Datainspektionen

Datum	Diarienr
2010-06-29	1390-2009

Landstingsstyrelsen
Örebro läns landsting
Box 1613
701 16 Örebro

Beslut efter tillsyn enligt personuppgiftslagen (1998:204) – Sammanhållen journalföring 6 kap. patientdatalagen

Datainspektionens beslut

Datainspektionen konstaterar att Landstingsstyrelsen, Örebro läns landsting (Landstingsstyrelsen)

1. i strid med 6 kap. 2 § 3 st. patientdatalagen tillgängliggör patientuppgifter för andra vårdgivare, samt
2. inte lever upp till kraven på behörighetsstyrning i 6 kap. 7 §, 4 kap. 2 § patientdatalagen och 2 kap. 6 § SOSFS 2008:14.

Datainspektionen förelägger Landstingsstyrelsen att

1. upphöra att tillgängliggöra patientuppgifter för andra vårdgivare till dess att berörda patienter fått information om vad den sammanhållna journalföringen innebär samt haft möjlighet att utnyttja sin rätt att motsätta sig tillgängliggörandet, samt
2. ta fram rutiner och en teknisk funktionalitet som möjliggör att behörigheterna kan begränsas till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Härutöver bedömer Datainspektionen att Landstingsstyrelsen är personuppgiftsansvarig för tillgängliggörandet, inklusive mellanlagringen, av patientuppgifter som härrör från den egna verksamheten. Datainspektionen förutsätter därför att Landstingsstyrelsen klargör detta genom att vidta relevanta korrigeringar i anslutningsavtal och personuppgiftsbiträdesavtal avseende Inera AB och Tieto.

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

Vidare bedömer Datainspektionen att Landstingsstyrelsen har förutsättningar att leva upp till kraven på åtkomstkontroll enligt 6 kap. 7 §, 4 kap. 3 § patientdatalagen och 2 kap. 11 § SOSFS 2008:14. Datainspektionen förutsätter dock att Landstingsstyrelsen utvärderar och kontinuerligt utvecklar logguppföljningarna för att uppnå en verkningsfull åtkomstkontroll i enlighet med kraven i 4 kap. 3 § patientdatalagen.

Redogörelse för tillsynsärendet

Datainspektionen genomförde den 12 och 13 oktober 2009 fyra olika inspektioner av den sammanhållna journalföring som sker i Örebro inom ramen för NPÖ, Nationell Patientöversikt. Tillsynen har omfattat hanteringen av personuppgifter i den sammanhållna journalföringen som sker genom NPÖ hos Landstingsstyrelsen, Vård- och omsorgsnämnderna Öster och Väster samt Attendo Care AB. Tillsynen är begränsad till frågor om personuppgiftsansvar samt rutiner för information till registrerade, inhämtande av samtycke inför direktåtkomst till vårddokumentation, behörighetsstyrning och åtkomstkontroll.

I ärendet har i huvudsak följande framkommit avseende Landstingsstyrelsens hantering av personuppgifter i NPÖ.

Omfattningen av den sammanhållna journalföringen

Inom ramen för den sammanhållna journalföringen i NPÖ tillgängliggör Landstingsstyrelsen sedan den 7 maj 2009 patientuppgifter, som sträcker sig tre år bakåt i tiden, om ca 270 000 patienter för Vård- och omsorgsnämnderna och Attendo Care. Dessa bedriver hälso- och sjukvård i omsorgsboenden, där de har möjlighet att bereda sig direktåtkomst till de patientuppgifter som Landstingsstyrelsen tillgängliggjort i den sammanhållna journalföringen. Vid inspektionstillfället hade direktåtkomst förekommit till uppgifter rörande 600 av de 270 000 patienterna. Vård- och omsorgsnämnderna och Attendo Care tillgängliggör inte sina patientuppgifter i den sammanhållna journalföringen.

