Regionstyrelsen
Region Skåne
291 89 Kristianstad

Tillsyn enligt personuppgiftslagen (1998:204) - behörighetstilldelning, spärrar, loggar m.m. enligt patientdatalagen

Datainspektionens beslut

Datainspektionen konstaterar att Regionstyrelsen, Region Skåne behandlar personuppgifter:

1. I strid med 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § Socialstyrelsen föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40), eftersom regionen underlåter att begränsa behörigheterna till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Detta innebär att merparten av regionens användare har tilldelats en alltför vid behörighet i Melior, på grund av en otillräcklig behovs- och riskanalys.
2. Utan att ha tillräckliga rutiner och uppföljning gällande hantering av samtycke, innan en spärr får hävas av en behörig befattningshavare enligt 4 kap. 5 § patientdatalagen.
3. I strid med 4 kap. 4 § och 6 kap. 2 § patientdatalagen och 4 kap. 5 § och 4 kap. 7-8 §§ HSLF-FS 2016:40, eftersom regionen inte kan spärra vårddokumentation med en teknisk funktion i system som kan nås via Melior, såsom Sektra Ris.
4. I strid med 6 kap. 2 § och 8 kap. 6 § punkten 6 patientdatalagen, eftersom regionen inte informerar patienterna om vilka system som patientuppgifter kan vara aktuella i och i vilka system regionen kan upprätta spärrar.

5. I strid med 6 kap. 4 § patientdatalagen, eftersom regionen saknar rutiner för hävande av spärrar inom ramen för den sammanhållna journalföringen i Melior.
6. I strid med 7 kap. 3 § patientdatalagen, eftersom regionen som personuppgiftsansvarig inte kan säkerställa att patienterna har erhållit information innan patienters personuppgifter behandlas i kvalitetsregister.
7. I strid med 4 kap. 3 § patientdatalagen och 4 kap. 9 § punkterna 1-2 HSLF-FS 2016:40, eftersom det av loggen inte framgår vilka åtgärder som har vidtagits med uppgifter om en patient eller vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits.
8. I strid med 8 kap. 5 § patientdatalagen och 4 kap. 10 § HSLF-FS 2016:40, eftersom regionen på begäran av en patient inte kan lämna information om den direktåtkomst och den elektroniska åtkomst till uppgifter om patienten som förekommit, vilket vanligtvis sker genom utlämnande av s.k. loggutdrag.

Datainspektionen förelägger Regionstyrelsen, Region Skåne att:

1. Begränsa behörigheterna i Melior till vad som behövs för att den enskilde 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, samt revidera behovs- och riskanalysen i enlighet med dessa bestämmelser.
2. Se till att det finns instruktioner till behöriga befattningshavare som anger när och hur spärrar kan hävas enligt 4 kap. 5 § patientdatalagen. Instruktionerna ska även omfatta hur detta ska dokumenteras. Därutöver ska regionen se till att det finns rutiner för uppföljning av att instruktionerna efterlevs.
3. Uppfylla kravet på spärrar enligt 4 kap. 4 § och 6 kap. 2 § patientdatalagen och 4 kap. 5 § och 4 kap. 7-8 §§ HSLF-FS 2016:40, såväl i den inre sekretessen som i system för sammanhållen journalföring, genom att vidta åtgärder för att införa en teknisk funktion för spärr när det gäller vårddokumentationen i de system där sådana tekniska funktioner saknas, såsom Sektra Ris.
4. Informera patienterna, enligt 6 kap. 2 § och 8 kap. 6 § punkten 6 patientdatalagen om vilka system som patientuppgifter kan vara aktuella i och i vilka system regionen kan upprätta spärrar. Denna

information kan exempelvis ges på regionens webb. Informationen ska också framgå av blanketten gällande spärrar.

5. Införa rutiner för att häva spärrar i enlighet med 6 kap. 4 första stycket patientdatalagen.
6. Säkerställa att patienterna har erhållit information enligt 7 kap. 3 § patientdatalagen innan patienters personuppgifter behandlas i kvalitetsregister, genom att ta fram och införa rutiner och även införa funktioner som kontrollerar att rutinerna följs.
7. Vidta åtgärder så att det av loggarna, i enlighet med 4 kap. 3 § patientdatalagen och 4 kap. 9 § punkterna 1-2 HSLF-FS 2016:40, framgår vilka åtgärder som har vidtagits med uppgifter om en patient och vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits.
8. Åtgärda bristen, i enlighet med 8 kap. 5 § patientdatalagen och 4 kap. 10 § HSLF-FS 2016:40, på så sätt att patienten ska erhålla information om den direktåtkomst och elektroniska åtkomst till patienten som har förekommit, vilket innebär att det även ska framgå från vilken vårdenhet någon har tagit del av uppgifterna.

Upplysning

Beslutet kan komma att följas upp. Uppföljningen kommer då att ske i enlighet med EU:s dataskyddsförordning, som börjar tillämpas den 25 maj 2018. Dataskyddsförordningen kommer efter detta datum att vara det primära regelverket och patientdatalagen kommer att vara kompletterande lagstiftning.

Sammanfattning

Datainspektionen har granskat integritetsskyddande åtgärder i Regionstyrelsen, Region Skånes (regionen) huvudjournalsystem Melior, för att se om regionen har ett integritetsskydd i enlighet med gällande lagstiftning. Granskningen vidtogs efter klagomål.

Datainspektionen har funnit flera brister i Melior, såsom följande:

- Regionen ger personalen en för vid behörighet, då merparten av regionens vårdpersonal har möjlighet att ta del av alla uppgifter om alla patienter som inte har spärrat sina uppgifter hos regionen och hos de vårdgivare som ingår i den sammanhållna journalföringen.

- Regionen kan inte utföra verkningsfulla åtkomstkontroller, eftersom det saknas nödvändig dokumentation i loggarna. Detta innebär även att patienterna inte kan få den information från regionen som de lagligen har rätt till, när de begär ut ett s.k. loggutdrag.
- Det saknas teknisk funktion för spärrar i Sektra Ris, som är ett röntgensystem som nås via Melior. Det innebär att patienterna inte kan spärra sina uppgifter för åtkomst i Sektra Ris.
- Regionen har inte någon uppföljning av om patienterna faktiskt har lämnat samtycke innan vårdpersonalen tar del av patientens spärrade uppgifter.
- Regionen kan inte säkerställa att patienterna har erhållit information om den aktuella personuppgiftsbehandlingen, innan patienters personuppgifter behandlas i kvalitetsregister.

Datainspektionen kan konstatera att ovanstående innebär att patienterna hos regionen inte får det integritetsskydd som de lagligen har rätt till.

Redogörelse för tillsynsärendet

Klagomål
Datainspektionen har mottagit ett klagomål rörande behandling av personuppgifter som har genomförts av Regionstyrelsen, Region Skåne (härefter regionen). Klagomålet rör personuppgiftsbehandlingen i journalsystemen hos regionen. Klaganden har anfört att personuppgifter har behandlats i strid med vissa bestämmelser i 4, 6 och 7 kap. patientdatalagen, bl.a. vad gäller behörighetsstyrning, spärrhantering, historiken i loggarna samt att en patient inte kan motsätta sig att ingå i system för såväl sammanhållen journalföring, som kvalitetsregister.

