Styrelsen för Capio S:t Görans Sjukhus AB
S:t Göransgatan 141
112 81 Stockholm

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

Innehållsförteckning

Datainspektionens beslut

Datainspektionen har vid granskning den 3 april 2019 konstaterat att Capio S:t Görans Sjukhus AB 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. Capio S:t Görans Sjukhus AB inte har genomfört behovs- och riskanalyser innan tilldelning av behörigheter sker i journalsystemen Cambio Cosmic, Nationell patientöversikt och TakeCare i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) och 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 Capio S:t Görans Sjukhus AB 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.

[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).

2. Capio S:t Görans Sjukhus AB inte har begränsat användarnas behörigheter för åtkomst till journalsystemen Cambio Cosmic, Nationell patientöversikt och TakeCare till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att Capio S:t Görans Sjukhus AB 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 att Capio S:t Görans Sjukhus AB för överträdelserna av artikel 5.1 f och 5.2 samt 32.1 och 32.2 i dataskyddsförordningen ska betala en administrativ sanktionsavgift på 30 000 000 (trettio miljoner) kronor.

Datainspektionen förelägger med stöd av artikel 58.2 d dataskyddsförordningen Capio S:t Görans Sjukhus AB att genomföra och dokumentera erforderliga behovs- och riskanalyser för journalsystemen Cambio Cosmic, Nationell patientöversikt och TakeCare och att därefter, med stöd av dessa behovs- och riskanalyser, 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, i enlighet med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen, 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40.

Redogörelse för tillsynsärendet

Datainspektionen inledde tillsyn genom en skrivelse den 22 mars 2019 och har på plats den 3 april 2019 granskat Capio S:t Görans Sjukhus AB i fråga om deras beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Tillsynen har även omfattat hur Capio S:t Görans har tilldelat behörigheter för åtkomst till huvudjournalsystemet Cambio Cosmic (nedan Cosmic) samt journalsystemen Nationell patientöversikt (nedan NPÖ) och 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 journalsystemen.

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

Med anledning av vad som framkommit om Capio S:t Görans uppfattning i fråga om begränsning av läsbehörigheten för sina användare i TakeCare, ombads Capio S:t Görans att särskilt yttra sig över vad som framkommit i ett yttrande från Karolinska Universitetssjukhuset, som också använder TakeCare, där de tekniska möjligheterna rörande TakeCare beskrevs.

Vad som framkommit i ärendet

Capio S:t Görans har i huvudsak uppgett följande.

Personuppgiftsansvaret
Capio S:t Görans är vårdgivare och personuppgiftsansvarig.

Verksamheten
Capio S:t Görans är ett aktiebolag som driver akutsjukhus enligt ett vårdavtal med Region Stockholm. Capio S:t Görans har 3 084 pågående anställda. Utöver detta finns det 340 uppdragstagare, t.ex. hyrpersonal och studenter.

Capio S:t Görans ingår i Capio-koncernen som i november 2018 blev uppköpt av och numera ingår i den franska koncernen Ramsay Générale de Santé S.A.

Capio S:t Görans gör gällande att enligt det avtal, som Capio Group tecknade med Region Stockholm, avseende drift av S:t Görans Sjukhus ska bolaget Capio S:t Görans Sjukhus hanteras som en helt fristående verksamhet, skild från Capio Group/Ramsay Générale de Santé, varför omsättning för Capio Group och Ramsay Générale de Santé inte är tillämpligt för Capio S:t Görans Sjukhus.

Journalsystem
Capio S:t Görans använder sedan 2005 Cosmic som huvudjournalsystem inom ramen för den inre sekretessen samt för sammanhållen journalföring inom Capio-koncernen. Utöver detta använder Capio S:t Görans NPÖ och TakeCare för sammanhållen journalföring.

I journalsystemet Cosmic finns det personuppgifter om 492 264 unika patienter. Cosmic har 2 764 aktiva användare. Capio S:t Görans ingår i journalsystemet TakeCare tillsammans med ett stort antal andra vårdgivare. I TakeCare finns det uppgifter om cirka 3 miljoner unika patienter registrerade. Det är 606 personer vid Capio S:t Görans som har åtkomst till journalsystemet TakeCare.

Inre sekretess

Behovs- och riskanalys
Capio S:t Görans har i huvudsak uppgett följande.

Capio S:t Görans har uppgett att de tidigare har genomfört en behovs- och riskanalys. Den finns dock inte bevarad. Mot bakgrund av denna behovs- och riskanalys tog Capio S:t Görans fram riktlinjer för behörighetstilldelning, som används av verksamhetscheferna vid tilldelning av behörigheter.