Från och med den 6 december 2009 kan Landstingstyrelsen, Vård- och omsorgsnämnderna samt Attendo Care även bereda sig direktåtkomst till vårddokumentation om ca 450 000 patienter som Landstinget i Östergötland successivt tillgängliggör i NPÖ. Vidare innebär Landstinget i Östergötlands anslutning till NPÖ att de 270 000 patientuppgifter Landstingsstyrelsen tidigare gjort tillgängliga i NPÖ nu även tillgängliggjorts för Landstinget i Östergötland.

Längre fram i tiden står fler vårdgivare i begrepp att ansluta sig till NPÖ. Exempelvis har Landstinget i Sörmland aviserat att tillgängliggöra patientuppgifter från och med 24 juni 2010. Det innebär i sin tur att Landstinget i Sörmland också får möjlighet att ta del av Landstingsstyrelsens tidigare tillgängliggjorda patientuppgifter.

Information till patienter
Information om NPÖ framkommer i en rad olika sammanhang, framför allt i media. Informationen har bl.a. förekommit i lokalradio, lokalTV, Nerikes Allehanda, Länsposten, Länstidningen Tebladet och landstingets hemsida. Från och med december 2009 finns även viss information i kallelser inför patientbesök. Informationen har till stor del handlat om att på ett övergripande plan beskriva vad NPÖ innebär, framför allt för äldreomsorgen. I den information som går ut i samband med kallelser finns vissa uppgifter om patientens inflytande vid sammanhållen journalföring.

Informationen ovan har i vissa delar publicerats efter Landstingsstyrelsen tillgängliggjort uppgifter rörande de 270 000 patienterna.

Patienternas inflytande – spärr i sammanhållen journalföring
Vid inspektionstillfället hade ingen patient motsatt sig att patientuppgifter tillgängliggörs för andra vårdgivare.

Behörighetsstyrning vid sammanhållen journalföring
I och med att Landstinget i Östergötland i december 2009 tillgängliggjorde patientuppgifter i NPÖ, uppstod en möjlighet för Landstingsstyrelsen att låta egna användare få behörighet att genom direktåtkomst ta del av en annan vårdgivares uppgifter.

Landstingsstyrelsen uppger att huvudansvaret för behörighetstilldelningen ligger på respektive verksamhetschef. För behörighetstilldelning till NPÖ gör verksamhetschefen en bedömning om personen i sin yrkesutövning kan träffa patienter från annan vårdgivare eller vid patientkontakt kan ha behov av att ta del av medicinsk information om behandling utförts vid annan vårdgivare. Behovs- och riskanalysen innebär att verksamhetschefen gör egna bedömningar och begränsar behörigheterna dels i förhållande till medarbetarens uppdrag med patienterna, dels till vad som är nödvändigt för en god och säker vård. I riskanalysen tas hänsyn till vilka risker det kan innebära om personalen har för lite eller för mycket tillgång till patientuppgifter. Behörigheten kan dock inte avgränsas till att avse vissa patienter eller verksamheter. En tilldelad behörighet innebär således en möjlighet till direktåtkomst beträffande alla patienter vars patientuppgifter tillgängliggörs i den sammanhållna journalföringen.

De användare som tilldelas en behörighet i NPÖ ska genomgå en utbildning i patientdatalagen och i användandet av NPÖ. I samband med att användaren får sin behörighet får denne även signera en ansvarsförbindelse som förtydligar villkoren för att i ett enskilt fall bereda sig direktåtkomst till uppgifter hos andra vårdgivare. I ansvarsförbindelsen uppmärksammas även en rad andra frågor relaterade till integritetsskydd och informationssäkerhet.

Åtkomstkontroll vid sammanhållen journalföring
Åtkomst till uppgifter i den sammanhållna journalföringen loggas. Av loggarna framgår bl.a. användarens identitet, datum, klockslag, åtgärden med uppgifterna (läst, intygat m.m.) och patientens identitet.

Landstingsstyrelsen har en rutin för åtkomstkontroll vid sammanhållen journalföring. Av denna rutin följer bl.a. att loggkontroll görs av 20 slumpmässigt utvalda användare varje månad. Vidare finns ett formulär för dokumentation av genomförda loggkontroller.

