Aleris Närsjukvård AB
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 granskningen den 24 april 2019 konstaterat att Aleris Närsjukvård AB (tidigare Praktikertjänst N.Ä.R.A. 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 Närsjukvård AB inte har genomfört en behovs- och riskanalys innan tilldelning av behörigheter sker i journalsystemet TakeCare och Nationell patientöversikt (NPÖ) 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 Aleris Närsjukvård 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 Närsjukvård AB inte begränsar användarnas behörigheter för åtkomst till journalsystemet TakeCare och NPÖ 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 Aleris Närsjukvård 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 Närsjukvård AB 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 12 000 000 (tolv miljoner) kronor.

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Aleris Närsjukvård AB att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemen TakeCare och NPÖ 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,

[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).

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 24 april 2019 granskat om Aleris Närsjukvård AB beslut om tilldelning av behörigheter har föregåtts av en behovs- och riskanalys. Granskningen har även omfattat hur Aleris Närsjukvård AB tilldelat behörigheter för åtkomst till huvudjournalsystemet TakeCare och NPÖ, och vilka åtkomstmöjligheter de tilldelade behörigheterna ger inom såväl ramen för den inre sekretessen enligt 4 kap. patientdatalagen, som den sammanhållna journalföringen enligt 6 kap. patientdatalagen. Utöver detta har Datainspektionen även granskat vilken dokumentation av åtkomst (loggar) som finns i journalsystemen.

Datainspektionen har endast granskat användares åtkomstmöjligheter till journalsystemen, dvs. vilken vårddokumentation användaren faktiskt kan ta del av och läsa. Tillsynen omfattar inte vilka funktioner som ingår i behörigheten, dvs. vad användaren faktiskt kan göra i journalsystemen (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 Närsjukvård AB:s uppfattning kring de tekniska möjligheterna att begränsa läsbehörigheten för sina användare i TakeCare, ombads Aleris Närsjukvård AB 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 Närsjukvård AB har i huvudsak uppgett följande.

Personuppgiftsansvaret
Aleris Närsjukvård AB är personuppgiftsansvarig och vårdgivare.

Verksamheten

Den 15 maj 2019 inkom Praktikertjänst N.Ä.R.A. AB med en skrivelse till Datainspektionen med information om att Praktikertjänst N.Ä.R.A. AB avyttrats från Praktikertjänst-koncernen (org.nr. 556077-2419) den 1 april 2020 och bytt namn till Aleris Närsjukvård AB (org.nr. 556743-1951). Med anledning av detta begärde Datainspektionen kompletterande information från Aleris Närsjukvård AB. Av kompletteringarna framgår bland annat följande.

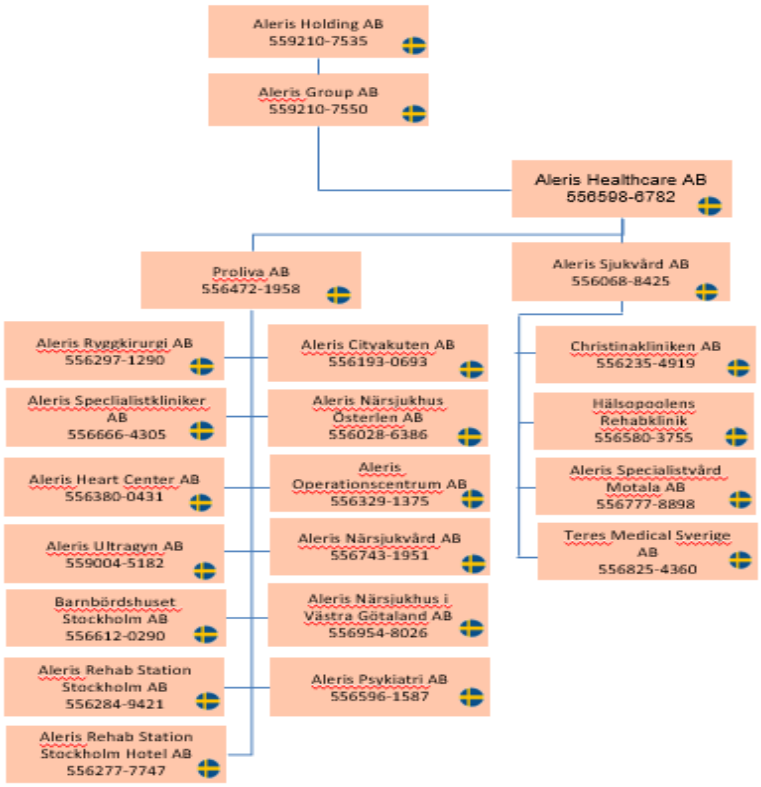
Den 1 oktober 2019 köps Aleris Healthcare AB (org.nr 556598-6782) med dotterbolag upp av Triton. I samband med förvärvet skapas det nya koncernmoderbolaget, Aleris Group AB (org.nr 559210-7550).

