Hälso- och sjukvårdsnämnden
Region Gävleborg
801 88 Gävle

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

Datainspektionens beslut

Datainspektionen konstaterar att Hälso- och sjukvårdsnämnden i region Gävleborg behandlar personuppgifter:

1. I strid med 4 kap. 2 § och 6 kap. 7 § patientdatalagen (2008:355) eftersom det inte finns några behörighetsbegränsningar i den gemensamma databasen i huvudjournalsystemet Melior (GEM) och webbapplikationen SIEview.
2. I strid med 4 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, HSLF-FS 2016:40 (jämfört med 2 kap. 6 § Socialstyrelsens föreskrifter Informationshantering och journalföring i hälso- och sjukvården, SOSFS 2008:14), eftersom regionen inte har utfört någon behovs- och riskanalys innan behörighetstilldelningen, vilket har lett till att det saknas behörighetsbegränsningar för användarna.
3. I strid med 4 kap. 4 § patientdatalagen då det saknas en teknisk funktion för att kunna spärra vårddokumentation inom ramen för den inre sekretessen i den gemensamma databasen i huvudjournalsystemet Melior (GEM) och webbapplikationen SIEview.
4. I strid med 6 kap. 2 § patientdatalagen då det saknas en teknisk funktion för patienterna att motsätta sig att ingå i systemen för sammanhållen journalföring, vad gäller huvudjournalsystemet Melior och webbapplikationen SIEview, som regionen ingår i tillsammans med Aleris.

Datainspektionen förelägger Hälso- och sjukvårdsnämnden i region Gävleborg att:

1. Vidta åtgärder så att behörigheterna begränsas i enlighet med 4 kap. 2 § och 6 kap. 7 § patientdatalagen.
2. Uppfylla kravet på att beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys enligt 4 kap. 2 § HSLF-FS 2016:40.
3. Uppfylla kravet på spärrar enligt 4 kap. 4 § patientdatalagen i den inre sekretessen, genom att omgående vidta åtgärder för att införa en teknisk funktion för spärr när det gäller vårddokumentationen i den gemensamma databasen i huvudjournalsystemet Melior (GEM) och webbapplikationen SIEview, inklusive vårddokumentationen beträffande ”Fria aktiviteter” som är åtkomlig mellan vårdenheter.
4. Upphöra med systemen för sammanhållen journalföring, till dess att regionen har genomfört en behörighetstilldelning för användarna enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40 samt har infört tekniska funktioner för spärrar enligt 6 kap. 2 § patientdatalagen i de aktuella systemen.

Vidare förelägger Datainspektionen Hälso- och sjukvårdsnämnden i region Gävleborg att till inspektionen inkomma med en redovisning i form av en åtgärdsplan, som utvisar hur regionen snarast ska uppfylla kraven på behörighetsstyrning och tekniska funktioner för spärrar. Åtgärdsplanen ska vara Datainspektionen tillhanda senast den 22 juni 2017.

Datainspektionen förutsätter att Hälso- och sjukvårdsnämnden i region Gävleborg framöver informerar personalen om alla relevanta bestämmelser i patientdatalagen, inklusive bestämmelsen om aktiva val.

Redogörelse för tillsynsärendet

Datainspektionen har mottagit ett klagomål rörande behandling av personuppgifter som har genomförts av Hälso- och sjukvårdsnämnden i region Gävleborg (regionen). Klagomålet rör personuppgiftsbehandlingen i en ny databas hos regionen inom ramen för huvudjournalsystemet Melior, som kallas för GEM (gemensam Meliorjournal). Klagomålet kom anonymt från personal som uppgav sig arbeta hos regionen.

Datainspektionen har den 9 augusti 2016 inlett tillsyn mot regionen i syfte att granska hur GEM är uppbyggt utifrån integritetsskyddsaspekterna, t.ex. vad gäller behörighetsstyrning i enlighet med bestämmelserna i patientdatalagen. Granskningen har framförallt avgränsats till att gälla åtkomsten till vårddokumentation i den nya gemensamma databasen i Melior, GEM.
En inspektion genomfördes på plats hos regionen den 27 september 2016. Regionen har i huvudsak uppgett följande.