Datainspektionen inleder tillsyn
Datainspektionen har den 13 oktober 2017 inlett tillsyn mot regionen i syfte att granska hur huvudjournalsystemet Melior är uppbyggt utifrån integritetsskyddsaspekterna, i enlighet med klagomålet.

En inspektion genomfördes hos regionen den 25 oktober 2017.
Datainspektionen granskade vid detta tillfälle Meliors funktioner utifrån behörighetsstyrning, spärrhantering, behandlingshistoriken i loggarna samt om en patient kan motsätta sig att ingå i system för sammanhållen

journalföring och i kvalitetsregister. Datainspektionen följde även upp ett av inspektionen tidigare fattat beslut som ingick i det s.k. ”spärrprojektet”, med diarienummer 2038-2013.

I samband med att Datainspektionen skickade inspektionsprotokollet till regionen för eventuella synpunkter, den 6 november 2017, ställde inspektionen även fyra kompletterande frågor.

Regionen inkom den 21 november 2017 med ett yttrande till Datainspektionen. Yttrandet innehöll vissa synpunkter på inspektionsprotokollet samt svar på frågorna. Regionen har även inkommit med ytterligare information den 19 och 23 januari 2018.

Regionen har i huvudsak uppgett följande.

Personuppgiftsbehandling i Melior

Systemet som omfattas av tillsynen heter Melior (218 Service Pack 1, Patch 200). Driften av systemet sköts av Tieto. Melior används framförallt inom slutenvården, men även inom den öppenvård som ges på sjukhusen i regionen.

Behörighetstilldelning

Det finns tre roller i Melior; 1) Vårdgivarroll, 2) Vårdenhetsroll och 3) övriga roller som kräver unik behörighet, exempelvis systemsupport, kvalitetsgranskning, loggranskning, uppdrag av domstol etc.

Regionen uppger att det finns ca 30 000 behörighetskonton, dvs. unika användare, hos regionen. Majoriteten av användarna har tilldelats en vårdgivarroll utöver en vårdenhetsroll. Endast ett fåtal användare, i huvudsak undersköterskor, har enbart en vårdenhetsroll.

Vårdgivarrollen ger åtkomstmöjlighet i Melior till samtliga personuppgifter hos vårdgivaren inom ramen för den inre sekretessen. Vårdgivarrollen ger samtidigt åtkomstmöjlighet till samtliga ospärrade personuppgifter i Melior hos andra vårdgivare inom ramen för den sammanhållna journalföringen.

En vårdenhetsroll ger ingen åtkomst till uppgifter hos andra vårdgivare, utan enbart till personuppgifter från den vårdenhet som vårdenhetsrollen avser. Vårdenhetsrollen används även för att spärra uppgifter.

Vårdenhetsrollen används av vårdpersonal inom den vårdenhet personalen tillhör, för att kunna dokumentera och läsa såväl spärrad som ospärrad information inom den egna vårdenheten utan att behöva ange samtycke eller nödåtkomst (eftersom detta sker inom den vårdenhet som informationen är spärrad till). Rollen tilldelas bara den personal som har ett uppdrag på aktuell vårdenhet. Systemtekniskt används denna roll vid spärrhantering för att tilldela rättigheter på vårdkontakt genom att peka ut vilken vårdenhet som får läsa och då blir automatiskt alla andra roller obehöriga.

De övriga rollerna som kräver unik behörighet motsvarar vårdgivarrollen, men har olika namn för att tydliggöra för vilken eller vilka arbetsuppgifter befattningshavaren tagit del av personuppgifter. Denna lösning underlättar för patienterna att få reda på i vilken roll en personal tagit del av uppgifterna.

Regionen uppger att det finns nya riktlinjer för behörighetsstyrningen, som även lämnas in till Datainspektionen under inspektionen och har bifogats protokollet, där det anges tydligare att verksamhetschefen ska göra en behovs- och riskanalys i samband med behörighetstilldelningen. Det beskrivs även hur denna ska göras samt att det ska ske en omprövning av behörigheterna varje år. Det finns även en framtagen mall för detta.

Datainspektionen har tagit del av riktlinjerna - *”Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter*” - och i dessa finns tydliga instruktioner om hur en behovs- och riskanalys ska genomföras utifrån bestämmelserna i patientdatalagen och HSLF-FS 2016:40. Det framgår även av riktlinjerna att regionen i september 2011 genomförde ”en övergripande behovs- och riskanalys utifrån tre patientscenarier som identifierades. Analysgruppen föredrog då en lösning där personal gavs en vid behörighet till patientuppgifter inom vårdgivaren. Detta skulle öka patientsäkerheten då tillgång till underlag finns för genomförande av korrekt behandling. Analysgruppen bedömde att riskerna med vid behörighet kunde hanteras med hjälp av loggkontroll. Man konstaterade också att fortsatt arbete är nödvändigt för att i detalj analysera behörighetstilldelningen till journalsystemet”.

Vidare anges i behovs- och riskanalysen att det ska vara en *”koppling mellan yrkeskategori eller verksamhetsställe som en medarbetare tillhörde och dennes behov av behörighet. Detta är inte är i enlighet med Patientdatalagen där*

behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter". Därefter beskrivs grunderna för hur tilldelning av behörigheter ska ske, rutin för genomförande samt grundläggande regler.

Alla åtkomster loggas, men följs inte upp specifikt. Regionen uppger dock att det av regionens riktlinjer som finns för logguppföljning, framgår att uppföljning ska ske t.ex. vad avser forcering av spärr.

Spärrhantering i Melior

Regionen uppger att det efter Datainspektionens förra tillsyn har gjorts två stora uppdateringar av Melior; år 2015 infördes aktiva val och år 2017 infördes s.k. *"hård spärr"*, vilket innebär att patientuppgifter tekniskt kan spärras inom ramen för sammanhållen journalföring. En teknisk funktion för *"inre spärr"*, dvs. spärr inom ramen för den egna verksamheten, fanns redan vid förra inspektionstillfället och denna spärr sätts manuellt.

Det finns idag ca 5000 patienter som har begärt spärrade journaler, vilket innebär spärrade vårdkontakter i någon form.

Spärr enligt 4 kap. patientdatalagen

Inom regionen kan användaren ta del av spärrade uppgifter om en patient, men får inte göra detta utan patientens samtycke enligt 4 kap. 5 § första stycket punkt 1 patientdatalagen. När det gäller den "inre spärren" så spärras vårdkontakten, dvs. den dokumentation som upprättas kring ett vårdtillfälle eller en vårdepisod. Regionen uppger att det är vårdenhetsrollen som används för att sätta spärr, och att det alltid görs en spärranteckning i journalen när en spärr sätts. Detta görs för att vårdpersonalen ska komma ihåg att anmäla spärr när nya vårdkontakter upprättas.

