Aleris Sjukvård AB
c/o Aleris Specialistvård Sabbatsberg
Box 6401
113 82 Stockholm
Stockholms län

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

Innehållsförteckning

Datainspektionens beslut

Datainspektionen har vid granskning den 8 april 2019 konstaterat att Aleris Sjukvård AB behandlar personuppgifter i strid med artikel 5.1 f och 5.2 samt artikel 32.1 och 32.2 i dataskyddsförordningen[1] genom att

1. Aleris Sjukvård AB inte har genomfört en en behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemet TakeCare, i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) och 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Det innebär att Aleris Sjukvård AB inte har vidtagit lämpliga organisatoriska åtgärder för att kunna säkerställa och kunna visa att behandlingen av personuppgifterna har en säkerhet som är lämplig i förhållande till riskerna.

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

Datainspektionen beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen att Aleris Sjukvård AB, för överträdelse av artikel 5.1 f och 5.2 samt artikel 32.1 och 32.2 i dataskyddsförordningen, ska betala en administrativ sanktionsavgift på 15 000 000 (femton miljoner) kronor.

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Aleris Sjukvård AB att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemet TakeCare och att därefter, med stöd av behovs- och riskanalysen, tilldela varje användare

[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).

individuell behörighet för åtkomst till personuppgifter som begränsas till enbart vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, i enlighet med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen, 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40.

Redogörelse för tillsynsärendet

Datainspektionens tillsyn inleddes genom en tillsynsskrivelse den 22 mars 2019 och har skett såväl skriftligen som genom inspektion på plats den 8 april 2019. Tillsynen har avsett kontroll av om Aleris Sjukvård AB:s (nedan kallat Aleris) beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Tillsynen har även omfattat hur Aleris har tilldelat behörigheter för åtkomst till huvudjournalsystemet TakeCare, och vilka åtkomstmöjligheter de tilldelade behörigheterna ger inom såväl ramen för den inre sekretessen enligt 4 kap. patientdatalagen, som den sammanhållna journalföringen enligt 6 kap. patientdatalagen. Utöver detta har Datainspektionen granskat vilken dokumentation av åtkomst (loggar) som finns i journalsystemet.

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

Inspektionen är en av flera inspektioner inom ramen för ett egeninitierat tillsynsprojekt hos Datainspektionen, där bl.a. Karolinska Universitetssjukhuset har ingått. Med anledning av vad som framkommit om Aleris uppfattning kring de tekniska möjligheterna att begränsa läsbehörigheten för sina användare i TakeCare, ombads Aleris att särskilt yttra sig över ett yttrande från Karolinska Universitetssjukhuset, som också använder TakeCare, där de tekniska möjligheterna rörande TakeCare beskrevs.

Vad som framkommit i ärendet

Aleris har i huvudsak uppgett följande.

Personuppgiftsansvaret
Aleris är vårdgivare och personuppgiftsansvarig.

Verksamheten
Aleris ägarstruktur har ändrats efter att Datainspektionens granskning inleddes. Aleris nya ägarstruktur visas i Aleris komplettering från den 16 november 2020. Av kompletteringen framgår bland annat följande.

Aleris ingår, sedan den 1 oktober 2019, i det nybildade koncernmoderbolaget, Aleris Group AB (org.nr. 559210-7550), och är ett dotterbolag till Aleris Healthcare AB (org.nr. 556598–6782). Aleris Group AB ägs av Triton.

Koncernomsättningen för Aleris Group AB uppgick till 1 215 385 000 kronor mellan den 1 oktober 2019 och den 31 december 2019. Eftersom Aleris Group AB bildades i samband med ägarbytet då Aleris Healthcare AB med dotterbolag förvärvades finns endast omsättningssiffror att tillgå denna period.

Årsomsättningen för Aleris Healthcare AB uppgick till 30 223 866 kronor under 2019.

Journalsystem
Aleris använder sedan den 28 maj 2012 TakeCare som huvudjournalsystem för den inre sekretessen och inom ramen för den sammanhållna journalföringen.

Federation Samverkan TakeCare (FSTC) är beställare av journalsystemet TakeCare och CompuGroup Medical (CGM) är leverantör av journalsystemet och ansvarar för de funktioner som systemet har för att styra behörigheter.