Den 1 april 2020 köps Proliva AB (org.nr. 556472-1958) och tillhörande dotterbolag upp av Triton. Proliva AB får Aleris Group AB som koncernmoder.

Praktikertjänst N.Ä.R.A. AB ägdes före den 1 april 2020, till ett hundra procent av Provliva AB. Provliva AB ägdes i sin tur till ett hundra procent av koncernmoderbolaget Praktikertjänst AB.

Efter avyttringen den 1 april 2020 ägs Aleris Närsjukvård AB fortsatt till ett hundra procent av Proliva AB och är därmed en del av Aleris Group AB. Proliva AB ägs i sin tur till ett hundra procent av Aleris Healthcare AB. Koncernmoderbolaget för hela ”Aleris-koncernen” inklusive ”Proliva-koncernen” är Aleris Holding AB (org.nr 559210-7535).

Följande bild visar ägarstrukturen för Aleris Närsjukvård AB efter avyttringen den 1 april 2020.



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 Närsjukvård AB använder TakeCare som huvudjournalsystem inom ramen för den inre sekretessen och deltar i TakeCares system för sammanhållen journalföring. TakeCare har använts av Aleris Närsjukvård AB sedan år 2009. Digitala journaler var fortfarande en relativ nyhet år 2009 och dessa var framförallt inriktade på patientsäkerhet genom att dokumentationen var utformad utifrån medicinska-omvårdnadsbehov samt införande av läkemedelsjournal. Aleris Närsjukvård AB har under åren vid uppföljningsmöten med CompuGroup Medical (CGM), som är leverantör av journalsystemet och ansvarar för de funktioner som systemet har för att styra

behörigheter, och Centrum för Samverkan TakeCare (CSTC), påtalat brister rörande patientsäkerhet och datasäkerhet.

Aleris Närsjukvård AB använder även Nationell patientöversikt, NPÖ, inom ramen för den sammanhållna journalföringen.

Antalet patienter och anställda
Antalet registrerade patienter i TakeCare, hos Aleris Närsjukvård AB, uppgick vid inspektionstillfället till 55 061.

Antalet anställda hos Aleris Närsjukvård AB uppgick vid inspektionstillfället till 1 150 månadsanställda**.** Antalet befattningshavare som har åtkomstmöjlighet till TakeCare uppgick till 1 700, vilket i huvudsak även inkluderar ST-läkare, inhyrd personal och studenter. Siffran 1 700 motsvarar aktiva konton. Skillnaden mellan aktiva konton och anställda beror på att det finns mycket inhyrd personal och vid inspektionstillfället fanns det ett hundratal studenter som praktiserade hos Aleris Närsjukvård AB.

Antalet anställda som har åtkomstmöjlighet till NPÖ uppgick vid inspektionstillfället till 335 och utgörs till största delen av läkare (158 läkare, 87 sjuksköterskor, 82 fysioterapeuter, 4 arbetsterapeuter, 3 medicinska sekreterare och 1 kiropraktor).

Inre sekretess

Behovs- och riskanalys
Aleris Närsjukvård AB har i huvudsak uppgett följande.

Det finns en mall för behovs- och riskanalys, *Tilldelning av behörigheter, behovs- och riskanalys, mall: Funktionsbeskrivningar och uppdrag*, och det är verksamhetschefer och enhetschefer som ska utföra behovs- och riskanalysen innan tilldelning av behörigheter i systemen.

Av mallen framgår bl.a. att risker och behov måste vägas inför tilldelning av en behörighetsprofil och att det är ansvarig chef som utför en behovs- och riskanalys av medarbetarens behov av behörigheter till åtkomst av personuppgifter. Bedömningen görs bland annat utifrån arbetsuppgifter och arbetsplats. Om medarbetaren har behov av åtkomst till TakeCare för ändamålet ”Läsa och skriva i en vårdrelation” kryssas denna ruta i av chefen.

Vidare ska tre frågor besvaras av ansvarig chef genom att denne kryssar i en eller två rutor med påståenden under varje fråga. En av dessa tre frågor rör patientens integritet - ”Vilka risker gällande patientintegritet innebär det att behörigheten ges? (motivera i form av tillgång till patientuppgifter)”. Det finns två påståenden som kan kryssas i:

- ”Möjlighet att aktivt välja att öppna annan journal inom spärrområdet (vårdområdet) genom sin behörighet (häva intern sekretess)”, eller
- ”Risk för åtkomst av, för vårdtillfället, ej nödvändiga patientuppgifter i TakeCare genom möjligheten till sammanhållen journal/läsbehörighet”.

