Region Östergötland
Att: Regionstyrelsen
581 91 Linköping

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

Innehåll

Datainspektionens beslut

Datainspektionen har vid granskning den 10 april 2019 konstaterat att Regionstyrelsen, Region Östergötland (Regionstyrelsen) behandlar personuppgifter i strid med artikel 5.1 f och 5.2, artikel 24.1 och artikel 32.1 och 32.2 i dataskyddsförordningen[1] genom att

1. Regionstyrelsen inte har genomfört behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemet Cosmic, 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 Hälso- och sjukvårdsnämnden 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. Regionstyrelsen inte begränsar användarnas behörigheter för åtkomst till journalsystemet Cosmic 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 Regionstyrelsen 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 och 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning att Regionstyrelsen, för överträdelse av artikel 5.1 f och 5.2 samt artikel 32.1 och 32.2 i dataskyddsförordningen, ska betala en administrativ sanktionsavgift på 2 500 000 (två miljoner femhundra tusen) kronor.

Datainspektionen förelägger enligt artikel 58.2 d i dataskyddsförordningen Regionstyrelsen att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemet Cosmic och att därefter, med stöd av behovs- och riskanalysen, tilldela varje användare individuell behörighet för åtkomst till personuppgifter till enbart vad som behövs för att den enskilde ska kunna

[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).

fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med artikel 5.1 f och artikel 24.1 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 10 april 2019 granskat om Regionstyrelsens beslut om tilldelning av behörigheter, som rör Universitetssjukhuset i Linköping, har föregåtts av en behovs- och riskanalys. Granskningen har även omfattat hur Regionstyrelsen tilldelat behörigheter för åtkomst till huvudjournalsystemet Cambio Cosmic (Cosmic), 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, dvs. vilken vårddokumentation användaren faktiskt kan ta del av och läsa. Granskningen omfattar inte vilka funktioner som ingår i behörigheten, dvs. vad användaren faktiskt kan göra i journalsystemet (exempelvis signera, utfärda recept, skriva remisser etc.).

Tidigare granskning av behovs- och riskanalyser
Datainspektionen har tidigare genomfört en tillsyn avseende om Landstingsstyrelsen hade genomfört en dokumenterad behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Av Datainspektionens beslut med diarienummer 1600-2013, meddelat den 27 mars 2015, framgår att Landstingsstyrelsen inte uppfyllde kravet på att genomföra en behovs- och riskanalys enligt nämnda föreskrifter. Landstingsstyrelsen förelades därför att genomföra en dokumenterad behovs- och riskanalys för huvudjournalsystemet.

Vad som framkommit i ärendet

Regionstyrelsen har i huvudsak uppgett följande.

Personuppgiftsansvarig
Regionstyrelsen är vårdgivare och personuppgiftsansvarig.

Journalsystem
Region Östergötland (regionen) använder Cosmic som huvudjournalsystem inom ramen för den inre sekretessen och deltar i Cosmics system för sammanhållen journalföring tillsammans med 20 privata vårdgivare. Cosmic består av ett antal moduler. Införandet av Cosmic påbörjades under februari 2007 och slutfördes i december 2008, och de privata vårdgivarna och sammanhållen journalföring lades till 2009. Cambio är leverantör av detta system.

Regionen ingår i en kundgrupp, ”Kundgrupp Cosmic”, som består av åtta regioner och en privat vårdgivare. Dessa vårdgivare samarbetar när det gäller utveckling och kravställning gentemot leverantören Cambio, men var och en av dessa vårdgivare sköter driften av sin egen installation av systemet.

Antalet patienter och anställda
Den 8 april 2019 fanns det 838 093 unika patienter registrerade i Cosmic. Siffran är en totalsumma för samtliga patienter som finns i Cosmic, dvs. den inkluderar även de patienter som ingår i systemet för sammanhållen journalföring.

Under maj 2019 fanns det 516 416 unika patienter registrerade i Cosmic vid Universitetssjukhuset i Linköping. Den 7 september 2019 hade totalt 7 014 befattningshavare vid Universitetssjukhuset i Linköping åtkomst till Cosmic.

Inre sekretess

Behovs- och riskanalys
Regionstyrelsen har i huvudsak uppgett följande.