GEM

Regionen använder Melior som huvudjournalsystem. GEM var ett regionbeslutat verksamhetsprojekt som avslutades i april 2016 efter två års arbete. Patientsäkerheten och behovet av en samlad läkemedelslista var viktiga utgångspunkter för projektet. I arbetet deltog en projektgrupp bestående av flera olika specialister, men några jurister involverades aldrig. Projektet ledde fram till att en och samma, helt ny, databas numera används för alla verksamhetsområden inom regionen. Det är i denna databas, som kallas för GEM, som alla verksamhetsområden numera lägger in sina patientuppgifter.

Tidigare, innan projektet avslutades, bestod Melior av 15 olika databaser – en för varje verksamhetsområde. Om hälso- och sjukvårdspersonal behövde ta del av patientinformation från ett annat verksamhetsområde än det egna, fick personalen välja att klicka på knappen Domän i Melior till det aktuella verksamhetsområdets databas. Ingen separat inloggning behövdes.
De ursprungliga 15 databaserna finns fortfarande kvar för åtkomst till historisk vårddokumentation och är tillgängliga för hälso- och sjukvårdspersonal utifrån deras tidigare behörighetsprofil.

Verksamhetscheferna har tidigare bestämt vilka som ska ha tillgång till de 15 ursprungliga databaserna. När en behörighetsprofil skapades togs hänsyn till vilken yrkeskategori den anställde tillhörde samt vilken avdelning som personen arbetade vid. Det fanns även riktlinjer om att åtkomsten till BUP och psykiatrin skulle vara ”mer stängda” än de övriga databaserna. Dessa behörighetsbegränsningar finns kvar i de 15 ursprungliga databaserna.

För GEM finns det inte några behörighetsbegränsningar alls, vare sig på individ- eller gruppnivå. Alla har tillgång till allt i GEM, eftersom det har bedömts vara viktigt ur ett patientsäkerhetsperspektiv. Det finns bara två roller i journalsystemet – en för de som arbetar inom regionen och en för de

som arbetar inom Aleris (ett privat vårdföretag som driver Bollnäs sjukhus). Det har inte gjorts någon behovs- och riskanalys i samband med beslutet att tilldela samtliga denna behörighet. Det är dock möjligt att skapa fler roller i systemet.

När det gäller skyddet för personuppgifter i Melior har regionen fokuserat på uppföljningsdelen med kontroll av loggar för att upptäcka obehörig åtkomst.

I webbapplikationen SIEview finns bl.a. en sammanställning över en patients alla diagnoser och operationer samt var de är dokumenterade. Det går även att ta del av journalanteckningar via SIEview. All vårdpersonal har via denna applikation åtkomst till information i alla Melior-databaser, dvs. även till information från de 15 databaserna som funnits sedan tidigare. Vidare har personalen genom SIEview åtkomst till information från dessa databaser även om de inte normalt sett har behörighet till en viss databas, t.ex. BUP eller Psykiatri. Regionens personal har även åtkomst till uppgifter hos Aleris genom SIEview.

Spärr enligt 4 kap. patientdatalagen

Patienter kan välja att spärra vårdtillfällen inom regionen. Det finns ingen teknisk funktion som gör det möjligt att spärra alla vårdtillfällen från en viss enhet eller för en viss patient, men det går att få manuellt satta spärrar på samtliga vårdtillfällen från en enhet. Personal från andra verksamhetsområden kan då ta del av de spärrade uppgifterna (endast läsbehörighet) med funktionen ”forcera spärr”, vilket innebär ett aktivt val som måste motiveras med nödsituation eller samtycke innan åtkomsten ges. Inom det egna verksamhetsområdet finns funktionen ”Skriv i spärrad journal” som måste användas för att kunna dokumentera i en spärrad journal.

Det går inte att spärra information som benämns ”Fria aktiviteter” mellan vårdenheter. Vårdgivaren har bedömt att det är sådan information som samtliga vårdenheter behöver ta del av. Om en patient har spärrat information från ett visst vårdtillfälle visas inte diagnoskoder m.m. i SIEview.

Sammanhållen journalföring enligt 6 kap. patientdatalagen

Regionen ingår i system för sammanhållen journalföring med Aleris, vad gäller huvudjournalsystemet Melior och SIEview. För att personalen hos de båda vårdgivarna ska kunna ta del av patientinformation hos varandra, måste personalen använda funktionen ”forcera spärr”. Denna situation har dock

ingenting att göra med om patienten har begärt en spärr enligt 6 kap. patientdatalagen, utan signalerar enbart att hälso- och sjukvårdspersonalen går över en vårdgivargräns. ”Spärren” är således en signal till vårdpersonalen att man kommer att ta del av uppgifter hos en annan vårdgivare och funktionen utgör ett aktivt val. Vårdpersonalen får ange om åtkomsten sker som nödåtkomst eller registrera ett samtycke från patienten. Vid samtycke kan vårdpersonalen välja hur länge spärren ska vara ”forcerad”. Vårdpersonalen kan skriva en kommentar i ett fritextfält när ”spärren” forceras.