Alla funktioner i journalsystemet är skapade av CGM, men det är Aleris som väljer vilka funktioner som en viss personalkategori ska ha tillgång till bland de funktioner som finns inlagda. Aleris har inga tekniska möjligheter att göra ändringar i TakeCare eftersom Aleris inte har någon rådighet över journalsystemet. Aleris är endast användare av systemet.

Aleris har inte kunnat ställa några krav på CGM vid upphandlingen av journalsystemet. Bolaget har till exempel påpekat att det funnits problem med journalsystemet bestående i, såvitt avser behörighetstilldelningen, att

systemet inte kan separera läs- och utskriftbehörigheter för en läsfunktion. CGM har inte varit intresserade av att ändra detta trots synpunkter från Aleris.

Det är FSTC som kan beställa ändringar av funktionerna och det är sedan upp till CGM om de vill utföra ändringarna eller inte. Aleris har en representant i FSTC som kan framföra Aleris önskemål. Aleris har dock inte fått något gehör för bolagets synpunkter.

Antal patienter och anställda
Aleris hade 796 350 unika patienter i TakeCare per den 20 maj 2019. Hur många av dessa som var avlidna gick dock inte att ta fram.

Under maj 2019 fanns det 1 058 aktiva användare, 807 aktiva konton och 63 enheter i journalsystemet TakeCare. Antalet aktiva användare (dvs. anställda och konsulter som kan ha tillgång till TakeCare) har beräknats genom att räkna antalet aktiva AD-konton på relevanta kostnadsställen.

Inre sekretess

Aleris har i huvudsak uppgett följande.

Behovs- och riskanalys
Aleris har uppgett att behovs- och riskanalyser riktade mot TakeCare utförs av ett utsett riskanalysteam i syfte att se över gällande behörighetstilldelning och eventuellt bestämma nya villkor för behörighetstilldelning. Behörigheter begränsas alltid till vad som behövs för att medarbetaren ska kunna utföra sitt arbete och medverka till säker vård. Behovet kontra risken för otillbörlig åtkomst avvägs alltid mot varandra innan behörigheter ges. Generella behörighetsprofiler finns, vid behov tilldelas specifika behörigheter. De senare granskas särskilt vid efterföljande analys av utsett riskanalysteam. Vad som särskilt beaktas är vilka risker som kan uppstå om en medarbetare har för bred behörighet kontra för låg behörighet och därmed inte tillgång till relevant patientinformation. Resultatet från behovs- och riskanalysen ligger sedan till grund för val av den behörighetsprofil som används vid tilldelning av behörigheter inom Aleris.

Behörighet till TakeCare beställs av ansvarig chef vilket framgår av dokumentet, ”Behörighetsstyrning TakeCare”. Av dokumentet framgår även att behörigheten är personlig och att dess omfattning baseras på

användarens yrkesroll och organisatoriska hemvist. Vidare framgår att vårdgivaren ska se till att behörigheten för åtkomst till patientuppgifter begränsas till vad en användare behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården.

Aleris har ett dokument som benämns ”Behovs- och riskanalys-TakeCare”. Dokumentet har sett ut som det gör i dag sedan den 28 maj 2012 då TakeCare infördes och gäller både för den inre sekretessen och inom ramen för den sammanhållna journalföringen. Av dokumentet framgår de olika profilerna, så kallade behörighetsgrupper. Dokumentet visar bland annat läsrättigheterna samt skrivrättigheterna för respektive behörighetsgrupp. Alla profiler förutom tekniker har tilldelats läsbehörighet till uppgifterna i TakeCare. Behörigheten för varje grupp har motiverats. Läkarna ska till exempel kunna utföra sina arbetsuppgifter och ansvarar för patientinformation, medan systemförvaltaren måste kunna felsöka, administrera och lägga upp användare, system och lokala administratörer. Under rubriken ”Risk vid begränsad åtkomst” anges att användaren ”inte kan utföra sina arbetsuppgifter fullt ut”. Denna motivering anges för samtliga profiler (förutom de lokala administratörerna där motiveringen är ”Kan ej hantera behörigheter samt genomföra korrigeringsåtgärder”). Under rubriken ”Risk vid omfattande åtkomst” anges bland annat att ”Det finns en risk för röjande av patientinformation”. Liknande motivering anges för alla profiler.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter
Aleris har uppgett att det är systemförvaltaren som har den högsta behörighetsnivån, dvs. full behörighet, i TakeCare. Den lokala administratören har behörighet till sin egen enhet och är den som tilldelar behörigheterna inom enheten. Vilken behörighet en administratör lägger på en användare beror på den verksamhet användaren tillhör och på användarens arbetsuppgifter. Samtliga användare får det ”minsta de ska ha för att klara sig” när det gäller åtkomstmöjligheter. Åtkomsten kan dock utökas vid behov. Det finns grundprofiler för exempelvis undersköterskor, som får den behörighet som behövs för att de ska kunna utföra sina arbetsuppgifter. Om chefen bedömer att undersköterskorna behöver en utökad behörighet ser de lokala administratörerna till att den behörigheten ”läggs på” grundprofilen. Behövs inte den utökade behörigheten kan den tas bort från grundprofilen.