Det finns tre dokument som är hänförliga till behovs- och riskanalys; *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys* (instruktioner och en övergripande riktlinje), *Behovs- och riskanalys av behörigheter* (dokumentet avser tilldelningen av behörigheter för medarbetare inom 12 centrum) och *Styrning av behörigheter* (riktlinjer för

tilldelning, förändring, borttagning och uppföljning av behörigheter i regionens IT-stöd).

Från 2013 fram till 2015 fördes diskussioner hos regionen avseende behovs- och riskanalys. En skriftlig behovs- och riskanalys fanns per centrum från hösten 2015, vilken senare mynnade ut i den gemensamma behovs- och riskanalysen för alla centrum 2018. Dokumentet *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys* fastställdes genom beslut av Regionstyrelsen.

Syftet med dokumentet *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys* är att ge tydliga instruktioner till de som har ansvar inom respektive verksamhet så att bedömningarna inför behörighetstilldelningar sker enhetligt inom Region Östergötland. Det framkommer bl.a. av dokumentet att ”vårdgivaren, dvs. Regionstyrelsen, ansvarar för att varje användare tilldelas en individuell behörighet för åtkomst till patientuppgifter och att tilldelningen ska föregås av en behov- och riskanalys. Varje verksamhetschef eller motsvarande ska utifrån detta dokument och riktlinjen ”Styrning av behörigheter” genomföra en behovs- och riskanalys för användarna inom den egna enheten och för de som arbetar på uppdrag av verksamhetschefen. För att behörigheterna i varje enskild verksamhet varken ska bli för vida eller för snäva behöver verksamhetschefen ha möjlighet att utforma behörigheterna så att de verkligen motsvarar den enskilda verksamhetens förutsättningar”.

När det gäller riskanalysen framgår följande. ”Behovs- och riskanalysen ska identifiera och förteckna verksamhetens uppdrag, de olika yrkeskategorierna som finns i verksamheten samt de uppdrag som medarbetaren har i verksamheten. Risker som uppstår om medarbetaren inom verksamheten inte har tillgång till relevant patientinformation ska identifieras och förtecknas i behovs- och riskanalysen och värderas enligt gällande rutin för riskanalys. Vidare ska även risker relaterade till för bred eller generös tillgång till vårdinformation identifieras och förtecknas i behovs- och riskanalysen på samma sätt som risker enligt ovan. Behovs- och riskanalysen används för att se till att de behörighetsprofiler som finns för respektive verksamhet är korrekta.”

Vidare uppges att ”det finns patientuppgifter och patientgrupper inom regionen som är särskilt skyddsvärda t.ex. personer med skyddade personuppgifter. Det kan inom respektive vårdenhet eller motsvarande finnas ytterligare patientuppgifter och patientgrupper som är särskilt

skyddsvärda t.ex. utifrån vård/diagnos. Riskerna med åtkomst till dessa uppgifter behöver belysas i behovs- och riskanalysen".

Dokumentet *Behovs- och riskanalys av behörigheter* är giltigt från och med april 2019, och är version sex av detta dokument. I dokumentet finns bl.a. information om att samtliga behörigheter ska bygga på en behovs- och riskanalys där behörigheterna begränsas till vad som är nödvändigt för att medarbetarna ska kunna utföra sina arbetsuppgifter. Detta för att undvika en otillbörlig informationsspridning men också för att medarbetarna ska ha rätt förutsättningar för att kunna genomföra sitt arbete. Det framgår även att en avvägning av behov och risk ska ske och att en för vid behörighet kan leda till:

- en obefogad spridning av patientuppgifter/personuppgifter
- en ekonomisk risk
- förlorad riktighet i form av felaktig radering eller förändrad information, samt att
- en för snäv behörighet kan innebära att användaren inte kan utföra sina arbetsuppgifter.

Följande nämns specifikt om Cosmic. "För behörigheter i Cosmic har behovet grupperats i användar- och yrkesroller. Risken för obehörig informationsspridning har för varje roll vägts upp av behovet av information".

I dokumentet *Styrning av behörigheter* finns riktlinjer för styrning av behörigheter till regionens IT-stöd.

Under inspektionen uppgav Regionstyrelsen att det inte fanns någon dokumenterad behovs- och riskanalys, utan ansåg att den ifyllda blanketten som rör beställning av behörigheter är resultatet av en behovs- och riskanalys. Regionstyrelsen har därefter kommit in med en synpunkt över detta och anfört att dokumentet *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys* utgör ett "underlag för den riskanalys som är genomförd. Ifylld blankett som rör beställning av behörigheter baseras på det uppdrag som den anställde har och behörigheten ges utifrån behov och risk".