Det framgår även att om ansvarig chef svarar nej på något av påståendena ska behovet av behörighet övervägas en gång till innan behörighet ges och motivering ska anges skriftligt.

Det finns en rutin som är kopplad till mallen, *Bedömning av behörigheter för åtkomst till uppgifter om patienter samt till andra system*, och den rutinen anges utgöra instruktion till verksamhetschefen och enhetschefen hur denne ska gå tillväga vid tilldelning av behörigheter. Av rutinen framgår att behörigheter till elektroniska system som innehåller patientuppgifter ska begränsas till vad som behövs för att medarbetaren ska kunna fullgöra sina arbetsuppgifter i vården. Vidare framgår att chefen, i samband med en ny medarbetares tillträde till anställning, gör en bedömning av vilka behörigheter den nya medarbetaren behöver. Det finns inga ytterligare instruktioner, utan det hänvisas istället till ett annat dokument.

När beställningen av behörigheter görs kan supportfunktionen ge feedback om de ser något som uppfattas som väldigt avvikande. Att det praktiska arbetet med uppläggningen av behörigheter i TakeCare är separerad från cheferna, blir därför en kontrollfunktion i förhållande till cheferna.

Det finns ingen ”färdig svarsmall” för hur en riskanalys ska se ut, utan riskanalysen utgörs av att aktuell verksamhetschef eller enhetschef gör en bedömning som den sedan kan nedteckna i en fritextruta i dokumentet *Tilldelning av behörigheter – behovs och riskanalys, mall: Funktionsbeskrivningar och uppdrag*.

Verksamhetschefen eller enhetschefen ska besvara frågan i mallen som lyder: ”Vilka risker skulle en alltför begränsad behörighetstilldelning medföra?” Exempel på ansvarig chefs riskanalyser när det gäller om medarbetare har behov av åtkomst till uppgifter i TakeCare är:

- ”Inget behov utifrån patientsäkerhet att medarbetaren har behörighet i TC eller andra patientrelaterade system”.
- ”Minskad tillgänglighet för patienter då samarbete sker med såväl geriatrik som ASIH och SPSV för att optimalt använda personella resurser. Minskad kontinuitet för patienter alternativt risk för patientosäker journalföring av läkemedelsadministrering.”
- ”Försvåra patientarbetet och förhindra möjligheten att hjälpas åt för att bibehålla tillgänglighet för patienter vid arbetstoppar eller frånvaro. Även försvåra möjlighet till frekventa extrapass i andra ASIH-team”.

Behörighetstilldelning för åtkomst till personuppgifter
Aleris Närsjukvård AB har i huvudsak uppgett följande.

Aleris Närsjukvård AB använder sig av bolaget Acceptus framtagna behörighetsmallar i TakeCare. Acceptus är en central förvaltare av TakeCare. Med utgångspunkt från vilka behörigheter som ingår i dessa mallar har Aleris Närsjukvård AB gjort en egen lista över olika behörigheter och behov som rollerna har.

Behörighetstilldelningen går i stort sett till på följande sätt. I ett första lager finns ”grunden” för tilldelningen, t.ex. rollen som sjuksköterska eller läkare. I det andra lagret läggs behörighet på utifrån vilken enhet användaren arbetar på, t.ex. ”Handen-geriatriken” och i det tredje lagret läggs behörighet utifrån vilka uppgifter personen ifråga ska kunna ta del av. Det är arbetsuppgifterna som styr vilka behörigheter som ska tilldelas respektive roll.

Därefter fyller den aktuella verksamhetschefen eller enhetschefen i en krysslista i ett dokument som heter ”Tilldelning av behörigheter, behovs- och riskanalys, mall: funktionsbeskrivningar och uppdrag”, tillsammans med aktuell medarbetare. Den ifyllda listan över vilka ändamål som en medarbetare kan ha behov av när det gäller åtkomst till uppgifter i TakeCare, är det som utgör det egentliga behovet. Verksamhetschefen eller enhetschefen lägger sedan en beställning till supporten som utför den faktiska uppläggningen av behörigheterna i TakeCare.

Det ingår obegränsad läsbehörighet i alla behörighetsprofiler som används av Aleris Närsjukvård AB i TakeCare, men inte nödvändigtvis behörighet att upprätta vårddokumentation.

Det är endast de befattningshavare som deltar aktivt i vården av en patient som har en åtkomstmöjlighet till personuppgifter i TakeCare. Samtliga användare hos Aleris Närsjukvård AB har individuella behörigheter, med eget SITHS-kort och eget datakonto inom Aleris Närsjukvård AB. Ett SITHS-kort är en e-legitimation som gör det möjligt för användare att identifiera sig med stark autentisering vid inloggning i e-tjänster.

