Hälso- och sjukvårdsnämnden vid
Region Västerbotten
Köksvägen 11
901 89 Umeå

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

Innehållsförteckning

Datainspektionens beslut

Datainspektionen har vid granskningen den 14 maj 2019 och den 12 december 2019 konstaterat att Hälso- och sjukvårdsnämnden vid Region Västerbotten 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. Hälso- och sjukvårdsnämnden inte har genomfört behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemet NCS Cross, 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. Hälso- och sjukvårdsnämnden inte har begränsat användarnas behörigheter för åtkomst till journalsystemet NCS Cross 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 Hälso- och sjukvårdsnämnden 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 Hälso- och sjukvårdsnämnden, för överträdelserna 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 femhundratusen) kronor.

[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).

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Hälso- och sjukvårdsnämnden att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemet NCS Cross 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 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 14 maj 2019 och den 12 december 2019 granskat om Hälso- och sjukvårdsnämndens beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Granskningen har även omfattat hur Hälso- och sjukvårdsnämnden tilldelat behörigheter för åtkomst till huvudjournalsystemet NCS Cross, 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 användarens åtkomstmöjligheter till journalsystemet, 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.).

Tidigare granskning av behovs- och riskanalyser

Datainspektionen har tidigare genomfört en tillsyn avseende om dåvarande Landstingsstyrelsen, Västerbottens läns landsting hade genomfört en dokumenterad behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården. Av Datainspektionens beslut med diarienummer 1615-2013, meddelat den 27 mars 2015, framgår att Landstingsstyrelsen inte uppfyllde kravet på att

genomföra en behovs- och riskanalys enligt nämnda föreskrifter, och förelades därför att genomföra en sådan för huvudjournalsystemet.

Vad som framkommit i ärendet

Hälso- och sjukvårdsnämnden har i huvudsak uppgett följande.

Personuppgiftsansvarig

Den 1 januari 2019 gjordes en omorganisation som innebar att Region Västerbotten bildades. Det finns ingen myndighet under Hälso- och sjukvårdsnämnden. Hälso- och sjukvårdsnämnden bedriver hälso- och sjukvård inom regionen och är personuppgiftsansvarig för den behandling av personuppgifter som verksamheten utför i huvudjournalsystemet NCS Cross.

Journalsystem

Huvudjournalsystemet som används kallas NCS Cross och står för Nordic Clinical Suite. Det är möjligt att i NCS Cross ta del av vårddokumentation från och med 1993 då systemet infördes. Vid den tidpunkten var behörighetstilldelningen mer begränsad och användarna hade åtkomst till färre uppgifter än i dagens system. De så kallade Medarbetaruppdragen tillkom 2014–2015. Medarbetaruppdragen reglerar på vilken organisatorisk nivå åtkomst kan ske i NCS Cross och krävs för att få åtkomst till systemet.

NCS Cross används inom ramen för sammanhållen journalföring tillsammans med sju andra vårdgivare.

I samband med att dataskyddsförordningen började tillämpas gjorde leverantören en generell genomgång av systemet och informerade om att inga funktionella anpassningar behövde göras.

Det finns 101 databaser i NCS Cross utifrån att varje klinik i princip har en egen databas. Inom Region Västerbotten är antalet enheter 84 (aktiva databaser). Inom NCS Cross finns så kallade skyddade enheter.

I NCS Cross finns möjlighet att styra personalens åtkomstmöjligheter på olika sätt vad gäller behörighetsstyrning bland annat genom medarbetaruppdragen och funktioner för att spärra journal.

Skyddade uppgifter, om patienter med skyddad identitet hos Skatteverket, är inte tillgängliga i NCS Cross.

Antalet patienter och anställda
Antalet unika registrerade patienter i NCS Cross inom ramen för den inre sekretessen är 652 995. Antalet patienter som finns registrerade inom ramen för sammanhållen journalföring är 665 564.