För att komma åt spärrad information utan att behöva forcera spärren, måste användaren ha en vårdenhetsroll. Det går alltså inte att komma åt en spärrad information om användaren enbart har en vårdgivarroll. Om användaren endast har behörighet utifrån en vårdgivarroll, måste användaren även få behörighet utifrån en vårdenhetsroll för att komma åt den spärrade informationen.

Melior möjliggör spärr framåt i tiden om den framtida uppgiften hör till samma vårdkontakt.

Om en användare forcerar en spärr ska detta dokumenteras och kommenteras.

Patientens möjlighet att begränsa elektronisk åtkomst för vårdsyfte

Med vårdgivarrollen har vårdpersonal möjlighet att öppna och läsa spärrad information från en annan vårdenhet inom vårdgivaren om samtycke från patienten för åtkomst föreligger, alternativt att det är fråga om en nödåtkomst i en akut situation där patienten inte kan tillfrågas. Vårdpersonalen måste ange vilken av dessa förutsättningar som är tillämplig innan informationen blir tillgänglig, och sätter då ett kryss i en av två rutor.

För att användaren sedan ska kunna gå vidare i Melior måste användaren även skriva en kommentar i en kommentarruta. Vad som de facto skrivs i rutan har egentligen ingen betydelse, utan det räcker med att ”något” skrivs där för att användaren ska kunna gå vidare i Melior.

Regionen uppger att det inte går att kontrollera om användaren rent faktiskt har fått patientens samtycke eller inte, innan användaren sätter krysset i rutan. Regionen uppger även att regionen har svårt att se att någon sådan kontroll skulle vara tekniskt möjlig att implementera.

Spärr enligt 6 kap. patientdatalagen

I dagsläget ingår, enligt uppgift, 17 vårdgivare i Melior.

Om patienten begär en spärr inom ramen för sammanhållen journalföring spärras uppgifterna med en teknisk funktion, vilket gör det omöjligt för andra vårdgivare att ta del av uppgifter om patienten. Denna s.k. ”hårda spärr” infördes under våren 2017.

Under en speciell ikon på journalmappen kan användaren se om det finns spärrad information hos en annan vårdgivare, denna kan dock inte öppnas.

Eftersom spärren vid sammanhållen journalföring är en hård teknisk spärr kan den inte forceras i systemet, utan administrativ teknisk personal måste vidta åtgärder om en sådan ska hävas – t.ex. vid nödöppning. En sådan hävning kan bara ske på uppdrag av den vårdgivare som satt spärren.

Regionen uppger att det idag saknas administrativa rutiner vad gäller hävande av spärrar inom sammanhållen journalföring utanför kontorstid. På dagtid kan man be administratören hos regionen att häva spärren.

Spärrar i andra system

Spärrar som är satta i Melior gäller endast i Melior. Om användaren gör ett s.k. uthopp, dvs. får åtkomst till ett annat system via Melior exempelvis till röntgensystemet Sektra Ris, beror patientens spärrmöjligheter på hur det ser ut i detta system. När det gäller Sektra Ris finns det idag inga tekniska spärrar i det systemet. Regionen uppger även att det finns vissa system som bara kan nås via Melior.

På grund av antalet system hos regionen och att systemen har olika spärrfunktioner, kan det vara svårt för administrationen att i praktiken hantera en begäran från en patient om att spärra allt hos regionen. Regionen uppger att det inte sker några specifika informationsinsatser till patienterna vad gäller hänvisning att enskilda system inom regionen saknar spärrfunktioner. Det finns däremot information om patienters rättigheter och möjligheter att begära spärr och vad detta innebär.

Administration av spärr inom regionen

Regionen uppger att om en patient vill begära spärr kan patienten göra det via 1177.se eller genom att fylla i och skicka in en blankett. En kopia av blanketten ”*Ansökan om spärr av patientuppgifter*” lämnas in till Datainspektionen vid inspektionen. Av blanketten framgår att patienten ska fylla i uppgift om hos vilken vårdgivare uppgifterna finns och där spärren upprättas (regionen), uppgift om patienten, uppgift om spärråtgärd och spärrens omfattning. Spärrens omfattning består av: ”alla vårdenheter inom vårdgivaren”, ”för sammanhållen journalföring, dvs. spärra mina patientuppgifter inom angiven vårdgivare gentemot andra vårdgivare” och ”endast på specifika vårdenheter inom vårdgivaren”, och där ska patienten ange vilken/vilka vårdenheter som berörs. En underskrift av en anställd krävs i tillägg till patientens godkännande och underskrift.

På blankettens baksida finns ”Anvisningar”, där förtydliganden av begrepp görs. Ett exempelvis på detta är följande. ”Spärra för sammanhållen journalföring, dvs spärra mina patientuppgifter inom vårdgivaren gentemot andra vårdgivare – här begär patienten att hans/hennes samtliga uppgifter hos angiven vårdgivare spärras gentemot andra vårdgivare.”

När regionen hanterar en begäran från en patient om att 1) spärra hela journalen eller 2) spärra ett visst vårdtillfälle/vårdkontakt uppger regionen att de tillgodoser patientens önskemål och spärrar uppgifterna i Melior. På grund av antalet system hos regionen och att systemen har olika spärrfunktioner, kan det dock vara svårt för administrationen att i praktiken hantera en begäran från en patient om att spärra allt hos regionen.

Uppföljning av tidigare beslut rörande spärr i Melior

Datainspektionen har tidigare granskat regionen inom ramen för det s.k. ”spärrprojektet”, vilket innebar att alla landsting, regioner samt fem privata vårdgivares spärrhantering i journalsystem som innehöll vårddokumentation granskades. Ett beslut, dnr 2038-2013, fattades av inspektionen den 19 december 2014. Av beslutet framgick bl.a. att regionen dels omgående skulle införa tekniska spärrar i bl.a. Melior inom ramen för den sammanhållna journalföringen, dels att regionen inte får behandla uppgifter om patienter som har begärt spärrar fram till dess att spärrarna är införda i Melior. Detta beslut följdes nu upp av inspektionen.

Regionen uppger att bristerna i Melior numera är åtgärdade i och med den nya versionen av Melior, som infördes under våren 2017. Regionen uppger dock att regionen inte vidtog någon åtgärd fram till dess att den nya versionen infördes under våren 2017. Tanken var att regionen skulle ha infört den nya versionen tidigare, men av olika anledningar fördröjdes införandet.

Kvalitetsregister

Regionen uppger att patienten ska få information innan uppgifterna registreras i kvalitetsregistren, men att det inte finns någon central samordning av informationen.

Regionen har information på regionens webbplats. Regionen träffar registerhållare för de register som regionen är centralt personuppgiftsansvarig (CPUA) för två gånger per år. Vid dessa tillfällen står information och diskussion om patientinformationen ofta på agendan. Inom regionens kvalitetsregisternätverk (Skånsk kvalitetskraft) tas ofta frågan om patientinformation upp. I nätverket ingår företrädare för 15 större kvalitetsregister, såväl dagliga användare som registerhållare. Vidare arrangeras en gång om året en kvalitetsregisterkonferens med olika aktuella

programpunkter. På konferensen deltar ca 150-200 medarbetare med koppling till kvalitetsregister. Patientinformationen har vid flera tillfällen tagits upp.

