Digital Medical Supply Sweden AB (KRY)
Torsgatan 21
113 21 Stockholm

Tillsyn enligt dataskyddsförordningen och patientdatalagen – behovs- och riskanalys och frågor om åtkomst i journalsystem Till Digital Medical Supply Sweden AB (KRY)

Innehåll

Datainspektionens beslut

Datainspektionen har vid inspektion på plats den 4 april 2019 konstaterat att Digital Medical Supply Sweden AB (KRY) 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. KRY inte har genomfört behovs- och riskanalyser som uppfyller kraven enligt bestämmelserna i 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) och 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) innan tilldelning av behörigheter sker i journalsystemet ProReNata och Nationell patientöversikt. Detta innebär att KRY inte i tillräcklig utsträckning 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. KRY inte har visat att KRY begränsat användarnas behörigheter för åtkomst till journalsystemet ProReNata och Nationell patientöversikt begränsats till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården i enlighet

[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).

med 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att KRY inte har vidtagit tillräckliga åtgärder för att kunna säkerställa och kunna visa en lämplig säkerhet för personuppgifterna.

Datainspektionen konstaterar att KRY sedan inspektionen den 4 april 2019 har förbättrat sina behovs- och riskanalyser men att analyserna inte i alla delar uppfyller de krav som gäller enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) och 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen KRY att senast den sista februari 2021 komplettera behovs- och riskanalyserna för journalsystemen ProReNata och Nationell patientöversikt genom att utveckla analysen av riskerna för de registrerades rättigheter och friheter och att därefter, med stöd av behovs- och riskanalyserna, göra en förnyad bedömning gällande tilldelning av behörigheter så att varje användare får åtkomst till enbart de personuppgifter som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med 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 4 april 2019 granskat om KRY:s beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Tillsynen har även omfattat hur KRY tilldelat behörigheter för åtkomst till huvudjournalsystemet ProReNata och Nationell patientöversikt 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 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).

Vad som framkommit i ärendet

KRY har i huvudsak uppgett följande.

Personuppgiftsansvarig

KRY är vårdgivare och personuppgiftsansvarig.

Verksamhet

KRY bedriver vård via videomöten, s.k. videovård, som sker genom att patienten laddar ner appen KRY. KRY är den tekniska plattformen och även varumärket som KRY använder utåt mot patienter. Appen är tillgänglig för mobila enheter med operativsystemen iOS eller Android.

Det är KRY:s moderbolag Webbhälsa AB (nedan Webbhälsa) som har utvecklat appen och som sköter driften av den tekniska plattformen. Webbhälsa äger varumärket KRY, utvecklar tekniken och servar vårdgivaren KRY med licenser. Det är två separata legala enheter men personalen sitter tillsammans på samma kontor.

Det är historiska skäl som ligger bakom att det är två bolag men en verksamhet. När KRY skapades vände sig Webbhälsa till regioner och landsting för att erbjuda tjänsten, men det tog lång tid att få vårdgivare att börja använda tjänsten. Därför startade Webbhälsa bolaget KRY som en egen vårdgivare som bedriver vård via appen KRY.

Journalsystem

KRY har uppgett att journalsystemet som används av KRY heter ProReNata och har använts sedan verksamheten startade i mars 2016. För sammanhållen journalföring används systemet Nationell patientöversikt (NPÖ).

Användare och patienter

Det fanns vid tidpunkten för inspektionen 490 personer med åtkomst till ProReNata. Den 8 april 2019 var det totala antalet patienter registrerade i ProReNata 450 331.

Inre sekretess

Behovs- och riskanalys
Under inspektionen och efterföljande granskning har i huvudsak följande kommit fram.

Under inspektionen den 4 april 2019 tog Datainspektionen in en behovs- och riskanalys daterad 11 mars 2019. Den 10 maj 2019 inkom KRY med en reviderad behovs- och riskanalys daterad 2 maj 2019 där även sammanhållen journalföring ingår men som i övrigt i huvudsak innehåller samma behovs- och riskanalys som dokumentet daterat 11 mars 2019. Den 20 mars 2020 inkom KRY med en ny reviderad version daterad 1 mars 2020 som innehåller en till stor del omarbetad analys.

