

Feelgood Företagshälsovård AB
Box 101 11
100 55 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - Behovs- och riskanalys samt riktlinjer till befattningshavare som utför loggkontroller

Datainspektionens beslut

Feelgood Företagshälsovård (vårdgivaren) uppfyller inte kravet att genomföra en behovs- och riskanalys enligt 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) jämfört med 2 kap. 6 § andra stycket andra meningen Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Vårdgivaren föreläggs därför att ta fram en dokumenterad behovs- och riskanalys enligt nämnda föreskrift för huvudjournalssystemet.

Datainspektionen konstaterar att vårdgivarens befattningshavare som utför loggkontroller inte har fått tillräcklig vägledning om vad som kan utgöra obehörig åtkomst. Vårdgivaren föreläggs därför att ta fram en skriftlig vägledning riktad till befattningshavare som utför loggkontroller, så att befattningshavarna på ett verkningsfullt sätt kan kontrollera om elektronisk åtkomst ägt rum obehörigen enligt 4 kap. 3 § första stycket andra meningen patientdatalagen (2008:355).

Redogörelse för tillsynsärendet

Bakgrunden till tillsynen är att Datainspektionen tidigare konstaterat brister hos en vårdgivare (beslut den 28 augusti 2013, ärende 920-2012 avseende

Styrelsen för Karolinska universitetssjukhuset, KS).¹ Datainspektionen konstaterade i ärendet att behörighetstilldelningen var alltför grovmaskig, vilket var en konsekvens av att vårdgivaren inte hade gjort behovs- och riskanalyser för att begränsa personalens elektroniska åtkomst. Vidare saknades en vägledning till befattningshavare som utförde loggkontroller om vad som kan utgöra obehörig elektronisk åtkomst, däremot fanns det en rutin för riktad logganalys.

Datainspektionen har därefter i ett större tillsynsprojekt granskat landsting och regioner (ärende 1598-2013 – 1619-2013) och funnit att många vårdgivare inte uppfyller kravet på en dokumenterad behovs- och riskanalys och att ge vägledning till de som har att bedöma vad som är obehörig åtkomst.

Datainspektionen har nu inlett tillsyn mot två privata och en landstingsägd vårdgivare för att granska dessa frågor. I detta ärende granskas om FeelGood Företagshälsovård AB har tagit fram en dokumenterad behovs- och riskanalys för huvudjournalssystemet och om det finns vägledning till befattningshavare som ska utföra loggkontroller om vad som kan utgöra obehörig åtkomst.

Skäl för beslutet

Datainspektionen har ställt följande fråga: Har ni en dokumenterad behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14? När upprättades dokumentet?

Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) upphävdes och ersattes den 1 mars 2017 av Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Bestämmelsen om behovs- och riskanalys finns i 4 kap. 2 § i de nya föreskrifterna och motsvarar 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14.

Datainspektionen har begärt in och mottagit kopior på de dokument som vårdgivaren har hänvisat till.

¹ <http://www.datainspektionen.se/Documents/beslut/2013-08-26-riskanalys.pdf>

Feelgood Företagshälsovård AB har uppgett följande. Det finns en dokumenterad behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen. Dokumentet benämns "Journalåtkomst-inre sekretess".

I dokumentet, som getts in till Datainspektionen, hänvisas till 2 kap. 6 § SOSFS 2008:14. Därefter räknas följande punkter upp.

- *Begränsas journalåtkomst till vad som är nödvändigt för att ge en god och säker vård.*
- *Varje användare tilldelas en individuell behörighet och åtkomst till patientuppgifter.*
- *Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.*
- *Vårdgivaren ska ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter.*

Under rubriken utförande anges sedan följande:

Ur detta följer att inom Feelgood företagshälsovård

- *Endast vårdpersonal ska ha läs- och skrivbehörigheter i patientdelen av journalsystemet J4.*
- *Vid vissa kvalitetsmätningar och uppföljning kan viss administrativ personal tilldelas behörighet endast i kvalitetsuppföljningssyfte.*
- *Vid nyanställning tilldelas nya användare behörighet utifrån den definierade yrkesrollen, till vilken den tillhör.*

Datainspektionen kan konstatera att vårdgivaren är personuppgiftsansvarig enligt 2 kap. 6 § patientdatalagen (2008:355). Vårdgivaren 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 4 kap. 2 § HSLFS-FS 2016:40 jämfört med dess tidigare lydelse i 2 kap. 6 § SOSFS 2008:14. Dessa bestämmelser kompletterar bestämmelsen om inre sekretess i 4 kap. 1 § patientdatalagen.