Det finns cirka 10 000 anställda inom Region Västerbotten. Inom regionen har 9 139 användare ett giltigt medarbetaruppdrag och aktivt konto i NCS Cross. Antalet aktiva användarkonton inom regionen är 12 366. Anledningen till differensen i antalet användare är att verksamheterna inte har rapporterat in till förvaltningen att behörigheten ska avslutas. Åtkomsten till NCS Cross stoppas ändå eftersom de användare som inte har ett medarbetaruppdrag inte kan logga in i applikationen. Processen är automatiserad så att AD-kontot och därmed också medarbetaruppdraget stängs av automatiskt när anställningen upphör.

Inre sekretess

Behovs- och riskanalys
Av Datainspektionens beslut från den 27 mars 2015 framgår att Landstingsstyrelsen, Västerbottens läns landsting, förelades att ta fram en dokumenterad behovs- och riskanalys för huvudjournalsystemet.

Mot denna bakgrund har Hälso- och sjukvårdsnämnden uppgett bland annat följande.

Hälso- och sjukvårdsnämnden har följt Datainspektionens tidigare beslut och tagit fram dokumenten *Riktlinje för informationssäkerhet- och förvaltning och drift* samt *Mall – Behovs- och riskanalys vid behörighetstilldelning*. Styrdokumentet och mallen har upprättats för att ge verksamhetscheferna verktyg i samband med behörighetstilldelningen. Dokumenten *Användarprofiler* är exempel som tydliggör att behörigheter inte tilldelas generellt utan individuellt. Dokumenten är även exempel på genomförda analyser vid faktiska behörighetstilldelningar inom olika enheter.[2] Behovs- och riskanalysen görs utifrån verksamhetsperspektivet och inte från integritetsperspektivet.

[2] Dokumenten har kommit in till Datainspektionen.

Nämnden vet inte i vilken utsträckning mallen *Mall – Behovs- och riskanalys vid behörighetstilldelning* används ute i verksamheten, då man endast ser resultatet av själva behörighetsbeställningen. Nämnden har utgått från att verksamhetscheferna gör en behovs- och riskanalys före beställning av behörigheter. Nämnden har dock inte sett någon dokumenterad behovs- och riskanalys varken för den inre sekretessen eller för den sammanhållna journalföringen.

Av riktlinjerna för informationssäkerhet framgår att behörighet ska tilldelas efter en analys av vilken information olika personalkategorier i olika verksamheter behöver. Av riktlinjerna framgår också att riskanalysen ska ta hänsyn till vilka risker det kan innebära om personalen har för lite eller för mycket tillgång till olika patientuppgifter. Då behoven varierar mellan olika typer av verksamheter ansvarar verksamhetschefen för att behovs- och riskanalys genomförs på enhetsnivå. Enligt riktlinjerna ska verksamheten dokumentera behovs- och riskanalysen vid tilldelning av medarbetaruppdraget.

Av riktlinjerna framgår också bland annat att förutom regelbunden kontroll av användarnas behörighetsbehov ska översyn av behörigheterna ske efter organisations- och systemförändring.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Hälso- och sjukvårdsnämnden har i huvudsak uppgett följande.

För att en befattningshavare ska kunna ta del av personuppgifter i NCS Cross behöver flera förutsättningar vara uppfyllda. Befattningshavaren måste ha ett aktivt användarkonto i regionens domän (AD). Det förutsätter i sin tur att befattningshavaren finns registrerad i HR-systemet. För att kunna logga in i domänen behöver befattningshavare ett SITHS-kort med ett eller flera giltiga certifikat. För att därefter kunna logga in i NCS Cross behöver befattningshavaren dels ha ett giltigt så kallat medarbetaruppdrag, dels blivit tilldelad en behörighet i NCS Cross. Medarbetaruppdraget reglerar på vilken organisatorisk nivå åtkomst kan ske i NCS Cross. Det är verksamhetscheferna på de olika enheterna som beslutar om tilldelning av medarbetaruppdraget till sin personal på vårdenheten.