Regionen är CPUA för ca 20 regionala kvalitetsregister, och uppger att regionen arbetar aktivt med informationen kring dessa. Regionen uppger vidare att det är verksamhetschefens ansvar att patienterna blir informerade. Regionen anser att det inte är tillräckligt att sätta upp anslag i väntrum, utan informationen ska lämnas individuellt till patienten.

Regionen uppger även att patienten kan motsätta sig registrering. Så som det hanteras inom regionen är det den personal på respektive vårdenhet som har till uppgift att överföra uppgifter till ett regionalt eller nationellt kvalitetsregister som har patientkontakt och i praktiken ska se till att patienterna informeras dels om vad kvalitetsregister har för syfte, dels vilka rättigheter patienten har. Till sin hjälp har personalen normalt stöd från kvalitetsregistrets administrativa del, t.ex. med foldrar och exempel på patientinformation. För att tillhandahålla sådant stöd har registerhållaren och CPUA en tydlig roll och regionen arbetar aktivt med information i de kvalitetsregister där regionen är CPUA.

Regionen uppger slutligen att ansvaret att information faktiskt sker till patienten ligger på den lokalt personuppgiftsansvarige vårdgivaren och i slutändan verksamhetschefen som ansvarar för att personalen känner till gällande regler och att rutiner följs. Det ingår enligt regionen i verksamhetschefens uppdrag att se till att all berörd personal har kunskap om gällande lagar, regelverk, rutiner och ansvarsfördelning. Regionen uppger att detta naturligtvis även gäller patientdatalagen och de krav som ställs både vad avser spärr och regler kring hantering av uppgifter i kvalitetsregister.

Det finns ingen central funktion som tillser att patientens motsättande omhändertas, men det finns riktlinjer beträffande hur patientens motsättande ska omhändertas. Regionen utgår från att informationen ges till patienterna. Såvitt regionen känner till följs patientens motsättande inte upp på central nivå eller hur verksamhetschefen agerar i praktiken vad gäller den information som ska lämnas till patienten.

Personuppgiftsombudet hos regionen har vid en handfull tillfällen hjälpt patienter att radera uppgifter om sig själv i utpekade kvalitetsregister. Regionen har ingen uppfattning om hur ofta det sker att patienten utnyttjar

sin rättighet att motsätta sig behandling av deras uppgifter i ett nationellt eller regionalt kvalitetsregister.

Dokumentation av åtkomsten (loggar)

Regionen uppger att det finns tillgänglig information till patienterna om hur de ska läsa sitt loggutdrag. Verktygen som beskrivs i loggen finns även beskrivet i informationen som skickas till patienten tillsammans med loggutdragen.

Ett loggutdrag avseende en patient innehåller den behandlingshistorik som finns tillgänglig kring vad som hänt med patientens personuppgifter i Melior. Det finns ingen ytterligare, mer detaljerad eller fördjupad information om användarnas åtkomst till patienternas personuppgifter lagrad i systemet. Det framgår inte från vilken vårdenhet den som loggar in tillhör. Det framgår heller inte vad användaren har gjort i dokumentationsmodulen, dvs. om användaren har skrivit, läst eller gjort något annat. Sådan detaljerad information kan regionen inte ta fram.

Det är möjligt att söka på en specifik patient eller på specifik personal. Behandlingshistoriken beskriver vilken del av journalen användaren har varit inne i, men inte specifikt vilken information (vilka vårdkontakter) som användaren tagit del av.

Även s.k. aktiva val som görs utanför den egna vårdenheten loggas. Därtill loggas spärrar, dvs. om patienten har spärr så loggas forceringen av spärren. Användningen av loggverktyget loggas inte.

Regionen har begärt utveckling av loggen. Det finns krav från regionen på bättre loggar till nästa version, men regionen vet inte om kravet kommer att realiseras eller inte. Kravställningen har översänts till Datainspektionen. Av kravställningen framgår vissa framställda önskemål vad gäller förbättringar av loggningsfunktionen i Melior, bl.a. att det ska finnas en loggningsfunktion som visar vad användaren gjort i journalen och inte bara *”att man gått in i den, dvs samma presentation som i folderlogg*”, att kunna välja enhet utifrån organisationsstrukturen samt kunna välja flera enheter samtidigt och på flera nivåer samt att enhetsnamnet ska presenteras på loggen.

SVD-projektet (Sammanhållen Digital Vårdmiljö)

Regionen informerar Datainspektionen om SVD-projektet, som är en upphandling av nästa generations journalsystem. I september 2017 meddelades ett tilldelningsbeslut. Upphandlingen har dock överklagats och ärendet ligger hos förvaltningsrätten. Tanken är att merparten av regionens it-stöd, inklusive Melior, ska ersättas av det nya systemet. Planen var att systemet skulle ha tagits i drift under hösten 2017 fram till årsskiftet. Regionen uppger att införandeprojektet kommer att sträckas över flera år.

Tidigare granskningar av regionen

I sammanhanget vill Datainspektionen informera om följande. Inspektionen har flera gånger tidigare bedrivit tillsyn mot regionen. Av intresse i sammanhanget kan nämnas följande granskningar som rörde nationella kvalitetsregister (dnr 61-2010, dnr 426-2012 och dnr 681-2013), en patients begäran om loggutdrag (dnr 1431-2013), patientens rätt till spärr (dnr 726-2011, dnr 1402-2012 och dnr 2038-2013), behovs- och riskanalys samt riktlinjer för obehörig åtkomst (dnr 1605-2013 och 686-2015) och åtkomsten till personuppgifter i systemet Sesam (dnr 1863-2015).

I beslutet den 27 mars 2015, med dnr 1605-2013, förelades regionen av Datainspektionen att ta fram en dokumenterad behovs- och riskanalys enligt Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) för Melior. Av skälen till beslutet framgår att regionen har uppgett att en behovs- och riskanalys genomfördes i september 2011 för Melior. Analysen förordar en ”vid behörighet” till patientuppgifter och riskerna med detta ”bedöms kunna hanteras” genom att ”…regelverk, logguppföljning och andra aktiviteter minskar riskerna med för mycket patientuppgifter”. Regionens sammanfattande bedömning är att fortsatt arbete är nödvändigt för att mer i detalj analysera behörighetstilldelningen till Melior. Regionen har också uppgett att nämnda analys utgjort grund för fortsatt arbete vad gäller behörighet.

Datainspektionen ansåg bl.a. att regionen inte har genomfört en behovs- och riskanalys i syfte att begränsa en användares behörighet till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, och till vad som behövs för att ge en god och säker vård.

Regionen begärde därefter omprövning av beslutet i den del som avsåg riktlinjer till befattningshavare som utför loggkontroller (dnr 686-2015). Den

del som avsåg att regionen inte har genomfört en behovs- och riskanalys i syfte att begränsa en användares behörighet till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården, begärde regionen inte omprövning av.

Skäl för beslutet

Behörighetstilldelning enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen

Det framgår av 4 kap. 2 § och 6 kap. 7 § patientdatalagen, som hänvisar till 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.