I samband med inspektionstillfället den 3 april 2019 uppgav Capio S:t Görans att de inte hade bestämt när det ska göras en behovs- och riskanalys, men om en ny händelse inträffar – t.ex. om det öppnas en ny klinik – då görs det en ny behovs- och riskanalys. Den 19 mars 2020 inkom Capio S:t Görans med en handling benämnd ”*Behovs- och riskanalys, behörighetsprofiler i Cosmic Klinisk personal*”, som är daterad den 14 januari 2020.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Capio S:t Görans har i huvudsak uppgett följande.

Capio S:t Görans är uppdelat i kliniker och det är verksamhetscheferna vid respektive klinik, som ansvarar för att bedöma vilken behörighet som ska tilldelas respektive medarbetare. Capio S:t Görans kräver att vårdpersonalen följer patientdatalagen vid åtkomst till patientuppgifter. Capio S:t Görans har riktlinjer för behörighetstilldelning som är utarbetade efter en behovs- och riskanalys för behörighetstilldelning enligt uppsatta profiler i Cosmic.

Capio S:t Görans ser sin verksamhet som ett ”akut basakutuppdrag”, vilket innebär att inflödet av patienter och de uppgifter som ska utföras huvudsakligen kommer från akutmottagningen. För att akutflödet och akutsjukhusuppdraget ska kunna genomföras behövs breda tilldelningar av behörigheter. Capio S:t Görans framhåller att de har en omfattande verksamhet inom akutsjukvård, med cirka 100 000 akutbesök per år. Detta innebär att det är väldigt låg andel i förväg planerad vård på sjukhuset.

I dessa riktlinjer anges att de är sjukhusövergripande och utgör ram för det ansvar, gällande tilldelning av åtkomst och behörighet för journaluppgifter. I riktlinjerna anges att med begreppet *behörighet* avses den tekniska möjligheten att ta del av uppgifter, dvs. vad en medarbetare kan göra, inte vad medarbetaren får göra i ett enskilt fall. Av riktlinjerna framgår att Capio S:t Görans har gjort bedömningen att inom den inre sekretessen har som regel samtliga medarbetare i patientnära arbete på sjukhusets kliniker ett generellt behov av åtkomst och därmed behörighet till dessa enheters samlade dokumentation. Tillgång till information utanför respektive verksamhetsområde kräver aktiva val i systemet. Patienter med ökat behov av integritetsskydd har möjlighet till sekretess även mellan de traditionella klinikerna genom att begära en spärr. Denna spärr är dock möjlig att bryta. En spärr får dock, enligt riktlinjerna, inte läggas mellan kliniker som tillsammans deltar i en gemensam vårdprocess, eller på sådan information som skall finnas tillgänglig i samtliga vårdprocesser på sjukhuset.

I riktlinjerna anges att med begreppet *tillåten åtkomst* avses frågan om när det är tillåtet att ta del av journaluppgifter, vilket huvudsakligen beror på medarbetarens behov i det enskilda fallet och riktlinjerna anger ett antal exempel på situationer där åtkomst är tillåten. Riktlinjerna innehåller således instruktioner som begränsar vad medarbetarna får göra inom det utrymme för åtkomst som de har tilldelats enligt ovanstående stycke, dvs. det utrymme som är tekniskt möjligt att tillgå inom ”*behörigheten*”. Enligt dessa instruktioner krävs det att en medarbetare deltar i vården av en patient för att det ska vara tillåtet att ta del av personuppgifter om denne. Utöver detta är åtkomst tillåten vid systematiskt kvalitetsarbete på uppdrag av verksamhetschef.

Capio S:t Görans har även tagit fram rutiner för tilldelning av behörighet. Av dessa framgår väsentligen likalydande bedömningar avseende den inre

sekretessen. Bedömningen är att behovet av att kunna tillgodogöra sig klinisk information om respektive patient är avgörande för att kunna bedriva en sjukvård med god kvalitet och patientsäkerhet. Utifrån detta har som regel samtliga medarbetare med kliniska uppdrag tillgång till Cosmics centrala funktioner. Tillgång till information utanför respektive verksamhetsområde kräver aktiva val i systemet. Risken att medarbetare otillbörligen har tillgång till patientuppgifter reduceras av konfiguration som kräver aktiva val samt regelbunden och systematisk logguppföljning.

Verksamhetscheferna har möjlighet att få stöd från chefläkare, dataskyddsombud samt sjukhusets chief medical information officer vid denna bedömning. Behörighetsadministratörer vid Capio S:t Görans har stor erfarenhet av behörighetsstrukturen. De gör kontroll av roll och beställd profil före tilldelning av behörigheter.

I Cosmic finns det färdiga roller för olika kategorier av medarbetare, t.ex. läkare och sjuksköterska. Därutöver finns det färdiga profiler för andra roller såsom sjuksköterskestudenter eller läkarkandidater. Capio S:t Görans framhåller att de medarbetare som deltar i patientnära arbete har ett generellt behov till samtlig dokumentation på sjukhusets kliniker. Medarbetarna kan läsa all information i Cosmic. Det finns inga begränsningar i åtkomstmöjligheter i de behörigheter som Capio S:t Görans tilldelar medarbetarna.