Alla områden inom Aleris Närsjukvård AB är upplagda som ”boxar” vilka motsvarar vårdenheter. Initialt kan användaren enbart läsa vårddokumentation inom den egna ”boxen”/vårdenheten, vilket i TakeCare kallas för ett spärrområde. Ett exempel på ”box”/vårdenhet är Dalen-geriatriken. I detta fall ser användaren enbart uppgifter om Dalen-geriatrikens patienter. Inom en ”box”/vårdenhet kan användaren se all information, dvs. all vårddokumentation om patienten. Det gäller även om enheten kan vara uppdelad i mindre enheter eller team.

Om användaren arbetar inom vårdenheten ”avancerad sjukvård i hemmet” (ASIH) finns indelningen ”nord eller syd”. Då ska användaren endast få behörighet till norra eller södra delen. Om användaren har behov av behörighet utöver det, t.ex. om en läkare arbetar över hela verksamhetsområdet, får denne behörighet till det. Åtkomsten för användarna inom ASIH är begränsad på sådant sätt att de initialt inte kan komma åt uppgifter inom geriatriksjukhusen, eller se en lista över vilka patienter som finns registrerade där, om inte chefen beställer en sådan behörighet.

Inom ramen för den inre sekretessen kan användaren själv genom aktiva val kryssa i rutor som ger åtkomst till vårddokumentation hos alla vårdenheter inom Aleris Närsjukvård AB, antingen genom att det finns ett samtycke från patienten eller att det rör sig om en nödsituation. Aleris Närsjukvård AB kräver inte att samtycket från patienten dokumenteras. Den vårdenhet som medarbetaren har en aktiv tjänstgöring vid är förvald.
Användaren kan efter ett aktivt val klicka sig vidare till all information som finns om patienten inom ramen för den inre sekretessen hos Aleris

Närsjukvård AB (dvs. till alla olika vårdenheter inom Aleris Närsjukvård AB) i TakeCare. Den enda informationen som inte alla användare har åtkomst till rör sjukintygen till Försäkringskassan. Aleris Närsjukvård AB uppger att användarna informeras om att de inte får gå in i journaler och läsa utan att vara behöriga till det. Aleris Närsjukvård AB anser att det är en brist att bolaget inom ramen för den inre sekretessen inte kan begränsa läsbehörigheten mellan verksamheterna i Aleris Närsjukvård AB.

Den enda möjlighet som finns att begränsa åtkomsten till en vårdenhet, är om vårdenheten är en s.k. skyddad enhet. Begränsningar kan då göras avseende vilka andra enheters journal den aktuella vårdenhetens användare kan se, och om andra vårdgivares användare ska kunna se journal hos den aktuella vårdenheten. Aleris Närsjukvård AB använder sig inte av dessa skyddade enheter i TakeCare eftersom bolaget anser att detta skulle kunna innebära en patientsäkerhetsrisk.

Sammanhållen journalföring

Aleris Närsjukvård AB har i huvudsak uppgett följande.

Behovs- och riskanalys

Det finns ingen specifik behovs- och riskanalys framtagen för sammanhållen journalföring.

Behörighetstilldelning avseende åtkomst till personuppgifter om patienter

Aleris Närsjukvård AB deltar i system för sammanhållen journalföring genom journalsystemet TakeCare och journalsystemet NPÖ, som är ett nationellt system för sammanhållen journalföring.

Inom ramen för sammanhållen journalföring i TakeCare kan användarna ta del av all vårddokumentation hos andra vårdgivare som ingår i systemet. Dessförinnan måste användaren först välja en specifik vårdgivare och då visas en dialogruta. Användaren måste då göra ett aktivt val för att komma vidare genom att klicka i en av två rutor; en ruta för samtycke från patienten eller en ruta för nödsituation. Genom att klicka i något av alternativen får användaren sedan åtkomst till den specifika vårdgivarens journaler. Aleris Närsjukvård AB informerar användarna om att de inte får gå in i journaler och läsa utan att vara behöriga till det.

Användare kan genom sammanhållen journalföring obegränsat läsa det som skrivits på andra vårdgivares enheter, med patientens samtycke, med undantag av om patienten valt att spärra sin journal eller om enheten är en så kallad skyddad enhet.

Om användaren vill ta del av vårddokumentation hos en annan vårdgivare måste användaren dokumentera att man erhållit ett samtycke från patienten. Det går inte att behörighetsmässigt, för en yrkesgrupp, begränsa att man bara tar del av journaler inom Aleris Närsjukvård AB.