Bestämmelserna ska läsas tillsammans med 4 kap. 1-3 §§ HSLF-FS 2016:40 (jämfört med 2 kap. 6 § SOSFS 2008:14) där det bl.a. framgår att vårdgivaren, innan denne beslutar om tilldelning av behörighet, ska göra en behovs- och riskanalys.

Regionen har uppgett att det finns olika typer av roller i Melior; vårdgivarroll, vårdenhetsroll samt vissa övriga roller som kräver specifik behörighet. Det finns även nya riktlinjer för behörighetsstyrningen, där det tydligare anges att verksamhetschefen ska göra en behovs- och riskanalys i samband med behörighetstilldelningen, hur denna ska göras samt att det ska ske en omprövning av behörigheterna varje år. Det finns även en framtagen mall för detta.

Datainspektionens bedömning

Bestämmelserna i patientdatalagen syftar till att omhänderta både integritetsskydd och patientsäkerhet, se 1 kap. 2 § patientdatalagen. Lagstiftaren har således gjort en avvägning när det gäller hur informationen ska behandlas för att uppfylla såväl patientsäkerhet som integritetskrav.

Datainspektionen kan konstatera att kraven på vårdgivarens behörighetstilldelning i 4 kap. 2 § och 6 kap. 7 § patientdatalagen är tydliga.

Behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Datainspektionen kan konstatera att en majoritet av regionens användare har tilldelats en vårdgivarroll utöver en vårdenhetsroll. Den enda kategorin användare som inte har tilldelats en vårdgivarroll är undersköterskor. Detta innebär att en majoritet av regionens användare kan ta del av all ospärrad information om patienter - såväl inom den inre sekretessen hos regionen, som inom ramen för den sammanhållna journalföringen vad gäller de vårdgivare som ingår i systemet.

Eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden, är detta en vidare behörighet än vad som är tillåtet enligt patientdatalagen. Regionen bryter inte enbart mot patientdatalagens bestämmelser, utan även mot bestämmelser som rör hälso- och sjukvårdssekretess i 25 kap. offentlighets- och sekretesslagen (2009:400).

Regionen bedömer, enligt sina riktlinjer, att riskerna med en vid behörighet kan hanteras med hjälp av loggkontroll.

Datainspektionen kan konstatera att en vid behörighetstilldelning inte kan ”hanteras med hjälp av loggkontroll”. Behörighetstilldelningen är en preventiv åtgärd medan loggkontrollen är en reaktiv åtgärd. Även om en vårdgivare har en systematisk och verkningsfull loggkontroll i enlighet med bestämmelserna i patientdatalagen och HSLF-FS 2016:40, kan detta inte ersätta kravet på en individuell tilldelning av behörighet, som utgår från en väl underbyggd behovs- och riskanalys.

Regionen uppger att en behovs- och riskanalys har legat till grund för behörighetstilldelningen men då en majoritet av regionens användare har tilldelats en vårdgivarroll utöver en vårdenhetsroll, konstaterar Datainspektionen att behovs- och riskanalysen inte uppfyller kraven (jfr även Datainspektionens beslut med dnr 1605-2013).

Mot bakgrund av ovanstående kan Datainspektionen konstatera att regionen fortfarande behandlar personuppgifter i strid med 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40, eftersom regionen underlåter att begränsa behörigheterna till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Detta innebär att merparten av regionens användare har tilldelats en alltför vid behörighet i Melior, på grund av en otillräcklig behovs- och riskanalys.

Datainspektionen konstaterar vidare att regionen medvetet har valt att frångå bestämmelserna i patientdatalagen. Detta framgår av regionens egna riktlinjer som anger att den koppling som har gjorts i behovs- och riskanalysen mellan yrkeskategorier eller det verksamhetsställe som en medarbetare tillhör och dennes behov av behörighet, inte är i enlighet med patientdatalagen.

Datainspektionen förelägger regionen att begränsa behörigheterna i Melior till vad som behövs för att den enskilde 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, samt revidera behovs- och riskanalysen i enlighet med dessa bestämmelser.

Patientens rätt till spärr enligt 4 kap. 4 § och 6 kap. 2 § patientdatalagen

Reglerna om vårdgivarens skyldighet att tillhandahålla en möjlighet för patienten att spärra sin vårddokumentation i it-system återfinns i 4 kap. 4 § och 6 kap. 2 § patientdatalagen. Vidare kompletteras patientdatalagens bestämmelser av HSLF-FS 2016:40. Se särskilt 4 kap. 5 § och 4 kap. 7-8 §§ HSLF-FS 2016:40 (jämfört med 2 kap. 7-10 §§ SOSFS 2008:14).

Av 4 kap. 4 § första stycket patientdatalagen framgår att personuppgifter som dokumenterats för ändamål som anges i 2 kap. 4 § punkterna 1 och 2 hos en vårdenhet eller inom en vårdprocess, inte får göras tillgängliga genom elektronisk åtkomst för den som arbetar vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare, om patienten motsätter sig det. I sådana fall ska uppgiften genast spärras. Vårdnadshavare till ett barn har dock inte rätt att spärra barnets uppgifter. Uppgift om att det finns spärrade uppgifter får vara tillgänglig för andra vårdenheter eller vårdprocesser.

Av 6 kap. 2 § fjärde stycket patientdatalagen framgår att om en patient motsätter sig att andra uppgifter än dem som anges i andra stycket samma lagrum görs tillgängliga för andra vårdgivare genom sammanhållen journalföring ska uppgifterna genast spärras. Vårdnadshavaren till ett barn kan dock inte spärra uppgifter om barnet. Av paragrafen framgår således att patientens rätt att motsätta sig att uppgifter tillgängliggörs i den

sammanhållna journalföringen omfattar samtliga uppgifter, utom uppgift om att det finns spärrade uppgifter och vilken vårdgivare som har spärrat dessa.

Regionen har uppgett att det infördes en s.k. ”*hård spärr*” i Melior under våren 2017, vilket innebär att patientuppgifter tekniskt kan spärras inom ramen för sammanhållen journalföring. En teknisk funktion för ”*inre spärr*” fanns redan vid det förra inspektionstillfället, och denna spärr sätts manuellt.

Datainspektionens bedömning (Melior)

Datainspektionen konstaterar att det finns tekniska funktioner för spärrar i Melior - dels i den inre sekretessen, dels inom ramen för den sammanhållna journalföringen.

Patientens möjlighet att begränsa elektronisk åtkomst för vårdsyfte

Det framgår av 4 kap. 5 § patientdatalagen att en spärr enligt 4 § första stycket får hävas av en behörig befattningshavare hos vårdgivaren om

1. Patienten samtycker till det, eller
2. Patientens samtycke inte kan inhämtas och informationen kan antas ha betydelse för den vård som patienten oundgängligen behöver.

Uppgift om vårdenheter eller vårdprocesser som spärrat uppgifterna ska i det fall som avses i 2 göras tillgängliga. Därefter får bara sådana uppgifter som kan antas ha betydelse för vården av patienten göras tillgängliga.

Av förarbetena till patientdatalagen (prop. 2007/08:126 s. 243) framgår följande.