Aktiva val
Capio S:t Görans har uppgett att Cosmic är konfigurerat på så sätt att medarbetare först och främst får se det som de behöver för sin tjänst. Detta innebär bland annat att Cosmic initialt visar uppgifter hänförliga till den klinik där medarbetaren i fråga är verksam, den så kallade ”hemmakliniken”. Medarbetare har dock möjlighet att genom ”aktiva val” ta del av uppgifter som rör patienter vid andra kliniker. Detta innebär att information om på vilka andra vårdenheter eller i vilka andra vårdprocesser det finns uppgifter om en viss patient inte görs tillgänglig utan att den användaren har gjort ett ställningstagande till om han eller hon har rätt att ta del av denna information. Användaren kan efter ett aktivt val klicka sig vidare till all information som finns om patienten inom ramen för den inre sekretessen hos Capio S:t Görans, där användaren bland annat kan ta del av en ”totaljournal” för patienten. Då ser medarbetaren all information om patienten, frånsett den information som har belagts med en spärr.

Sammanhållen journalföring

Capio S:t Görans har i huvudsak uppgett följande.

Behovs- och riskanalys

Capio S:t Görans har uppgett att de tidigare har genomfört en behovs- och riskanalys. Den finns dock inte bevarad. Mot bakgrund av denna behovs- och riskanalys tog Capio S:t Görans fram riktlinjer för behörighetstilldelning, som används av verksamhetscheferna vid tilldelning av behörigheter.

Den 19 mars 2020 inkom Capio S:t Görans med två dokument benämnda ”*Behovs- och riskanalys, behörighetsprofiler i NPÖ*” respektive ”*Behovs- och riskanalys, läsbehörighet i TakeCare*”. Dessa dokument är daterade den 17 januari 2020.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter

Capio S:t Görans har uppgett följande om behörighetstilldelningen inom ramen för den sammanhållna journalföringen.

Capio S:t Görans kräver att vårdpersonalen följer patientdatalagen vid åtkomst till patientuppgifter, all åtkomst loggas och åtkomst följs upp genom loggkontroller.

Capio S:t Görans sjukhus agerar personuppgiftsbiträde för de andra vårdgivarna inom Capio-koncernen som använder Cosmic och personuppgiftsbiträdesavtal finns etablerade avseende tillhandahållandet av drift- och förvaltningsrelaterade tjänster. Medarbetare på Capio S:t Görans kan ta del av patientuppgifter som rör uppmärksamhetssignalen (UMS) för andra bolag inom Capio-koncernen. Uppmärksamhetssignalen visar information om varningar (läkemedel, födoämnen), observanda, smitta och behandling/tillstånd som måste uppmärksammas (ex: dialys). Enskilda patienters kontaktöversikt kan visas för användare som med särskilda val anger två olika inställningar. Då visas vårdkontaktens datum och klockslag, Medicinskt ansvarig och vårdande enhet samt vårdkontaktens status.

När det gäller de övriga journalsystemen är den normala gången att personalen först använder sig av Cosmic och därefter NPÖ. Om informationen saknas i NPÖ kan användning av TakeCare komma ifråga. Det är ett medvetet agerande från personalens sida när de tar del av uppgifter i TakeCare.

En förutsättning för att kunna ta del av uppgifter i NPÖ eller TakeCare är att medarbetaren är inloggad i Cosmic och arbetar med en specifik patient. När medarbetaren därefter aktiverar och loggar in sig i NPÖ eller TakeCare, kommer den aktuella patientens personnummer att föras över till NPÖ eller TakeCare och därigenom styra tillgången till uppgifter på så sätt att medarbetaren kan ta del av uppgifter som rör patienten i fråga.

De ovan nämnda riktlinjerna för behörighetstilldelning anger bland annat följande i fråga om sammanhållen journalföring. Behörigheter, dvs. teknisk möjlighet att ta del av uppgifter i sammanhållen journalföring, måste styras efter medarbetarnas behov av att kunna utföra sitt arbete på samma sätt som för lokala journaler. Behörighet bör erbjudas samtliga läkare i klinisk tjänst samt annan nyckelpersonal som koordinatorer och administrativ personal vilka behöver tillgång till denna typ av uppgifter för att förebygga, utreda, behandla eller planera för patienter i vårdkedjan. För att tillgång till sammanhållen journal ska vara tillåten krävs aktivt samtycke från patienten. Förutsättningen för att få fråga om samtycke är att det finns en pågående, planerad eller avslutad vårdrelation och att inhämtande av uppgifterna bidrar till patientens hälsa.

