Styrelsen för Karolinska Universitetssjukhuset
Karolinska Universitetssjukhuset Solna
171 76 Stockholm

Tillsyn enligt dataskyddsförordningen – behovs- och riskanalys och frågor om åtkomst i journalsystem

Innehåll

Datainspektionens beslut

Datainspektionen har vid granskning den 27 mars 2019 konstaterat att Styrelsen för Karolinska Universitetssjukhuset (Karolinska Universitetssjukhuset) behandlar personuppgifter i strid med artikel 5.1 f och 5.2 samt artikel 32.1 och 32.2 i dataskyddsförordningen[1] genom att

1. Karolinska Universitetssjukhuset i egenskap av personuppgiftsansvarig inte uppfyller kravet på att det ska ha genomförts en behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemet TakeCare, i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) samt 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Detta innebär att Karolinska Universitetssjukhuset inte har vidtagit lämpliga organisatoriska åtgärder för att kunna säkerställa och kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.

2. Karolinska Universitetssjukhuset inte har begränsat användarnas behörigheter för åtkomst till journalsystemet TakeCare till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen samt 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att Karolinska Universitetssjukhuset inte har vidtagit åtgärder för att kunna säkerställa och kunna visa en lämplig säkerhet för personuppgifterna.

Datainspektionen beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen samt 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning att Karolinska Universitetssjukhuset, för överträdelse av artikel 5.1 f och 5.2

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

samt artikel 32.1 och 32.2 i dataskyddsförordningen ska betala en administrativ sanktionsavgift på 4 000 000 (fyra miljoner) kronor.

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Karolinska Universitetssjukhuset att se till att erforderlig behovs- och riskanalys genomförs och dokumenteras för journalsystemet TakeCare och att därefter, med stöd av behovs- och riskanalysen, varje användare tilldelas individuell behörighet för åtkomst till personuppgifter till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen, 4 kap. 2 § och 6 kap. 7 § patientdatalagen samt 4 kap. 2 § HSLF-FS 2016:40.

Redogörelse för tillsynsärendet

Datainspektionen inledde tillsyn genom skrivelse den 22 mars 2019 och har på plats den 27 mars 2019 granskat om Karolinska Universitetssjukhusets beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Granskningen har även omfattat hur Karolinska Universitetssjukhuset tilldelat behörigheter för åtkomst till huvudjournalsystemet TakeCare, och vilka åtkomstmöjligheter de tilldelade behörigheterna ger inom såväl ramen för den inre sekretessen enligt 4 kap. patientdatalagen, som den sammanhållna journalföringen enligt 6 kap. patientdatalagen. Utöver detta har Datainspektionen även granskat vilken dokumentation av åtkomst (loggar) som finns i journalsystemet.

Datainspektionen har endast granskat användares åtkomstmöjligheter till journalsystemet, det vill säga vilken vårddokumentation användaren faktiskt kan ta del av och läsa. Granskningen omfattar inte vilka funktioner som ingår i behörigheten, det vill säga vad användaren faktiskt kan göra i journalsystemet (exempelvis utfärda recept, skriva remisser etc.).

Tidigare granskning av Karolinska Universitetssjukhusets behörighetsstyrning
Datainspektionen har tidigare genomfört en tillsyn avseende Karolinska Universitetssjukhusets behörighetsstyrning m.m. Av Datainspektionens beslut med diarienummer 920-2012, meddelat den 26 augusti 2013, framgår att Karolinska Universitetssjukhuset bl.a. förelades att genomföra en behovs- och riskanalys som underlag för tilldelning av behörigheter i TakeCare. Med

anledning av beslutet inkom Karolinska Universitetssjukhuset med ett skriftligt svar den 18 december 2013. Av svaret framgår bl.a. att Karolinska Universitetssjukhuset hade inlett ett arbete med att ta fram en åtgärdsplan och en behovs- och riskanalys.

Vad som framkommit i ärendet

Karolinska Universitetssjukhuset har i huvudsak uppgett följande.

Personuppgiftsansvarig
Karolinska Universitetssjukhuset utgör en egen myndighet inom Region Stockholm. Det är styrelsen för Karolinska Universitetssjukhuset som är personuppgiftsansvarig för den behandling av personuppgifter som Karolinska Universitetssjukhuset utför i huvudjournalsystemet TakeCare.

Organisation
Vården på Karolinska Universitetssjukhuset är organiserad utifrån medicinska temaområden och ett antal funktioner som samlar kompetenser. Vårdavdelningar, mottagningar och dagvård är organiserade efter teman. Varje tema är indelat i ett antal patientområden, som samlar likartade patientflöden. Funktion är ett kompetensområde som löper tvärs genom teman. En funktion bistår med kompetenser och resurser, som används i många olika patientgrupper och därmed i flera teman. Det finns en patientområdeschef respektive en funktionsområdeschef för varje område.

Journalsystem
Karolinska Universitetssjukhuset använder TakeCare som huvudjournalsystem, och deltar i TakeCares system för sammanhållen journalföring.

Det är Karolinska Universitetssjukhuset som förvaltar TakeCare, och som har tecknat avtalet med leverantören. Karolinska Universitetssjukhuset har därmed ett stort antal personuppgiftsbiträdes- och underbiträdesavtal med andra vårdgivare.

Det finns både en regional och en lokal organisation för TakeCare. Den regionala organisationen utgörs av en förvaltningsgrupp (styrgrupp), som förutom Karolinska Universitetssjukhuset består av representanter för sex andra vårdgivare.

Användare och patienter
Karolinska Universitetssjukhuset har nästan 16 000 anställda totalt. Antalet användare i journalsystemet TakeCare som är anställda på Karolinska Universitetssjukhuset är 12 285 stycken, varav 1 328 stycken användare är inaktiva. Vid inspektionstillfället fanns det således 10 957 aktiva användare. Ett användarkonto inaktiveras automatiskt om ingen inloggning skett på 60 dagar.

Journalsystemet TakeCare innehåller journaler för cirka 3 miljoner patienter. Av dessa är 1 970 000 patientjournaler registrerade på, och de facto patienter hos, Karolinska Universitetssjukhuset.