Med anledning av att Karolinska Universitetssjukhuset i ett yttrande har uppgett att det finns möjligheter att begränsa åtkomsten i TakeCare anför Aleris Närsjukvård AB att bolaget har kännedom om de skyddade enheterna och att åtkomsten, genom de skyddade enheterna, kan begränsas inom ramen för den inre sekretessen och inom den sammanhållna journalföringen. Aleris Närsjukvård AB anser dock att de skyddade enheterna utgör en patientsäkerhetsrisk, eftersom begränsningarna inte kan hävas efter inhämtat samtycke från patienterna eller i akuta situationer. Aleris Närsjukvård AB anser även att det skulle innebära en patientsäkerhetsrisk om sammanhållen journalföring valdes bort. Risken bedöms vara extra stor inom Aleris Närsjukvård ABs verksamheter eftersom patienterna som vårdas där ofta har kontakt med många vårdgivare och därmed har ett stort behov av sammanhållen vård.

NPÖ
Om en användare som tilldelats behörighet vill använda sig av NPÖ kan detta ske på två sätt. Användaren kan antingen gå direkt in i NPÖ och knappa in ett valfritt personnummer som systemet sedan söker fram, eller så går användaren först in i TakeCare och knappar in patientens personnummer och gör därefter ett så kallat ”uthopp” till den information som finns om patienten i NPÖ.

Dokumentation av åtkomsten (loggar)
Aleris Närsjukvård AB har uppgett följande.

TakeCare
Den dokumentation som visas vid uttag av åtkomstloggarna i TakeCare är; uppgifter om patienten, vilken användare som har öppnat journalen, vilken tidsperiod någon varit inne, alla öppningar av journalen som gjorts på den

patienten under den valda tidsrymden, klockslag och datum för det senaste öppnandet. Avseende vilken användare som öppnat journalen anges personnummer och identifikationsnummer för den specifika enheten, exempelvis ASIH. Det framgår även från vilken enhet användaren har varit inne genom att det anges specifik avdelning på aktuell vårdenhet.

I det vanliga loggutdragen framgår det inte vilka åtgärder som användaren har vidtagit eller hur länge någon varit inne i den aktuella journalen, eller vilken journalanteckning som har öppnats, men den informationen framgår av de fördjupade loggutdragen. De fördjupande loggutdragen erhålls först efter att Aleris Närsjukvård AB gör en beställning hos Acceptus som i sin tur vänder sig till CGM.

NPÖ
Den dokumentation som visas vid uttag av åtkomstloggar i NPÖ är; uppgifter om patienten, vilken användare som har öppnat journalen, från vilken enhet användaren har varit inne, exempelvis Dalen geriatriken, datum och tidpunkt för öppningen samt vilka åtgärder användaren har vidtagit.

Aleris Närsjukvård AB:s yttrande över Datainspektionens skrivelse
Aleris Närsjukvård AB har i synpunkter på skrivelsen *Slutlig kommunicering inför beslut* som inkom till Datainspektionen den 16 mars 2020 uppgett bland annat följande.

Efter Datainspektionens inspektion har Aleris Närsjukvård AB, tillsammans med vissa andra aktörer, tagit initiativ till och bedrivit ett arbete med tekniska förändringar och förbättringar av möjligheterna till individuella behörighetstilldelningar i TakeCare och indirekt i NPÖ. Detta arbete har lett till implementering av nya tekniska lösningar hos systemleverantören som numera i betydande avseenden har rättat till de brister hos Aleris Närsjukvård AB som tidigare föranletts av systemet tekniska begränsningar.

Aleris Närsjukvård AB anför vidare att ytterligare en granskning skedde under 2019 av Inspektionen för vård och omsorg (IVO). IVO granskade efterlevnaden av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). En del av granskningen rörde informationssäkerhet inkluderande hantering av behörigheter och riskarbete. Av IVO: s beslut framgår, när det gäller behörighetstilldelning och riskarbete, följande. ”Riskanalyser görs även gällande personalen,

exempelvis i samband med medarbetarsamtalen. Bakgrundskontroller görs på samtliga anställda utifrån tre olika nivåer. Stor vikt läggs vid behörighetsstyrningen. Praktikertjänst N.Ä.R.A. AB beslutar om varje medarbetares accessnivå till företagets information. Borttagning av behörigheter när anställningen upphör sker automatiskt via ett behörighetssystem." Aleris Närsjukvård AB uppger att det av IVO: s slutliga beslut framgår att bolaget i samtliga avseenden uppfyller NIS-lagen och det gällande direktivet.

Aleris Närsjukvård AB uppger även att i samband med införandet av dataskyddsförordningen och NIS-lagen har bolaget prioriterat rutiner och processer inom patientsäkerhetsarbetet högst, följt av pågående förändringsarbete avseende resterande integritetssäkrande åtgärder. När det gäller behörighetstilldelningen så har den alltid, även vid inspektionstillfället, präglats av snävast möjliga behörighet, avvägt mot aktuell roll/uppdrag i bolaget och det behov av stöd i verksamhets- och patientsäkerhetshänseende som erfordras för respektive befattning och arbetsuppgifter, med beaktande av minsta möjliga påverkan avseende informationssäkerhet och personlig integritet. Som tidigare redogjorts för har dock den tekniska plattformen för TakeCare vid tidpunkten för inspektionstillfället medfört att Aleris Närsjukvård AB då inte kunde införa dessa begränsningar fullt ut, vilket nu har korrigerats i systemet.