Capio S:t Görans framför att de varit föremål för Inspektionen för vård och omsorgs (IVO) tillsyn enligt patientsäkerhetslagen, som avsåg granskning av hur Capio S:t Görans säkerställer att patienter får rätt läkemedel vid inskrivning till vårdavdelning samt utskrivning till annan klinik. Denna inspektion avslutades utan kritik efter att Capio S:t Görans beskrivit redan vidtagna samt planerade åtgärder som avsåg bland annat att säkerställa tillgången till läkemedelsinformation och journalinformation hos andra vårdgivare, främst genom TakeCare och NPÖ. Capio S:t Görans framhåller att IVO belyste vikten av att medarbetare med vårduppdrag har tillräckligt omfattande behörighet för NPÖ och TakeCare samt vilka risker som skulle kunna uppstå för patientsäkerheten om läkare och koordinerande sjuksköterskor inte skulle ha tillräckligt bred behörighet.

NPÖ
I NPÖ kan framförallt läkare och sjuksköterskor ta del av samtliga tillgängliggjorda uppgifter rörande patienten. Om det finns ytterligare kategorier av personer med medarbetaruppdrag kan även dessa ges åtkomst. Det finns inte någon möjlighet för medarbetaren att söka fritt i NPÖ.

TakeCare
Behörighet till TakeCare tilldelas som regel läkare samt övriga yrkesroller som har ett särskilt uppdrag att koordinera vård mellan Capio S:t Görans och övriga vårdgivare inom Region Stockholm.

I TakeCare används funktionen ”CapioLäs”. Det är en färdig behörighetsprofil och det finns ingen möjlighet att välja någon annan behörighetsprofil, oavsett vilken titel medarbetaren har. Behörigheten innebär endast en läsbehörighet i TakeCare och det är främst läkare som tilldelas denna efter behov, men det kan även finnas behov hos andra personer. Alla medarbetare som är verksamma på akutmottagningen samt de personer som deltar i patientens senare akutflöde har exempelvis läsbehörighet i TakeCare. Dessa personer har tillgång till all information i TakeCare. Detta förutsätter dock att medarbetaren klickar på journalfilter i TakeCare, vilket medför att det går att ta del av uppgifter hos andra vårdgivare. Capio S:t Görans har åtkomst i form av läsrättigheter, genom förstahandsval, till information som tillhör Karolinska sjukhuset och SLSO inom Region Stockholm.

Capio S:t Görans framhåller att de är Sveriges största akutmottagning, räknat i patienter per dygn. Då vården inom Region Stockholm inte använder samma huvudjournalsystem används NPÖ för sammanhållen journalföring. NPÖ saknar dock ett flertal typer av informationsmängder, framförallt information om ordinerade och administrerade läkemedel, varför Capio S:t Görans på senare år även använder TakeCare som används av övriga vårdgivare i regionen. Analyser av patientsäkerhetsärenden utpekade bristen på tillgång till läkemedelsinformation som en negativ faktor. Tillgång till sammanhållen journalföring föregås alltid av ett samtycke, när det kan inhämtas, och dokumenteras i patientjournalen.

Capio S:t Görans anför vidare att läsrättigheterna i TakeCare har ett filter som primärt tillåter läsning av information som uppstått inom Stockholms läns sjukvårdsområde alternativt Karolinska sjukhuset. Valet av vårdgivare utgår från beslut om patientströmmar i regionens övergripande plan. I och med att Capio S:t Görans är ett akutsjukhus kan man inte i förväg veta vilka informationsmängder som behövs i det enskilda fallet, utan bara att informationstillgången måste vara god för att säkerställa en god och patientsäker vård. Detta innebär att lästillgången till system för sammanhållen journalföring måste vara bred. Utifrån detta gör

medarbetaren aktiva val enligt patientdatalagen för att tillgodogöra sig den information som behövs för att ta hand om en patient på bästa sätt.

Vid tillgång till TakeCare måste man vara inloggad i Cosmic på en specifik patient, men det går att rensa listan och ta del av patientuppgifter för ett annat personnummer. All åtkomst loggas och åtkomst följs upp genom loggkontroller.

Dokumentation av åtkomsten (loggar)
Capio S:t Görans har huvudsakligen uppgett följande.

I Cosmic innehåller loggarna ett flertal kategorier av uppgifter, bland annat loggdatum, loggsjukhus, patientens personnummer, loggpersonnummer, patienttabell, patientens namn, kön, sekretess, dygndel (dag, kväll eller natt), loggklinik, loggenhet, logganvändar-ID (namn på personen, titel och yrke), modul, vilken aktivitet som utförts, loggargument (informationsmängd), tidsstämpel och datum.

I TakeCare innehåller loggarna kategorierna tidpunkt och datum (när någon har varit inne), namn på den som har varit inne och patientens personnummer.

Vid inspektionstillfället den 3 april 2019 begärde Datainspektionen att Capio S:t Görans kompletterade ärendet med utskrivna loggar för Cosmic, NPÖ och TakeCare.

När Datainspektionen tog emot de utskrivna loggarna för respektive journalsystem kunde inspektionen konstatera att när det gällde loggutdraget för TakeCare framgick det inte vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits. Datainspektionen begärde att i kompletterande information från Capio S:t Görans få besked huruvida denna information är tillgänglig på annat vis.