Den sammanhållna journalföringen i TakeCare omfattar ca 200-400 vårdgivare. Det är idag möjligt att söka på samtliga personnummer som finns i TakeCare. Det förs dock diskussioner regionalt om att i vissa fall begränsa möjligheten att söka information till ett begränsat antal patienter, till exempel patienter på ett visst boende.

Inre sekretess

Behovs- och riskanalys
Karolinska Universitetssjukhuset kan inte inkomma med någon utförd behovs- och riskanalys för TakeCare. Det är respektive patientområdes- och funktionsområdeschef som ska genomföra och dokumentera behovs- och riskanalyser innan tilldelning av behörigheter. Det utreds dock regelmässigt vilka behov som finns och vilka behörigheter anställda ska tilldelas, exempelvis vid nyanställningar. Den mall för behovs- och riskanalyser som finns i Karolinska Universitetssjukhusets riktlinjer ifylls dock inte regelmässigt.

Karolinska Universitetssjukhuset kan inte svara på om arbetet som inleddes efter Datainspektionens tidigare tillsynsbeslut från den 26 augusti 2013 resulterade i en behovs- och riskanalys för TakeCare.

Efter inspektionen har Karolinska Universitetssjukhuset påbörjat ett arbete för att säkerställa att behovs- och riskanalyser genomförs i hela organisationen. Bland annat har en behovs- och riskanalys genomförts för funktionen Perioperativ Medicin och Intensivvård i enlighet med Karolinska Universitetssjukhusets riktlinjer.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Det finns cirka 40 behörighetsprofiler i TakeCare som innehåller funktioner som till exempel ”läsa recept”. Av dessa är 26 stycken så kallade läsa-funktioner. Det finns bland annat två behörighetsprofiler för sjuksköterskor, där det som skiljer profilerna åt är att den ena har automatiserad inloggning. Det innebär att inloggning sker automatiskt på den vårdenhet man tillhör för den ena behörighetsprofilen, men inte för den andra. Även för läkare finns det två behörighetsprofiler. Det som skiljer profilerna åt är att den ena har tillgång till en så kallad akutliggare. Som användare kan man ha flera olika behörighetsprofiler, dock högst fem. Till exempel kan en medicinkandidat ha blivit tilldelad behörigheter från flera olika enheter. Personalen bockar i sådana fall själva i journalfiltret i TakeCare, vilket innebär att de gör ett aktivt val för att ta del av patientens information på olika enheter. Om en användare bockar i valet ”alla enheter” så behövs det inget ytterligare aktivt val för att ta del av information om patienten från alla enheter. Även om det finns olika behörighetsprofiler, så uppger Karolinska att användarna ”har tillgång till alla patienter i TakeCare”.

Alla konton är individuella, det vill säga det finns inget konto som flera användare kan använda sig av (gruppkonto).

I styrdokumentet ”Beslut om behörighetstilldelning” från 2015 (senast uppdaterad den 23 oktober 2018)[2] ges en allmän beskrivning av regelverket och förutsättningarna för att tilldela behörigheter. Det innehåller också en beskrivning av ett tillvägagångssätt för att göra en behovs- och riskanalys, som utgår från användarens behov av att ha tillgång till personuppgifter om patienter i sitt arbete och avser tilldelning av behörighetsprofil. I riktlinjen erinras vidare om vissa relevanta frågeställningar. Det anges också att en del av exemplen inte matchar med de behörighetsprofiler som står till buds.

Efter inspektionen utförde Karolinska Universitetssjukhuset en behovs- och riskanalys för funktionen Perioperativ Medicin och Intensivvård. I denna anges att de risker som ska beaktas är sådana som uppstår om medarbetare inom verksamheten inte har tillgång till relevant information, samt risker relaterade till för bred eller generös tillgång till patientinformation.

[2] Riktlinjen ”Tilldelning av behörigheter” är framtagen av jurister och fastställd av chefsläkaren inom området kvalitet och patientsäkerhet.

Åtkomst till Stockholms läns sjukvårdsområdes personuppgifter om patienter
Vid inspektionen framkom att användare vid Karolinska Universitetssjukhuset har åtkomst till uppgifter om patienter inom Stockholms läns sjukvårdsområde (SLSO). Enligt Karolinska Universitetssjukhuset beror detta på att Karolinska Universitetssjukhuset och SLSO anges som ”en och samma” vårdenhet i TakeCare. Det innebär att användare vid Karolinska Universitetssjukhuset tekniskt sett har åtkomst även till uppgifter om patienter vid SLSO inom den inre sekretessen, och vice versa.

Vad gäller bakgrunden och motiven till att Karolinska Universitetssjukhuset och SLSO anges som en vårdenhet i TakeCare, har Karolinska Universitetssjukhuset hänvisat till ett verkställighetsbeslut daterat 2010-01 och ett styrelsemötesprotokoll. Av protokollet framgår att landstingsdirektören i verkställighetsbeslutet har slagit fast att Stockholms läns landstings (SLL) förvaltningar som bedriver hälso- och sjukvård tillhör vårdgivaren SLL och att detta innebär att Karolinska Universitetssjukhuset och SLSO, tills vidare, ska ligga kvar på oförändrat sätt som en och samma vårdgivare i TakeCare.

Sammanhållen journalföring

Behovs- och riskanalys
Det har inte utförts någon behovs- och riskanalys innan personalen har medgetts åtkomst till andra vårdgivares vårddokumentation inom ramen för sammanhållen journalföring.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Användare vid Karolinska Universitetssjukhuset har åtkomst till andra vårdgivares uppgifter om patienter i TakeCare inom ramen för sammanhållen journalföring. Åtkomst bereds utifrån patient, och kräver patientens samtycke. När man söker på en patient visas de vårdgivare som patienten tidigare sökt vård hos. Detta ger en indikation om att det kan finnas information om patienten hos en annan vårdgivare. Informationen kan vara viktig vid till exempel läkemedelsförskrivning. Genom att göra ett aktivt val och klicka in sig på en viss enhet kan man få åtkomst till informationen.

Det finns ett beslut från Region Stockholm om att varje vårdgivare som väljer att använda sig av journalsystemet TakeCare även måste ingå i sammanhållen journalföring.

Karolinska Universitetssjukhuset har ett styrdokument ”Åtkomst till patientjournal, riktlinje”, som gäller från 17 augusti 2018[3]. Riktlinjen innehåller en allmän beskrivning av regelverket och i den anges förutsättningarna för att ta del av vårddokumentationen i TakeCare i vissa situationer.