> ”Spärren kan hävas när patienten själv samtycker till det. Här räcker det alltså inte med att patienten inte motsätter sig att behörig personal vid en annan vårdenhet eller vårdprocess tar del av uppgifterna. Det fordras ett samtycke från patientens sida. Det ska vara ett sådant samtycke som avses i personuppgiftslagen (1998:204), dvs. det ska vara frivilligt, särskilt och otvetydigt. Angående dessa begrepps innebörd, se författningskommentaren till 6 kap. 3 §. Samtycket kan lämnas när som helst av patienten. Det behöver alltså inte ske i samband med något vårdtillfälle.”

Dessutom framgår följande (a.a. s. 243 fjärde stycket).

> ”Vidare kan spärren forceras av en annan vårdenhet eller vårdprocess, t.ex. akutmottagningen, om informationen kan antas ha betydelse för den vård eller behandling som patienten oundgängligen behöver. En förutsättning härför är att något samtycke inte kan inhämtas. Det kan bero på att patienten är medvetslös eller alltför medtagen för att kunna ta ställning till frågan. Vidare kan saken brådska så att det inte finns någon tid att inhämta samtycke. Om patienten i ett sådant läge är oundgängligen i behov av vård eller behandling, får spärren alltså hävas av behörig befattningshavare vid en annan vårdenhet eller vårdprocess. Det ska i princip vara fråga om en allvarlig akutsituation, då patienten på grund av sitt hälsotillstånd eller andra skäl inte kan ta ställning till samtyckesfrågan och då uppgifterna bedöms vara av vital betydelse för de vård- eller behandlingsinsatser som omgående måste sättas in. Det ska alltså av hänsyn till patientsäkerheten inte vara möjligt att avvakta en tid för att patienten ska kunna lämna sitt samtycke. En patient som i denna situation vidhåller en spärr och alltså motsätter sig att någon utanför vårdenheten eller vårdprocessen tar del av uppgifterna, ska respekteras hur ogrundad eller irrationell patientens inställning än kan tyckas vara.”

Datainspektionens bedömning

Det är bara i undantagsfall som en spärr kan forceras utan att patienten har lämnat ett samtycke till det. I alla övriga fall ska patientens samtycke inhämtas och detta samtycke ska vara frivilligt, särskilt och otvetydigt.

Regionen har uppgett att användaren måste skriva en kommentar i en kommentarruta när en spärr ska forceras, men att det räcker med att ”något” skrivs i denna ruta för att användaren ska kunna gå vidare i Melior och att det inte går att kontrollera om användaren rent faktiskt har fått patientens samtycke eller inte.

Det är regionens ansvar i egenskap av personuppgiftsansvarig att se till att dessa regler följs. Det kan ske med såväl tekniska som organisatoriska åtgärder och att de rutiner som skapas också ska följas upp.

Datainspektionen konstaterar att regionen behandlar personuppgifter utan att ha tillräckliga rutiner och uppföljning gällande hantering av samtycke, innan en spärr får hävas av en behörig befattningshavare enligt 4 kap. 5 § patientdatalagen.

Datainspektionen förelägger regionen att se till att det finns instruktioner till behöriga befattningshavare som anger när och hur spärrar kan hävas enligt 4 kap. 5 § patientdatalagen. Instruktionerna ska även omfatta hur detta ska dokumenteras. Därutöver ska regionen se till att det finns rutiner för uppföljning av att instruktionerna efterlevs.

Patientens rätt till spärr enligt 4 kap. 4 § och 6 kap. 2 § patientdatalagen i system som kan nås via Melior

Om användaren får åtkomst till ett annat system via Melior, beror patientens spärrmöjligheter på hur spärrfunktionaliteten ser ut i detta system. Det har framkommit att patienterna fortfarande inte kan motsätta sig att ingå i t.ex. röntgensystemet Sektra Ris som nås via Melior.

Datainspektionens bedömning

Enligt patientdatalagen är det vårdgivarens skyldighet att tillgodose patienternas rättighet att spärra vårddokumentation i den inre sekretessen såväl som i system för sammanhållen journalföring.

Datainspektionen vill här också påpeka att inspektionen tidigare i flera beslut har förelagt regionen, senast i dnr 2038-2013, att införa funktioner för spärrar i de system som innehåller vårddokumentation.

Datainspektionen konstaterar att regionen fortfarande behandlar personuppgifter i strid med 4 kap. 4 § och 6 kap. 2 § patientdatalagen och 4 kap. 5 § och 4 kap. 7-8 §§ HSLF-FS 2016:40, eftersom regionen fortfarande inte kan spärra vårddokumentation med en teknisk funktion i vissa system som kan nås via Melior, eftersom regionen inte kan spärra vårddokumentation med en teknisk funktion i system som kan nås via Melior, såsom Sektra Ris.

Datainspektionen förelägger därför regionen att uppfylla kravet på spärrar enligt 4 kap. 4 § och 6 kap. 2 § patientdatalagen och 4 kap. 5 § och 4 kap. 7-8 §§ HSLF-FS 2016:40, i den inre sekretessen såväl som i system för sammanhållen journalföring, genom att omgående vidta åtgärder för att införa en teknisk funktion för spärr när det gäller vårddokumentationen i de system där sådana tekniska funktioner saknas, såsom Sektra Ris.

Hantering av spärr inom regionen

När det gäller regionens blankett ”Ansökan om spärr av patientuppgifter” saknas det uppgift om vilka system regionen har och i vilka system som regionen upprättar spärrar.

Datainspektionens bedömning

Det ska av blanketten framgå vilka system som patientuppgifter kan vara aktuella i och i vilka system regionen kan upprätta spärrar. Denna information ska patienten kunna erhålla i samband med att patienten fyller i blanketten, förslagsvis under ”Anvisningar” på sid. 2.

Datainspektionen konstaterar att regionen behandlar personuppgifter i strid med 6 kap. 2 § och 8 kap. 6 § punkten 6 patientdatalagen, eftersom regionen inte informerar patienterna om vilka system som patientuppgifter kan vara aktuella i och i vilka system regionen kan upprätta spärrar.

Datainspektionen förelägger regionen att informera patienterna om vilka system som patientuppgifter kan vara aktuella i och i vilka system regionen kan upprätta spärrar. Denna information kan exempelvis ges på regionens webb. Informationen ska också framgå av blanketten gällande spärrar.

Datainspektionen vill i sammanhanget även informera om följande. Det är viktigt att patienterna på ett enkelt sätt kan ta del av blanketten som rör spärr av patientuppgifter. Även om det är bra att blanketten kan nås via 1177.se, så är det inte alla patienter som använder sig av denna tjänst. Det är således en förutsättning att blanketten även finns lätt tillgänglig, väl synlig, hos regionen så att det är enkelt för alla patienter att ta del av denna blankett.

Administrativa rutiner för hävande av spärrar

Eftersom spärren vid sammanhållen journalföring är en hård teknisk spärr kan den inte forceras i systemet, utan administrativ teknisk personal måste vidta åtgärder om en sådan ska hävas – t.ex. vid nödöppning. En sådan hävning kan bara ske på uppdrag av den vårdgivare som satt spärren.