Tidigare granskning av behovs- och riskanalyser
För att visa hur Regionstyrelsen har agerat efter Datainspektionens tidigare beslut mot Landstingsstyrelsen presenterade Regionstyrelsen dokumentet

Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys, beslutat den 26 september 2016.

Behörighetstilldelning för åtkomst till personuppgifter
Regionstyrelsen har i huvudsak uppgett följande.

Samtliga tilldelade behörigheter till Cosmic är individuella och det finns inga grupp-konton.

Utifrån en befattningshavares uppdrag samt aktuell vårdenhet och vårdgivare görs en beställning av behörighet av den lokala administratören på uppdrag av verksamhetschefen. Verksamhetschefens uppgifter i detta avseende kan delegeras till vårdenhetschefen, men verksamhetschefen har det yttersta ansvaret för beställningen. Denna ges till de som arbetar på supporten och administreras centralt.

Det finns olika behörighetsprofiler för olika roller. En behörighetsprofil består av ett antal rättighetsnycklar som sätts per modul i Cosmic. Med rättighetsnycklar menas ”nycklar i systemet” som kan användas för att slå på eller av en behörighetsprofil eller att fördela en specifik behörighetsprofil. Behörighetsprofilerna kopplas i sin tur till olika yrkesroller, som utgår från befattningshavarens uppdrag.

En användares behörighetsprofil avgör vilka åtkomstmöjligheter och vilka befogenheter denne har i Cosmic. Det går inte att styra om exempelvis en läkare kan se en viss rad i Cosmic, detta sker genom tilldelningen av rättighetsnycklar. Rättighetsnycklarna innebär att det finns en teknisk funktion för att detaljstyra individuella behörigheter, men det är generellt sett så att olika yrkesroller tilldelas behörighetsprofiler utifrån en matris. Matrisen är rådgivande och ger förslag på olika behörighetsprofiler i Cosmic som kan vara lämpliga för olika yrkesroller. Av matrisen framgår att det finns 22 behörighetsprofiler utifrån användarroll och yrkesroll. Två av dessa behörighetsprofiler benämns ”valfri yrkesroll”. Det framgår vidare av matrisen att i praktiken samtliga behörighetsprofiler, frånsett ”Valfri yrkesroll” i två avseenden, bör tilldelas åtkomst till Cosmicmodulerna ”Vårddokumentation – Bas”, ”Läkemedel – Bas”, ”Remiss – Bas” och ”Vårdadministration – Bas”.

Grundläggande behörighetsprofiler i Cosmic

- Vårddokumentation – Bas: ger läs- och skrivrättigheter till sju olika fönster, läsrätt i fönstret Journal, samt tillåtelse ”att läsa Vitalparametrar i Patientöversikten”.
- Remiss – Bas: ger läs- och skrivrättigheter till fem olika fönster, och omfattar även läsbehörighet för medicinsk information på remiss. Behörigheten ska ges till alla användare av Remissmodulen.
- Läkemedel – Bas: ger behörighet att öppna och läsa information i läkemedelsmodulen och det ger även behörighet att öppna och läsa information från ”gamla” läkemedel; dvs. läkemedelslistan, inskrivningsbeslut, ordinationslistan och recept.

Tilldelade behörigheter vid Universitetssjukhuset i Linköping per den 7 september 2019

- modulen Vårddokumentation: 6 221 användare
- modulen Läkemedel: 6 102 användare
- modulen Remiss: 5 848 användare
- modulen Vårdadministration: 5 956 användare

Under inspektionen uppgavs att vårdpersonal – exempelvis läkare, sjuksköterskor och undersköterskor, tilldelas behörighetsprofilen ”Vårddokumentation – Bas”, vilket innebär att de kan öppna journaler och har läsbehörighet. Det uppgavs även att det inte görs någon behovs- och riskanalys utifrån varje tilldelning av behörighetsprofil. Regionstyrelsen har därefter kommit in med synpunkter över detta och anför följande. ”Vårdpersonal kan tilldelas behörighetsprofilen ”Vårddokumentation – Bas”, men det görs inte per automatik”. Vidare anförs att ”baserat på de riktlinjer som finns framtagna inom Region Östergötland avseende behörighetsstyrning m.m. sker en tilldelning av behörigheter baserat på behov samt en underliggande riskbedömning.”