Aleris har uppgett att samtliga konton inom Aleris är individuella och att behörigheterna tilldelas utifrån dokumentet, ”Behovs- och riskanalys-TakeCare”. Som tidigare nämnts framgår det av dokumentet att alla yrkesprofiler förutom tekniker har tilldelats läsbehörighet till uppgifterna i TakeCare.

Aleris har emellertid uppgett att alla användare har olika läsbehörighet i journalsystemet utifrån vilka systemfunktioner som de har tillgång till av Aleris. Enligt Aleris går det att styra bort åtkomstmöjligheter till TakeCare genom att ge olika personal behörighet till olika funktioner. Varje personalkategori får endast behörighet till de funktioner som de behöver för att kunna utföra sitt arbete. Tekniker har exempelvis begränsad behörighet beroende på vad de ska göra i systemet. De får endast läsbehörighet om de har behov av det i sitt arbete. Ett annat exempel gäller användare som bara kommer att sitta i kassan och som därmed inte behöver ha en läsbehörighet. Det finns ingen personal som bara har till uppgift att hantera kassan i nuläget.

Genom att välja olika funktioner för olika användare görs det en skillnad i vad olika användare kan göra i systemet, t.ex. såvitt avser vidimera, signera, etc. Totalt finns det 640 olika systemfunktioner som det går att välja att ge behörighet till. Bland dessa funktioner har Aleris valt ut de funktioner som olika personalkategorier behöver ha tillgång till för att bedriva ett säkert patientarbete. Av dokumentet ”Profiler och behörigheter” framgår de olika behörigheter som respektive personalkategori har tilldelats i TakeCare, t.ex. diktera ljudfiler, läsa aktiviteter, signera, läsa akutuppgifter, läsa journaltext, vidimering, läsa remiss, administrera läkemedelsordination, läsa skannade dokument och godkänna vårdtillfällen. Av dokumentet framgår bland annat att samtliga profiler dvs. läkare, sjuksköterskor, undersköterskor, paramedicinare, sekreterare, ”administrativt”, studerande och ”Receptionist Rehab” har behörighet att ”läsa journaltext” och att alla förutom ”Receptionist Rehab” har behörighet att ”läsa skannade dokument” i TakeCare. Det framgår även att endast läkare har behörighet att ”läsa akutuppgifter” och att alla profiler förutom undersköterska och ”administrativt” kan ”läsa diagnoser” i TakeCare.

Aleris har uppgett att utgångspunkten är att en användare på en enhet bara har läsbehörighet till de patientjournaler som finns på enheten. En användare som behöver läsa journalanteckningar från en annan enhet måste

göra ett aktivt val i systemet. Med aktiva val menas att användaren får göra ett antal ”klick” och välja aktuell enhet (denna funktion kallas för journalfilter). Behörighet att kunna utnyttja journalfiltret ges till de användare som har behov av detta för att kunna utföra sitt arbete. Användaren kan aldrig av misstag läsa en patientjournal från en annan enhet.

Aleris har uppgett att det finns funktioner i TakeCare för att en vårdgivare ska kunna ”isolera” en vårdenhet och därigenom ”stänga ute” andra vårdgivares och vårdenheters åtkomstmöjligheter till enhetens vårddokumentation, så kallade skyddade enheter. Aleris bedriver dock inte någon verksamhet som kräver skyddade enheter och har därför inte använt sig av denna funktion.

Sammanhållen journalföring

Aleris har i huvudsak uppgett följande.

Behovs- och riskanalys

Dokumentet ”Behovs- och riskanalys- TakeCare” gäller även för systemet för sammanhållen journalföring.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter

Behörighetstilldelningen sker på samma sätt som inom ramen för den inre sekretessen.

