Datainspektionen

Datum	Diarienr
2013-08-26	920-2012

Styrelsen för Karolinska
universitetssjukhuset
Sjukhusledningen C1:89
141 86 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – behörighetsstyrning m.m. enligt patientdatalagen

Datainspektionens beslut

1. Styrelsen för Karolinska universitetssjukhuset (KS) föreläggs att genomföra en behovs- och riskanalys för journalsystemet TakeCare (TakeCare).

2. KS föreläggs att ta fram riktlinjer som underlag för KS´ bedömning av vad som är obehörig elektronisk åtkomst enligt 4 kap. 3 § patientdatalagen.

3. KS ska redovisa resultatet av behovs- och riskanalysen enligt punkt 1 och framtagna riktlinjerna enligt punkt 2. Skriftlig redovisning ska ges in till Datainspektionen senast den 20 december 2013.

Ärendet avslutas, men kommer att följas upp enligt ovan.

Redogörelse för tillsynsärendet

Syftet med tillsynen är att kontrollera hur KS begränsar den elektroniska åtkomsten till patientuppgifter inom ramen för den inre sekretessen enligt 4 kap. 1 § patientdatalagen. Syftet är också att kontrollera hur KS arbetar med verkningsfulla loggуppföljningar när misstanke har uppkommit om obehörig elektronisk åtkomst till patientuppgifter.

Datainspektionen genomförde en inspektion hos KS den 20 juni 2012. KS har därefter gett synpunkter på inspektionsprotokollet och svarat på komplet-

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

terande frågor, bland annat om planerat arbete för översyn och vidareutveckling av behörighetsstyrningen i TakeCare.

Skäl för beslutet

Nedan bedömer Datainspektionen frågor om behörighetsstyrning och åtkomstkontroll enligt 4 kap. 2 och 3 §§ patientdatalagen.

Behörighetsstyrning

Följande har framkommit. Hos KS har 10 000 befattningshavare åtkomst i TakeCare. Det tillkommer 9 000 befattningshavare hos SLSO (Styrelsen för Stockholms läns sjukvårdsområde med landstingsdrivna vårdcentraler och öppenvårdspsykiatri). Det finns behörighetsprofiler som kan överskrida en spärr och det är sjuksköterska, läkare och paramedicinare (avser enligt KS kuratorer, ortopister, dietister, arbetsterapeuter, logopeder, psykologer och audionomer). Nuvarande behörighetsprofiler är enligt KS ett resultat av analyser. Landstingsrevisorerna har dock varit kritiska till utformningen av nuvarande behörigheter. KS kommer under andra kvartalet 2013 att tillsammans med systemleverantören påbörja en översyn och vidareutveckling av behörighetstilldelningen i TakeCare. Behörighet ska harmonisera med den nationella katalogtjänsten HSA som används av många landsting. En användare ska kunna tilldelas en behörighet utifrån användarens ”olika roller” och behörigheten ska harmonisera med medarbetaruppdrag och uppdragsområden i HSA-katalogen. KS har den 5 juli 2013 uppgett att en tidplan rörande genomförandet kommer att finnas i början av hösten och att ett första möte ägde rum den 19 juni 2013.

En vårdgivare ska begränsa en användares behörigheter till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården och till vad som är nödvändigt för att ge god och säker vård. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Detta framgår av 4 kap. 2 § patientdatalagen och 2 kap. 6 § SOSFS 2008:14. Reglerna kompletterar bestämmelsen om inre sekretess i 4 kap. 1 § patientdatalagen, som även omfattar uppgifter om avlidna, se 1 kap. 1 § andra stycket patientdatalagen.

I propositionen 2007/08:126 *Patientdatalag m.m.* uttalar regeringen att syftet med 4 kap. 2 § patientdatalagen är att inpränta skyldigheten för den ansvariga vårdgivaren att göra aktiva och individuella behörighetstilldelningar utifrån

analyser av vilken information olika personalkategorier och olika slags verksamheter behöver (s. 148).

Regeringen uttalar vidare (aa s. 149). Men det behövs inte bara behovsanalyser. Även riskanalyser måste göras där man tar hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Skyddade personuppgifter som är sekretessmarkerade, uppgifter om kända personer och uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier som kan kräva särskilda riskbedömningar [regeringen skriver också att riskanalyser är särskilt viktiga avseende tillgängligheten till nämnda kategorier av patienter, aa s. 240]. Generellt kan sägas att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. Avgörande för beslut om behörighet för t.ex. olika kategorier av hälso- och sjukvårdspersonal till elektronisk åtkomst till uppgifter i patientjournaler bör vara att behörigheten ska begränsas till vad befattningshavaren behöver för ändamålet en god och säker patientvård. En mer vidsträckt eller grovmaskig behörighetstilldelning bör – även om den skulle ha poänger utifrån effektivitetssynpunkt – anses som en obefogad spridning av journaluppgifter inom en verksamhet och bör som sådan inte accepteras.

Regeringen uttalar också att patientens rätt att spärra information inte innebär en inskränkning av vårdgivarnas skyldigheter att utifrån bl.a. behovs- och riskanalyser begränsa den elektroniska tillgängligheten till elektroniska patientuppgifter inom sin verksamhet och patientens rätt till inre spärrar utgör bara ett komplement till vårdgivarnas ansvar i detta avseende (aa s. 152).