Tvåstegsautentisering ”att du verkligen är den du är” och att åtkomsten stängs för användaren när hen slutar är exempel på faktiska åtgärder som vidtagits för att förhindra onödig spridning av personuppgifter.

Vilken behörighet personalen tilldelas utgår från den behovsanalys som görs inför tilldelningen, det vill säga var och med vad den anställde arbetar. Exempelvis kan kuratorer och sjukgymnaster vara anställda på olika enheter, vilket innebär att de har fler medarbetaruppdrag och därmed måste ges behörighet till fler enheter. Detsamma gäller akutläkare som även har tillgång till fler enheter än den egna akutdatabasen.

Personalens åtkomst till databaser utgår från det behov som finns. Ett medarbetaruppdrag kan därmed innebära att en anställd kan få behörighet till flera databaser. En sjuksköterska på Neurocentrum kan exempelvis få ett medarbetaruppdrag med behörighet till åtta databaser eftersom kliniken har åtta databaser och sjuksköterskans arbete kräver åtkomst till samtliga.

Åtkomstmöjligheter (läsbehörighet) till vårddokumentation i NCS Cross
Varje anställd har en läsbehörighet som anpassas utifrån den enskildes uppdrag. Om en anställd tilldelas läsbehörighet inom hela Region Västerbotten gäller det enbart vårddokumentation. Skyddade enheter är exkluderade.

I NCS Cross behörighetskontrollsystem finns två typer av behörigheter dels *Egen behörighet*, dels *Tjänsteroll*.

Egen behörighet innebär att en befattningshavare ges tillgång till de funktioner i journalsystemet som är relevanta för befattningshavarens arbetsuppgifter, exempelvis förskrivning av läkemedel. Egen behörighet innebär också att befattningshavaren ges läs- och skrivbehörighet till de delar av journalsystemet (databaser) som är kopplade till den eller de vårdenheter där befattningshavaren är verksam.

Behörighet enligt *Tjänsteroll* innebär att en befattningshavare även ges läsbehörighet till andra databaser i journalsystemet. Befattningshavaren kan då ges tjänsterollen *Läsbehörighet VLL* som innebär åtkomstmöjlighet (läsbehörighet) till samtliga enheters vårddokumentation i Region Västerbotten, utom skyddade enheter. Befattningshavare kan tilldelas en annan läsbehörighet än Läsbehörighet VLL. Läsbehörighet till

personuppgifter hos skyddade enheter ges bara inom ramen för tilldelning av Egen behörighet.

Den modul som hanterar journalen i NCS Cross rubriceras *Vårddokumentation*. Modulen innehåller all dokumentation som finns om patienten i enlighet med 2 kap. 4 § 1 patientdatalagen. Det finns även andra moduler, till exempel *Vårdadministration* som innehåller uppgifter i enlighet med 2 kap. 4 § 2 patientdatalagen.

Läkarna tilldelas nästan alltid *Läsbehörighet VLL*. När det gäller sjuksköterskorna beställs ofta Läsbehörighet VLL, vilket innebär att en majoritet av sjuksköterskorna tilldelas denna läsbehörighet. Har personalen tilldelats skrivbehörighet i systemet innebär det att personalen också har läsbehörighet i det. Antalet befattningshavare som har *Läsbehörighet VLL* i NCS Cross är totalt 7 586. Av dessa är 2 290 läkare, 3 759 är sjuksköterskor, 124 är undersköterskor inklusive barnsköterskor och 956 är paramedicinare. Uppgifterna gäller för december 2019.