I behovs- och riskanalysen daterad 11 mars 2019 ingår bland annat en beskrivning av behov i verksamheten, risker och hantering av risker.

I dokumentet anges bland annat följande avseende behov i verksamheten för hälso- och sjukvårdspersonal:

Med anledning av verksamhetens medicinska inriktning, digitala natur och frånvaro av fysisk närvaro i olika geografiska områden, är hälso- och sjukvårdspersonal hos KRY organiserade i en enda personalpool som schemaläggs av administrativ personal för möten med alla typer av patienter. Hälso- och sjukvårdspersonal är således inte organiserade uteslutande baserat på nödvändig kompetens i det enskilda fallet (t.ex. allmänläkare, sjuksköterska eller psykolog), schemaläggning och tillgänglighet. Även om viss typ av behandling, t.ex. behandling av barn under 6 månaders ålder eller behandling av vissa symtom typiska för t.ex. kvinnor, ska skötas av viss specialiserad personal så är denna personals arbete inte begränsat till dessa symtom då de även träffar andra typer av patienter. För det fall KRY vårdverksamhet förändras över tid, genom t.ex. ett större antal tillgängliga medarbetare, flera olika vårdpersonalkategorier eller vårdprocesser (såsom t.ex. specialistvård) kommer en uppdaterad behovs- och riskanalys att genomföras för att säkerställa patientsäkerheten men också tillse att respekt för patientens integritet ständigt iakttas.

För att säkra god kvalitet, tillgänglighet och kostnadseffektivitet är det av yttersta vikt att personal som deltar i den faktiska vården inom ramen för KRY öppenvård och i en patientrelation, har en god och tillräcklig kännedom om patientens medicinska historik. Alla kliniker och relevant administrativ personal (såsom medicinska sekreterare som har relevant utbildning för sitt uppdrag) som anlitas av KRY kan komma att träffa alla patienter som söker vård via KRY och kan då komma att delta i vården av dessa och således behöva tillgång till patientens journal för att kunna fullgöra sina arbetsuppgifter.

Sammanfattningsvis är det KRY bedömning att det av såväl verksamhetens art och unika särprägel finns ett stort behov av att inte begränsa behörighet för medicinsk och relevant administrativ personal till vissa geografiskt eller demografiskt avgränsade patientgrupper i nuläget. För övriga typer av behörigheter finns ett mer begränsat behov i enlighet med vad som anges ovan.

Under rubriken ”risker” anges att KRY ser ett antal risker med en bred behörighet och anger att riskerna enligt KRY:s uppfattning främst är:

- Obehörig åtkomst för hälso- och sjukvårdspersonal eller relevant administrativ personal till följd av okunskap om regler och rutiner kring sekretess och patientsäkerhet;
- Obehörig åtkomst för hälso- och sjukvårdpersonal eller relevant administrativ personal till följd av misstag eller annars på grund av mänsklig faktor;
- Obehörig åtkomst för hälso- och sjukvårdspersonal eller relevant administrativ personal till följd av medvetet missbruk;
- Obehörig åtkomst för tredje man till följd av att hälso- och sjukvårdspersonal eller relevant administrativ personal förlorar utrustning eller, medvetet eller omedvetet, delar med sig av inloggningsuppgifter till system; och
- Obehörig åtkomst för tredje man till följd av dataintrång.

Under rubriken ”hantering av risker” anges att KRY bedömning är att de risker som följer av en bred behörighetstilldelning kan begränsas väsentligt och till en acceptabel nivå genom de organisatoriska och tekniska säkerhetsåtgärder som vidtagits av KRY och som främst omfattar:

- Rutiner för rekrytering, inklusive bakgrundskontroller, för att minimera risken för att olämpliga individer ges åtkomst till personuppgifter om patienter;
- Rutiner för onboarding, vilken bl.a. omfattar handledning och utbildning kring användning av system, utrustning, relevanta författningar och rutiner kring sekretess och patientsäkerhet för att öka medvetenheten om skyldigheter, rättigheter och ansvar;
- Signering av erinran om sekretess och/eller sekretessåtaganden för att preventivt minska risk för otillåten åtkomst och för att öka kunskapen om sekretess och patientsäkerhet;
- Användning av utrustning som tillhandahålls och kontrolleras av KRY;