Åtkomst till personuppgifter om patienter i Cosmic
Läkemedelslistan i Cosmic är gemensam. Det innebär att alla med behörighet har åtkomst till läkemedelslistan samt till alla uppgifter som finns där. Det finns dock möjlighet att begränsa åtkomsten till uppgifter i läkemedelslistan.

Under rubriken ”Alla anteckningar” i Cosmic finns alla journalanteckningar som har skrivits om patienten inom regionen. Vid inspektionstillfället uppgavs att informationen under ”Alla anteckningar” är åtkomlig för i princip all vårdpersonal. Regionstyrelsen har därefter kommit in med en synpunkt över detta och anför att åtkomsten till ”Alla anteckningar” kräver

att användaren har tilldelats behörighet ”läsa journalanteckningar” och att det även krävs ett aktivt val för att få upp ”Alla anteckningar”.

Begränsningar i åtkomsten till Cosmic beträffande ”Alla anteckningar” (*Aktiva val)*
När det gäller val av anteckningar i Cosmic går det till på följande sätt. Fönstret Journal öppnas och användaren hamnar först på ”Enhetens anteckningar”, som visar anteckningar från Medicinskt ansvarig enhet och dess underenheter. Vill användaren läsa anteckningar från andra enheter inom Region Östergötland eller privata vårdgivare som arbetar på uppdrag av regionen görs ett aktivt val, dvs. användaren klickar på rubriken ”Alla anteckningar”.

Följande visas under ”Alla anteckningar”:

- Vårdgivarens anteckningar.
- Vissa enheter som bedöms ha extra känslig information, dvs. sekretess runt enheten, visas som *Sekretessklassad information*.
- Anteckningar med extra känslig information visas som *Sekretessklassad information*.
- Annan vårdgivare visas som *Sekretessklassad information*.
- Privat vårdgivare visas som *Sekretessklassad information* och sekretessen bryts genom att användaren klickar på anteckningen och svarar Ja i meddelanderutan som visas. Det framgår av informationen i meddelanderutan att informationen är sekretessklassad och för att få tillgång till informationen behöver sekretessgränsen brytas. Om informationen är skriven av en annan vårdgivare behövs samtycke från patienten om det inte är nödläge. Användaren får därefter frågan – Vill du fortsätta att få tillgång till informationen Ja/Nej/Avbryt.

Reglerna kring sekretessklassad information styr hur en anteckning ska presenteras och vilken åtgärd som krävs för att få tillgång till informationen, beroende på vilken enhet som har skrivit den och vilken enhet användaren som läser är inloggad mot. Användaren bestämmer vid dokumentationen vilken sekretessklass anteckningen ska tillhöra genom att välja olika sökordsmallar. Särskilt känslig information har sekretessklass 4.1. Sekretessklass på en mall ska stå i parentes efter mallnamnet, ex Kurator (3) och Kurator (4.1). I reglerna kring sekretessklassad information anges sedan vilken åtgärd som krävs för att bryta sekretessen. I Region Östergötland används tre nivåer:

- *Ingen åtkomst med loggning*
- *Skapa journalreferens med loggning*

- *Varning med loggning*

Sekretessklassen *”Ingen åtkomst med loggning”* innebär att journalanteckningar skrivna på vissa enheter inte kan läsas i Cosmic av den egna vårdgivaren (förutom den specifika enheten som den tillhör) eller av annan vårdgivare. För att läsa anteckningar från enheter med denna typ av sekretessklassning behöver användaren få verksamhetsuppdrag till enheten, vilket beslutas av verksamhetschef. Under inspektionen uppgavs att det fanns tre enheter inom Universitetssjukhuset i Linköping som hade denna sekretessklass: LSS Linköping, BUP Traumaenheterna Linköping och Barn och ungdomspsykiatriska kliniken US. Efter inspektionen har det inkommit kompletterande uppgifter från Regionstyrelsen där det framkommer att det har skett en sänkning av sekretessklassen hos flertalet av enheterna inom BUP, men efter ett beslut från verksamhetschef har det bedömts att Trauma-enheterna fortsatt ska ha hög sekretess utan extern åtkomst.