Begränsningar i åtkomst till uppgifter i NCS Cross
Det finns inga direkta hinder för att införa funktioner som begränsar läsbehörigheten och därmed åtkomsten i NCS Cross. Systemet möjliggör tilldelning av behörigheter som ger användare skilda åtkomstmöjligheter. Det går att göra på individnivå. Man kan även avgränsa åtkomsten till vissa enheter. Tekniskt är det exempelvis möjligt att exkludera BUP från åtkomstmöjligheter. Verksamhetscheferna kan begränsa åtkomsten och styra behörigheterna så att personalen på en enhet bara har åtkomst till uppgifter om vård och behandling på aktuell enhet och inte sådana uppgifter på andra enheter.

Inom NCS Cross 84 enheter finns följande sex skyddade enheter. 1) Enheten klinisk genetik, 2) Enheten barn- och ungdomshabiliteringen 3) Sektion barn- och ungdomshabiliteringen inom enheten barn- och ungdomsklinik Västerbotten 4) Sektion barnahus, inom enheten barn- och ungdomspsykiatri Västerbotten 5) Företagshälsovården 6) LSS-enheterna inom handikappverksamhet, Syn- och hörselhabiliteringen och Stöd och habilitering för vuxna samt sektionen myndighetsutövning i enheten Stöd och habilitering för vuxna.

Ett aktivt val för åtkomst krävs av användaren när patienten har spärrat sin vårddokumentation.

Sammanhållen journalföring
Hälso- och sjukvårdsnämnden har i huvudsak uppgett följande.

Behovs- och riskanalys
Mallen *Mall – Behovs- och riskanalys vid behörighetstilldelning* gäller också för den sammanhållna journalföringen. Behovsanalys som görs inför behörighetstilldelning inkluderar även analys för åtkomst inom ramen för sammanhållen journalföring.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Om en anställd har tilldelats läsbehörighet i den inre sekretessen innebär det att hen även tilldelats läsbehörighet för den sammanhållna journalföringen.

Åtkomstmöjligheter (läsbehörighet) till vårddokumentation i NCS Cross
Läsbehörigheten inom den sammanhållna journalföringen är densamma som för den inre sekretessen. Det innebär att personalen kan ta del av all vårddokumentation om samtliga patienter som finns i systemet för den sammanhållna journalföringen. Som grund till detta ligger medarbetaruppdragat.

Begränsningar i åtkomst till uppgifter i NCS Cross
De anställda måste göra aktiva val för att få tillgång till information i den sammanhålla journalföringen, det vill säga svara på frågan om patienten gett sitt samtycke alternativt ange att det föreligger nödläge för att kunna ta del av uppgifterna.

Dokumentation av åtkomsten (loggar)
Hälso- och sjukvårdsnämnden har uppgett bland annat följande.

Varje gång en användare går in i NCS Cross loggas aktiviteten. Sökningen på en patient kan göras på personnummer eller reservnummer. Enligt riktlinjerna ska systemet en gång per månad välja ut tio användare på en enhet. Vid en sådan loggkontroll visas alla patientjournaler som respektive användare öppnat för inloggning under den kontrollerade loggperioden samt alla aktiviteter som gjorts i vårdportalen: tid, aktivitet, personnummer,

patient, journal, information, personal, titel, placering, uppdragsgivare, syfte och datum.

I loggutdraget anges under rubriken *Uppdragsgivare* vid vilken enhet åtgärderna vidtagits, det vill säga vilken vårdenhets medarbetaruppdrag användaren använt vid inloggningen. Under rubriken *Journal* anges den databas som personalen hämtat uppgifter från, det vill säga vid vilken vårdenhets dokumentation användaren läser i.

Databasen kallad *Medicincentrum* innehåller vårddokumentation från två vårdenheter, dels Medicincentrum, dels Hjärtcentrum. Om exempelvis inloggning görs i databasen Medicincentrum av en läkare som arbetar på enheten Medicincentrum kommer det i loggutdraget anges Medicincentrum både under rubriken Uppdragsgivare och rubriken Journal. Om läkaren däremot arbetar på Hjärtcentrum kommer det i loggutdraget under rubriken Uppdragsgivare att anges Hjärtcentrum.