Tekniska begränsningar i TakeCare avseende åtkomst till personuppgifter om patienter

De tekniska begränsningar avseende användares åtkomstmöjlighet som används av Karolinska Universitetssjukhuset rör så kallade skyddade enheter i TakeCare. Det finns för närvarande sex sådana enheter, bland annat ANNOVA, SESAM-mottagningen och barnskyddsteamet.

Vad gäller de skyddade vårdenheterna är det inte möjligt att begränsa behörigheter på individnivå, men däremot kan tillgången till journaldokumentation avseende dessa patienter avgränsas till en definierad användargrupp. De skyddade enheterna syns inte vid sammanhållen journalföring och de ingår inte heller i standardprofilrollen i journalfiltret.

Besluten om skyddade enheter har föregåtts av en bedömning utifrån såväl ett patientsäkerhets- som ett integritetsperspektiv. Skyddade vårdenheter används i dag endast i en begränsad omfattning. Detta eftersom en mer omfattande användning skulle medföra betydande patientsäkerhetsrisker.

Karolinska Universitetssjukhuset har i ett kompletterande yttrande uppgett följande.

Tekniska begränsningar avseende enskilda befattningshavares åtkomster:
Det elektroniska journalsystemet TakeCare möjliggör begränsning av åtkomst genom att varje vårdenhet kan styra vilken information som respektive användargrupp (vanligtvis yrkesgrupp) vid enheten kan se samt vad respektive användargrupp kan göra. Vårdenheten kan vidare styra vilken information som andra användargrupper vid andra vårdenheter kan se respektive göra. Som TakeCare är konfigurerat idag möjliggörs dock endast styrning på

[3] Riktlinjen ”åtkomst till patientjournal, riktlinje” är framtagen av jurister och fastställd av chefsläkaren inom området kvalitet och patientsäkerhet.

användargruppsnivå. Någon möjlighet till teknisk begränsning för enskilda befattningshavares åtkomstmöjligheter finns inte. Detta gäller såväl inom den s.k. inre sekretessen som inom ramen för åtkomst genom sammanhållen journalföring. Beträffande sjukhusets s.k. skyddade vårdenheter går det heller inte att begränsa behörigheter på individnivå, men däremot kan tillgången till journaldokumentationen avseende dessa patienter avgränsas till en definierad användargrupp.

Möjligheten för en vårdgivare att välja bort åtkomsten till de övriga vårdgivarnas patientdokumentation i TakeCare
Efter beslut från Region Stockholm måste varje vårdgivare som väljer att använda sig av journalsystemet TakeCare även ingå i sammanhållen journalföring. Detta innebär att en vårdgivare inte kan begränsa andra vårdgivares åtkomst till den egna vårddokumentationen. Den enskilda vårdgivaren kan däremot styra sina användares tillgång till uppgifter i den sammanhållna journalföringen. Journalsystemet TakeCare erbjuder funktioner som ger vårdgivaren möjlighet att begränsa sina användares behörighet på sådant sätt att de endast har tillgång till journalanteckningar från exempelvis en särskilt angiven grupp med andra vårdgivare. För att illustrera detta har Karolinska Universitetet hänvisat till en skärmdump, som visar behörighet per vårdgivare.

Av skärmdumpen går det att utläsa att det på enhetsnivå går att styra behörigheten hos en enhets användare i förhållande till andra vårdgivares enheter genom att sätta upp dem på ”se dokument”- eller ”inte se dokument”-listorna. Av den senare listan framgår det att det går att blockera enheter hos andra vårdgivare. Det framgår dock inte att funktionen finns per vårdgivare, utan man måste blockera den aktuelle vårdgivarens alla enheter om man vill blockera en vårdgivare.

Dokumentation av åtkomsten (loggar)

Karolinska Universitetssjukhuset har förevisat olika loggar och uppgett i huvudsak följande.

Det finns två olika typer av loggar, fördjupade loggar och riktade loggar. Fördjupad logginformation kan begäras på antingen användaren (medarbetaren) eller på patienten. En riktad logginformation kan begäras av till exempel en patient.

Av en skärmdump, som visar dokumentationen i loggar, framgår att följande uppgifter registreras i loggen; patient, status, tidpunkt, användare, system, utfört serveranrop (åtgärd) och från vilken vårdenhet åtgärden utfördes.

Motivering av beslutet

Gällande regler

Dataskyddsförordningen den primära rättskällan
Dataskyddsförordningen, ofta förkortad GDPR, infördes den 25 maj 2018 och är den primära rättsliga regleringen vid behandling av personuppgifter. Detta gäller även inom hälso- och sjukvården.

De grundläggande principerna för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. En grundläggande princip är kravet på säkerhet enligt artikel 5.1 f, som anger att personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Av artikel 5.2 framgår den så kallade ansvarsskyldigheten, det vill säga att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i punkt 1 efterlevs.

Artikel 24 handlar om den personuppgiftsansvariges ansvar. Av artikel 24.1 framgår att den personuppgiftsansvarige ansvarar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Åtgärderna ska genomföras med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers fri-och rättigheter. Åtgärderna ska ses över och uppdateras vid behov.

Artikel 32 reglerar säkerheten i samband med behandlingen. Enligt punkt 1 ska den personuppgiftsansvarige och personuppgiftsbiträdet med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (...). Enligt punkt 2 ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring,

förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

I skäl 75 anges att vid bedömningen av risken för fysiska personers rättigheter och friheter ska olika faktorer beaktas. Bland annat nämns personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

Vidare följer av skäl 76 att hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

Även skälen 39 och 83 innehåller skrivningar som ger vägledning om den närmare innebörden av dataskyddsförordningens krav på säkerhet vid behandling av personuppgifter.

Dataskyddsförordningen och förhållandet till kompletterande nationella bestämmelser
Enligt artikel 5.1 a i dataskyddsförordningen ska personuppgifterna behandlas på ett lagligt sätt. För att behandlingen ska anses vara laglig krävs rättslig grund, genom att åtminstone ett av villkoren i artikel 6.1 är uppfyllda. Tillhandahållande av hälso- och sjukvård är en sådan uppgift av allmänt intresse som avses i artikel 6.1 e.