Inom ramen för sammanhållen journalföring i TakeCare kan användarna ta del av all vårddokumentation hos andra vårdgivare som ingår i systemet. Användaren kan initialt se om en patient är aktuell hos andra vårdgivare, men inte vilka. För att kunna se vilka dessa vårdgivare är måste användaren klicka vidare i systemet, dvs. göra aktiva val. Användaren måste därefter klicka i rutan ”samtycke” eller ”nödåtkomst” för att få åtkomst till den specifika vårdgivarens journaler.

Aleris har anfört följande med anledning av att Karolinska Universitetssjukhuset i ett yttrande har uppgett att det finns möjligheter att begränsa åtkomsten i TakeCare.

Det finns en funktion för att ”isolera” en vårdenhet och därigenom stänga ute andra vårdgivares och vårdenheters åtkomstmöjligheter (så kallade

skyddade enheter). En vårdgivare kan således ur ett tekniskt perspektiv begränsa andra vårdgivares tillgång till den egna vårddokumentationen. Aleris har dock bedömt att bolaget inte bedriver någon verksamhet som behöver spärras och att det är mer patientsäkert att låta patientuppgifterna vid Aleris enheter vara tillgängliga för andra vårdgivare. Enligt Aleris är det dessutom inte tillåtet att implementera sådana begränsningar om en vårdgivare använder journalsystemet TakeCare och samtidigt ingår i sammanhållen journalföring. Detta efter beslut från Region Stockholm. Det innebär att alla användare hos Aleris har åtkomst till alla patientuppgifter hos de andra vårdgivarna i TakeCare, frånsett när patienterna har begärt att få sina uppgifter spärrade (en så kallad vårdgivarspärr).

Enligt Aleris är det, ur ett patientsäkerhetsperspektiv, inte praktiskt möjligt att välja bort enstaka vårdgivares tillgång till den egna vårddokumentationen i TakeCare (med undantag för skyddade enheter). Antingen är vårdgivaren med i systemet för sammanhållen journalföring eller inte. Det går inte att begränsa tillgången för behöriga personer till andra vårdgivares information och samtidigt på ett meningsfullt sätt delta i sammanhållen journalföring. Enligt Aleris är det inte möjligt att i förväg avgöra vilka uppgifter som i ett visst fall kan få betydelse för en patientsäker vård. Aleris har därför beslutat att inte aktivt spärra andra vårdgivares journaler. Däremot kan, såsom nämnts, en vårdgivare själv spärra andra vårdgivares tillgång i TakeCare där dessa har gjort bedömningen att deras patienters journaler inte ska vara tillgängliga för andra vårdgivare. Dessa enheter är i TakeCare markerade med en asterisk. Det har på så vis redan gjorts ett urval av vårdenheter som Aleris personal inte har tillgång till.

Dokumentation av åtkomsten (loggar)

Av Aleris loggdokumentation framgår bland annat följande: användarens och patientens identitet, vårdenhet, datum, klockslag, uppgift om att användaren har dokumenterat i journalen under de senaste 18 månaderna samt uppgift om att patienten har haft kontakt med vårdenheten under de senaste 18 månaderna.

Aleris har möjlighet att göra riktade loggkontroller. Det innebär att Aleris kan se exakt vad en användare har gjort i systemet. Om patienten eller Aleris misstänker dataintrång kan Aleris även göra en fördjupad loggkontroll.

Även alla aktiviteter som sker inom ramen för sammanhållen journalföring loggas i systemet. Det innebär också att alla aktiva val loggas i systemet. Om användaren exempelvis valt ”samtycke” eller ”nödåtkomst”, för att kunna ta del av en patients uppgifter hos en annan vårdgivare, kommer detta att framgå av loggdokumentationen.

Aleris yttrande över Datainspektionens skrivelse

Aleris har i synpunkter på skrivelsen *Slutlig kommunicering inför beslut* som inkom till Datainspektionen den 20 mars 2020 uppgett bland annat följande. Datainspektionen bör beakta siffrorna för den ekonomiska enheten där de påstådda bristerna ägt rum, det vill säga Aleris Sjukvård AB.

Aleris har aktivt verkat för att kontinuerligt stärka den inre och yttre sekretessen, inbegripet funktionaliteten i TakeCare. Då Aleris vidtagit adekvata åtgärder för att, genom FSTC, stärka integriteten inom TakeCare bör faktiska brister i TakeCare inte bedömas ligga Aleris till last.