- Rutiner för tilldelning, ändring och borttagning av behörigheter för att preventivt minimera risk för att behörigheter inte är adekvata över tid;
- Tekniska redskap för att preventivt minimera behovet för slagningar i journalsystemet och därmed risken för olovlig åtkomst, t.ex. som ett resultat av misstag eller otillräcklig kunskap. I hälso- och sjukvårdspersonals arbete för digital vård, kommer endast aktuellt patient vara tillgänglig. I detta system kan ej annan patient än den som mötet berör att öppnas. För att kunna söka på andra patienter måste aktuell personal aktivt göra en otillåten slagning;
- Inhämtande av godkännande från patient innan medicinska sekreterare gör slagningar i patientjournal; och
- Tydlig information till relevant personal samt rutin för loggning och kontroll i syfte att preventivt få anställda att avhålla sig från otillåten åtkomst och för att reaktivt upptäcka och följa upp kring sådan access. Samtliga journalöppningar som inte finns kopplade till en aktiv vårdrelation/utfört patientmöte loggas och gås igenom manuellt.

Under rubriken ”slutsatser” anges bland annat:

En bred behörighet för medicinsk och administrativ personal till patienters journaler är därför motiverad under nuvarande förhållanden i KRY för att kunna tillhandahålla en patientsäker vård, förutsatt att KRY driver ett fortsatt effektivt säkerhetsarbete för att identifiera, utvärdera och hantera risker i sin verksamhet.

Denna slutsats behöver dock omprövas regelbundet och kan komma att ändras i takt med att KRY växer, förändrar medicinsk inriktning, utvecklar sitt affärskoncept och under andra liknande omständigheter. En förutsättning för att kunna begränsa behörighet för olika kliniker, är att vi trots detta kan säkerställa tillgänglighet för patienter. En uppdelning mellan kliniker för vilken grupp av patienter som man har, förutsätter en betydligt större personalstyrka än den som idag finns tillgänglig för KRY, men är ett önskvärt mål att sikta mot på sikt.

I den andra revideringen daterad 1 mars 2020 har KRY till stor del omarbetat analysen och identifierat risker baserat på vissa slags uppgifter och patientgrupper i form av uppgifter om personer med skyddad identitet,

offentliga personer, medarbetare och personalens egna uppgifter. Vidare har KRY i den reviderade analysen även bedömt sannolikhet och konsekvens för de identifierade riskerna. Analysen innehåller även mer detaljerad genomgång av behov av åtkomst för de olika personalkategorierna. Till skillnad från de tidigare versionerna av analysen har KRY kommit fram till att en snäv behörighet räcker för läkare, sjuksköterskor och psykologer, utom så kallade plusläkare, pluspsykologer och läkare bakjour. Den snäva behörigheten uppges innebära att användarna endast kan ta del av uppgifter om patienter (såväl interna journaler som NPÖ) vid patientmöte. Vidare anges att åtkomst tilldelas i samband med personalen schemaläggs med patient och dras automatiskt tillbaka 4 månader efter att åtkomst tilldelats samt att innan möte med patient har skett kan inte slagning på sådan patient ske.

Behörighetstilldelning för åtkomst till personuppgifter
Under inspektionen framkom i huvudsak följande.

Klinisk personal, vid tidpunkten för inspektionen, läkare, sjuksköterskor och psykologer samt administrativ personal i form av medicinska sekreterare, har faktisk åtkomst till alla uppgifter i alla patientjournaler i ProReNata. Det finns begränsningar i form av organisatoriska och tekniska kontroller, vilket enligt KRY varit en viktig del i bedömningen av behörighetsstyrningen där KRY tänkt på vilken annan säkerhet som kan erbjudas.

KRY granskar systematiskt alla journalaccesser. All åtkomst granskas och matchas mot huruvida kliniker haft möte med patienten den dagen. I annat fall flaggas åtkomsten och gås igenom för att se om det finns en annan rimlig förklaring till åtkomsten. Det sker en kontroll var fjärde vecka när det gäller aktiva konton (genom att personalschemat gås igenom). Om exempelvis en läkare inte har ett pass inbokat de närmsta fyra veckorna så inaktiveras läkarens konto. Om en läkare med inaktivt konto har ett pass inlagt de närmsta fyra veckorna aktiveras kontot.