I yttrande den 19 mars 2020 framförde Capio S:t Görans att det finns två typer av loggutdrag för TakeCare, enkel respektive fördjupad, och att det i båda former av loggutdrag redovisas vårdenhet. Capio S:t Görans bifogade loggutdrag för att styrka detta. Av det fördjupade loggutdraget för TakeCare framgår vid vilken vårdenhet åtgärderna vidtagits.

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 s.k. ansvarsskyldigheten, dvs. 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 skäl 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 6.1. c och myndighetsutövning 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 (s.k. 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.

Av 1 kap. 2 § patientdatalagen framgår att patientdatalagens syfte är att informationshanteringen inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet. Vidare ska personuppgifter 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.

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 patientsäkerhet som integritetskrav.

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, se 1 kap. 1 § patientdatalagen.

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, dvs. reglerar medarbetares möjligheter att elektroniskt och automatiskt bereda sig tillgång till personuppgifter som finns elektroniskt tillgängliga i en vårdgivares organisation (se prop. 2007/08:126 s. 141 och s. 239).

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

Bestämmelserna i 6 kap. patientdatalagen rör sammanhållen journalföring, vilket innebär att en vårdgivare – under de villkor som anges i 2 § i samma kapitel i den lagen – 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 det sammanhållna journalföringssystemet (se prop. 2007/08:126 s. 247).

Av 6 kap. 7 § patientdatalagen följer att bestämmelserna i 4 kap. 2 och 3 §§ - även gäller för behörighetstilldelning och åtkomstkontroll vid sammanhållen

journalföring. Kravet på att vårdgivaren ska utföra en behovs- och riskanalys innan tilldelning av behörigheter i systemet sker, gäller således 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
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 artiklarna 5.1 f och 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 och 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 frågan 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. 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 för åtkomst till personuppgifter om patienter. 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 fråga 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,
- 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 med utgångspunkt i behandlingens art, omfattning, sammanhang och ändamål (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 det inte sker någon annan åtkomst än den som behovs- och riskanalysen visar är befogad.

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.

Vid inspektionstillfället den 3 april 2019 efterfrågade Datainspektionen en dokumenterad behovs- och riskanalys. Capio S:t Görans uppgav att de tidigare har genomfört en behovs- och riskanalys, men att den dock inte fanns bevarad. Capio S:t Göran uppgav att de mot bakgrund av denna behovs- och riskanalys hade tagit fram riktlinjer för behörighetstilldelning, som ska användas av verksamhetscheferna vid respektive klinik när de beslutar om tilldelning av behörigheter. Capio S:t Görans har även tagit fram rutiner för tilldelning av behörighet. Capio S:t Görans har den 19 mars givit in nya dokument som anges vara behovs- och riskanalyser rörande de tre aktuella journalsystemen Cosmic, NPÖ och TakeCare.

Datainspektionen har ovan beskrivit vilka krav som gäller vid genomförandet av en behovs- och riskanalys. I en sådan ska 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 såväl på organisatorisk som på individuell nivå. Det är således frågan om en strategisk analys på strategisk nivå, som ska ge en behörighetsstruktur som är anpassad till verksamheterna.

Datainspektionen kan konstatera att vare sig riktlinjerna för tilldelning av behörighet, rutinerna för tilldelning av behörighet eller något av de tre nya dokumenten som anges vara behovs- och riskanalyser innehåller någon bedömning i fråga om vilka behov som olika befattningshavare och olika slags verksamheter behöver. En grundläggande förutsättning för att en vårdgivare ska kunna uppfylla kravet på att begränsa den elektroniska åtkomsten till personuppgifter om patienter till vad respektive befattningshavare behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården är att vårdgivaren genomför en behovs- och riskanalys. Det saknas också en analys där Capio S:t Görans beaktar negativa konsekvenser för registrerade, olika kategorier av uppgifter, kategorier av registrerade samt i vilken utsträckning omfattningen av antalet personuppgifter och registrerade påverkar risken för fysiska personers rättigheter och friheter till följd av Capio S:t Görans behandling av personuppgifter i Cosmic, NPÖ och TakeCare. Det saknas också särskilda riskbedömningar utifrån om det förekommer t.ex. skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter eller andra faktorer som kräver särskilda skyddsåtgärder. Det saknas även bedömning av hur sannolik och allvarlig risken för de registrerades rättigheter och friheter bedöms vara.

Datainspektionen kan konstatera att riktlinjerna för tilldelning av behörighet, rutinerna för tilldelning av behörighet och de tre nya dokumenten som anges vara behovs- och riskanalyser saknar en grundläggande inventering av användarnas behov av åtkomst och analys av risker, och det har heller inte gjorts någon bedömning av användarnas faktiska behov i förhållande till de integritetsrisker som personuppgiftsbehandlingen ger upphov till.