Loggposterna som genereras avser både den inre sekretessen och den sammanhållna journalföringen.

Hälso- och sjukvårdsnämnden har till Datainspektionen kommit in med loggutdrag med dokumentation av de åtkomster (loggar) som skapades med anledning av inspektionens granskning.

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 enligt 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 behandling av personuppgifter.

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

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

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

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

> Behörighet för personalens elektroniska åtkomst till uppgifter om patienter ska begränsas till vad befattningshavaren behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården. Däri ligger bl.a. att behörigheter ska följas upp och förändras eller inskränkas efter hand som ändringar i den enskilde befattningshavarens arbetsuppgifter ger anledning till det. Bestämmelsen motsvarar i princip 8 § vårdregisterlagen. Syftet med bestämmelsen är att inpränta skyldigheten för den ansvariga vårdgivaren att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver. Men det behövs inte bara behovsanalyser. Även riskanalyser måste göras där man tar hänsyn till olika slags risker som kan vara förknippade med en alltför vid tillgänglighet avseende vissa slags uppgifter. Skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter är exempel på kategorier som kan kräva särskilda riskbedömningar.
>
> Generellt sett kan sägas att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas. Avgörande för beslut om behörighet för t.ex. olika kategorier av hälso- och sjukvårdspersonal till elektronisk åtkomst till uppgifter i patientjournaler bör vara att behörigheten ska begränsas till vad befattningshavaren behöver för ändamålet en god och säker patientvård. En mer vidsträckt eller grovmaskig behörighetstilldelning bör – även om den skulle ha poänger utifrån effektivitetssynpunkt - anses som en obefogad spridning av journaluppgifter inom en verksamhet och bör som sådan inte accepteras.
>
> Vidare bör uppgifter lagras i olika skikt så att mer känsliga uppgifter kräver aktiva val eller annars inte är lika enkelt åtkomliga för personalen som mindre känsliga uppgifter. När det gäller personal som arbetar med verksamhetsuppföljning, statistikframställning, central ekonomiadministration och liknande verksamhet som inte är individorienterad torde det för flertalet befattningshavare räcka med tillgång till uppgifter som endast indirekt kan härledas till enskilda patienter. Elektronisk åtkomst till kodnycklar, personnummer och andra uppgifter som

direkt pekar ut enskilda patienter bör på detta område kunna vara starkt begränsad till enstaka personer.

Inre sekretess
Bestämmelserna i 4 kap. patientdatalagen rör den inre sekretessen, 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 § 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 således även i system för sammanhållen journalföring.

Dokumentation av åtkomst (loggar)

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

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

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

Datainspektionens bedömning

Personuppgiftsansvariges ansvar för säkerheten

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

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

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

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

Det är dessutom frågan om känsliga personuppgifter. Uppgifterna rör 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 kan 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 för åtkomst till personuppgifter om patienter. Såväl behoven som riskerna måste bedömas utifrån de uppgifter som behöver behandlas i verksamheten, vilka processer det är frågan om och vilka risker för den enskildes integritet som föreligger.

Bedömningarna av riskerna behöver ske utifrån organisationsnivå, där exempelvis en viss verksamhetsdel eller arbetsuppgift kan vara mer integritetskänslig än en annan, men också utifrån individnivå, om det är frågan om särskilda omständigheter som behöver beaktas, såsom exempelvis att det är fråga om skyddade personuppgifter eller uppgifter om allmänt kända 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 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.