Utformningen av behörigheterna baseras på den digitala karaktären hos tjänsten som KRY erbjuder, att vården har allmän inriktning och inte är specialiserad, att patienterna är spridda över hela landet, att kötiden för patienten ska vara så kort som möjlig och att personalen är organiserad i en enda personalpool. En patient som ringer in får hjälp av en läkare en dag och en helt annan läkare nästa dag, och läkarna kan sitta på helt olika platser i

Sverige. Det kräver enligt KRY att läkarna måste kunna se varandras journaluppgifter för att kunna ge god vård.

KRY har gjort bedömningen att all information som finns om patienterna är relevant för vårdpersonalen, men KRY är medveten om att detta kan komma att förändras i takt med att organisationen växer.

I behovs- och riskanalysen daterad 1 mars 2020 har KRY gjort en mer detaljerad analys av behovet av åtkomst till uppgifter i ProReNata utifrån de olika personalkategoriernas arbetsuppgifter och kommit fram till att en snäv behörighet är tillräcklig för läkare, sjuksköterskor och psykologer på det sätt som beskrivs i avsnittet ovan i redogörelsen av den reviderade behovs- och riskanalysen.

Sammanhållen journalföring

Under inspektionen och efterföljande granskning har i huvudsak följande kommit fram.

Behovs- och riskanalys
Vid inspektionen fanns ingen särskild behovs- och riskanalys för åtkomst till NPÖ. KRY har inkommit med två reviderade behovs- och riskanalyser daterade 2 maj 2019 och 1 mars 2020 som omfattar användning av nationell patientöversikt (NPÖ) i verksamheten. Behovs- och riskanalysen daterad 2 maj 2019 innehåller i övrigt i huvudsak samma behovs- och riskanalys som dokumentet daterat 11 mars 2019.

I behovs- och riskanalysen daterad 1 mars 2020 har KRY gjort en mer detaljerad analys av behovet av åtkomst till uppgifter i NPÖ utifrån de olika personalkategoriernas arbetsuppgifter.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
KRY har uppgett att vårdgivaren ingår i system för sammanhållen journalföring genom NPÖ som ”konsument”. Det innebär att personalen hos KRY kan ta del av uppgifterna i NPÖ, men KRY ”producerar” (tillgängliggör) inga egna uppgifter i NPÖ.

Vid tidpunkten för inspektionen framkom att all personal som hade åtkomst till ProReNata också hade åtkomst till NPÖ.

Av den reviderade behovs- och riskanalysen daterad 1 mars 2020 framgår att all personal som har åtkomst till ProReNata som utgångspunkt inte har ett behov av åtkomst till uppgifter i NPÖ. Sjuksköterskor och vårdadministratörer anges som utgångspunkt ha ett behov av åtkomst till ProReNata men inte till NPÖ.

Dokumentation av åtkomsten (loggar)
KRY har uppgett följande.

För varje slagning i ProReNata skapas ett loggmeddelande med information om vilken personal som vid en given tidpunkt gjort en slagning. Tidpunkt avser både datum och klockslag. Det framgår vilken patient det rör, användarens identitet, vad användaren har vidtagit för åtgärd, exempelvis signering, anteckning och läsning. Eftersom KRY inte är organiserade i flera olika vårdenheter framgår endast en enhet som är densamma för all personal.

Det finns tre olika typer av loggar i ProReNata; besöksloggar, serverloggar och händelseloggar. Besökslogg visar när en användare besökt en journal och när den lämnat journalen. Serverlogg visar när systemet registrerat ett serveranrop till en journal och kan innebära att användare har läst men även andra skäl. Händelselogg visar loggade systemhändelser som påverkar en användare eller patient, exempelvis läst, skrivit eller signerat.

Åtkomst till NPÖ loggas av Inera och är tillgängliga för administratörer hos KRY.

KRY har efter inspektionstillfället noterat att den specifika åtgärden makulering av anteckning (icke signerad) inte loggas särskilt i ProReNata. KRY har tagit upp detta med ProReNata AB vilka på KRY:s begäran har utvecklat sådan loggning. Även makuleringar av anteckningar kommer därför att loggas från och med den 16 maj 2019 i syfte att ge KRY än bättre möjligheter att följa upp och säkerställa en god och säker vård.