Ett stort antal patienter omfattas av den hälso- och sjukvård som bedrivs inom Stockholms läns landsting av KS (och SLSO) i det inre sekretessområdet. Datainspektionen anser att KS för närvarande har en alltför vidsträckt och grovmaskig behörighetstilldelning. Att patienten har en spärrmöjlighet i TakeCare innebär inte att KS kan låta bli att göra verkningsfulla behovs- och riskanalyser för TakeCare. Mot bakgrund av behovs- och riskanalysens avgörande betydelse som underlag för en väl avvägd behörighetstilldelning, finns det skäl att förelägga KS att genomföra en behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14. KS ska redovisa resultatet av behovs- och riskanalysen senast den 20 december 2013.

Ett exempel på ett analysområde kan enligt Datainspektionen vara behovs- och riskanalyser gällande befattningshavare som inte deltar i den direkta vården av patienter, utan som av annat skäl kan behöva patientuppgifter för sitt arbete inom hälso- och sjukvården, jämför 4 kap. 1 § patientdatalagen. Här bör KS beakta regeringens uttalande om att när det gäller personal som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individ-orienterad, torde det för flertalet befattningshavare räcka med tillgång till uppgifter som endast indirekt kan härledas till enskilda patienter (aa s. 149).

I övrigt är också en befattningshavares faktiska arbetsuppgifter, organisatoriska tillhörighet m.m. av betydelse.

Åtkomstkontroll

Följande har framkommit. KS har den 6 mars 2012 antagit dokumentet *Rutinbeskrivning Riktad logganalys* som beskriver handläggningen när en patient har begärt loggutdrag eller när misstanke om otillbörlig/obehörig journalöppning uppkommit på annat sätt, till exempel genom personalens iakttagelser. Enligt dokumentet ska ett fördjupat loggutdrag tas fram vid misstanke om otillbörlig journalöppning eller om användaren i ett första steg inte kan precisera vad denne gjort i patientens journal. Verksamhetschef eller motsvarande chef pekas ut som de som i olika steg gör bedömningar kring om den elektroniska åtkomsten varit befogad eller inte. Enligt KS ska verksamhetscheferna ge närmare instruktioner.

Enligt 4 kap. 3 § patientdatalagen ska en vårdgivare se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivaren ska också göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter. Bestämmelsen kompletterar den om inre sekretess i 4 kap. 1 § patientdatalagen, som även omfattar uppgifter om avlidna, se 1 kap. 1 § andra stycket patientdatalagen.

Regeringen har uttalat att vårdgivarna för att främja patientsäkerheten bör åläggas att systematiskt och fortlöpande företa kontroller av om obehörig åtkomst till uppgifter om patienter förekommer. Vidare uttalar regeringen att en sådan bestämmelse inte bara innebär att faktiska dataintrång med större säkerhet kommer att kunna beivras, utan också bör få en starkt avhållande verkan på personal som, om risken för upptäckt är liten, kan frestas att olovligen läsa uppgifter (aa s. 149 f).

I det här sammanhanget är det också av intresse att en vårdgivare på begäran av en patient ska lämna information om den direktåtkomst och elektroniska åtkomst till uppgifter om patienten som förekommit. Det framgår av 8 kap. 5 § patientdatalagen. Bestämmelsen har kompletterats av Socialstyrelsen som föreskriver att informationen till patienten ska vara utformad på ett sådant sätt att patienten kan bedöma om åtkomsten varit befogad eller inte, 2 kap. 12 § SOSFS 2008:14. Den information som lämnas måste enligt regeringen vara begriplig och vägledande för patienten när han eller hon själv ska bilda sig en uppfattning om huruvida åtkomsten varit befogad eller inte (aa s. 265).

Enligt Datainspektionen saknar dokumentet *Rutinbeskrivning Riktad logganalys* riktlinjer som kan utgöra underlag för KS att bedöma om en elektronisk åtkomst är obehörig eller inte. Det har inte framkommit att det finns andra instruktioner eller riktlinjer för vad som utgör obehörig elektronisk åtkomst.

Loggkontrollerna kan inte bli verkningsfulla om vårdgivaren saknar riktlinjer för vad som utgör obehörig elektronisk åtkomst. Enligt Datainspektionen riskerar vårdgivaren att åsidosätta den inre sekretessen om vårdgivaren inte har gjort klart internt vad som är en obehörig elektronisk åtkomst. Mot denna bakgrund finns det skäl att förelägga KS att utarbeta riktlinjer för vad som utgör obehörig elektronisk åtkomst. KS ska redovisa riktlinjerna till Datainspektionen senast den 20 december 2013.

Ärendet avslutas, men kommer att följas upp.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet skall ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö i närvaro av chefsjuristen Hans-Olof Lindblom, tillsynschefen Erik Janzon och avdelningsdirektören Suzanne Isberg, föredragande.

Kristina Svahn Starrsjö

Suzanne Isberg

Kopia till:

Personuppgiftsombudet, Karolinska universitetssjukhuset,
Norrbacka S3:01, 171 76 Stockholm

Socialstyrelsen, 106 30 Stockholm

Inspektionen för vård och omsorg, Box 45184, 104 30 Stockholm