Hälso- och sjukvårdsnämndens arbete med behovs- och riskanalys
När Datainspektionen har efterfrågat en dokumenterad behovs- och riskanalys har Hälso- och sjukvårdsnämnden uppgett att nämnden har gjort en behovs- och riskanalys, men enbart utifrån verksamhetsperspektivet, inte utifrån integritetsperspektivet. Datainspektionen vill därför framhålla att det inte räcker med att göra en behovsanalys. Som tidigare har beskrivits, framgår av artikel 32 i dataskyddsförordningen och Socialstyrelsens föreskrifter, krävs att Hälso- och sjukvårdsnämnden även måste göra en riskanalys där nämnden beaktar olika risker som kan vara förknippade med en alltför vid tillgänglighet av olika typer av personuppgifter om patienter för att sedan väga verksamhetens behov mot riskerna för den enskildes integritet. Dessutom måste den personuppgiftsansvarige, enligt i dataskyddsförordningens krav på ansvarsskyldighet enligt artikel 5, kunna visa att man bland annat vidtagit lämpliga organisatoriska åtgärder.

Hälso- och sjukvårdsnämnden har hänvisat till att verksamhetscheferna ansvarar för att en behovs- och riskanalys görs. Datainspektionen vill därför även framhålla att nämnden som personuppgiftsansvarig inte kan frånsäga sig ansvaret för analysen och utifrån den vidta lämpliga tekniska och organisatoriska åtgärder. Det innebär att nämnden borde ha säkerställt

genomförandet av en behovs- och riskanalys enligt 4 kap. 2 § HSLF-FS 2016:40 och dokumenterat den.

En behovs- och riskanalys ska göras på strategisk nivå
Hälso- och sjukvårdsnämnden har uppgett att nämnden efter Datainspektionens tidigare föreläggande tagit fram dokument för att ge verksamhetscheferna verktyg vid tilldelning av behörigheter. Nämnden har hänvisat till dokumenten *Riktlinje för informationssäkerhet – förvaltning och drift* och mallen *Mall- Behovs- och riskanalys vid behörighetstilldelning*

Datainspektionen konstaterar att riktlinjerna och mallen handlar om tilldelning av behörigheter och att dokumenten utgår från att en behovs- och riskanalys ska göras i anslutning till den faktiska tilldelningen. (I riktlinjerna anges exempelvis att en riskanalys ska göras för att belysa olika slags risker förknippade med för omfattande tillgänglighet och att dokumentation av genomförd behovs- och riskanalys ska arkiveras på enheten. I mallen hänvisas till patientdatalagen och att beslut om tilldelning ska föregås av en behovs- och riskanalys). Datainspektionen vill därför understryka att en behovs- och riskanalys ska fastställa en övergripande behörighetsstruktur som i sin tur ska ligga till grund för den behörighetstilldelning som ska göras för varje enskild befattningshavare. Den strategiska analys som ska vidtas är alltså vidare än den analys som görs vid själva tilldelningen av behörigheterna. En riktigt genomförd behovs- och riskanalys är en förutsättning för en korrekt tilldelning av behörigheter.

Hälso- och sjukvårdsnämnden har dessutom hänvisat till dokumenten *Användarprofiler* som exempel på genomförda analyser vid faktiska behörighetstilldelningar. Datainspektionen konstaterar även i detta fall att det inte är frågan om någon behovs- och riskanalys.

Datainspektionens sammanfattande bedömning
Såsom angivits ovan ska i en behovs- och riskanalys såväl behoven som riskerna bedömas utifrån de uppgifter som behöver behandlas i verksamheten, vilka processer det är frågan om och vilka risker för den enskildes integritet som föreligger på såväl organisatorisk som individuell nivå. Det är således fråga om en strategisk analys på strategisk nivå, som ska ge underlag för en behörighetsstruktur som är anpassad till verksamheterna. Den bör mynna ut i instruktioner om behörighetstilldelning men det är inte instruktionerna till den som tilldelar behörigheter som är analysen.