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

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

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

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

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

Av artikel 9 framgår att behandling av särskilda kategorier av personuppgifter (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.

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 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 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 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 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 och 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 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 kan noteras att det i artikel 32.2 anges 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 Socialstyrelsens föreskrifter som kompletterar patientdatalagen finns det angivet i 4 kap. 2 § HSLF-FS 2016:40, 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 exempelvis 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 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 det inte sker någon annan åtkomst än den som behovs- och riskanalysen visar är befogad ska kunna ske.

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

När Datainspektionen under inspektionen efterfrågade en dokumenterad behovs- och riskanalys inkom KRY med ett dokument daterat 11 mars 2019 med rubriken ”Behörighetstilldelning Behovs- och riskanalys”. KRY har därefter den 10 maj 2019 inkommit KRY med en reviderad behovs- och riskanalys daterad 2 maj 2019 där även sammanhållen journalföring ingår men som i övrigt i huvudsak innehåller samma behovs- och riskanalys som dokumentet daterat 11 mars 2019. Den 20 mars 2020 inkom KRY med en ny reviderad version daterad 1 mars 2020 som innehåller en till stor del omarbetad analys.

KRY har i behovs- och riskanalysen från den 11 mars 2019 gjort en analys avseende den inre sekretessen där behovet av åtkomst till personuppgifter i journalsystemet har vägts mot risker som KRY anser följa av åtkomstbehörigheten. Det framgår att syftet är att baserat på analysen landa i en modell för behörighetstilldelning i verksamheten. I analysen har KRY identifierat och beskrivit behov av åtkomst utifrån hur KRY bedriver sin verksamhet. Vidare har KRY identifierat och beskrivit behov utifrån olika personalkategoriers arbetsuppgifter. KRY har kommit till en slutsats efter att

ha vägt behovet mot de av KRY identifierade riskerna och vidtagna åtgärder för att minska riskerna.

Datainspektionen kan konstatera att KRY har genomfört en behovs- och riskanalys som identifierar och analyserar behov och risker. Analysen är genomförd på strategisk nivå och ska utgöra en grund för verksamhetens behörighetstilldelning. Behoven och delvis också riskerna är analyserade utifrån de faktiska förutsättningarna i verksamheten. KRY har baserat på den analys som har genomförts identifierat tekniska och organisatoriska åtgärder för att minska risken för obehörig åtkomst.

KRY har däremot i sin inledande analys inte beaktat hur negativa konsekvenser för registrerade, olika kategorier av uppgifter, kategorier av registrerade, eller omfattningen av antalet personuppgifter och registrerade, påverkar risken för fysiska personers rättigheter och friheter vid KRY:s behandling av personuppgifter i ProReNata och Nationell patientöversikt. 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.

KRY har således vidtagit åtgärder som sannolikt minskar risken för fysiska personers rättigheter och friheter. Behoven är emellertid för generellt analyserade och riskerna för de registrerades rättigheter och friheter är inte i tillräcklig mån identifierade och bedömda. Bland annat saknas en djupare analys av riskerna för den enskildes integritet utifrån såväl olika kategorier av uppgifter som olika kategorier av registrerade.

Datainspektionen konstaterar sammanfattningsvis att KRY vid inspektionstillfället genomfört en behovs- och riskanalys på strategisk nivå, men att den inte uppfyllt de krav dataskyddsbestämmelserna ställer på en sådan analys eftersom KRY inte har beaktat riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter och inte beaktat olika slags risker för den enskildes integritet som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Datainspektionen konstaterar att KRY därigenom vid inspektionstillfället inte har genomfört en behovs- och riskanalys som uppfyller kraven som

ställs 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 KRY 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.

KRY har kompletterat med en behovs- och riskanalys daterad den 1 mars 2020. I den nya behovs- och riskanalysen har KRY till stor del omarbetat analysen och identifierat risker baserat på vissa slags uppgifter och patientgrupper i form av uppgifter om personer med skyddad identitet, offentliga personer, medarbetare och personalens egna uppgifter. Vidare har KRY i den reviderade analysen även bedömt sannolikhet och konsekvens för de identifierade riskerna. Analysen innehåller även mer detaljerad genomgång av behov av åtkomst för de olika personalkategorierna.