När det har skett en sekretessänkning på en enhet som haft *Ingen åtkomst* till att få ”normal” sekretess (*Varning med loggning)* blir informationen läsbar. Om det är en klinik inom Region Östergötland som sänkt sin sekretess så kan användaren läsa dessa anteckningar via vyn *Alla anteckningar*. För annan vårdgivare innebär det att anteckningen fortfarande visas som sekretessklassad information, men om de klickar på anteckningen så får de upp informationsrutan ”Visa sekretessklassad information”, vilket kan brytas genom att klicka Ja efter att ett samtycke är inhämtat.

Sekretessklassen *Skapa journalreferens med loggning* innebär att om en användare från en annan verksamhet ska läsa anteckningen så måste denne skriva en motivering till varför de bryter sekretessen. Detta gäller oavsett om användaren arbetar hos vårdgivaren som upprättat journalanteckningen eller hos en vårdgivare som kan ta del av anteckningen inom ramen för den sammanhållna journalföringen. Om anteckningen har upprättats av en annan vårdgivare ska även samtycke inhämtas och dokumenteras innan sekretessen får brytas och anteckningen får läsas. Det är dock inte tvingande utan sekretessen kan brytas även om detta inte är gjort.

Datainspektionen har efter inspektionen mottagit kompletterande uppgifter från Regionstyrelsen rörande vilka enheter inom Universitetssjukhuset i Linköping som har sekretessklassen *Skapa journalreferens med loggning*, och det är två vårdenheter: Psykiatriska kliniken i Linköping och Psykiatripartners Barn och Ungdom.

Sekretessregeln *”Varning med loggning”* innebär att om en användare på en annan verksamhet ska läsa anteckningen krävs att användaren klickar på Ja i en meddelanderuta. Detta Ja betyder olika saker beroende på om anteckningen är skriven på enhet inom samma vårdgivare (inre sekretess) eller av annan vårdgivare (sammanhållen journalföring).

Sammanhållen journalföring

Regionstyrelsen har i huvudsak uppgett följande.

Behovs- och riskanalys
Under inspektionen uppgavs att det inte har gjorts en särskild behovs- och riskanalys inom ramen för den sammanhållna journalföringen.
Regionstyrelsen ansåg att behovs- och riskanalysen som gjorts inom ramen för den inre sekretessen även innefattade den sammanhållna journalföringen.
Regionstyrelsen har därefter kommit in med en synpunkt över detta och anför att ”dokumentet *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys* utgör ett underlag för den riskanalys som är genomförd och även avser sammanhållen journalföring.

Behörighetstilldelning
Sker på samma sätt som inom ramen för den inre sekretessen.

Åtkomst till Cosmic
Inom ramen för den sammanhållna journalföringen måste användaren först göra ett aktivt val innan användaren kan ta del av anteckningar hos andra vårdgivare. Det innebär att en dialogruta kommer upp där det står ”visa sekretessklassad data”. Om användaren klickar i denna ruta kommer anteckningarna att visas. Användaren ska ha ett samtycke från patienten dessförinnan och det samtycket ska enligt instruktioner dokumenteras av användaren i Cosmic.

Begränsningar i åtkomsten till Cosmic (*Aktiva val)*
Vissa enheter står utanför sammanhållen journalföring, antingen helt eller delvis. Det går inte att bryta sekretessen när åtgärden ”Ingen åtkomst” har använts.

Dokumentation av åtkomsten (loggar)
Regionstyrelsen har uppgett följande.

Dokumentation i åtkomstloggarna från Cosmic:

- uppgifter om patienten,
- vilken användare som har öppnat journalen (HSA-ID och användarroll),
- vilken tidsperiod någon varit inne i journalen,
- klockslag och datum för det senaste öppnandet,
- vilka åtgärder som har vidtagits,
- från vilken vårdenhet användaren har varit inne.

Motivering av beslutet

Gällande regler

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

De grundläggande principerna för att behandla 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 för 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 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 bestämmelse 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) som huvudregel 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).

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 behandlingen 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 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 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.

Enligt 4 kap. 2 § HSLF-FS 2016:40 ska vårdgivaren 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 – 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. 2 § 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
Som tidigare beskrivits ställs det i artikel 24.1 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 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 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 skrevs 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 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 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 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.

Det är således fråga 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.