Sammanfattningsvis konstaterar Datainspektionen att Hälso- och sjukvårdsnämnden inte har kommit in med någon dokumenterad behovs- och riskanalys. Nämnden har dessutom uppgett att den inte sett någon dokumenterad sådan. Hälso- och sjukvårdsnämnden har därmed inte kunnat visa att nämnden genomfört en behovs- och riskanalys i den mening som avses i 4 kap. 2 § HSLF-FS 2016:40, vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen. Detta innebär att Hälso- och sjukvårdsnämnden inte har vidtagit lämpliga organisatoriska åtgärder i enlighet med artikel 5.1 f och artikel 31.1 och 31.2 för att kunna säkerställa och, i enlighet med artikel 5.2, kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Som har redovisats ovan kan en vårdgivare ha ett berättigat intresse av att ha en omfattande behandling av uppgifter om enskildas hälsa. 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.

Att Hälso- och sjukvårdsnämndens tilldelning av behörigheter inte har föregåtts av en behovs- och riskanalys innebär att nämnden inte har analyserat användarnas behov av åtkomst till uppgifterna, riskerna som denna åtkomst kan medföra och därmed inte heller identifierat vilken åtkomst som är befogad för användarna utifrån en sådan analys. Nämnden har därmed inte använt sig av lämpliga åtgärder i enlighet med artikel 32 i dataskyddsförordnigen, för att begränsa användarnas åtkomst till patienternas personuppgifter i journalsystemet.

Detta har i sin tur inneburit att det funnits en risk för obehörig åtkomst och obefogad spridning av personuppgifter dels inom ramen för den inre sekretessen, dels inom ramen för den sammanhållna journalföringen.

I ärendet har framkommit att antalet registrerade patienter i NCS Cross inom den inre sekretessen är drygt 650 000 och inom ramen för sammanhållen journalföring drygt 665 000. I ärendet har även framkommit att det finns cirka 10 000 anställda inom regionen och att drygt 7 500 befattningshavare har tilldelats *Läsbehörighet VLL* i NCS Cross. Denna behörighet ger åtkomstmöjlighet (läsbehörighet) till samtliga enheters vårddokumentation i Region Västerbotten, utom den som upprättats på skyddade enheter. Det är av totalt 84 enheter frågan om sex skyddade enheter. Sammanfattningsvis konstaterar Datainspektionen att det innebär att merparten av de anställda har haft faktiska åtkomstmöjligheter till vårddokumentationen om merparten av patienterna i NCS Cross.

Vårddokumentation innebär att det är fråga om hälsouppgifter, så kallade känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen. Genom att den personuppgiftsansvarige endast begränsat åtkomsten av behörigheter i NCS Cross till uppgifter som finns på skyddade enheter har det alltså 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.

Hälso- och sjukvårdsnämnden har uppgett att ett *aktivt val* för åtkomst krävs av användaren när patienten har spärrat sin vårddokumentation. Datainspektionen vill framhålla att ett aktivt val är en integritetshöjande åtgärd men inte 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 möjlighet till åtkomst till dem. Av förarbetena till patientdatalagen, prop. 2007/08:126, s. 149, framgår att uppgifter dessutom behöver lagras i olika skikt så att mer känsliga uppgifter kräver aktiva val eller annars inte är lika enkelt åtkomliga för personalen som mindre känsliga uppgifter.

Mot denna bakgrund kan Datainspektionen konstatera att Hälso- och sjukvårdsnämnden har behandlat personuppgifter i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen genom att nämnden inte har begränsat användarnas behörigheter för åtkomst till journalsystemet NCS Cross till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Detta innebär att Hälso- och sjukvårdsnämnden inte har vidtagit åtgärder för att kunna säkerställa och, i enlighet med artikel 5.2 i dataskyddsförordningen, kunna visa en lämplig säkerhet för personuppgifterna.

Dokumentation av åtkomsten (loggar)

Utifrån de loggar som skapades med anledning av inspektionens granskningar tillsammans med den information som nämnden lämnat om rubriceringen i loggutdragen konstaterar Datainspektionen att det av loggutdragen framgår följande:

- under rubriken *Aktivitet,* vilka åtgärder som har vidtagits med uppgifter om en patient, exempelvis att ”läsa”.
- under rubrikerna *Journal* vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits
- under rubriken *Tid* vid vilken tidpunkt åtgärderna vidtagits
- under rubrikerna *Patient* och *Personal* användarens och patientens identitet.