Spärr enligt 6 kap. patientdatalagen

Det går inte att spärra patientuppgifter med en teknisk funktion i Melior inom ramen för sammanhållen journalföring. Även om en patient väljer att motsätta sig att ingå i den sammanhållna journalföringen är det fortfarande tekniskt möjligt för vårdpersonal hos de anslutna vårdgivarna, dvs. hos regionen och Aleris, att bereda sig åtkomst till uppgifter hos den andra vårdgivaren genom att använda sig av funktionen ”forcera spärr”.

Funktionen ”forcera spärr” används dels när hälso- och sjukvårdspersonalen går över en vårdgivargräns, dels när en patient har begärt att få en spärr enligt 6 kap. patientdatalagen (samt även enligt 4 kap. patientdatalagen). Regionen uppger att det är oklart om regionens hälso- och sjukvårdspersonal vet skillnaden mellan de olika situationerna.

Information till anställda

Inom regionen hålls regelbundet utbildning för nyblivna chefer och i denna utbildning ingår information om offentlighet- och sekretesslagen och patientdatalagen. Tanken är att cheferna sedan ska förmedla kunskapen vidare till sin personal, men någon uppföljning av om detta sker i praktiken görs inte. Det finns även en möjlighet för cheferna att be någon av de som håller i utbildningen att komma ut till enheterna och informera om chefen själv begär det. Regionen uppger att det är omöjligt att hålla en central utbildning för 5 500 anställda.

De anställda har dock en möjlighet att genomgå en e-utbildning i informationssäkerhet och i den utbildningen ingår information om patientdatalagen. Utbildningen är inte obligatorisk och det finns inte någon uppföljning av hur många anställda som faktiskt går denna utbildning. Vidare

finns det information på intranätet, bl.a. i form av ”Frågor och svar” och utbildningsmaterial i form av en PowerPoint-presentation. Utbildningsmaterialet skickas regelbundet till samtliga anställda per e-post. Det finns ingen information om aktiva val och vad det innebär.

Regionen arbetar för närvarande med att ta fram en läroplattform för samtliga utbildningar som används inom regionen och genom denna plattform kommer det att bli möjligt att följa upp vilka som har eller inte har gått specifika utbildningar. Målsättningen är att plattformen ska vara på plats senast om ett halvår, och utbildningen om patientdatalagen kommer antagligen att länkas in i läroplattformen. Regionen kan komma att se över om utbildningen ska vara obligatorisk.

Regionen uppger att man kan bli bättre på att informera sina anställda med tanke på klagomålet. Regionen anser dock att det är svårt att dra några slutsatser utifrån ett brev.

Tidigare tillsyner av landstinget Gävleborg

I sammanhanget vill Datainspektionen informera om följande. Inspektionen har flera gånger tidigare bedrivit tillsyn mot landstinget Gävleborg (landstinget), numera region Gävleborg, bl.a. vad gäller behovs- och riskanalyser och spärrhantering.

I besluten den 15 juni 2012, dnr 734-2011, samt den 31 maj 2013, dnr 1523-2012, granskade Datainspektionen landstingets spärrhantering i bl.a. huvudjournalsystemet Melior. När det gäller Melior framkom att det saknades en teknisk funktion för spärrar i den inre sekretessen såväl som inom ramen för den sammanhållna journalföringen, men att en möjlighet till fullständiga tekniska spärrar planerades att vara införd under den senare delen av fjärde kvartalet 2013. Fram tills dess skulle det finnas en tillfällig övergångslösning. Datainspektionen konstaterade att landstinget hade kommit en bra bit på väg i och med detta, och förutsatte att landstinget fortsätter och slutför införandet av tekniska spärrfunktioner i enlighet med de tidsplaner som landstinget hade uppgett till Datainspektionen.