Av den inskickade grundmall som används vid behovs- och riskanalysen framgår att vissa mindre justeringar har skett. Bland annat har den tidigare frågan "Vilka risker skulle en alltför begränsad behörighetstilldelning medföra" tagits bort och ersatts med frågan "Något mer?", svarsalternativen ja respektive nej, följt av en fritextruta.

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.

Dataskyddförordningen 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 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 § i detta 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 det sammanhållna journalföringssystemet (se prop. 2007/08:126 s. 247).

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

Dokumentation av åtkomst (loggar)

Av 4 kap. 3 § patientdatalagen framgår att en vårdgivare ska se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och systematiskt kontrolleras.
Enligt 4 kap. 9 § HSLF-FS 2016:40 ska vårdgivaren ansvara för att

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

Datainspektionens bedömning

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

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

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

Hälso- och sjukvården har stort behov av information i sin verksamhet. Det är därför naturligt att digitaliseringens möjligheter tillvaratas så mycket som möjligt inom vården. Sedan patientdatalagen infördes har en mycket

omfattande digitalisering skett inom vården. Såväl uppgiftssamlingarna storlek som hur många som delar information med varandra har ökat väsentligt. Denna ökning innebär samtidigt att kraven ökar på den personuppgiftsansvarige, eftersom bedömningen vad som är en lämplig säkerhet påverkas av behandlingens omfattning.

Det är dessutom frågan om känsliga personuppgifter. Uppgifterna rör 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 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.

När Datainspektionen har efterfrågat en dokumenterad behovs- och riskanalys har Aleris Närsjukvård AB hänvisat till dokumentet *Tilldelning av behörigheter, behovs- och riskanalys, mall: Funktionsbeskrivningar och uppdrag.* I dokumentet anges att ansvarig chef ska utföra en behovs- och riskanalys vid anställning av en medarbetare utifrån medarbetarens behov av behörigheter till åtkomst av personuppgifter och att bedömningen görs utifrån arbetsuppgifter och arbetsplats. När det gäller riskanalysen av en medarbetare som ska anställas, består denna av en fråga – ”Vilka risker skulle en alltför begränsad behörighetstilldelning medföra?” Inför tilldelningen av en behörighetsprofil anges det att risker och behov måste vägas. Den integritetsrisk som tas upp i dokumentet består också av en fråga – ”Vilka risker gällande patientintegriteten innebär det att behörigheten ges?” Det enda förslag på risk som ges är ”risk för åtkomst av, för vårdtillfället, ej nödvändiga patientuppgifter i TakeCare genom möjligheten till sammanhållen journalföring”.

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 frågan om en strategisk analys på strategisk nivå, som ska ge 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.

Vid Datainspektionens granskning har Aleris Närsjukvård AB inte kunnat förevisa någon behovs- och riskanalys - vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen. Aleris Närsjukvård AB: s dokument saknar den grundläggande inventeringen av användarnas behov av åtkomst och analys av risker, och det har heller inte gjorts någon avvägning mellan behov och de faktiska integritetsrisker som personuppgiftsbehandlingen ger upphov till.
Aleris Närsjukvård AB har i sin analys inte beaktat 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 av Aleris Närsjukvård AB: s behandling av personuppgifter i TakeCare och NPÖ. Det saknas också särskilda riskbedömningar utifrån om det förekommer t.ex. skyddade personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer, uppgifter från vissa mottagningar eller medicinska specialiteter eller andra faktorer som kräver särskilda skyddsåtgärder. Det saknas även bedömning av hur sannolik och allvarlig risken för de registrerades rättigheter och friheter bedöms vara.

Datainspektionen konstaterar sammanfattningsvis att dokumenten *Tilldelning av behörigheter, behovs- och riskanalys, mall: Funktionsbeskrivningar och uppdrag*, *Bedömning av behörigheter för åtkomst till uppgifter om patienter samt till andra system och Behörighetsroller/profiler i patientdatasystem*, som har redovisats av Aleris Närsjukvård AB inte uppfyller de krav som ställs på en behovs- och riskanalys och att Aleris Närsjukvård AB inte har kunnat visa att de genomfört en behovs- och riskanalys i den mening som avses i 4 kap. 2 § HSLF-FS 2016:40, vare sig inom ramen för den inre sekretessen eller inom ramen för den sammanhållna journalföringen, enligt 4 respektive 6 kap. patientdatalagen. Detta innebär att Aleris Närsjukvård AB 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.