Datainspektionen konstaterar att dokumentationen av åtkomsten (loggarna) i NCS Cross är i överensstämmelse med de krav som ställs i 4 kap. 9 § HSLF-

FS 2016:40 och att Hälso- och sjukvårdsnämnden därmed i denna del har vidtagit lämpliga tekniska åtgärder enligt artikel 32 i dataskyddsförordningen.

Val av ingripande

Rättslig reglering

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

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

För myndigheter får enligt artikel 83.7 i dataskyddsförordningen nationella regler ange att myndigheter kan påföras administrativa sanktionsavgifter. Enligt 6 kap. 2 § dataskyddslagen kan sanktionsavgifter beslutas för myndigheter, men till högst 5 000 000 kronor alternativt 10 000 000 kronor beroende på om överträdelsen avser artiklar som omfattas av artikel 83.4 eller 83.5 i dataskyddsförordningen.

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

Föreläggande

Hälso- och sjukvården har 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.

Datainspektionens tillsyn har visat att Hälso- och sjukvårdsnämnden har underlåtit att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i journalsystemet NCS Cross genom att inte följa de krav som ställs i patientdatalagen och Socialstyrelsens föreskrifter och därigenom inte uppfyller kraven i artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen. Underlåtenheten omfattar såväl den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen förelägger därför, med stöd av 58.2 d i dataskyddsförordningen, Hälso- och sjukvårdsnämnden att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemet NCS Cross inom ramen för såväl den inre sekretessen som inom ramen för den sammanhållna journalföringen. Hälso- och sjukvårdsnämnden ska vidare, med stöd av behovs- och riskanalysen, tilldela varje användare individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Sanktionsavgift

Datainspektionen kan konstatera att överträdelserna i grunden avser Hälso- och sjukvårdsnämndens skyldighet att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifter enligt 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 personuppgifter om patienter i huvudjournalsystemet hör till kärnan i en vårdgivares verksamhet, att behandlingen omfattar många patienter och möjligheten till åtkomst avser en stor andel av de anställda. I detta fall rör det sig om omkring 650 000 antal patienter inom ramen för den inre sekretessen och omkring 665 000 patienter inom ramen för den sammanhållna journalföringen. Av sammanlagt 84 vårdenheter finns begränsningar i åtkomstmöjligheterna till enbart sex enheter, de så kallade skyddade enheterna.

Datainspektionen kan dessutom konstatera att Hälso- och sjukvårdsnämnden inte följt Datainspektionens beslut från den 27 mars 2015. I beslutet förelades dåvarande Landstingsstyrelsen i Västerbottens läns landsting att genomföra en dokumenterad behovs- och riskanalys enligt det dåvarande kravet i 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14, vilket motsvarar nuvarande bestämmelse i 4 kap. 2 § HSLF-FS 2016:40. Detta är en försvårande omständighet, enligt artikel 83.2 e i dataskyddsförordningen.

De brister som nu konstaterats har således varit kända för Hälso- och sjukvårdsnämnden under flera års tid vilket innebär att agerandet skett uppsåtligt och därmed bedöms som allvarligare. Datainspektionen konstaterar också att Hälso- och sjukvårdsnämndens uppgift om att de analyser som därefter gjorts enbart utgår från verksamhetsperspektivet, vilket är särskilt allvarligt.

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

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

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

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

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

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer Datainspektionen den administrativa sanktionsavgiften för Hälso- och sjukvårdsnämnden 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 även chefsjuristen Hans-Olof Lindblom, enhetscheferna Katarina Tullstedt och Malin Blixt samt juristen Caroline Cruz Julander medverkat.

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

Bilaga: Hur man betalar sanktionsavgift

Kopia för kännedom till Dataskyddsombudet

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag 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.