Motivering av beslut

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 ska den personuppgiftsansvarige och personuppgiftsbiträdet 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 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, se 1 kap. 1 § patientdatalagen.

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

Krav på att göra en 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 till tillgång till personuppgifter som finns elektroniskt tillgängliga i en vårdgivares organisation.

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

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

Sammanhållen journalföring
Bestämmelserna i 6 kap. patientdatalagen rör sammanhållen journalföring, vilket innebär att en vårdgivare – under de villkor som anges i 2 § samma kapitel i den lagen – får ha direktåtkomst till personuppgifter som behandlas av andra vårdgivare för ändamål som rör vårddokumentation. Tillgången till information sker genom att en vårdgivare gör de uppgifter om en patient som vårdgivaren registrerar om patienten tillgängliga för andra vårdgivare som deltar i det sammanhållna journalföringssystemet (se prop. 2007/08:126 s. 247).

Av 6 kap. 7 § patientdatalagen följer att bestämmelserna i 4 kap. 2 och 3 §§ - även gäller för behörighetstilldelning och åtkomstkontroll vid sammanhållen journalföring. Kravet på att vårdgivaren ska utföra en behovs- och riskanalys innan tilldelning av behörigheter i systemet sker, gäller således även i system för sammanhållen journalföring.

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

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

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

Datainspektionens bedömning

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

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

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

Hälso- och sjukvården har ett 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 uppgiftssamlingarnas storlek som hur många som delar information med varandra har ökat väsentligt. Denna ökning innebär samtidigt att kraven ökar på den personuppgiftsansvarige, eftersom bedömningen av 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 av dessa personer och att uppgifterna 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 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 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 frågan om skyddade personuppgifter, allmänt kända personer eller på annat sätt särskilt utsatta personer. Även storleken på systemet påverkar riskbedömningen. Av förarbetena till patientdatalagen framgår att ju mer omfattande ett informationssystem är, desto större mängd olika behörighetsnivåer måste det finnas (prop. 2007/08:126 s. 149). Det är således frågan om en strategisk analys på strategisk nivå, som ska ge en behörighetsstruktur som är anpassad till verksamheten och denna ska hållas uppdaterad.

Regleringen ställer sammanfattningsvis krav på att riskanalysen identifierar

- olika kategorier av uppgifter,

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

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

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

Riskanalysen ska också omfatta en bedömning av hur sannolik och allvarlig risken för de registrerades rättigheter och friheter är med utgångspunkt i behandlingens art, omfattning, sammanhang och ändamål (skäl 76).

Det är således genom behovs- och riskanalysen som den personuppgiftsansvarige tar reda på vem som behöver åtkomst, vilka uppgifter åtkomstmöjligheten ska omfatta, vid vilka tidpunkter och i vilka sammanhang åtkomsten behövs, och samtidigt analyserar vilka risker för den enskildes fri- och rättigheter som behandlingen kan leda till. Resultatet ska sedan leda till de tekniska och organisatoriska åtgärder som behövs för att säkerställa att 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.

Aleris har uppgett att behörigheterna tilldelas utifrån dokumentet, ”Behovs- och riskanalys-TakeCare”. Av dokumentet framgår att alla behörighetsprofiler förutom tekniker har tilldelats läsbehörighet i systemet, och att risken vid begränsad åtkomst är att användaren inte kan utföra sina arbetsuppgifter fullt ut. Denna motivering anges för samtliga användare. Vidare anges att den enda risken vid omfattande åtkomst är att användaren ser information som han/hon inte har rätt att se vilket kan innebära röjande av patientinformation. Liknande motivering anges för alla profiler. Det innebär att Aleris gör samma bedömning för alla profiler oavsett användarens arbetsuppgift och behov.

Datainspektionen kan konstatera att dokumentet, ”Behovs- och riskanalys-TakeCare” inte innehåller någon analys av de olika profilernas behov av åtkomst till patienternas uppgifter. Aleris har endast uppgett vad respektive profil ”måste kunna utföra” i journalsystemet och alltså inte analyserat vilken information som det är frågan om eller hur behoven ser ut i de olika verksamhetsdelarna och för olika yrkesroller. Dokumentet saknar även en analys av riskerna för den enskildes fri- och rättigheter som en alltför vid behörighet kan medföra. Behovs- och riskanalysen måste ske på en strategisk nivå som ska ge en behörighetsstruktur som är anpassad till verksamheten.