Enligt Aleris Närsjukvård AB finns en möjlighet att begränsa användarnas åtkomst till patienternas uppgifter, inom ramen för den inre sekretessen, i TakeCare genom de så kallade skyddade enheterna. Aleris Närsjukvård AB har dock inte infört sådana enheter. Den enda begränsning av åtkomst som finns i systemet rör sjukintygen till Försäkringskassan, vilka inte alla användare har åtkomst till.

Aleris Närsjukvård AB har uttryckt det som att behörigheterna i den inre sekretessen till viss del begränsas av så kallade aktiva val, vilket innebär att användaren initialt enbart kan läsa vårddokumentation inom den egna ”boxen”/vårdenheten. Inom en ”box”/vårdenhet kan användaren se all information, dvs. all vårddokumentation om patienten. Det gäller även om

enheten kan vara uppdelad i mindre enheter eller team. Inom ramen för den inre sekretessen kan användaren själv genom aktiva val kryssa i rutor som ger åtkomst till vårddokumentation hos alla vårdenheter inom Aleris Närsjukvård AB, antingen genom att det finns ett samtycke från patienten eller att det rör sig om en nödsituation.

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

Aleris Närsjukvård AB använder aktiva val enligt 4 kap. 4 § HSLF-FS 2016:40. Det är i och för sig en integritetshöjande åtgärd. Det innebär dock inte att åtkomstmöjligheten till personuppgifter i systemet har begränsats för användaren på så sätt att de inte längre är åtkomliga, utan uppgifterna är fortfarande elektroniskt åtkomliga. Genom att användaren klickar i rutan för samtycke eller nödåtkomst kan denne fortfarande ta del av alla personuppgifter, vilket innebär att alla användare som gör dessa aktiva val kan ta del av patienternas uppgifter och inte enbart de användare som har ett behov. Detta innebär att de aktiva valen inte är 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 kunna ha åtkomst till dem.

Aleris Närsjukvård AB har heller inte infört några begränsningar inom ramen för den sammanhållna journalföringen i systemet TakeCare, även om det finns möjligheter för vårdgivaren att begränsa användarens åtkomst till personuppgifter hos andra vårdgivare.

När det gäller åtkomst till personuppgifter om patienter inom ramen för den sammanhållna journalföringen i systemet NPÖ har 335 användare vid Aleris Närsjukvård AB tilldelats behörighet. Datainspektionen kan konstatera att det har gjorts en begränsning vad gäller antalet användare, utifrån de 1 700

användare som finns hos Aleris Närsjukvård AB, men det framgår inte varför 335 av 1700 medarbetare har fått denna åtkomstmöjlighet. Det framgår heller inte att det har gjorts någon begränsning av vilken dokumentation dessa användare kan ta del av i NPÖ.

Enligt Aleris Närsjukvård AB kan användaren antingen gå direkt in i NPÖ och knappa in ett valfritt personnummer som systemet sedan söker fram, eller så går användaren först in i TakeCare och knappar in patientens personnummer och gör därefter ett uthopp till den information som finns om patienten i NPÖ.
Eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden, behöver användarnas åtkomst till journalsystemen begränsas för att spegla detta. Aleris Närsjukvård AB har inte begränsat användarnas behörigheter för åtkomst till patienternas personuppgifter i journalsystemet, vare sig inom ramen för den inre sekretessen i systemet TakeCare eller inom ramen för den sammanhållna journalföringen i systemen TakeCare och NPÖ. Detta innebär att en majoritet av användarna har haft en faktisk åtkomst till en majoritet av patienternas personuppgifter i TakeCare. I systemet NPÖ har samtliga 335 användare haft åtkomst till de personuppgifter som behandlas inom ramen för NPÖ.

Att tilldelningen av behörigheter inte har föregåtts av en behovs- och riskanalys innebär att Aleris Närsjukvård AB 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 Närsjukvård AB har därmed inte använt sig av lämpliga åtgärder, i enlighet med artikel 32 dataskyddsförordningen, 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.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att Aleris Närsjukvård AB har behandlat personuppgifter i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen genom att Aleris Närsjukvård AB inte har begränsat användarnas behörigheter för åtkomst till journalsystemet TakeCare och NPÖ 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 Aleris Närsjukvård AB 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)
Datainspektionen kan konstatera att det av loggarna i TakeCare och NPÖ framgår uppgifter om den specifika patienten, vilken användare som har öppnat journalen, åtgärder som har vidtagits, vilken journalanteckning som har öppnats, vilken tidsperiod användaren har varit inne, alla öppningar av journalen som gjorts på den patienten under den valda tidsrymden och klockslag och datum för det senaste öppnandet.