I beslutet den 27 mars 2015, dnr 1612-2013, granskade Datainspektionen bl.a. om landstinget hade en dokumenterad behovs- och riskanalys enligt 2 kap. 6 § andra stycket andra meningen SOSFS 2008:14. Av skälen till beslutet framgår att landstinget uppgett att det finns en rutin för behovs- och

riskanalyser på remiss i verksamheten samt att målet är att rutinen ska börja gälla senast den 13 januari 2014. Datainspektionen hade inget att invända mot den beskrivna rutinen, men konstaterade att någon behovs- och riskanalys innan behörighetstilldelningen inte hade genomförts. Med anledning av detta förelades landstinget att genomföra en dokumenterad behovs- och riskanalys enligt ovanstående paragraf för huvudjournalsystemet Melior.

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 själv uppgett att det inte finns några behörighetsbegränsningar vare sig på individ- eller gruppnivå i GEM, det finns enbart en roll i journalsystemet för användarna hos regionen. Det har heller inte gjorts någon behovs- och riskanalys i samband med beslutet att tilldela samtliga denna enda behörighet. Användarna hos regionen som har åtkomst till GEM har således tillgång till allt eftersom det av regionen har bedömts vara viktigt ur ett patientsäkerhetsperspektiv.

Datainspektionens bedömning

Bestämmelserna i patientdatalagen är viktade på ett sådant sätt att om vårdgivaren lever upp till kraven i bestämmelserna omhändertas 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. För att uppfylla dessa krav ska lagen följas.

Ett fungerande integritetsskydd är vidare en viktig del av patientsäkerheten så att informationen för patienten behandlas på ett för patienten betryggande sätt. Funktioner som säkrar integritetsskyddet måste därför vara inbyggda i journalsystemet för att kunna fungera i praktiken.

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. Regionen får därför inte använda endast en roll till samtliga användare, eftersom olika användare har olika arbetsuppgifter inom olika arbetsområden. Regionen bryter därmed inte enbart mot patientdatalagens bestämmelser, utan även mot bestämmelserna som rör hälso- och sjukvårdssekretess i 25 kap. offentlighets- och sekretesslagen (2009:400).

Av 4 kap. 2 § HSLF-FS 2016:40 framgår att det finns ett krav på att vårdgivaren, innan denne beslutar om tilldelning av behörighet, ska göra en behovs- och riskanalys. Datainspektionen finner det anmärkningsvärt att regionen fortfarande inte har genomfört en sådan behovs- och riskanalys, med tanke på Datainspektionens tidigare beslut (dnr 1612-2013) om föreläggande att genomföra en dokumenterad behovs- och riskanalys. Dåvarande landstinget uppgav att målsättningen var att rutinen avseende en behovs- och riskanalys skulle börja gälla senast den 13 januari 2014, men någon sådan rutin fanns inte vid inspektionstillfället. Datainspektionen kan därmed konstatera att regionen inte lever upp till ovanstående krav.

Mot bakgrund av ovanstående kan Datainspektionen konstatera att regionen behandlar personuppgifter i strid med 4 kap. 2 § och 6 kap. 7 § patientdatalagen eftersom det inte finns några behörighetsbegränsningar i den gemensamma databasen i huvudjournalsystemet Melior (GEM) och inte heller i webbapplikationen SIEview.

Vidare behandlar regionen personuppgifter i strid med 4 kap. 2 § HSLF-FS 2016:40 eftersom regionen inte har utfört någon behovs- och riskanalys innan behörighetstilldelningen, vilket har lett till att det saknas behörighetsbegränsningar för användarna.

Datainspektionen förelägger regionen att dels vidta åtgärder så att behörigheterna begränsas i enlighet med 4 kap. 2 § och 6 kap. 7 §

patientdatalagen, dels uppfylla kravet på att beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys enligt 4 kap. 2 § HSLF-FS 2016:40.

Vidare förelägger Datainspektionen regionen att till inspektionen inkomma med en redovisning, i form av en åtgärdsplan, som utvisar hur regionen ska uppfylla kraven på behörighetstilldelning i patientdatalagen. Åtgärdsplanen ska vara Datainspektionen tillhanda senast den 22 juni 2017.

Patientens rätt till spärr enligt 4 kap. 4 § och 6 kap. 2 § patient-datalagen

Reglerna om vårdgivarens skyldighet att tillhandahålla en möjlighet för patienten att spärra sin vårddokumentation i vissa 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 (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 inte finns några tekniska funktioner som tillgodoser patientens rätt att spärra sina uppgifter, varken i den inre sekretessen eller inom ramen för den sammanhållna journalföringen med

Aleris. När det gäller systemen för sammanhållen journalföring kan patienterna således inte motsätta sig att ingå i dessa system.