Till skillnad från de tidigare versionerna av analysen har KRY kommit fram till att en snäv behörighet räcker för läkare, sjuksköterskor och psykologer, utom så kallade plusläkare, pluspsykologer och läkare bakjour. Den snäva behörigheten uppges innebära att användarna endast kan ta del av uppgifter om patienter (såväl interna journaler som NPÖ) vid patientmöte. Vidare anges att åtkomst tilldelas i samband med personalen schemaläggs med patient och dras automatiskt tillbaka 4 månader efter att åtkomst tilldelats samt att innan möte med patient har skett kan inte slagning på sådan patient ske.

Datainspektionen kan konstatera att den nya behovs- och riskanalysen innehåller en fördjupad behovsanalys där såväl organisation, olika yrkeskategorier och olika arbetsuppgifter har beaktats. Beträffande riskbedömningen så är även den fördjupad och beaktar i vart fall olika kategorier av registrerade. Det ingår också en bedömning av hur sannolik eller allvarlig risken för de registrerades rättigheter och friheter är. KRY har utifrån de nya rollerna skapat mer begränsade åtkomstmöjligheter.

KRY har utifrån sin särskilda verksamhet inte en så komplex organisation att det krävs ytterligare bedömningar avseende behoven. Vad avser riskerna så är de fortfarande inte analyserade utifrån kategorier av uppgifter. Uppgifter

som kan uppfattas som mer integritetskänsliga är exempelvis uppgifter som rör sexualliv, missbruk, psykisk ohälsa eller hot eller våld särskilt om det är i nära relationer. Även analysen utifrån kategorier av registrerade kan fördjupas genom att de kategorier som faktiskt behandlas i verksamheten genomgås. Att verksamheten har en homogen struktur innebär att det blir ännu viktigare att analysera dessa risker och bedöma om och hur de kan åtgärdas eftersom en så stor andel av personalen behöver tilldelas samma typ av åtkomst.

Behörighetstilldelning för åtkomst till personuppgifter om patienter
Som har redovisats ovan kan en vårdgivare ha ett berättigat intresse av att ha en omfattande behandling av uppgifter om enskildas hälsa. Oaktat detta ska åtkomstmöjligheter till personuppgifter om patienter vara begränsade till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter.

När det gäller tilldelning av behörighet för elektronisk åtkomst enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen framgår det av förarbetena, prop. 2007/08:126 s. 148-149, 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.

Det framgår att KRY vid tidpunkten för inspektionen inte hade begränsat hälso- och sjukvårdspersonals och medicinska sekreterares åtkomstmöjligheter till uppgifter om patienter vare sig inom ramen för den inre sekretessen i journalsystemet ProReNata, eller inom ramen för sammanhållen journalföring i journalsystemet NPÖ. KRY hade däremot infört åtgärder för att undvika obehörig åtkomst bland annat i form av loggning och manuell genomgång av samtliga journalöppningar som inte var kopplade till en aktiv vårdrelation eller utfört patientmöte samt inaktivering av konton var fjärde vecka för läkare utan pass inbokade de närmaste fyra veckorna.

Eftersom den behov- och riskanalys som KRY hade genomfört vid tidpunkten för inspektionen inte i tillräcklig utsträckning tog 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 KRY inte visat att läsbehörigheterna har begränsats på så sätt som dataskyddsförordningen och patientdatalagen kräver.

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. KRY har genom senare vidtagna åtgärder minskat den risken genom förbättrade analyser och därefter vidtagna åtgärder.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att KRY vid inspektionstillfället har behandlat personuppgifter i strid med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen genom att KRY, i enlighet med artikel 5.2 och 24.1, inte har kunnat visa att KRY begränsat användarnas behörigheter för åtkomst till journalsystemet ProReNata och Nationell patientöversikt 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.

I behovs- och riskanalysen daterad 1 mars 2020 framgår att KRY har infört begränsningar av åtkomst till personuppgifter om patienter. Till skillnad från de tidigare versionerna av analysen har KRY kommit fram till att en snäv behörighet räcker för läkare, sjuksköterskor och psykologer, utom så kallade plusläkare, pluspsykologer och läkare bakjour. Den snäva behörigheten uppges innebära att användarna endast kan ta del av uppgifter om patienter

(såväl interna journaler som NPÖ) vid patientmöte. Vidare anges att åtkomst tilldelas i samband med personalen schemaläggs med patient och dras automatiskt tillbaka 4 månader efter att åtkomst tilldelats samt att innan möte med patient har skett kan inte slagning på sådan patient ske.