Sammanfattningsvis kan Datainspektionen konstatera att vare sig riktlinjerna för tilldelning av behörighet, rutinerna för tilldelning av behörighet eller något av de tre nya dokumenten som anges vara nya behovs- och riskanalyser uppfyller de krav som ställs på en behovs- och riskanalys och att Capio S:t Görans inte har kunnat visa att de genomfört en behovs- och riskanalys i den mening som avses i 4 kap. 2 § HSLF-FS 2016:40, vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen, enligt 4 respektive 6 kap. patientdatalagen.

Detta innebär att Capio S:t Görans inte har vidtagit lämpliga organisatoriska åtgärder i enlighet med artikel 5.1 f och artikel 31.1 och 31.2 för att kunna säkerställa och, i enlighet med artikel 5.2, kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.

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. Detta gör sig särskilt gällande inom akutsjukvården. 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, bl.a. 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.

Capio S:t Görans framhåller att deras verksamhet är ett akutsjukhus. De gör gällande att det behövs breda tilldelningar av behörigheter i och med att det är en mycket låg andel i förväg planerad vård på sjukhuset.

Datainspektionen ifrågasätter inte att medarbetare vid Capio S:t Görans behöver omfattande åtkomstmöjligheter till patienternas personuppgifter för att kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Detta innebär dock inte att det är tillåtet att utan föregående behovs- och riskanalys tilldela samtliga medarbetare med kliniska uppdrag sådana omfattade åtkomstmöjligheter. Capio S:t Görans omfattas av en skyldighet att, efter att ha genomfört behovs- och riskanalyser i den mening som avses i 4 kap. 2 § HSLF-FS 2016:40, tilldela respektive medarbetar en individuell behörighet som är begränsad till vad denne behöver för att kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

När det gäller den inre sekretessen framgår det att mer än 2 700 medarbetare vid Capio S:t Görans använder Cosmic, som innehåller uppgifter om cirka 490 000 unika patienter. Det har framkommit att Capio S:t Görans inte har begränsat användarnas behörighet för åtkomst till personuppgifter inom ramen för den inre sekretessen i journalsystemet Cosmic.

Capio S:t Görans har uppgett att behörigheterna inom den inre sekretessen till viss del begränsas av så kallade *aktiva val*. När det gäller åtkomst till uppgifter inom en vårdgivares verksamhet, så följer det av 4 kap. 4 § HSLF-FS 2016:40 att vårdgivaren ”ska ansvara för att information om på vilka andra vårdenheter eller i vilka andra vårdprocesser det finns uppgifter om en viss patient inte kan göras tillgänglig utan att den behörige användaren har gjort ett ställningstagande till om han eller hon har rätt att ta del av denna information (aktivt val). Uppgifterna får sedan inte göras tillgängliga utan att den behörige användaren gör ytterligare ett aktivt val.”

Att Capio kräver aktiva val av sina användare innebär inte att medarbetarnas åtkomstmöjligheter till personuppgifterna i systemet har begränsats på så sätt att de inte längre är tekniskt åtkomliga för användaren. Det innebär endast att användaren, för att denne ska kunna ta del av uppgifterna, måste ”klicka” sig fram i journalsystemet. Detta innebär i sin tur att alla användare som gör sådana aktiva val kan ta del av samtliga patienters uppgifter och inte enbart de uppgifter som respektive användare har ett behov att ta del av.

Datainspektionen konstaterar att patientdatalagen ställer krav på både begränsning av behörigheter och aktiva val. Funktionen aktiva val är en integritetshöjande åtgärd, men utgör inte en sådan begränsning av

behörigheter som avses i 4 kap. 2 § patientdatalagen. Av förarbetena till patientdatalagen, prop. 2007/08:126, s. 149 anges att syftet med bestämmelserna är att inpränta skyldigheten för den ansvarige vårdgivaren att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver. Eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden, behöver användarnas åtkoms till uppgifterna begränsas för att återspegla detta. Av förarbetena framgår att uppgifter dessutom behöver 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.

Datainspektionen kan med anledning av ovanstående konstatera att de aktiva valen inte är en åtkomstbegränsning enligt 4 kap. 2 § patientdatalagen, eftersom denna bestämmelse kräver att behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

4 kap. 4 § patientdatalagen ger patienter rätt att begära *spärr av vårddokumentationen*. En spärr är dock inte en sådan åtkomstbegränsning som avses i 4 kap. 2 § patientdatalagen, eftersom en spärr är något som efterfrågas av patienten själv. Det är således ett ställningstagande som inte behandlar frågan om hur vårdgivaren ska begränsa åtkomsten till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Capio S:t Görans anger att de använder systematisk logguppföljning för att reducera risken för att medarbetare otillbörligen tar del av patientuppgifter. Datainspektionen konstaterar att patientdatalagen inte lämnar något utrymme för vårdgivare att kompensera frånvaron av behovs- och riskanalys, eller en alltför bred tilldelning av behörighet till åtkomst, med en omfattande logguppföljning.