I propositionen 2007/08:126 *Patientdatalag m.m.* uttalar regeringen (s. 148 f) 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. Det framgår också att 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. Regeringen uttalar vidare att 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.

Ett exempel på ett särskilt analysområde, utöver det som primärt omfattar individorienterad vård och behandling, är enligt Datainspektionen behovs- och riskanalyser gällande befattningshavare som inte deltar i den direkta vården av patienter, utan som av andra skäl kan behöva patientuppgifter för sitt arbete inom hälso- och sjukvården, jämför 4 kap. 1 § patientdatalagen. Även här måste en vårdgivare enligt 4 kap. 2 § första stycket andra meningen begränsa behörigheter till vad som behövs för att anställda ska kunna fullgöra arbetsuppgifter inom hälso- och sjukvården. Av särskild vikt är att vårdgivarna beaktar regeringens uttalande att det för flertalet befattningshavare som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad, torde räcka med tillgång till uppgifter som endast indirekt kan härledas till enskilda patienter (a.a. s. 149).

Datainspektionen konstaterar att det således är vårdgivaren som ska begränsa en användares behörighet 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. Vårdgivaren ska göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken information olika personalkategorier och olika slags verksamheter behöver. Vårdgivaren ska också göra riskanalyser där vårdgivaren tar hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Det innebär att behovs- och riskanalyser har en avgörande betydelse för en väl avvägd behörighetstilldelning. En generös behörighetstilldelning innebär ofta en obefogad spridning av patientuppgifter (a.a. s. 240).

Arbetet måste genomföras fortlöpande eftersom verksamheten är föränderlig både avseende personal och hur personuppgiftsbehandlingen sker. Att

vårdgivaren ska göra en dokumenterad behovs- och riskanalys, innebär att vårdgivaren ska skapa rutiner som säkerställer att behörighetstilldelningen sker i enlighet med gällande bestämmelser och utifrån den specifika verksamhet som vårdgivaren bedriver. Vårdgivaren måste inrätta rutiner som anger vilka behov och risker som ska beaktas inför varje behörighetstilldelning och *hur* en behovs- och riskanalys ska utföras, samt inrätta kontrollinstrument för att följa upp att de föreskrivna åtgärderna faktiskt vidtas ute i verksamheten. Detta kan jämföras med en företagslednings ansvar för ekonomistyrning och redovisning – eller hur systematiskt arbetsmiljöarbete ska utföras.

Vårdgivarens rutiner måste vara så tydliga för den personal, som har i uppgift att genomföra behovs- och riskanalyser inför behörighetstilldelningar i verksamheten, att bedömningarna blir enhetliga och förhindrar obefogad spridning. Vårdgivaren måste även på ett verkningsfullt och strukturerat sätt kontrollera att rutinerna följs och att tilldelningen av behörigheter sker i enlighet med de instruktioner som getts. Om brister upptäcks måste vårdgivaren som ansvarig agera.

Vårdgivaren har utarbetat ett dokument, *Journal åtkomst – inre sekretess*, av vilket det framgår att vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Av dokumentet framgår också vissa faktorer som vårdgivaren ska ta hänsyn till vid tilldelning av behörigheter. Datainspektionen saknar dock rutiner för hur behovs- och riskanalyser ska göras inför varje enskild behörighetstilldelning innehållandes anvisningar till de befattningshavare som tilldelar behörigheter om vilka kriterier som behörigheter ska tilldelas utifrån och vilka behov och risker som ska beaktas i varje enskilt fall. Vårdgivaren måste även ha möjlighet att kontrollera att rutinerna följs. Sammantaget har det därmed inte framkommit i ärendet att vårdgivaren har en dokumenterad behovs- och riskanalys. Datainspektionen anser därför att det finns skäl att förelägga vårdgivaren att genomföra en dokumenterad behovs- och riskanalys enligt 4 kap. 2 § HSLFS-FS 2016:40 jämfört med 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14 för huvudjournalssystemet.