Inom hälso- och sjukvården kan även de rättsliga grunderna rättslig förpliktelse i artikel 6.1 c och myndighetsutövning enligt artikel 6.1 e aktualiseras.

När det är frågan om de rättsliga grunderna rättslig förpliktelse, allmänt intresse respektive myndighetsutövning får medlemsstaterna, enligt artikel 6.2, behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen till nationella förhållanden. Nationell rätt kan närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Men det finns inte bara en möjlighet att införa nationella regler utan också en

skyldighet; artikel 6.3 anger att den grund för behandlingen som avses i punkt 1 c och e *ska* fastställas i enlighet med unionsrätten eller medlemsstaternas nationella rätt. Den rättsliga grunden kan även innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

Av artikel 9 framgår att behandling av särskilda kategorier av personuppgifter (så kallade känsliga personuppgifter) är förbjuden. Känsliga personuppgifter är bland annat uppgifter om hälsa. I artikel 9.2 anges undantagen då känsliga personuppgifter ändå får behandlas.

Artikel 9.2 h anger att behandling av känsliga personuppgifter får ske om behandlingen är nödvändig av skäl som hör samman med bland annat tillhandahållande av hälso- och sjukvård på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda. Artikel 9.3 ställer krav på reglerad tystnadsplikt.

Det innebär att såväl de rättsliga grunderna allmänt intresse, myndighetsutövning och rättslig förpliktelse som behandling av känsliga personuppgifter med stöd av undantaget i artikel 9.2 h behöver kompletterande regler.

Kompletterande nationella bestämmelser
För svenskt vidkommande är såväl grunden för behandlingen som de särskilda villkoren för att behandla personuppgifter inom hälso- och sjukvården reglerade i patientdatalagen (2008:355), och patientdataförordningen (2008:360). I 1 kap. 4 § patientdatalagen anges att lagen kompletterar dataskyddsförordningen.

Patientdatalagens syfte är att informationshanteringen inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet. Dess syfte är även att personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Dessutom ska dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem (1 kap. 2 § patientdatalagen).

Enligt 2 kap. 6 § patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I en region och en kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

De kompletterande bestämmelserna i patientdatalagen syftar till att omhänderta både integritetsskydd och patientsäkerhet. Lagstiftaren har således genom regleringen gjort en avvägning när det gäller hur informationen ska behandlas för att uppfylla såväl kraven på patientsäkerhet som rätten till personlig integritet vid behandling av personuppgifter.

Socialstyrelsen har med stöd av patientdataförordningen utfärdat föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Föreskrifterna utgör sådana kompletterande regler, som ska tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården.

Nationella bestämmelser som kompletterar dataskyddsförordningens krav på säkerhet återfinns i 4 och 6 kap. patientdatalagen samt 3 och 4 kap. HSLF-FS 2016:40.

Krav på att göra behovs- och riskanalys
Vårdgivaren ska enligt 4 kap. 2 § HSLF-FS 2016:40 göra en behovs-och riskanalys, innan tilldelning av behörigheter i systemet sker.

Att det krävs såväl analys av behoven som riskerna framgår av förarbetena till patientdatalagen, prop. 2007/08:126 s. 148-149, enligt följande.

Behörighet för personalens elektroniska åtkomst till uppgifter om patienter ska begränsas till vad befattningshavaren behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården. Däri ligger bl.a. att behörigheter ska följas upp och förändras eller inskränkas efter hand som ändringar i den enskilde befattningshavarens arbetsuppgifter ger anledning till det. Bestämmelsen motsvarar i princip 8 § vårdregisterlagen. Syftet med bestämmelsen är att inpränta skyldigheten för den ansvariga vårdgivaren att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver. 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 allmänt kända personer,

uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier som kan kräva särskilda riskbedömningar.

Generellt sett 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.

Vidare bör uppgifter lagras i olika skikt så att mer känsliga uppgifter kräver aktiva val eller annars inte är lika enkelt åtkomliga för personalen som mindre känsliga uppgifter. När det gäller personal som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad torde det för flertalet befattningshavare räcka med tillgång till uppgifter som endast indirekt kan härledas till enskilda patienter. Elektronisk åtkomst till kodnycklar, personnummer och andra uppgifter som direkt pekar ut enskilda patienter bör på detta område kunna vara starkt begränsad till enstaka personer.

Inre sekretess

Bestämmelserna i 4 kap. patientdatalagen rör den inre sekretessen, det vill säga reglerar hur integritetsskyddet ska hanteras inom en vårdgivares verksamhet och särskilt medarbetares möjligheter att bereda sig tillgång till personuppgifter som finns elektroniskt tillgängliga i en vårdgivares organisation.

Det framgår av 4 kap. 2 § patientdatalagen att vårdgivaren ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Av 4 kap. 2 § HSLF-FS 2016:40 följer att vårdgivaren ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.

Sammanhållen journalföring

Bestämmelser i 6 kap. patientdatalagen rör sammanhållen journalföring, vilket innebär att en vårdgivare – under de villkor som anges i 2 § i samma kapitel – får ha direktåtkomst till personuppgifter som behandlas av andra

vårdgivare för ändamål som rör vårddokumentation. Tillgången till information sker genom att en vårdgivare gör de uppgifter om en patient som vårdgivaren registrerar om patienten tillgängliga för andra vårdgivare som deltar i den sammanhållna journalföringen (se prop. 2007/08:126 s. 247).

Av 6 kap. 7 § patientdatalagen följer att bestämmelserna i 4 kap. även gäller för behörighetstilldelning vid sammanhållen journalföring. Kravet på att vårdgivaren ska utföra en behovs- och riskanalys innan tilldelning av behörigheter i systemet sker, gäller även i system för sammanhållen journalföring.

Dokumentation av åtkomst (loggar)
Av 4 kap. 3 § patientdatalagen framgår att en vårdgivare ska se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och systematiskt kontrolleras.

Enligt 4 kap. 9 § HSLF-FS 2016:40 ska vårdgivaren ansvara för att

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient,
2. det av loggarna framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits,
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
4. användarens och patientens identitet framgår av loggarna.