Av 6 kap. 4 § patientdatalagen framgår att om det finns spärrade uppgifter om en patient och det föreligger fara för dennes liv eller det annars föreligger allvarlig risk för dennes hälsa, får vårdgivaren, om patienten inte kan häva spärren enligt 2 § fjärde stycket, ta del av uppgift om vilken eller vilka

vårdgivare som har spärrat uppgifterna. Om vårdgivaren med ledning av denna uppgift bedömer att de spärrade uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver, får vårdgivaren begära hos den vårdgivare som har spärrat uppgifterna att denne häver spärren.

Av 30 § första stycket personuppgiftslagen framgår bl.a. att den eller de personer som arbetar under den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Datainspektionens bedömning

Datainspektionen konstaterar att det inom regionen saknas instruktioner för hävande av spärrar inom ramen för den sammanhållna journalföringen, vilket är en förutsättning för att regionen ska kunna häva spärrarna på ett godtagbart och säkert sätt.

Datainspektionen konstaterar att regionen behandlar personuppgifter i strid med 6 kap. 4 § patientdatalagen, eftersom regionen saknar rutiner för hävande av spärrar inom ramen för den sammanhållna journalföringen i Melior.

Datainspektionen förelägger regionen att införa rutiner för att häva spärrar i enlighet med 6 kap. 4 första stycket patientdatalagen.

Kvalitetsregister

Det framgår av 7 kap. 2 § patientdatalagen att personuppgifter inte får behandlas i ett nationellt eller regionalt kvalitetsregister, om den enskilde motsätter sig det. Om den enskilde motsätter sig personuppgiftsbehandlingen sedan den påbörjats, ska uppgifter utplånas ur registret så snart som möjligt.

Det framgår vidare av 7 kap. 3 § patientdatalagen att innan personuppgifter behandlas i ett nationellt eller regionalt kvalitetsregister, ska den personuppgiftsansvarige se till att den enskilde utöver den information som ska lämnas enligt 8 kap. 6 §, får information om:

1. rätten att när som helst få uppgifter om sig själv utplånade ur registret,
2. i vilken utsträckning personuppgifter inhämtas från någon annan källa än från den enskilde själv eller dennes patientjournal, och

3. vilka kategorier av mottagare som personuppgifter kan komma att lämnas ut till.

Om det inte är möjligt att lämna informationen innan personuppgiftsbehandlingen påbörjas, ska den lämnas så snart som möjligt därefter.

Av förarbetena till patientdatalagen (prop. 2007/08:126, s. 257) framgår bl.a. följande vad gäller 7 kap. 2 § patientdatalagen.

> ”I lagen uppställs inget krav på något samtycke från den enskilde i den mening som avses i personuppgiftslagen (1998:204) som förutsättning för personuppgiftsbehandling i ett nationellt eller regionalt kvalitetsregister. I stället ges den enskilde en möjlighet att motsätta sig personuppgiftsbehandlingen. Det är en ordning som i praktiken innebär att tyst samtycke räcker för personuppgiftsbehandling i ett kvalitetsregister. Inget hindrar naturligtvis en vårdgivare från att tillämpa en ordning där samtycke inhämtas. I många fall är det i hög grad lämpligt att det görs. Den enskilde ska som huvudregel före personuppgiftsbehandlingen informeras om rätten att motsätta sig den, se 3 §” *(prop. 2007/08:126, s. 257).*

Det framgår vidare av förarbetena (a.a. s. 189 f) att:

> ”Regeringens förslag utgör en ramlag vari de yttre gränserna för den tillåtna personuppgiftsbehandlingen anges. Inom ramen överlåts det åt vårdgivarna att göra bedömningar såsom t.ex. om det för ett visst register är etiskt lämpligt med en ordning som innebär att uttryckligt samtycke till registrering i kvalitetsregister inhämtas.”

Av förarbetena till patientdatalagen (prop. 2007/08:126, s. 191) framgår bl.a. följande vad gäller 7 kap. 3 § patientdatalagen.

> ”Det är här viktigt att framhålla att det av patientdatalagens allmänna bestämmelser om information följer att särskild information om kvalitetsregisterföringen i fråga måste ges till den enskilde, inte minst i fråga om att klargöra för patienten att registreringen är frivillig. Det är också viktigt att informationen lämnas före registreringen, vilket föreslås uttryckligen i patientdatalagen.”

Det framgår vidare av förarbetena (a.a. s. 258 f) att:

> ”Informationen ska lämnas innan personuppgiftsbehandlingen påbörjas. Som framgår av andra stycket kan dock informationen lämnas efter det att personuppgiftsbehandlingen har påbörjats, om det inte är möjligt att lämna den tidigare. I paragrafen föreskrivs att informationen ska ha det innehåll som framgår av 8 kap. 6. Därutöver ska den enskilde upplysas om hans eller hennes rätt att när som helst få uppgifter utplånade ur registret. Denna rätt innefattar bl. a. en rätt att motsätta sig behandlingen även sedan den har påbörjats, se 2 §.”
>
> ”Det finns inga föreskrifter om hur informationen ska lämnas. Det har överlåtits åt varje personuppgiftsansvarig att bestämma. Det är förutsatt att varje personuppgiftsansvarig utarbetar rutiner för hur informationsskyldigheten skall fullgöras.”

Datainspektionens bedömning

Datainspektionen konstaterar att regionen bl.a. uppger att patienten ska få information innan uppgifterna registreras i kvalitetsregistren, men att det inte finns någon central samordning av informationen.

Regionen uppger även att det inte sker någon uppföljning av hur detta fungerar i praktiken, dvs. om patienterna de facto erhåller informationen från regionen.

Datainspektionen konstaterar att det är regionen, i egenskap av personuppgiftsansvarig, som ska lämna patienterna information i enlighet med 7 kap. 3 § patientdatalagen. Det är även regionen som ansvarar för att utforma rutiner så att patienternas rätt till information tillgodoses, och som ska följa upp att dessa rutiner följs.

Eftersom det är tillräckligt med ett tyst medgivande från patienten, är det av central betydelse att patienten faktiskt får del av informationen beträffande vad syftet med kvalitetsregistret är, vilka kategorier av uppgifter som behandlas samt att det finns en möjlighet att motsätta sig att ingå i detsamma.

Regionen har angett att ansvaret att informera patienterna har delegerats till verksamhetschefen. Datainspektionen vill i sammanhanget informera regionen om att den personuppgiftsansvariges ansvar inte kan delegeras.

Arbetsuppgiften kan delegeras, men det är regionen som är ansvarig för att patienterna informeras.

Mot bakgrund av ovanstående konstaterar Datainspektionen att regionen behandlar personuppgifter i strid med 7 kap. 3 § patientdatalagen, eftersom regionen som personuppgiftsansvarig inte kan säkerställa att patienterna har erhållit information innan patienters personuppgifter behandlas i kvalitetsregister.

Datainspektionen förelägger regionen att säkerställa att patienterna har erhållit information enligt 7 kap. 3 § patientdatalagen innan patienters personuppgifter behandlas i kvalitetsregister, genom att ta fram och införa rutiner och även införa funktioner som kontrollerar att rutinerna följs.