KRY har således förbättrat begränsningen av åtkomst sedan inspektionen. Enligt vad som framgår i avsnittet ovan avseende den nya behovs- och riskanalysen krävs dock fortfarande vissa kompletteringar för att analysen ska vara heltäckande och kunna visa att åtkomsten har begränsats i enlighet med kraven i dataskyddsförordningen och patientdatalagen. Utifrån resultatet av dessa kompletteringar måste sedan KRY bedöma sin modell för behörighetstilldelning.

Dokumentation av åtkomsten (loggar)
Datainspektionen kan konstatera att det av loggarna i ProReNata och NPÖ framgår uppgifter om vilken personal som vid en given tidpunkt gjort en slagning. Tidpunkt avser både datum och klockslag. Det framgår vilken patient det rör, användarens identitet, vad användaren har vidtagit för åtgärd, exempelvis signering, anteckning och läsning. Eftersom KRY inte är organiserade i flera olika vårdenheter framgår endast en enhet som är densamma för all personal.

KRY har efter inspektionstillfället noterat att den specifika åtgärden makulering av anteckning (icke signerad) inte loggas särskilt i ProReNata men att KRY har uppgett att sådan loggning har införts från och med den 16 maj 2019. Datainspektionen konstaterar att dokumentationen av åtkomsten (loggarna) i ProReNata och NPÖ numera 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. Den övergripande utgångspunkten för påförande av sanktionsavgift är att det i det enskilda fallet bedöms vara effektivt, proportionellt och avskräckande (jfr artikel 83.1).

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.

Bedömning av om sanktionsavgift ska påföras
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.

I detta sammanhang innebär det ett ännu större 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 befattningshavaren 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.

Datainspektionen har konstaterat att KRY vid Datainspektionens inspektion genomfört en behovs- och riskanalys på strategisk nivå, men att analysen

inte fullt ut beaktat riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter och att KRY inte har beaktat olika slags risker för den enskildes integritet som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. KRY har därefter i mars 2020 utfört en ny behovs- och riskanalys. Den nya behovs- och riskanalysen går djupare än den tidigare och beaktar såväl organisation som olika yrkeskategorier och arbetsuppgifter. Riskbedömningen är även den fördjupad och innehåller nu även en bedömning av sannolikhet och allvarlighet av risker för registrerades grundläggande fri- och rättigheter. Även om behovsanalysen numera kan anses godtagbar saknas det dock fortfarande delar som avser riskbedömningen. Vad som närmare behöver åtgärdas beskriver Datainspektionen nedan under rubriken föreläggande.

Datainspektionens tillsyn har således visat att KRY inte har uppfyllt kravet på att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i journalsystemen genom att inte ha helt levt upp till de krav som följer av patientdatalagen och Socialstyrelsens föreskrifter om att genomföra behovs- och riskanalys, innan tilldelning av behörigheter i systemet sker. Därigenom har KRY inte heller kunnat visa att KRY har begränsat behörigheten för åtkomst till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Det innebär att KRY inte heller har uppfyllt kraven i artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen. Den bristande regelefterlevnaden omfattar såväl den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen kan konstatera att överträdelserna som utgångspunkt är allvarliga då det gäller bestämmelser som är grundläggande för att se till att behandlingen av personuppgifter omfattas av tillräckliga säkerhetsåtgärder till skydd för registrerades grundläggande fri-och rättigheter. Även uppgifternas karaktär, antal berörda registrerade, som i detta fall uppgår till omkring
450 000 patienter, som antalet anställda och tillgången för en stor del av de anställda till dessa patienters uppgifter talar i försvårande riktning.

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

överträdelser som kan ge en högre sanktionsavgift enligt artikel 83.5 i dataskyddsförordningen.

Det är således typiskt sett inte fråga om mindre överträdelser utan överträdelser som normalt ska leda till en administrativ sanktionsavgift.