När det gäller den sammanhållna journalföringen i TakeCare framgår det att Capio S:t Görans har begränsat antalet medarbetare som har tillgång till systemet till 606 medarbetare. Capio S:t Görans har dock inte gjorts någon begränsning i fråga om vilken dokumentation som dessa medarbetare kan ta del av, så dessa medarbetare har åtkomst till alla personuppgifter som behandlas i journalsystemet TakeCare, förutom vad avser uppgifter som

finns hos skyddade enheter hos andra vårdgivare eller de uppgifter som är spärrade av patienten enligt 6 kap. patientdatalagen.

Att tilldelningen av behörigheter i Cosmic, NPÖ och TakeCare inte har föregåtts av en behovs- och riskanalys innebär att Capio S:t Görans inte har analyserat användarnas behov av åtkomst till uppgifterna, riskerna som denna åtkomst kan medföra och därmed inte heller identifierat vilken åtkomst som är befogad för användarna utifrån en sådan analys. Användarnas läsbehörigheter har således inte begränsats på så sätt som bestämmelserna i patientdatalagen kräver och Capio S:t Görans har inte, i enlighet med artikel 32 dataskyddsförordningen, använt sig av några lämpliga tekniska åtgärder för att kunna begränsa användarnas åtkomst till patienternas uppgifter i journalsystemen.

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.

Capio S:t Görans har hänvisat till den bedömning som IVO tidigare gjort i ett tillsynsärende. Capio S:t Görans framhåller att IVO belyste vikten av att medarbetare med vårduppdrag har tillräckligt omfattande behörighet för NPÖ och TakeCare samt vilka risker som skulle kunna uppstå för patientsäkerheten om läkare och koordinerande sjuksköterskor inte skulle ha tillräckligt bred behörighet.

Vad som framkommer i IVOs granskning fråntar inte Capio skyldigheten att genomföra behovs- och riskanalyser till grund för sin behörighetstilldelning.

Eftersom den analys av behov och risker som Capio S:t Görans har genomfört inte har tagit hänsyn till riskerna för fysiska personers rättigheter och friheter eller de olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter har Capio S:t Görans inte visat att läsbehörigheterna har begränsats på så sätt som dataskyddsförordningen och patientdatalagen kräver.

Sammanfattningsvis kan Datainspektionen, mot bakgrund av vad som framgår av utredningen, konstatera att Capio S:t Görans, vare sig inom den inre sekretessen i Cosmic eller den sammanhållna journalföringen i NPÖ och TakeCare, har vidtagit de lämpliga tekniska eller organisatoriska åtgärder

som de skulle ha vidtagit, för att kunna säkerställa en säkerhetsnivå som är lämplig i förhållande till risken som behandlingen medför – i synnerhet för obehörig åtkomst till personuppgifter – i journalsystemen Cosmic, NPÖ och TakeCare.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att Capio S:t Görans behandlar personuppgifter i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen genom att Capio S:t Görans inte har begränsat användarnas behörigheter för åtkomst till journalsystemen Cosmic, NPÖ och 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 Capio S:t Görans 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 åtkomsten (loggar)
Datainspektionen kan konstatera att det av loggarna i Cosmic, NPÖ och 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.

Datainspektionen konstaterar att dokumentationen av åtkomsten (loggarna) i Cosmic, NPÖ och TakeCare är i överensstämmelse med de krav som framgår av 4 kap. 9 § HSLF-FS 2016:40.

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.

I artikel 83.2 dataskyddsförordningen 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 uppgiftssamlingarna 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 stort ansvar för den personuppgiftsansvarige att skydda uppgifterna från obehörig åtkomst, bland annat genom att ha en behörighetstilldelning som är än mer 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 Capio S:t Görans inte har vidtagit lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i journalsystemen Cosmic, NPÖ och TakeCare genom att inte följa de krav som ställs i patientdatalagen och Socialstyrelsens föreskrifter och därigenom inte uppfyller kraven i artikel 5.1 f samt 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 artikel 58.2 d dataskyddsförordningen Capio S:t Görans att genomföra och dokumentera erforderliga behovs- och riskanalyser för journalsystemen Cosmic, NPÖ och TakeCare inom ramen för såväl den inre sekretessen som inom ramen för den sammanhållna journalföringen. Capio S:t Görans ska vidare, med stöd av dessa behovs- och riskanalyser, 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 Capio S:t Görans skyldighet att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifter enligt dataskyddsförordningen.

I detta fall är det frågan om 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 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 uppgifter om patienter 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. Inom ramen för den inre sekretessen har mer än 2 700 medarbetare åtkomst till uppgifter som rör närmare 490 000 patienter. Utöver det har mer än 600 medarbetare, inom

ramen för den sammanhållna journalföringen, åtkomstmöjligheten till uppgifter rörande cirka 3 miljoner patienter i TakeCare.