Informationen i dokumentet ”Behovs- och riskanalys- TakeCare” är alltför bristfällig i förhållande till den information som krävs för att en korrekt behovs- och riskanalys ska kunna utföras. 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 såväl på organisatorisk som individuell nivå.

Aleris har i sin 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 Aleris behandling av personuppgifter i TakeCare. Det saknas också särskilda riskbedömningar utifrån om det förekommer till exempel 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 en bedömning av hur sannolik och allvarlig risken för de registrerades rättigheter och friheter bedöms vara.

Datainspektionen kan mot bakgrund av ovanstående konstatera att dokumentet ”Behovs- och riskanalys- TakeCare” inte uppfyller de krav som ställs på en behovs- och riskanalys och att Aleris inte har kunnat visa att bolaget har 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 enligt 4 kap. patientdatalagen eller inom ramen för den sammanhållna journalföringen enligt 6 kap. 7 § patientdatalagen. Det innebär att Aleris inte har vidtagit lämpliga organisatoriska åtgärder i enlighet med artikel 5.1 f och artikel 32.1 och 32.2 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.

Aleris har uppgett att det finns begränsningar vad gäller användarnas åtkomstmöjligheter i TakeCare då bolaget genom att välja olika funktioner för olika användare kan styra bort användarnas åtkomstmöjligheter i journalsystemet.

Enligt Aleris har alla användare olika läsbehörighet i journalsystemet beroende på vilka systemfunktioner som de har tillgång till. Av dokumentet ”Behovs- och riskanalys- TakeCare” framgår emellertid att alla yrkesprofiler förutom tekniker har tilldelats läsbehörighet till uppgifterna i TakeCare. Vidare framgår av dokumentet ”Profiler och Behörigheter” att samtliga yrkesprofiler, dvs. läkare, sjuksköterskor, undersköterskor, paramedicinare, sekreterare, administrativt, studerande och receptionist Rehab har behörighet att ”läsa journaltext”. Det innebär att i stort sätt alla yrkesprofiler har åtkomst till Aleris personuppgifter om patienter i TakeCare. Den begränsning som har införts är att olika yrkesprofiler har olika läsbehörigheter, till exempel kan läkare, sjuksköterska, paramedicinare ”läsa diagnoser” eller ”läsa recept” medan andra yrkesprofiler, till exempel ”administrativt” inte har de behörigheterna. Det framgår även att läkare är de enda som har behörighet att ”läsa akutuppgifter”.

Datainspektionen anser att det är positivt att Aleris har tilldelat olika läsbehörigheter i systemet, men att det inte är tillräckligt eftersom samtliga yrkesprofiler fortfarande har åtkomst till journaltexterna i TakeCare. Dessutom är indelningen grov då det enbart är en indelning utifrån yrkeskategorier och inte utifrån till exempel vilken organisatorisk tillhörighet, vilka arbetsuppgifter användaren har eller vilka patienters personuppgifter som användaren vid olika tidpunkter behöver ha åtkomst till. Eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden, behöver användarnas åtkomst till personuppgifter om patienter i TakeCare begränsas för att återspegla detta.

Mot denna bakgrund kan Datainspektionen konstatera att Aleris inte har begränsat användarnas behörigheter för åtkomst till patienternas personuppgifter i journalsystemet TakeCare. Det innebär i sin tur att en majoritet av användarna har haft faktisk åtkomst till vårddokumentationen om ett stort antal patienter i TakeCare.

Av granskningen framgår även att Aleris använder sig av så kallade aktiva val för åtkomst till personuppgifter om patienter samt funktionen *journalfilter*.

Att Aleris använder aktiva val innebär inte att åtkomstmöjligheten till personuppgifter i systemet har begränsats för användaren, utan uppgifterna är fortfarande elektroniskt åtkomliga. Det innebär att de aktiva valen inte är en sådan åtkomstbegränsning som avses i 4 kap. 2 § patientdatalagen, eftersom denna bestämmelse kräver att behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården och att endast de som har behov av uppgifterna ska ha åtkomst. Datainspektionen anser därmed att Aleris användning av aktiva val är en integritetshöjande åtgärd men att den inte påverkar de faktiska åtkomstmöjligheterna.

Aleris har vidare uppgett att det finns funktioner i TakeCare för att en vårdgivare ska kunna ”isolera” en vårdenhet och därigenom ”stänga ute” andra vårdgivares och vårdenheters åtkomstmöjligheter till enhetens vårddokumentation, så kallade skyddade enheter. Aleris anser dock att bolaget inte bedriver någon verksamhet som kräver skyddade enheter och har därför inte använt sig av denna funktion.