Dokumentation av åtkomsten (loggar)

När en vårdgivare utför en åtkomstkontroll granskar vårdgivaren it-systemets loggar, för att på så sätt kunna kontrollera om det t.ex. har skett någon obehörig åtkomst till personuppgifter i systemet. En åtkomstkontroll ska ske i enlighet med bestämmelserna i patientdatalagen och HSLF-FS 2016:40.

Det framgår av 4 kap. 3 § patientdatalagen att åtkomst till patientuppgifter ska dokumenteras och kunna kontrolleras. Bestämmelsen kompletteras av 4 kap. 9 § HSLF-FS 2016:40 (jämfört med 2 kap. 11 § SOSFS 2008:14). Av nämnda bestämmelse i föreskrifterna framgår att vårdgivaren ansvarar för att det i ledningssystemet finns rutiner som säkerställer att det av loggen ska framgå vilka åtgärder som har vidtagits med uppgifter om en patient, vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits, vid vilken tidpunkt åtgärderna vidtagits samt att användarens och patientens identitet ska framgå av loggarna.

Datainspektionens bedömning

Det har framkommit att det inte framgår av loggen i Melior vilka åtgärder som har vidtagits med uppgifter om en patient samt att det heller inte framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits. Regionen har kravställt för att få ”*bättre loggar till nästa version*”, bl.a. vad gäller att visa vad användaren gjort i journalen och inte bara ”*att man gått in i den, dvs. samma presentation som i folderlogg*”, att kunna välja enhet utifrån organisationsstrukturen, att kunna välja flera enheter samtidigt och på flera

nivåer samt att enhetsnamnet ska presenteras på loggen. Regionen uppger att de inte vet om kravet kommer att realiseras.

Det framgår av 4 kap. 9 § HSLF-FS 2016:40 vilken dokumentation av åtkomsten som ska framgå av loggen. Av punkterna 1-2 i nämnda bestämmelse framgår uttryckligen att loggarna ska visa vilka åtgärder som har vidtagits med uppgifter om en patient samt att det ska framgå vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits. Loggarna i Melior visar inte detta.

Genom att denna dokumentation saknas i loggen, kan regionen inte göra verkningsfulla åtkomstkontroller.

Mot bakgrund av ovanstående konstaterar Datainspektionen att regionen behandlar personuppgifter i strid med 4 kap. 3 § patientdatalagen och 4 kap. 9 § punkterna 1-2 HSLF-FS 2016:40, eftersom det av loggen inte framgår vilka åtgärder som har vidtagits med uppgifter om en patient eller vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits.

Datainspektionen förelägger regionen att vidta åtgärder så att det av loggarna, i enlighet med 4 kap. 3 § patientdatalagen och 4 kap. 9 § punkterna 1-2 HSLF-FS 2016:40, framgår vilka åtgärder som har vidtagits med uppgifter om en patient och vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits.

Patientens rätt att ta del av information från regionen

Det framgår av 8 kap. 5 § patientdatalagen att en vårdgivare på begäran av en patient ska lämna information om den direktåtkomst och den elektroniska åtkomst till uppgifter om patienten som förekommit.

Bestämmelsen kompletteras av 4 kap. 10 § HSLF-FS 2016:40 (jämfört med 2 kap. 10 § SOSFS 2018:14). Av bestämmelsen följer att av informationen som lämnas till patienten ska det framgå från vilken vårdenhet och vid vilken tidpunkt någon har tagit del av uppgifterna. Informationen ska vara utformad så att patienten kan bedöma om åtkomsten har varit befogad eller inte.

Av förarbetena till patientdatalagen (prop. 2007/08:126, s. 264 f) framgår bl.a. följande.

> Paragrafen är tillämplig inom både den allmänna och enskilda hälso- och sjukvården. Skyldigheten att lämna information är mer

> långtgående än den skyldighet som den allmänna hälso- och sjukvården har enligt tryckfrihetsförordningen att lämna ut allmänna handlingar och 15 kap. 4 § sekretesslagen (1980:100) att lämna uppgifter ur allmänna handlingar. Avsikten är att informationen ska vara anpassad och klargörande för den enskilde i syfte att han eller hon enkelt ska kunna tillgodogöra sig den. Den information som ska lämnas måsta alltså vara begriplig och vägledande för patienten när han eller hon själv ska bilda sig en uppfattning om huruvida åtkomsten varit befogad eller inte. Det bör t.ex. tydligt framgå när och från vilken enhet inom hälso- och sjukvården en slagning har skett. Vid sammanhållen journalföring bör vidare varje vårdgivare kunna redovisa vilken åtkomst till den egna verksamhetens journaluppgifter som har förekommit från andra vårdgivare. Även dessa andra mottagande vårdgivare bör kunna redovisa när direktåtkomst har använts.

Datainspektionens bedömning

Patienten har en laglig rätt att erhålla information från vårdgivaren om den direktåtkomst och den elektroniska åtkomst till uppgifter om patienten som förekommit, t.ex. från vilken vårdenhet någon har tagit del av patientens uppgifter. Det har dock framkommit att loggarna i Melior inte visar från vilken vårdenhet någon har tagit del av patientens uppgifter. Detta medför naturligtvis att patienten inte heller kan erhålla denna information från regionen.

Om patienten inte kan erhålla information om från vilken vårdenhet någon har tagit del av patientens uppgifter är det svårt för patienten att bedöma om en åtkomst har varit befogad eller inte, vilket är syftet med bestämmelsen.

Om vårdgivaren inte kan avgöra från vilken vårdenhet åtgärderna har vidtagits, kan vårdgivaren sannolikt heller inte avgöra om åtkomsten till uppgifterna har varit befogad eller inte. Detta innebär att det inte är möjligt att göra en bedömning av om någon obehörigen har tagit del av uppgifterna. Detta är en förutsättning för att vårdgivaren ska leva upp till kraven i patientdatalagen. Det är heller inte möjligt att bedöma om det har skett ett dataintrång eller annan brottslig handling.

Datainspektionen konstaterar att regionen har behandlat personuppgifter i strid med 8 kap. 5 § patientdatalagen och 4 kap. 10 § HSLF-FS 2016:40, eftersom regionen på begäran av en patient inte kan lämna information om

den direktåtkomst och den elektroniska åtkomst till uppgifter om patienten som förekommit, vilket vanligtvis sker genom utlämnande av s.k. loggutdrag.

Datainspektionen förelägger regionen att åtgärda bristen, i enlighet med 8 kap. 5 § patientdatalagen och 4 kap. 10 § HSLF-FS 2016:40, på så sätt att patienten ska erhålla information om den direktåtkomst och elektroniska åtkomst till patienten som har förekommit, vilket innebär att det ska framgå från vilken vårdenhet någon har tagit del av uppgifterna.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av juristen Maria Bergdahl. Vid den slutliga handläggningen har även it-säkerhetsspecialisten Magnus Bergström deltagit.

Katarina Tullstedt

Maria Bergdahl

Kopia till:
Personuppgiftsombud (via e-post för kännedom)