Datainspektionen har ställt följande fråga: Har ni skriftliga riktlinjer som beskriver/definierar vad som är obehörig åtkomst enligt lydelsen i 4 kap. 3 § första stycket andra meningen patientdatalagen, dvs. riktlinjer som utgör ett stöd för era befattningshavare som utför

loggkontrollerna? När upprättades dokumentet? Beskriv riktlinjerna till de befattningshavare som utför loggkontroller.

Datainspektionen har begärt in och mottagit kopior på de dokument som vårdgivaren har hänvisat till.

Vårdgivaren har gett in ett dokument som innehåller rutiner för loggkontroller. Av dokumentet framgår att vårdgivaren ska göra återkommande loggkontroller. Där åtkomst inte kan matchas mot en skapad journalpost väcker det misstanke om otillbörlig åtkomst. Enligt rutinen ska även stickprovskontroller göras vid

- larm från personalen,
- patient misstänker,
- behandling av kända personer
- behandling av egen personal

Om åtkomst, som upptäcks vid stickprovskontroll, inte kan matchas mot en skapad journalpost väcker det misstanke om otillbörlig åtkomst.

Datainspektionen konstaterar att enligt 4 kap. 3 § första stycket andra meningen patientdatalagen ska vårdgivare göra systematiska och återkommande kontroller av om någon obehörigen kommer åt patientuppgifter. Bestämmelsen kompletterar den om inre sekretess i 4 kap. 1 § 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 (a.a. s. 149 f). Datainspektionen anser att loggkontrollerna inte blir verkningsfulla om det saknas riktlinjer till befattningshavare som utför loggkontroller om vad som kan utgöra obehörig elektronisk åtkomst. I sådant fall riskerar en vårdgivare att åsidosätta den inre sekretessen.

Datainspektionen anser att vårdgivaren i viss mån har förutsättningar att kunna vägleda befattningshavare som utför loggkontroller så att dessa befattningshavare kan kontrollera om någon obehörigen kommer åt patientuppgifter enligt 4 kap. 3 § första stycket andra meningen patientdatalagen. Datainspektionen anser dock att det inte tillräckligt tydligt framgår vilka omständigheter som bör beaktas av befattningshavare som utför loggkontroller vid bedömningen av vad som kan vara obehörig åtkomst. Mot bakgrund av ovanstående anser Datainspektionen att det finns skäl att förelägga vårdgivaren att förtydliga vilka faktorer som ska beaktas vid bedömning av vad som är att anse som obehörig åtkomst så att befattningshavare som utför loggkontroller på ett verkningsfullt sätt kan kontrollera om någon obehörigheten kommer åt patientuppgifter enligt 4 kap. 3 § första stycket andra meningen patientdatalagen.

Övrigt

Datainspektionen bifogar en sammanställning av tillsynsprojektet beträffande landsting och regioner. Sammanställningen innehåller en övergripande redovisning av resultatet av tillsynsprojektet, tillämpliga rättsregler, beskrivning av goda exempel och Datainspektionens rekommendationer.

Tillsynsärendet omfattar inte frågan om vårdgivaren utför systematiska och återkommande loggkontroller enligt 4 kap. 3 § första stycket patientdatalagen.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag ni fick del av beslutet. 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 enhetschefen Katarina Tullstedt efter föredragning av juristen Martina Lindkvist. Vid den slutliga handläggningen av ärendet har även IT-säkerhetsspecialisten Magnus Bergström deltagit.

Katarina Tullstedt

Martina Lindkvist