Vid bedömningen av om sanktionsavgift ska påföras måste samtidigt prövas om det krävs med beaktande av att det ska vara fråga om en åtgärd som i det enskilda fallet är effektiv, proportionell och avskräckande.

Som framgått hade KRY vid tidpunkten för inspektionen gjort en behovs- och riskanalys på strategisk nivå samt vidtagit åtgärder som sannolikt minskar risken för fysiska personers rättigheter och friheter. KRY har således försökt att följa de krav som ställs vid behandling av personuppgifter och har i inte obetydlig utsträckning vidtagit åtgärder i syfte att efterleva kraven och minska riskerna. Datainspektionen bedömer att KRY:s bristande efterlevnad inte har inneburit att de registrerade har berövats skydd för sina rättigheter och friheter i samma omfattning som om inga eller enbart bristfälliga åtgärder hade vidtagits.

KRY har också själv vidtagit åtgärder för att försöka komma till rätta med brister i behovs- och riskanalysen efter Datainspektionens inspektion genom att upprätta och till Datainspektionen komma in med två reviderade behovs- och riskanalyser. Det ska också beaktas att KRY själv har uppmärksammat brist i loggningen och vidtagit åtgärder för att åtgärda den bristen.

Vid en sammanvägd bedömning finner Datainspektionen att de aktuella överträdelserna visserligen typiskt sett är av sådan karaktär att en administrativ sanktionsavgift normalt ska påföras men att det i det aktuella fallet inte är proportionellt med ett sådant ingripande från Datainspektionen. KRY bör istället föreläggas att vidta åtgärder för att se till att behandlingen sker i enlighet med dataskyddsförordningen.

Föreläggande
Vid beslut om föreläggande beaktar Datainspektionen de revideringar av behovs- och riskanalysen som KRY har gjort efter inspektionen.

KRY har under tillsynsärendet handläggning reviderat sin behovs- och riskanalys vid två tillfällen. Den första revideringen gjordes 2 maj 2019 och

den andra revideringen gjordes 1 mars 2020. Genom den första revideringen justerade KRY analysen till att även omfatta sammanhållen journalföring i NPÖ. I den andra revideringen har KRY till stor del omarbetat analysen och identifierat risker baserat på vissa slags uppgifter och patientgrupper i form av uppgifter om personer med skyddad identitet, offentliga personer, medarbetare och personalens egna uppgifter.

Vidare har KRY i den reviderade analysen även bedömt sannolikhet och konsekvens för de identifierade riskerna. Analysen innehåller även mer detaljerad genomgång av behov av åtkomst för de olika personalkategorierna. Till skillnad från de tidigare versionerna av analysen har KRY kommit fram till att en snäv behörighet räcker för läkare, sjuksköterskor och psykologer, utom så kallade plusläkare och bakjour. Den snäva behörigheten uppges innebära att användarna endast kan ta del av uppgifter om patienter (såväl interna journaler som NPÖ) vid patientmöte. Vidare anges att åtkomst tilldelas i samband med att personalen schemaläggs med patient och dras automatiskt tillbaka 4 månader efter att åtkomst tilldelats samt att innan möte med patient har skett kan inte slagning på sådan patient ske.

Datainspektionen konstaterar att KRY sedan inspektionen den 4 april 2019 har förbättrat sin behovs- och riskanalys så att den i allt större utsträckning uppfyller de krav som ställs på en behovs- och riskanalys. Datainspektionen konstaterar dock att analysen inte beskriver riskerna för de registrerade på annat sätt än att det anges att det finns risk för röjande av sekretess och integritetsskada eller integritetshot. Analysen saknar närmare beskrivning av vad sådan skada eller hot består av och hur behandlingens omfattning påverkar risken.

Datainspektionen förelägger därför KRY, med stöd av artikel 58.2 d i dataskyddsförordningen, att senast den sista februari 2021 komplettera behovs- och riskanalyserna för journalsystemen ProReNata och Nationell patientöversikt genom att utveckla analysen av riskerna för de registrerades rättigheter och friheter och att därefter, med stöd av behovs- och riskanalyserna, göra en förnyad bedömning gällande tilldelning av behörigheter så att varje användare får åtkomst till enbart de personuppgifter som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med artikel 32.1 och

32.2 i dataskyddsförordningen, 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40.

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

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

Bilaga: 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 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.