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

Yttrande över Datainspektionens skrivelse Slutlig kommunicering efter beslut
Aleris Närsjukvård AB har kompletterat sina tidigare uppgifter med ett yttrande som kom in till Datainspektionen den 16 mars 2020, där Aleris Närsjukvård AB anger att det har bedrivit ett arbete med tekniska förändringar och förbättringar av möjligheterna till individuella behörighetstilldelningar i TakeCare och indirekt i NPÖ. Arbetet har lett till implementering av nya tekniska lösningar hos systemleverantören som numera i betydande avseenden har rättat till de brister hos Aleris Närsjukvård AB som tidigare föranletts av systemets tekniska begränsningar. Aleris Närsjukvård AB anger även att det av IVO:s slutliga beslut framgår att bolaget i samtliga avseenden uppfyller NIS-lagen och det gällande direktivet, bland annat vad gäller hantering av behörigheter och riskarbete.

Datainspektionen anser att det är positivt att Aleris Närsjukvård AB har bidragit till att det har skett implementeringar i form av nya tekniska lösningar i TakeCare, vilket har rättat till brister hos Aleris Närsjukvård AB. Det framkommer dock inte vilka dessa brister är eller på vilket sätt bristerna har rättats till inom ramen för Aleris Närsjukvård ABs tilldelning av behörigheter.

Datainspektionen kan vidare konstatera att IVO:s granskning av Aleris Närsjukvård AB utgår från bestämmelser i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och det gällande direktivet, och inte utifrån dataskyddsförordningen och patientdatalagens bestämmelser. NIS-lagen syftar till att uppnå en hög nivå på säkerheten i nätverken och informationssystem för samhällsviktiga tjänster medan dataskyddsbestämmelserna syftar till att skydda de registrerades fri- och rättigheter vid behandling av personuppgifter.

Val av ingripande

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

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

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

Föreläggande
Hälso- och sjukvården har, som nämnts, stort behov av information i sin verksamhet. 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.

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 Aleris Närsjukvård AB inte har vidtagit lämpliga säkerhetsåtgärder för att ge skydd till personuppgifterna i TakeCare och NPÖ genom att inte följa de krav som ställs i patientdatalagen och Socialstyrelsens föreskrifter och därigenom inte uppfyller kraven i artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen. Underlåtenheten omfattar såväl den inre sekretessen enligt 4 kap. patientdatalagen som den sammanhållna journalföringen enligt 6 kap. patientdatalagen.

Datainspektionen förelägger därför, med stöd av artikel 58.2 d i dataskyddsförordningen, Aleris Närsjukvård AB att genomföra och dokumentera erforderlig behovs- och riskanalys för journalsystemen TakeCare och NPÖ inom ramen för såväl den inre sekretessen som inom ramen för den sammanhållna journalföringen. Aleris Närsjukvård AB 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 Aleris Närsjukvård AB:s skyldighet att vidta lämpliga säkerhetsåtgärder för att ge skydd till personuppgifter enligt dataskyddsförordningen.

I detta fall är det frågan om stora uppgiftssamlingar med känsliga personuppgifter och vidsträckta behörigheter. Vårdgivaren behöver med nödvändighet ha en omfattande behandling av uppgifter om enskildas hälsa. Den får dock inte vara oinskränkt utan ska baseras på vad enskilda medarbetare behöver för att kunna utföra sina uppgifter. Datainspektionen konstaterar att det är frågan om uppgifter som omfattar direkt identifiering av den enskilde genom såväl namn, kontaktuppgifter som personnummer, uppgifter om hälsa, men det också kan röra sig om andra privata uppgifter om exempelvis familjeförhållanden, sexualliv och livsstil. Patienten är beroende av att få vård och är därmed i en utsatt situation. Uppgifternas karaktär, omfattning och patienternas beroendeställning ger vårdgivare ett särskilt ansvar att säkerställa patienternas rätt till adekvat skydd för deras personuppgifter.

Ytterligare försvårande omständigheter är att behandlingen av 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. Inom ramen för den inre sekretessen har 1 700 personer åtkomst till uppgifter som rör omkring 55 000 patienter, bortsett från de uppgifter som rör sjukintygen till Försäkringskassan vilka inte alla användare har åtkomst till. Därtill kommer åtkomstmöjligheten för de 1 700 personerna till personuppgifterna inom ramen för den sammanhållna journalföringen genom TakeCare och de 335 användare som har åtkomst till de stora uppgiftssamlingarna i NPÖ.

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 Aleris Närsjukvård AB har tilldelat behörigheter utan att följa dessa krav innebär att agerandet skett uppsåtligt och därmed bedöms som allvarligare.

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

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

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

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 Närsjukvård AB 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 eftersom Provliva AB med tillhörande dotterbolag (däribland Aleris Närsjukvård AB) köpts upp och sedan den 1 april 2020 har Aleris Group AB som koncernmoder är det sannolikt så 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 Närsjukvård AB till 12 000 000 (tolv 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.