Vid bestämmande av överträdelsernas allvar kan också konstateras att överträdelserna även omfattar de grundläggande principerna i artikel 5 i dataskyddsförordningen, som tillhör de allvarligare överträdelserna 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.

Det maximala beloppet för sanktionsavgiften i detta fall är 20 000 000 EUR eller, om det gäller ett företag, upp till 4 % av den totala globala årsomsättningen under föregående år, beroende på vilket värde som är högst, enligt artikel 83.5 dataskyddsförordningen.

Begreppet ”ett företag” omfattar alla företag som bedriver en ekonomisk verksamhet, oavsett enhetens juridiska status eller det sätt på vilket det finansieras. Ett företag kan därför bestå av ett enskilt företag i meningen en juridisk person, men också av flera fysiska personer eller företag. Således finns det situationer där en hel grupp behandlas som ett företag och dess totala årliga omsättning ska användas för att beräkna beloppet för en överträdelse av dataskyddsförordningen från ett av dess företag.

Av beaktandeskäl 150 i dataskyddsförordningen framgår bland annat följande. […]Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget[…]

Detta innebär att bedömningen av vad som utgör ett företag ska utgå från konkurrensrättens definitioner. Reglerna för koncernansvar i EU:s konkurrenslagstiftning kretsar kring begreppet ekonomisk enhet. Ett moderbolag och ett dotterbolag betraktas som en del av samma ekonomiska enhet när moderbolaget utövar ett avgörande inflytande över dotterbolaget. Det avgörande inflytandet (dvs. kontrollen) kan antingen uppnås genom ägande eller genom avtal. Av rättspraxis framgår att ett hundraprocentigt ägande innebär en presumtion för att kontroll ska anses föreligga[2].

Capio S:t Görans gör gällande att enligt det vårdavtal, som Capio Group tecknade med Region Stockholm, avseende drift av S:t Görans Sjukhus ska bolaget Capio S:t Görans Sjukhus anses vara en helt fristående verksamhet, skild från Capio Group/Ramsay Générale de Santé, varför omsättning för Capio Group och Ramsay Générale de Santé inte är tillämpligt för Capio S:t Görans Sjukhus.

De omständigheter Capio S:t Görans anger till stöd för detta är följande. Capio S:t Görans framhåller att det aktuella vårdavtalet innebär att Capio S:t Görans inte kan ingå avtal med annat bolag i Capiokoncernen som föranleder förpliktelser för Capio S:t Görans utan att det på förhand skriftligen godkänts av Region Stockholm. Region Stockholm har en optionsrätt att återförvärva samtliga aktier i Capio S:t Görans vid vårdavtalets utgång. Capio S:t Görans verksamhetsinnehåll, patientvolymer och ersättningsnivåer uteslutande bestäms av Region Stockholm. Capio S:t Görans ägarbolag inte har några möjligheter att påverka dessa förhållanden genom egna beslut. Capio S:t Görans är skilt från samtliga andra bolag i Capiokoncernen i fråga om IT-infrastruktur.

Datainspektionen bedömer att den avtalsklausul som Capio S:t Görans åberopar förvisso indikerar att Capio S:t Görans ska hållas separat och inte sammanblandas med koncernens övriga tillgångar. Datainspektionen bedömer dock att detta inte visar att Ramsay Générale de Santé och Capio S:t Görans inte utgör en ekonomisk enhet på så sätt som avses enligt artiklarna 101 och 102 i EUF-fördraget. Datainspektionen utgår således från den ovan nämnda presumtionen och utgår från koncernen Ramsay Générale de Santé:s årsomsättning.

[2] Mål T-419/14 The Goldman Sachs Group, Inc. mot Europeiska kommissionen

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.

Capio S:t Görans betalningsförmåga påverkas av verksamhetens storlek. Datainspektionen har beräknat denna utifrån den totala globala omsättningen under föregående budgetår för Ramsay-koncernen som Capio S:t Görans ingår i. Enligt koncernens årsredovisning för räkenskapsåret 2018/2019 uppgick årsomsättningen till 3 401 miljoner euro. Datainspektionen kan konstatera att den maximala sanktionsavgiften som kan utgå är 136 miljoner euro.

Utifrån överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer Datainspektionen den administrativa sanktionsavgiften Capio S:t Görans till 30 000 000 (trettio miljoner) kronor.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av it-säkerhetsspecialisten Magnus Bergström. Vid den slutliga handläggningen har chefsjuristen Hans-Olof Lindblom och enhetschefen Katarina Tullstedt medverkat.

Lena Lindgren Schelin, 2020-12-02 (Det här är en elektronisk signatur)

Bilaga: Bilaga 1 – Hur man betalar sanktionsavgift

Kopia till: Dataskyddsombudet

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 ni fick del av beslutet. 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.