Datainspektionens bedömning

Personuppgiftsansvariges ansvar för säkerheten

Såsom beskrivits ovan ges i Socialstyrelsens föreskrifter vårdgivaren ett ansvar för informationshanteringen inom vården, såsom exempelvis att genomföra en behovs- och riskanalys innan tilldelning av behörigheter i systemet sker. Inom den offentliga hälso- och sjukvården sammanfaller inte alltid begreppet vårdgivare med den personuppgiftsansvarige.

Av såväl de grundläggande principerna i artikel 5, som artikel 24.1 dataskyddsförordningen, framgår det att det är den personuppgiftsansvariga som ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.

Datainspektionen kan konstatera att dataskyddsförordningen i egenskap av EU-förordning är direkt tillämplig i svensk rätt och att det i förordningen anges när kompletterande reglering ska eller får införas nationellt. Det finns exempelvis utrymme att i nationellt reglera vem som är personuppgiftsansvarig enligt artikel 4 dataskyddsförordningen. Det är däremot inte möjligt att ge avvikande reglering gällande den personuppgiftsansvariges ansvar att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Det innebär att Socialstyrelsens föreskrifter som anger att det är vårdgivaren som ska vidta vissa åtgärder, inte förändrar att ansvaret att vidta lämpliga säkerhetsåtgärder vilar på den personuppgiftsansvarige enligt dataskyddsförordningen. Datainspektionen kan konstatera att Karolinska Universitetssjukhuset, i egenskap av personuppgiftsansvarig, är ansvarig för att dessa åtgärder vidtas.

Som tidigare beskrivits ställs det i artikel 24.1 i dataskyddsförordningen ett generellt krav på den personuppgiftsansvarige att vidta lämpliga tekniska och organisatoriska åtgärder. Kravet avser dels att säkerställa att behandlingen av personuppgifterna utförs i enlighet med dataskyddsförordningen, dels att den personuppgiftsansvarige ska kunna visa att behandlingen av personuppgifterna utförs i enlighet med dataskyddsförordningen.

Säkerheten i samband med behandlingen regleras mer specifikt i artikel 5.1 f och artikel 32 i dataskyddsförordningen.

I artikel 32.1 anges det att de lämpliga åtgärderna ska vara såväl tekniska som organisatoriska och de ska säkerställa en säkerhetsnivå som är lämplig i förhållande till de risker för fysiska personers rättigheter och friheter som behandlingen medför. Det krävs därför att man identifierar de möjliga riskerna för de registrerades rättigheter och friheter samt bedömer sannolikheten för att riskerna inträffar och allvarligheten om de inträffar. Vad som är lämpligt varierar inte bara i förhållande till riskerna utan även utifrån behandlingens art, omfattning, sammanhang och ändamål. Det har således betydelse vad det är för personuppgifter som behandlas, hur många uppgifter det är frågan om, hur många som behandlar uppgifterna osv.

Hälso- och sjukvården har stort behov av information i sin verksamhet. Det är därför naturligt att digitaliseringens möjligheter tillvaratas så mycket som möjligt inom vården. Sedan patientdatalagen infördes har en mycket omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarna storlek som hur många som delar information med varandra har ökat väsentligt. Denna ökning innebär samtidigt att kraven ökar på den personuppgiftsansvarige, eftersom bedömningen vad som är en lämplig säkerhet påverkas av behandlingens omfattning.

Det är dessutom fråga om känsliga personuppgifter. Uppgifterna rör också personer som befinner sig i en beroendesituation då de är i behov av vård. Det är också ofta fråga om många personuppgifter om var och en av dessa personer och uppgifterna kan över tid komma att behandlas av väldigt många personer inom vården. Detta sammantaget ställer stora krav på den personuppgiftsansvarige.

Uppgifterna som behandlas måste skyddas såväl mot aktörer utanför verksamheten som mot obefogad åtkomst inifrån verksamheten. Det framgår av artikel 32.2 att den personuppgiftsansvarige, vid bedömning av lämplig säkerhetsnivå, i synnerhet ska beakta riskerna för oavsiktlig eller olaglig förstöring, förlust eller för obehörigt röjande eller obehörig åtkomst. För att kunna veta vad som är en obehörig åtkomst måste den personuppgiftsansvarige ha klart för sig vad som är en behörig åtkomst.

Behovs- och riskanalys

I 4 kap. 2 § Socialstyrelsens föreskrifter (HSLF-FS 2016:40) som kompletterar patientdatalagen, finns det angivet att vårdgivaren ska göra en behovs-och riskanalys innan tilldelning av behörigheter i systemet sker. Det innebär att nationell rätt föreskriver krav på en lämplig organisatorisk åtgärd som *ska* vidtas innan tilldelning av behörigheter till journalsystem sker.

En behovs- och riskanalys ska dels innehålla en analys av behoven, dels en analys av de risker utifrån ett integritetsperspektiv som kan vara förknippade med en alltför vid tilldelning av behörighet till åtkomst av patientuppgifter. Såväl behoven som riskerna måste bedömas utifrån de uppgifter som behöver behandlas i verksamheten, vilka processer det är frågan om och vilka risker för den enskildes integritet som föreligger.

Bedömningarna av riskerna behöver ske utifrån organisationsnivå, där exempelvis en viss verksamhetsdel eller arbetsuppgift kan vara mer integritetskänslig än en annan, men också utifrån individnivå, om det är frågan om särskilda omständigheter som behöver beaktas, såsom exempelvis att det är frågan om skyddade personuppgifter, allmänt kända personer eller på annat sätt särskilt utsatta personer. Även storleken på systemet påverkar riskbedömningen. Av förarbetena till patientdatalagen framgår att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. (prop. 2007/08:126 s. 149). Det är således frågan om en strategisk analys på strategisk nivå, som ska ge en behörighetsstruktur som är anpassad till verksamheten och denna ska hållas uppdaterad.

Regleringen ställer sammanfattningsvis krav på att riskanalysen identifierar

- olika kategorier av uppgifter (exempelvis uppgifter om hälsa),
- kategorier av registrerade (exempelvis sårbara fysiska personer och barn), eller
- omfattningen (exempelvis antalet personuppgifter och registrerade)
- negativa konsekvenser för registrerade (exempelvis skador, betydande social eller ekonomisk nackdel, berövande av rättigheter och friheter)

och hur de påverkar risken för fysiska personers rättigheter och friheter vid behandling av personuppgifter. Det gäller såväl inom den inre sekretessen som vid sammanhållen journalföring.