Region Östergötlands process för behovs- och riskanalys
När Datainspektionen har efterfrågat en dokumenterad behovs- och riskanalys har Regionstyrelsen hänvisat till tre dokument; *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys*, *Behovs- och riskanalys av behörigheter* och *Styrning av behörigheter*. Datainspektionen kan konstatera att det finns instruktioner och riktlinjer som berör behovs- och riskanalysen på användarnivå, som till viss del talar om hur man ska gå tillväga inför utförandet av en behovs- och riskanalys på användarnivå och att en behovs- och riskanalys på användarnivå ska göras innan tilldelning av behörigheter sker i systemet. Datainspektionen kan dock vidare konstatera att informationen i dessa dokument endast på en övergripande nivå redogör för hur man ska gå tillväga inför utförandet av denna analys och att det saknas väsentlig information för att en behovs- och riskanalys ska kunna utföras på ett korrekt sätt. Det saknas t.ex. en analys över vilket behov av uppgifter olika användare har och en analys över vilka risker som finns med åtkomst till exempelvis vissa kategorier av uppgifter eller olika typer av verksamheter som innehåller känsliga uppgifter. Vidare saknas den slutliga

analys som framkommer när behovet av uppgifter viktas mot den risk som åtkomsten till uppgifterna kan medföra. Det saknas även analyser av verksamheten, processerna och ett identifierat behov av uppgifter hos olika personalkategorier som finns hos Regionstyrelsen.

Regionstyrelsen har haft möjlighet att visa upp en dokumenterad behovs- och riskanalys för Datainspektionen, men har inte kunnat göra detta - vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen. Regionstyrelsen anser att dokumentet *Bedömning av behörighetstilldelning efter utförd behovs- och riskanalys* är en behovs- och riskanalys och ”utgör ett underlag för den riskanalys som är genomförd och att ifylld blankett som rör beställning av behörigheter baseras på det uppdrag som den anställde har och behörigheten ges utifrån behov och risk vilken även avser sammanhållen journalföring”. Datainspektionen kan konstatera att detta dokument inte utgör en faktisk behovs- och riskanalys.

Behörighetstilldelning är i och för sig viktiga organisatoriska åtgärder för att säkerställa korrekt åtkomst till personuppgifter. En behovsinventering utgör ett led i arbetet med en behovs- och riskanalys men den behöver kompletteras med en bedömning av riskerna för patienternas integritet och därvid bedöma och säkerställa åtgärder för att hantera riskerna för obefogad spridning.

Datainspektionen kan med anledning av ovanstående konstatera att det saknas en dokumenterad behovs- och riskanalys som visar att Regionstyrelsen har genomfört en behovs- och riskanalys i den mening som avses i 4 kap. 2 § HSLF-FS 2016:40, dels inom ramen för den inre sekretessen, dels inom ramen för den sammanhållna journalföringen enligt 4 resp. 6 kap. patientdatalagen. De dokument som har redovisats uppfyller inte de krav som ställs på en behovs- och riskanalys. Därigenom har Regionstyrelsen inte heller kunnat visa att tilldelade behörigheter är korrekta. Detta innebär en beaktansvärd risk för obefogad åtkomst till vård- och patientuppgifter.

Den personuppgiftsansvarige är ansvarig för att följa de grundläggande principerna om uppgiftsminimering och lämplig säkerhet enligt artikel 5, 24 och 32 i dataskyddsförordningen och har att visa att behandlingen av personuppgifterna utförs i enlighet med dataskyddsförordningen. Regionstyrelsen har såsom personuppgiftsansvarig inte uppfyllt ansvarsskyldigheten enligt artikel 5.2 dataskyddsförordningen genom att kunna visa att bestämmelserna efterlevs.

Datainspektionen kan mot bakgrund av ovanstående konstatera att Regionstyrelsen vid granskning den 10 april 2019 har behandlat personuppgifter i strid med artikel 5.1 f och 5.2, artikel 24.1 och artikel 32.1 och 32.2 i dataskyddsförordningen genom att inte ha uppfyllt kravet på att genomföra en behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemet Cosmic i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att Regionstyrelsen 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.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Som har redovisats 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, 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 förut 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 tilldelningen inte 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.

Det framgår att det i Cosmic finns fyra moduler som innehåller personuppgifter: ”Vårddokumentation – Bas”, ”Läkemedel – Bas”, ”Vårdadministration – Bas” och ”Remiss – Bas”. Regionstyrelsen har uppgett att av 7 014 användare vid Universitetssjukhuset i Linköping har 6 221 användare tilldelats basåtkomst till modulen Vårddokumentation, 6 102 användare har tilldelats basåtkomst till modulen Läkemedel, 5 956 användare har tilldelats basåtkomst till modulen Vårdadministration och 5 848 användare har tilldelats basåtkomst till modulen Remiss. Detta innebär att en majoritet av användarna har tilldelats åtkomstmöjlighet till de fyra modulerna i Cosmic.