Det går dock att få manuellt satta spärrar på samtliga vårdtillfällen från en enhet i den inre sekretessen, men det går inte att spärra information som benämns Fria aktiviteter mellan vårdenheter. Regionen har bedömt att det är sådan information som samtliga vårdenheter behöver ta del av. Om en patient har spärrat information från ett visst vårdtillfälle visas dock inte diagnoskoder m.m. i SIEview.

Datainspektionens bedömning

Patientens rätt till spärr gäller både i den inre sekretessen såväl som i system för sammanhållen journalföring. När patienten begär att dennes vårddokumentation ska spärras får vårddokumentationen inte finnas elektronisk tillgänglig för andra vårdenheter alternativt vårdprocesser eller, via direktåtkomst, för andra vårdgivare.

Det finns heller inte något stöd i patientdatalagen för vårdgivaren att undanta viss vårddokumentation från patientens spärrmöjlighet. Detta innebär att om patienten så önskar, ska vårdgivaren spärra all vårddokumentation i t.ex. journalsystemet.

Datainspektionen kan konstatera att regionen inte uppfyller kraven i 4 kap. 4 § och 6 kap. 2 § patientdatalagen, eftersom det saknas tekniska funktioner för spärrar i de aktuella systemen.

Datainspektionen finner det anmärkningsvärt att regionen fortfarande inte, trots att patientdatalagen numera har varit gällande rätt i snart nio år, har infört en teknisk funktion för spärrar i huvudjournalsystemet Melior. Inte minst på grund av Datainspektionens tidigare beslut (se dnr 734-2011 och dnr 1523-2012) där regionen (då landstinget) uppgav att en möjlighet till fullständiga tekniska spärrar planerades att vara införd under den senare delen av fjärde kvartalet 2013 och att det fram tills dess skulle finnas en tillfällig övergångslösning.

Patientens rätt till spärr enligt 4 kap. 4 § patientdatalagen

Datainspektionen konstaterar att regionen behandlar personuppgifter i strid med 4 kap. 4 § patientdatalagen, då det saknas en teknisk funktion för att kunna spärra vårddokumentation inom ramen för den inre sekretessen i den

gemensamma databasen i huvudjournalsystemet Melior (GEM) och webbapplikationen SIEview.

Datainspektionen förelägger regionen att snarast uppfylla kravet på spärrar enligt 4 kap. 4 § patientdatalagen i den inre sekretessen, genom att omgående vidta åtgärder för att införa en teknisk funktion för spärr när det gäller vårddokumentationen i den gemensamma databasen i huvudjournalsystemet Melior (GEM) och webbapplikationen SIEview, inklusive vårddokumentationen beträffande ”Fria aktiviteter” som är åtkomlig mellan vårdenheter.

Vidare förelägger Datainspektionen regionen att till inspektionen inkomma med en redovisning i form av en åtgärdsplan, som utvisar hur regionen snarast ska uppfylla kraven på tekniska funktioner för spärrar inom ramen för den inre sekretessen. Åtgärdsplanen ska vara Datainspektionen tillhanda senast den 22 juni 2017.

Patientens rätt till spärr enligt 6 kap. 2 § patientdatalagen

För att över huvudtaget kunna ingå i ett system för sammanhållen journalföring måste vårdgivaren först leva upp till kraven som finns i 6 kap. patientdatalagen. Detta innebär bl.a. att patienterna – innan vårdgivaren går med i, eller upprättar, ett system för sammanhållen journalföring – ska få information om vad det innebär och patienten ska ha en möjlighet att motsätta sig detta (dvs. spärra sin vårddokumentation). Utöver kravet på spärrar finns det även krav på att vårdgivaren ska leva upp till bestämmelser som bl.a. rör behörighetsstyrning, patientens samtycke och åtkomstkontroll. Av förarbetena till patientdatalagen framgår att bestämmelserna i 6 kap. patientdatalagen ”sammantaget ger ett fullgott integritetsskydd som klart uppväger den föreslagna lättnaden i sekretessen” (se prop. 2007/08:126, s. 129).

Det ovanstående syftar på att journalhandlingar och annan vårddokumentation normalt sett omfattas av hälso- och sjukvårdssekretess och presumeras vara hemliga. Om vårdgivaren ingår i ett system för sammanhållen journalföring gäller dock inte hälso- och sjukvårdssekretessen på grund av en sekretessbrytande bestämmelse i 25 kap. 2 § offentlighets- och sekretesslagen.