Riskanalysen ska även innefatta särskilda riskbedömningar exempelvis utifrån om det förekommer skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter (prop. 2007/08:126 s. 148-149).

Riskanalysen ska också omfatta en bedömning av hur sannolik och allvarlig risken för de registrerades rättigheter och friheter är och i vart fall fastställa om det är frågan om en risk eller en hög risk (skäl 76).

Det är således genom behovs- och riskanalysen som den personuppgiftsansvarige tar reda på vem som behöver åtkomst, vilka

uppgifter åtkomstmöjligheten ska omfatta, vid vilka tidpunkter och i vilka sammanhang åtkomsten behövs, och samtidigt analyserar vilka risker för den enskildes fri- och rättigheter som behandlingen kan leda till. Resultatet ska sedan leda till de tekniska och organisatoriska åtgärder som behövs för att säkerställa att inte någon annan åtkomst än den som behovs- och riskanalysen visar är befogad ska kunna ske.

När en behovs- och riskanalys saknas inför tilldelning av behörighet i systemet, saknas grunden för att den personuppgiftsansvarige på ett lagligt sätt ska kunna tilldela sina användare en korrekt behörighet. Den personuppgiftsansvarige är ansvarig för, och ska ha kontroll över, den personuppgiftsbehandling som sker inom ramen för verksamheten. Att tilldela användare en vid åtkomst till journalsystem, utan att denna grundas på en utförd behovs- och riskanalys, innebär att den personuppgiftsansvarige inte har tillräcklig kontroll över den personuppgiftsbehandling som sker i journalsystemet och heller inte kan visa att denne har den kontroll som krävs.

När Datainspektionen har efterfrågat en behovs- och riskanalys har Karolinska Universitetssjukhuset hänvisat till styrdokumentet ”Beslut om behörighetstilldelning, riktlinje”[4] (riktlinjer om behörighetstilldelning) och uppgett att det är respektive patientområdes- och funktionsområdeschef som ska genomföra och dokumentera behovs- och riskanalyser innan tilldelning av behörigheter. Enligt Karolinska Universitetssjukhuset görs det vid tilldelning av behörigheter, exempelvis vid nyanställningar, regelmässigt en utredning av vilket behov av behörighet som den anställda har även om den mall för behovs- och riskanalyser som finns i riktlinjen inte fylls i regelmässigt. Karolinska Universitetssjukhuset kunde vid tidpunkten för inspektionen inte uppvisa någon utförd behovs- och riskanalys, men har efteråt uppgett att de påbörjat ett arbete för att säkerställa att behovs- och riskanalyser utförs i verksamheten. De har även gett in en dokumenterad ”behovs- och riskanalys” för funktionsområdet Perioperativ Medicin.

Såsom angivits ovan ska i en behovs- och riskanalys såväl behoven som riskerna bedömas utifrån de uppgifter som behöver behandlas i verksamheten, vilka processer det är frågan om och vilka risker för den enskildes integritet som föreligger på såväl organisatorisk som individuell

[4] ”Beslut om behörighetstilldelning, riktlinje” som gäller från 23 oktober 2018.

nivå. Det är således frågan om en strategisk analys på strategisk nivå, som ska ge en behörighetsstruktur som är anpassad till verksamheterna. Den bör lämpligen mynna ut i instruktioner om behörighetstilldelning men det är inte instruktionerna till den som tilldelar behörigheter som är analysen.

Vid inspektionstillfället har Karolinska Universitetssjukhuset inte kunnat förevisa någon behovs- och riskanalys. Den senare ingivna behovs- och riskanalysen avseende funktionen Perioperativ Medicin uppfyller inte dataskyddsbestämmelsernas krav på en sådan analys enligt 4 kap. 2 § HSLF-FS 2016:40, då den utgör en generell beskrivning av arbetsuppgifter i TakeCare för några specifika yrkeskategorier. Dokumentet innehåller ingen analys av vilka uppgifter medarbetarna har behov av för att kunna utföra sina arbetsuppgifter. Dokumentet innehåller ingen analys av de risker som kan vara förknippade med en alltför vid tillgänglighet avseende olika typer av personuppgifter.

Datainspektionen konstaterar vidare att det tillvägagångssätt som beskrivs i riktlinjer om behörighetstilldelning för att analysera vilken behörighet som ska tilldelas en enskild användare utgår från de befintliga behörighetsprofilerna. Dessa är skapade utifrån vad användare behöver kunna göra med uppgifterna, till exempel läsa eller skriva, och inte utifrån vilka uppgifter om patienten som den enskilde användaren behöver ha tillgång till för att kunna utföra sitt arbete.

De behovs- och riskanalyser som beskrivs i Karolinska Universitetssjukhusets riktlinjer om behörighetstilldelning är inte någon analys enligt kraven på en behovs- och riskanalys enligt dataskyddsbestämmelserna. Karolinska Universitetssjukhuset har inte heller kunnat visa att det arbete som inleddes efter den tidigare granskningen 2013 resulterade i genomförandet av en behovs- och riskanalys för TakeCare i enlighet med föreläggandet.

Datainspektionens kan således konstatera att Karolinska Universitetssjukhusets tilldelning av behörigheter inte har föregåtts av en nödvändig behovs- och riskanalys.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter

Som har redovisats ovan kan en vårdgivare ha ett berättigat intresse av att ha en omfattande behandling av uppgifter om enskildas hälsa. Oaktat detta ska

åtkomstmöjligheter till personuppgifter om patienter vara begränsade till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter.

När det gäller tilldelning av behörighet för elektronisk åtkomst enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen framgår det av förarbetena, prop. 2007/08:126 s. 148-149, bland annat att det ska finnas olika behörighetskategorier i journalsystemet och att behörigheterna ska begränsas till vad användaren behöver för att ge patienten en god och säker vård. Det framgår även att ”en mer vidsträckt eller grovmaskig behörighetstilldelning bör anses som en obefogad spridning av journaluppgifter inom en verksamhet och bör som sådan inte accepteras.”