När det gäller begränsningar i Cosmic har Regionstyrelsen uteslutande redogjort för de personuppgifter som finns under ”Alla anteckningar” i modulen ”Vårddokumentation”. Regionstyrelsen har anfört att det finns tre typer av sekretessklassad information och att användarna har möjlighet att sekretessklassa information beträffande två av dessa tre sekretessklasser.

Beträffande sekretessklassen ”Ingen åtkomst med loggning”, sker denna klassning av vårdgivaren. Det finns två enheter vid Universitetssjukhuset i Linköping vars uppgifter har fått denna sekretessklass. Datainspektionen konstaterar att en reell begränsning av användarnas åtkomst har skett i dessa fall.

När det gäller de två andra sekretessklasserna, ”Skapa journalreferens med loggning” och ”Varning med loggning”, är personuppgifterna som har belagts med denna ”sekretess” fortfarande elektroniskt åtkomliga genom aktiva val. Genom att användaren klickar i rutan för samtycke eller nödåtkomst kan denne fortfarande ta del av alla personuppgifter, vilket innebär att alla användare som gör dessa aktiva val kan ta del av patienternas uppgifter och inte enbart de användare som har ett behov.

Av förarbetena till patientdatalagen, prop. 2007/08:126, s. 149, framgår att syftet med bestämmelsen om åtkomstbegränsning i 4 kap. 2 § patientdatalagen 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. Av förarbetena framgår att uppgifter dessutom bör 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.

Att Regionstyrelsen använder sig av ovanstående aktiva val är en integritetshöjande åtgärd, men innebär inte att dessa aktiva val utgör en sådan åtkomstbegränsning som avses i 4 kap. 2 § patientdatalagen. Denna bestämmelse kräver att behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, dvs. endast de som har behov av uppgifterna ska ha åtkomst, och någon sådan begränsning har inte skett. Datainspektionen ifrågasätter även Regionstyrelsens tillvägagångsätt när det gäller att användarna själva ska sekretessklassa informationen, och inte Regionstyrelsen själv.

Regionstyrelsen har uteslutande redogjort för de personuppgifter som finns under ”Alla anteckningar” i modulen ”Vårddokumentation” vad gäller möjligheten för användaren att sekretessklassa information. I övrigt har Regionstyrelsen inte anfört att det finns några begränsningar eller sekretessklasser när det gäller övriga personuppgifter eller i övriga moduler. Tvärtom har Regionstyrelsen t.ex. uppgett att alla som har åtkomst till Cosmic har åtkomst till modulen ”Läkemedel – Bas”, även om det finns möjlighet att begränsa åtkomsten till uppgifterna i denna modul.

Eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden, behöver användarnas åtkomst till uppgifterna i Cosmic begränsas för att återspegla detta. Regionstyrelsen har, bortsett från de uppgifter som har fått sekretessklassen ”Ingen åtkomst med loggning”, inte begränsat användarnas behörigheter för åtkomst till patienternas personuppgifter i journalsystemet, vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen i systemet Cosmic. Detta innebär att en majoritet av användarna vid Universitetssjukhuset i Linköping som har åtkomst till Cosmic, även har åtkomst till en majoritet av personuppgifterna som finns i de fyra modulerna.

Användarnas behörigheter har således inte begränsats på så sätt som bestämmelserna i patientdatalagen kräver och Regionstyrelsen har inte, i enlighet med artikel 32, använt sig av tillräckliga tekniska åtgärder för att begränsa användarnas åtkomstmöjligheter till personuppgifter i journalsystemen till enbart vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter. Detta innebär att tilldelningen av behörigheter har varit för omfattande, generell och genomförts för ett för den personliga integriteten för ingripande sätt och därigenom varit oproportionerlig i förhållande till ändamålet.

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, som omfattar 516 416 patienter, dels inom ramen för den sammanhållna journalföringen, som omfattar 838 093 patienter. Antalet användare är 7 014 stycken och antalet användare som har fått åtkomst till uppgifterna i de olika modulerna ligger mellan 5 848 – 6 221.