Vad gäller den sammanhållna journalföringen har alla användare hos Aleris åtkomst till alla personuppgifter om patienter hos de andra vårdgivarna i TakeCare, frånsett när patienterna har begärt att få sina uppgifter spärrade. Det framgår av granskningen att vårdgivaren har en möjlighet att aktivt spärra andras vårdgivares journaler, men att Aleris valt att inte göra det eftersom bolaget inte bedriver någon verksamhet som behöver spärras. Aleris anser att det är mer patientsäkert att låta uppgifterna vid Aleris enheter vara tillgängliga för andra vårdgivare.

Att tilldelningen av behörigheter inte har föregåtts av en behovs- och riskanalys innebär att Aleris 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. Aleris har därmed inte använt sig av lämpliga åtgärder, i enlighet med artikel 32, för att begränsa användarnas åtkomst till patienternas uppgifter i journalsystemet. Det 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.

Aleris har vidare uppgett att bolaget inte har några tekniska möjligheter att göra ändringar i TakeCare eftersom Aleris inte har någon rådighet över journalsystemet. Det framgår även att Aleris, inom ramen för den sammanhållna journalföringen, inte får implementera vissa begräsningar med hänvisning till beslut från Region Stockholm.

Grunden i dataskyddsförordningen består i att den personuppgiftsansvarige har ett ansvar att följa de skyldigheter som uppställs i förordningen för att överhuvudtaget få behandla personuppgifter i sin verksamhet. Att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhet är en sådan skyldighet (se artiklarna 5, 24 och 32 i dataskyddsförordningen). Datainspektionen anser därmed att Aleris i egenskap av personuppgiftsansvarig inte kan frånsäga sig ansvaret för att vidta de tekniska och organisatoriska åtgärder som krävs enligt ovannämnda artiklar.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att Aleris har behandlat personuppgifter i strid med artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen genom att Aleris inte har begränsat användarnas behörigheter för åtkomst till journalsystemet TakeCare till vad som enbart behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40. Det innebär att Aleris 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 åtkomst (loggar)
Av den dokumentation av åtkomst (loggar) som uppstod med anledning av Datainspektionens granskning framgår följande: datum, klockslag, användarens och patientens identitet, vilka åtgärder som vidtagits och

vårdenhet. Samma dokumentation framgår då användaren tar del av uppgifter inom ramen för sammanhållen journalföring.

Datainspektionen har inte något att erinra i denna del, eftersom dokumentationen av åtkomsten (loggarna) i TakeCare är i överensstämmelse med de krav som framgår av 4 kap. 9 § HSLF-FS 2016:40. Aleris har därmed vidtagit lämpliga tekniska åtgärder enligt artikel 32 i dataskyddsförordningen.

Val av ingripande

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

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

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

Föreläggande
Hälso- och sjukvården har stort behov av information i sin verksamhet. Det är därför naturligt att digitaliseringens möjligheter tillvaratas så mycket som möjligt inom vården. Sedan patientdatalagen skrevs har en mycket omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarna storlek som hur många som delar information med varandra har ökat väsentligt. Denna ökning innebär samtidigt att kraven ökar på den

personuppgiftsansvarige, eftersom bedömningen av vad som är en lämplig säkerhet påverkas av behandlingens omfattning.

I detta sammanhang innebär det att ett stort ansvar vilar på 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.

Datainspektionens tillsyn har visat att Aleris har underlåtit att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i journalsystemet TakeCare genom att inte följa de krav som ställs i patientdatalagen och Socialstyrelsens föreskrifter avseende genomförande av behovs-och riskanalys, innan tilldelning av behörigheter i systemet sker och att inte begränsa behörigheten för åtkomst till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Det innebär att Aleris även har underlåtit att följa kraven i artikel 5.1 f och artikel 32.1 och 32.2 i dataskyddsförordningen. Underlåtenheten omfattar såväl den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen förelägger därför med stöd av artikel 58.2 d i dataskyddsförordningen Aleris Sjukvård AB att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemet TakeCare och att därefter, 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, 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.