Det finns således ingen självständig ”rättighet” för en vårdgivare att ingå i ett system för sammanhållen journalföring, om vårdgivaren inte lever upp till kraven i 6 kap. patientdatalagen. För att ha en möjlighet att ingå i ett eller flera sådana system måste vårdgivaren de facto leva upp till kraven i 6 kap. patientdatalagen.

Datainspektionen kan konstatera att regionen behandlar personuppgifter i strid med 6 kap. 2 § patientdatalagen genom att det saknas en teknisk funktion för patienterna att motsätta sig att ingå i systemen för sammanhållen journalföring, vad gäller huvudjournalsystemet Melior och webbapplikationen SIEview, som regionen ingår i tillsammans med Aleris.

Datainspektionen kan vidare konstatera att detta innebär att regionen dels inte uppfyller kravet på en individuell behörighetsstyrning i 6 kap. 7 § patientdatalagen, dels inte uppfyller kravet på att det ska finnas en teknisk funktion för spärrar enligt 6 kap. 2 § patientdatalagen. Regionen saknar således ett rättsligt stöd för att behandla personuppgifter i system för sammanhållen journalföring.

Mot bakgrund av ovan konstaterar Datainspektionen att regionen behandlar personuppgifter i strid med 6 kap. 2 § patientdatalagen genom att det saknas en teknisk funktion för patienterna att motsätta sig att ingå i systemen för sammanhållen journalföring, vad gäller huvudjournalsystemet Melior och webbapplikationen SIEview, som regionen ingår i tillsammans med Aleris.

Datainspektionen förelägger regionen att snarast upphöra med systemen för sammanhållen journalföring, till dess att regionen har genomfört en behörighetstilldelning för användarna enligt 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 § HSLF-FS 2016:40 samt har infört tekniska funktioner för spärrar enligt 6 kap. 2 § patientdatalagen i de aktuella systemen.

Vidare förelägger Datainspektionen regionen att till inspektionen inkomma med en redovisning i form av en åtgärdsplan, som utvisar hur regionen snarast ska uppfylla kraven på behörighetsstyrning och tekniska funktioner för spärrar. Åtgärdsplanen ska vara Datainspektionen tillhanda senast den 22 juni 2017.

Information till de anställda om patientdatalagen

Det finns ingen specifik bestämmelse i patientdatalagen som rör vårdgivares skyldighet att informera sin personal om hur patientuppgifter ska hanteras. Eftersom personuppgiftslagen är subsidiär i förhållande till patientdatalagen, se 1 kap. 4 § patientdatalagen, får den personuppgiftsansvarige istället söka ledning utifrån personuppgiftslagens bestämmelser.

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. Av förarbetena till personuppgiftslagen (se Personuppgiftslagen, En kommentar, Sören Öman och Hans-Olof Lindblom, tredje upplagan, 2007, s. 363) följer att det inte klart framgår av EG-direktivet hur utförliga instruktioner den personuppgiftsansvarige måste lämna sina medhjälpare samt att inte heller personuppgiftslagen ger något klart besked i frågan. ”Att det är den personuppgiftsansvarige som har ansvaret för att se till att personuppgifter behandlas bara om det är lagligt, på ett korrekt sätt och i enlighet med god sed framgår av de grundläggande krav på behandlingen av personuppgifter som anges i 9 §. Mot den bakgrunden måste utgångspunkten vara att det är den personuppgiftsansvarige som i princip har ansvaret för att instruktionerna är så tydliga att otillåten behandling inte kommer utföras.”

Regionen har bl.a. uppgett att det inte finns någon information till personalen om aktiva val och vad det innebär samt att regionen kan bli bättre på att informera sina anställda om bestämmelserna i patientdatalagen med tanke på klagomålet. Regionen anser dock att det är svårt att dra några slutsatser utifrån ett brev.

Datainspektionens bedömning

Mot bakgrund av ovanstående anser Datainspektionen att den personuppgiftsansvariges möjlighet att instruera de anställda lämpligen borde kunna ske på olika sätt, t.ex. genom skriftliga instruktioner eller olika former av utbildningsinsatser. Utgångspunkten ska vara att den personuppgiftsansvarige ger de anställda den information de behöver för att kunna förhindra eventuell otillåten personuppgiftsbehandling.

Datainspektionen konstaterar att regionen åtminstone inte har informerat personalen om aktiva val.

Datainspektionen förutsätter därför att regionen framöver informerar personalen om alla relevanta bestämmelser i patientdatalagen, inklusive bestämmelsen om aktiva val.

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)