Inom hälso- och sjukvården är det den som behöver uppgifterna i sitt arbete som kan vara behörig att få åtkomst till dem. Det gäller såväl inom en vårdgivare som mellan vårdgivare. Det är, som redan nämnts, genom behovs- och riskanalysen som den personuppgiftsansvarige tar reda på vem som behöver åtkomst, vilka uppgifter åtkomsten ska omfatta, vid vilka tidpunkter och i vilka sammanhang åtkomsten behövs, och samtidigt analyserar vilka risker för den enskildes fri- och rättigheter som behandlingen kan leda till. Resultatet ska sedan leda till de tekniska och organisatoriska åtgärder som behövs för att säkerställa att ingen tilldelning av behörighet ger vidare åtkomstmöjligheter än den som behovs- och riskanalysen visar är befogad. En viktig organisatorisk åtgärd är att ge anvisning till de som har befogenhet att tilldela behörigheter om hur detta ska gå till och vad som ska beaktas så att det, med behovs- och riskanalysen som grund, blir en korrekt behörighetstilldelning i varje enskilt fall.

Förutom Karolinska Universitetssjukhusets riktlinje för tilldelning av behörigheter finns även ett styrdokument ”Åtkomst till patientjournal, riktlinje” (riktlinjer om åtkomster), som gäller från den 17 augusti 2018.[5] Riktlinjerna ger dock endast en allmän beskrivning av regelverket och beskriver förutsättningarna för tilldelningen av behörigheter respektive för att ta del av vårddokumentationen i TakeCare i olika situationer.

Datainspektionen konstaterar att även om varje användare de facto har tilldelats en individuell behörighet, så har de tilldelade behörigheterna inte

[5] Riktlinjen ”åtkomst till patientjournal, riktlinje” är fastställd av chefläkaren inom området kvalitet och patientsäkerhet, och jurister har deltagit i framtagandet området.

begränsats på ett sätt som säkerställer att användaren inte har åtkomstmöjlighet till fler personuppgifter om patienter eller personuppgifter om fler patienter än denne behöver för att utföra sitt arbete. De tilldelade behörigheterna innebär i stället att användaren har åtkomst till i princip alla personuppgifter om patienter i TakeCare. Detta eftersom det endast finns två behörighetsprofiler för sjuksköterskor respektive läkare, och där det enda som skiljer behörighetsprofilerna åt är att den ena sjuksköterskebehörigheten har automatiserad inloggning till den vårdenhet personalen tillhör och den ena läkarbehörigheten har tillgång till en så kallad akutliggare. Den begränsning som i övrigt framkommit avseende åtkomstmöjligheter till personuppgifter i journalsystemet avser så kallade skyddade enheter.

Datainspektionen anser mot denna bakgrund att det, eftersom tilldelningen av behörigheter inte föregåtts av en nödvändig behovs- och riskanalys, inte funnits förutsättningar att begränsa tilldelade behörigheter eller funnits stöd för att avgöra vad som är befogade åtkomstmöjligheter för befattningshavare på Karolinska Universitetssjukhuset.

Att tilldelningen av behörigheter inte har föregåtts av en behovs- och riskanalys innebär att Karolinska Universitetssjukhuset inte har analyserat användarnas behov av åtkomst till uppgifterna, riskerna som denna åtkomst kan medföra och därmed inte heller identifierat vilka åtkomstmöjligheter som är befogade för användarna utifrån en sådan analys. Karolinska Universitetssjukhuset har därmed inte vidtagit lämpliga organisatoriska åtgärder, i enlighet med artikel 32 dataskyddsförordningen, för att begränsa användarnas åtkomst till personuppgifter om patienter i journalsystemet.

Detta har i sin tur inneburit att det funnits en risk för obehörig åtkomst och obefogad spridning av personuppgifter dels inom ramen för den inre sekretessen, dels inom ramen för den sammanhållna journalföringen. Antalet användare vid Karolinska Universitetssjukhuset är närmare 11 000 och TakeCare innehåller personuppgifter rörande ca 3 miljoner patienter, varav ca 2 miljoner har varit patienter på Karolinska Universitetssjukhuset.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att Karolinska Universitetssjukhuset har behandlat personuppgifter i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen genom att Karolinska Universitetssjukhuset inte har begränsat användarnas

behörigheter för åtkomst till journalsystemet TakeCare till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att Karolinska Universitetssjukhuset inte har vidtagit åtgärder för att kunna säkerställa och, i enlighet med artikel 5.2 dataskyddsförordningen, kunna visa en lämplig säkerhet för personuppgifterna.

Dokumentation av åtkomst i loggar

Datainspektionen konstaterar att det av loggarna i TakeCare framgår uppgifter om den specifika patienten, vilken användare som har öppnat journalen, åtgärder som har vidtagits, vilken journalanteckning som har öppnats, vilken tidsperiod användaren har varit inne, alla öppningar av journalen som gjorts på den patienten under den valda tidsrymden och klockslag och datum för det senaste öppnandet. Enligt Datainspektionens bedömning är detta i överensstämmelse med de krav på dokumentation av åtkomster i loggarna som uppställs i Socialstyrelsens föreskrifter.

Val av ingripande

Rättslig reglering

Om det skett en överträdelse av dataskyddsförordningen har Datainspektionen ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a - j i dataskyddsförordningen. Tillsynsmyndigheten kan bland annat förelägga den personuppgiftsansvarige att se till att behandlingen sker i enlighet med förordningen och om så krävs på ett specifikt sätt och inom en specifik period.

Av artikel 58.2 i dataskyddsförordningen följer att Datainspektionen i enlighet med artikel 83 ska påföra sanktionsavgifter utöver, eller i stället för, andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

För myndigheter får enligt artikel 83.7 i dataskyddsförordningen nationella regler ange att myndigheter kan påföras administrativa sanktionsavgifter. Enligt 6 kap. 2 § dataskyddslagen kan sanktionsavgifter beslutas för myndigheter, men till högst 5 000 000 kronor alternativt 10 000 000 kronor

beroende på om överträdelsen avser artiklar som omfattas av artikel 83.4 eller 83.5 i dataskyddsförordningen.

I artikel 83.2 anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras, men också vad som ska påverka sanktionsavgiftens storlek. Av central betydelse för bedömningen av överträdelsens allvar är dess karaktär, svårighetsgrad och varaktighet. Om det är fråga om en mindre överträdelse får tillsynsmyndigheten, enligt skäl 148 i dataskyddsförordningen, utfärda en reprimand i stället för att påföra en sanktionsavgift.