Sanktionsavgift

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

I detta fall är det frågan om stora uppgiftssamlingar med känsliga personuppgifter och vidsträckta behörigheter. Vårdgivaren behöver med nödvändighet ha en omfattande behandling av uppgifter om enskildas hälsa. Den får dock inte vara oinskränkt utan ska baseras på vad enskilda medarbetare behöver för att kunna utföra sina uppgifter. Datainspektionen konstaterar att det är frågan om uppgifter som omfattar direkt identifiering av den enskilde genom såväl namn, kontaktuppgifter som personnummer, uppgifter om hälsa, men det 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 närmare 800 000 patienter och drygt 1 000 aktiva användare i journalsystemet.

Det är en central uppgift för den personuppgiftsansvarige att vidta åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till risken. Vid bedömningen av lämplig säkerhetsnivå ska 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, enligt artikel 32.2 i dataskyddsförordningen. Kraven för hälso- och sjukvårdsområdet, gällande nu aktuella säkerhetsåtgärder, har specificerats i patientdatalagen och i Socialstyrelsen föreskrifter. Av förarbetena till patientdatalagen framgår tydligt att krav ställs på såväl strategisk analys som att behörighetstilldelning sker individuellt och anpassas efter den aktuella situationen. Att stora mängder känsliga personuppgifter behandlas utan att grundläggande regelverk på området följs gör att förfarandet bedöms som allvarligare.

Datainspektionen tar också hänsyn till att Aleris inte har valt att begränsa åtkomsten inom ramen för den sammanhållna journalföringen. Enligt Aleris är det mer patientsäkert att låta uppgifterna vid Aleris enheter vara tillgängliga för andra vårdgivare. Det innebär att Aleris har prioriterat bort integritetsskyddet inom den sammanhållna journalföringen till förmån för patientsäkerheten, vilket är särskilt allvarligt.

Datainspektionen har även tagit hänsyn till att Aleris har använt sig av vissa integritetshöjande åtgärder, utfört vissa begränsningar vad gäller yrkeskategoriernas läsbehörighet samt dokumenterat åtkomsten på ett korrekt sätt.

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

Dessa faktorer innebär sammantaget att överträdelserna, att inte genomföra en behovs- och riskanalys och att inte begränsa användarnas behörigheter till enbart vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, 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 får enligt artikel 83.3 inte överstiga beloppet för den grövsta överträdelsen om det är frågan om en eller samma uppgiftsbehandlingar eller sammankopplade uppgiftsbehandlingar.
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.

När det gäller beräkning av beloppet framgår av artikel 83.5 i dataskyddsförordningen att företag som begår överträdelser som de aktuella kan påföras sanktionsavgifter på upp till tjugo miljoner EUR eller fyra procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

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

Av beaktandeskäl 150 i dataskyddsförordningen framgår bland annat följande. […] Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget[…]. Det innebär att bedömningen av vad som utgör ett företag ska utgå från konkurrensrättens definitioner. Reglerna för koncernansvar i EU:s konkurrenslagstiftning kretsar kring begreppet ekonomisk enhet. Ett moderbolag och ett dotterbolag betraktas som en del av samma ekonomiska enhet när moderbolaget utövar ett avgörande inflytande över dotterbolaget. Datainspektionen lägger därför som utgångspunkt omsättningen för Aleris Group AB till grund för beräkningen av sanktionsavgiftens storlek.

Aleris Group AB bildades i slutet av 2019. Några omsättningssiffror för hela 2019 finns således inte att tillgå. Det saknas därför uppgifter om den årliga omsättningen för bestämmandet av sanktionsavgiftens storlek. Aleris har uppgett att koncernomsättningen för Aleris Group AB uppgick till drygt 1,2 miljarder kronor mellan den 1 oktober 2019 och den 31 december 2019. Omräknat för ett helt år skulle det motsvara en omsättning på cirka 4,9 miljarder kronor.

Datainspektionen konstaterar att den faktiska årsomsättningen för Aleris Group AB innevarande år kommer att bli väsentligt högre.

Datainspektionen tillämpar i aktuellt ärende en försiktighetsprincip och uppskattar därför att bolagets årliga omsättning i vart fall motsvarar den för perioden oktober – december 2019 omräknat för helår, det vill säga cirka 4,9 miljarder kronor. Det högsta sanktionsbelopp som kan fastställas i aktuellt fall är 20 000 000 EUR vilket är drygt fyra procent av bolagets uppskattade omsättning.

Mot bakgrund av överträdelsernas allvar och att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bestämmer Datainspektionen den administrativa sanktionsavgiften för Aleris Sjukvård AB till 15 000 000 (femton miljoner) kronor.

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