i MidtEPJ samt for begrundelsen for omfanget af den adgang til oplysninger i systemet, som er tildelt de enkelte roller. Det gælder brugerrollerne kapelbetjent, piccoline, præst, musikterapeut, skolelærer og ingeniør.

På Datatilsynets spørgsmål har regionen oplyst, *at* det ikke er muligt at identificere, hvilke begrundelser der ligger bag oprettelse af de pågældende roller, *at* It-afdelingen ikke har dokumentation herfor, men at en rolle med deraf følgende tildeling af autorisation og adgang uden geografisk begrænsning inden for regionen tildeles efter vurdering og indstilling fra en ansvarlig leder for den pågældende person, samt *at* de omhandlede roller ikke nødvendigvis aktuelt er i brug.

For så vidt angår indholdet af/adgangene for de enkelte roller er det Datatilsynets umiddelbare opfattelse, at der som udgangspunkt ikke er grundlag for at give personale, der *ikke* er sundhedspersoner, system-

teknisk adgang til funktioner som f.eks. "Epikriselæser" og "Ejournal-adgang", jf. hertil kravene i persondatalovens § 5 og § 41, samt sikkerhedsbekendtgørelsens § 11, stk. 2.

Datatilsynet anmoder regionen om at oplyse, hvad man agter at foretage sig i anledning af tilsynets udtalelse.

1.3 På baggrund af det oplyste lægger Datatilsynet endvidere til grund, at der (fortsat) ikke er indført halvårlige kontroller af udstedte autorisationer, jf. sikkerhedsbekendtgørelsens § 17, stk. 2. Datatilsynet har tidligere påtalt dette forhold.

I den forbindelse bemærkes, at det på det foreliggende grundlag er Datatilsynets opfattelse, at en automatiseret autorisationskontrol baseret på "rollebaseret systemadgang" ikke kan erstatte den manuelle procedure for halvårlig kontrol af brugerautorisationer, som er foreskrevet i sikkerhedsbekendtgørelsen.

Region Midtjylland anmodes om at bekræfte, at kontrollerne nu etableres.

1.4 På baggrund af regionens svar, senest ved brev af 30. september 2014, er det fortsat uklart for Datatilsynet, om regionen har slettet brugere, der ikke længere er ansat i regionen, og har foretaget nødvendige ændringer i autorisationerne, eller om dette udelukkende vil ske fremadrettet som følge af en procedure, hvorefter brugere slettes, når ansættelsesforholdet ophører.

Endvidere rejser regionens besvarelse spørgsmål om, hvorvidt der er brugere, der logger ind i EPJ, uden at dette sker med regions-id knyttet til ansættelsen.

Region Midtjylland anmodes om at bekræfte, at den fornødne sletning – som regionen selv har forudsat gennemført senest pr. 1. juni 2014 – samt fornødne ændringer i autorisationerne nu er sket, og at den indførte procedure for sletning mv. omfatter alle brugere.

Datatilsynet skal understrege, at det er et ufravigeligt krav, at personer, der ikke (længere) er ansat, ikke har adgang til systemet.

1.5 Datatilsynet har noteret sig regionens oplysning om, at der fremover vil blive sikret gennemgang af regionens interne sikkerhedsbestemmelser mindst én gang årligt.

1.6 Datatilsynet forudsætter, at sletning af oplysninger sker i overensstemmelse med sletningsfristen i regionens anmeldelse af "Patientbehandling i regionalt regi". Såfremt sletningsfristen ønskes ændret, skal anmodning herom indgives til Datatilsynet. Hvis fortsat opbevaring af oplysningerne sker udelukkende med henblik på brug til forskning, skal behandlingen omfattes af en forskningsanmeldelse.

1.7 Datatilsynet forudsætter endelig, at regionen foretager logning af anvendelser i patientsystemet i overensstemmelse med bestemmelsen i sikkerhedsbekendtgørelsens § 19.

Datatilsynet finder sagens langstrakte forløb meget beklageligt. Uanset at dette til dels beror på tilsynets egen sagsbehandling, er det Datatilsynets opfattelse, at Region Midtjylland i væsentlig grad har bidraget til det meget lange forløb. Datatilsynet har således under forløbet måttet stille de samme spørgsmål flere gange, og i flere tilfælde har tilsynet fået uklare eller ufyldestgørende svar.

2. Som ovenfor nævnt finder Datatilsynet på baggrund af de oplysninger, som Region Midtjylland har afgivet, at MidtEPJ ikke lever op til persondatalovens regler, ligesom Datatilsynet finder det tvivlsomt, om systemet lever op til reglerne i sundhedslovens § 42 a.

Datatilsynet har derfor samtidig hermed orienteret Ministeriet for Sundhed og Forebyggelse om sagen.

Datatilsynet har i brevet til ministeriet endvidere peget på, at det fremgår af bemærkningerne til sundhedslovens § 42 a, stk. 2, at adgangen for visse grupper af sundhedspersoner til elektroniske systemer så vidt muligt skal administreres med henblik på at sikre, at *historiske* oplysninger er teknisk utilgængelige for de pågældende.

Datatilsynet vurderer umiddelbart, at det kan være praktisk vanskeligt at foretage en opdeling af oplysninger om aktuel behandling og historiske oplysninger, idet dette vil bero på en løbende, konkret vurdering af de pågældende oplysninger.

Tilsynet har derfor henledt ministeriets opmærksomhed på, om der er behov for generelt at se på denne problemstilling.

Kopi af brevet til ministeriet vedlægges.

3. Datatilsynet anmoder om at modtage regionens tilbagemelding inden 6 uger.

Folketingets Sundheds- og Forebyggelsesudvalg, Folketingets Retsudvalg og Danske Regioner modtager kopi af dette brev samt af brevet til ministeriet til orientering.

Det skal for god ordens skyld bemærkes, at Datatilsynet forventer at offentliggøre dette brev på tilsynets hjemmeside.

Med venlig hilsen

Henrik Waaben
Formand for Datarådet

Birgit Kleis
Kommitteret

Bilag: Kopi af Datatilsynets brev af dags dato til Ministeriet for Sundhed og Forebyggelse