Föreläggande

Hälso- och sjukvården har, som nämnts, stort behov av information i sin verksamhet och under senare år har en mycket omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarnas storlek som hur många som delar information med varandra har ökat väsentligt. Detta ökar kraven på den personuppgiftsansvarige, eftersom bedömningen vad som är en lämplig säkerhet påverkas av behandlingens omfattning.

Inom hälso- och sjukvården innebär det ett ännu större ansvar för den personuppgiftsansvarige att skydda uppgifterna från obehörig åtkomst, bland annat genom att ha en behörighetstilldelning som är finfördelad. Det är därför väsentligt att det sker en reell analys av behoven utifrån olika verksamheter och olika befattningshavare. Lika viktigt är det att det sker en faktisk analys av de risker som utifrån ett integritetsperspektiv kan uppstå vid en alltför vid tilldelning av behörighet till åtkomst. Utifrån denna analys ska sedan den enskilde befattningshavarens åtkomst begränsas. Denna behörighet ska sedan följas upp och förändras eller inskränkas efter hand som ändringar i den enskilde befattningshavarens arbetsuppgifter ger anledning till det.

Datainspektionens tillsyn har visat att Karolinska Universitetssjukhuset inte har vidtagit lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i journalsystemet genom att Karolinska Universitetssjukhuset i egenskap av personuppgiftsansvarig inte följt de krav som ställs i patientdatalagen och Socialstyrelsens föreskrifter. Karolinska Universitetssjukhuset har därigenom underlåtit att följa kraven i artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen. Underlåtenheten omfattar

såväl den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen förelägger därför, med stöd av 58.2 d i dataskyddsförordningen, Karolinska Universitetssjukhuset att se till att erforderlig behovs- och riskanalys för journalsystemet TakeCare genomförs inom ramen för såväl den inre sekretessen som inom ramen för den sammanhållna journalföringen. Behovs- och riskanalysen ska dokumenteras. Karolinska Universitetssjukhuset ska vidare, med stöd av behovs- och riskanalysen, tilldela varje användare individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Sanktionsavgift

Datainspektionen kan konstatera att överträdelserna i grunden avser Karolinska Universitetssjukhusets skyldighet att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifter enligt dataskyddsförordningen.

I detta fall är det frågan om mycket stora uppgiftssamlingar med känsliga personuppgifter och vidsträckta behörigheter. Vårdgivaren behöver med nödvändighet ha en omfattande behandling av uppgifter om enskildas hälsa. Den får dock inte vara oinskränkt utan ska baseras på vad enskilda medarbetare behöver för att kunna utföra sina uppgifter. Datainspektionen konstaterar att det är frågan om uppgifter som omfattar direkt identifiering av den enskilde genom såväl namn, kontaktuppgifter som personnummer, uppgifter om hälsa, men att det också kan röra sig om andra privata uppgifter om exempelvis familjeförhållanden, sexualliv och livsstil. Patienten är beroende av att få vård och är därmed i en utsatt situation. Uppgifternas karaktär, omfattning och patienternas beroendeställning ger vårdgivare ett särskilt ansvar att säkerställa patienternas rätt till adekvat skydd för deras personuppgifter.

Ytterligare försvårande omständigheter är att behandlingen av patientuppgifter i huvudjournalsystemet hör till kärnan i en vårdgivares verksamhet, att behandlingen omfattar många patienter och möjligheten till åtkomst avser en stor andel av de anställda. I detta fall rör det sig om omkring 2 000 000 patienter inom ramen för den inre sekretessen och omkring ytterligare 1 000 000 patienter inom ramen för den sammanhållna

journalföringen. Det finns endast sex så kallade skyddade enheter där uppgifterna inte är åtkomliga för användarna utanför dessa enheter.

Datainspektionen kan dessutom konstatera att Karolinska Universitetssjukhuset inte följt Datainspektionens tidigare föreläggande från den 26 augusti 2013 om att genomföra en behovs- och riskanalys som underlag för tilldelning av behörigheter enligt det dåvarande kravet i 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14, vilket motsvarar nuvarande bestämmelse i 4 kap. 2 § HSLF-FS 2016:40. Detta är en försvårande omständighet, enligt artikel 83.2 e dataskyddsförordningen.

De brister som nu konstaterats har således varit kända för Karolinska Universitetssjukhuset under flera års tid vilket innebär att agerandet skett uppsåtligt och därmed bedöms som allvarligare.

Vid bestämmande av överträdelsernas allvar kan också konstateras att överträdelserna även omfattar de grundläggande principerna i artikel 5 i dataskyddsförordningen, som tillhör de kategorier av allvarligare överträdelser som kan ge en högre sanktionsavgift enligt artikel 83.5 i dataskyddsförordningen.

Dessa faktorer innebär sammantaget att överträdelserna inte är att bedöma som mindre överträdelser utan överträdelser som ska leda till en administrativ sanktionsavgift.

Datainspektionen anser att dessa överträdelser har en nära anknytning till varandra. Den bedömningen grundar sig på att behovs- och riskanalysen ska ligga till grund för tilldelningen av behörigheterna. Datainspektionen bedömer därför att dessa överträdelser har så nära anknytning till varandra att de utgör sammankopplade uppgiftsbehandlingar enligt artikel 83.3 i dataskyddsförordningen. Datainspektionen bestämmer därför en gemensam sanktionsavgift för dessa överträdelser.

Den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande. Det innebär att beloppet ska bestämmas så att den administrativa sanktionsavgiften leder till rättelse, att den ger en preventiv effekt och att den dessutom är proportionerlig i förhållande till såväl aktuella överträdelser som till tillsynsobjektets betalningsförmåga.

Det maximala beloppet för sanktionsavgiften i detta fall är 10 miljoner kronor enligt 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer Datainspektionen den administrativa sanktionsavgiften för Karolinska Universitetssjukhuset till 4 000 000 (fyra miljoner) kronor.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av it-säkerhetsspecialisten Magnus Bergström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetscheferna Katarina Tullstedt och Malin Blixt, samt juristen Maja Savic medverkat.

Lena Lindgren Schelin, 2020-12-02 (Det här är en elektronisk signatur)
Bilaga:
Hur man betalar sanktionsavgift

Kopia för kännedom till:
Dataskyddsombud

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Datainspektionen om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.