Det framgår att Regionstyrelsen inte har begränsat hälso- och sjukvårdspersonals och medicinska sekreterares åtkomstmöjligheter till uppgifter om patienter vare sig inom ramen för den inre sekretessen eller inom ramen för sammanhållen journalföring i journalsystemet Cosmic.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att Regionstyrelsen vid granskning den 10 april 2019 har behandlat personuppgifter i strid med artikel 5.1 f och 5.2, artikel 24.1 och artikel 32.1 och 32.2 i dataskyddsförordningen genom att Regionstyrelsen inte har begränsat användarnas behörigheter för åtkomst till journalsystemet Cosmic till enbart vad som 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 Regionstyrelsen inte har vidtagit åtgärder för att kunna säkerställa och kunna visa en lämplig säkerhet för personuppgifterna.

Dokumentation av åtkomsten (loggar)
Datainspektionen kan konstatera att det av loggarna i Cosmic 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 har inte något att erinra i denna del, eftersom Regionstyrelsen uppfyller kraven på innehållet i dokumentation i loggarna vilket framgår av 4 kap. 9 § HSLF-FS 2016:40 och har därmed vidtagit lämpliga tekniska åtgärder enligt artikel 32 i dataskyddsförordningen,

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 och artikel 83.2 i dataskyddskyddsförordningen framgår att Datainspektionen har befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83. Vidare framgår att beroende på omständigheterna i det enskilda fallet ska administrativa sanktionsavgifter påföras utöver eller i stället för de övriga åtgärderna i artikel 58.2.

För myndigheter får enligt artikel 83.7 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 stort behov av information i sin verksamhet. Det är därför naturligt att digitaliseringens möjligheter tillvaratas så mycket som möjligt inom vården. Sedan patientdatalagen skrevs 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.

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.

Regionstyrelsen har i detta fall underlåtit att genomföra en behovs- och riskanalys, något som direkt föreskrivs i 4 kap. 2 § HLSF-FS 2016:40. Det innebär att Regionstyrelsen inte har haft någon grund för att bedöma vare sig behovet eller risken vid behörighetstilldelning. Det har också lett till att åtkomsten för medarbetarna inte har begränsats till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Det gäller såväl åtkomst inom den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen förelägger därför enligt artikel 58.2 d i dataskyddsförordningen Regionstyrelsen att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemet Cosmic och att därefter, med stöd av behovs- och riskanalysen, tilldela varje användare 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 24.1 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.

Sanktionsavgift

Datainspektionen kan konstatera att överträdelserna avser Regionstyrelsens skyldighet att med lämpliga säkerhetsåtgärder ge skydd till personuppgifter enligt artikel 32 i dataskyddsförordningen.

I detta fall är det fråga 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 fråga om uppgifter som omfattar direkt identifiering av den enskilde genom såväl namn, kontaktuppgifter som personnummer, uppgifter om hälsa, men det kan även 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 och behandlingen omfattar många patienter och möjligheten till åtkomst avser en stor andel av de anställda. I detta fall rör det sig om 516 416 unika patienter inom ramen för den inre sekretessen, och 794 626 unika patienter inom ramen för den sammanhållna journalföringen. Det finns endast två enheter där uppgifterna inte är åtkomlig för användarna utanför dessa enheter.

Det har vidare framkommit att Regionstyrelsen inte har åtgärdat det tidigare föreläggandet från Datainspektionen, daterat den 27 mars 2015, där Regionstyrelsen förelades att ta fram en dokumenterad behovs- och riskanalys som uppfyllde det dåvarande kravet 2 kap. 6 § § andra stycket andra meningen SOSFS 2008:14, vilket motsvarar nuvarande bestämmelse i 4 kap. 2 § HSLF-FS 2016:40. Detta är, enligt artikel 83.2 e dataskyddsförordningen, att anse som ytterligare en försvårande omständighet.

Datainspektionen konstaterar att de brister som nu konstaterats har varit kända för Regionstyrelsen 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 avser artikel 5 som anges tillhöra de allvarligare överträdelserna som kan ge en högre sanktionsavgift enligt artikel 83.5.

Dessa faktorer innebär sammantaget att de aktuella överträdelserna inte är att bedöma som mindre överträdelser utan överträdelserna 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 effektivt, proportionerligt 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.

Utifrån överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer Datainspektionen den administrativa sanktionsavgiften för Regionstyrelsen till 2 500 000 (två miljoner femhundra tusen) 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, enhetscheferna Katarina Tullstedt och Malin Blixt samt juristen Maja Savic medverkat.

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

Bilaga 1 – 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.