Samarbeten och avtal – personuppgiftsansvar m.m.
Den vårddokumentation som Landstingsstyrelsen tillgängliggör mellanlagras av Inera AB, f.d. Sjukvårdsrådgivningen SVR AB. Det sker i form av ett index över landstingets 270 000 patienter och i vilket eller vilka vårdsystem patienterna förekommer. Hos Inera AB finns också åtkomstloggar och labsvar. Inera AB anlitar en extern leverantör, Tieto, för driften av systemet. Inera AB ägs av alla landsting och regioner gemensamt och är inte en vårdgivare (källa:www.inera.se).

Samarbetet mellan Inera AB, Landstingsstyrelsen, Vård- och omsorgsnämnderna samt Attendo Care regleras i ett anslutningsavtal. I detta avtal framgår bl.a. att Inera AB är personuppgiftsansvarig för de uppgifter som mellanlagras i NPÖ. Vid sidan om anslutningsavtalet finns ett personuppgiftsbiträdesavtal där Inera AB benämns personuppgiftsansvarig och respektive vårdgivare, t.ex. Landstingsstyrelsen, personuppgiftsbiträde. Vidare framgår av bilaga 1 till anslutningsavtalet att vårdgivaren ansvarar för att åtkomstloggar granskas, medan Inera AB svarar för att loggar skapas och görs tillgängliga för vårdgivaren en gång per månad.

Tillämpliga rättsregler m.m.
Sammanhållen journalföring regleras huvudsakligen av 6 kap. patientdatalagen (2008:355). Bestämmelser rörande personuppgiftsansvar och frågor om behörighetsstyrning och åtkomstkontroll regleras i 2 kap. 6 §, 6 kap. 7 § respektive 4 kap. patientdatalagen. Vidare kompletteras patientdatalagens bestämmelser om bl.a. behörighetsstyrning och

åtkomstkontroll av föreskrifter i 2 kap. Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården. Om inte annat följer av bestämmelser i patientdatalagen gäller dessutom personuppgiftslagen (1998:204) för vårdgivares behandling av personuppgifter.

Sammanhållen journalföring
Sammanhållen journalföring innebär en möjlighet för vårdgivare att, under förutsättning att bestämmelserna i patientdatalagen följs, ha direktåtkomst till personuppgifter som hanteras av andra vårdgivare för ändamål som rör vårddokumentation. Tillgången till information sker genom att vårdgivare gör uppgifter om en patient elektroniskt tillgängliga för andra vårdgivare som deltar i den sammanhållna journalföringen. Enkelt uttryckt kan sammanhållen journalföring således sammanfattas som möjligheten för en vårdgivare att tillgängliggöra egna uppgifter och/eller ta del av uppgifter som andra vårdgivare tillgängliggjort.

Med *direktåtkomst* avses i detta avseende bl.a. att vårddokumentation görs elektroniskt tillgänglig (lämnas ut) över vårdgivargränser utan att det föregås av en särskild sekretessprövning. Direktåtkomsten kännetecknas även av att den som tillgängliggör uppgifter saknar kontroll över vilka uppgifter övriga vårdgivare vid ett visst tillfälle tar del av.

Personuppgiftsansvar
Av den grundläggande definitionen i 3 § personuppgiftslagen följer att med personuppgiftsansvarig avses ”den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter”. Vidare följer av 2 kap. 6 § patientdatalagen att en vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. Personuppgiftsansvaret omfattar även den behandling av personuppgifter vårdgivaren utför när denne tillgängliggör egna personuppgifter eller tar del av uppgifter som en annan vårdgivare har gjort tillgängliga i den sammanhållna journalföringen. I propositionen 2007/08:126 Patientdatalag m.m. (s. 255) framgår bl.a. följande med anledning av bestämmelsen i 2 kap. 6 § patientdatalagen.

> ”Bestämmelsen är tillämplig även vid personuppgiftsbehandling vid sammanhållen journalföring. Regeln innebär bl.a. att den vårdgivare som gör en personuppgift tillgänglig för andra genom att uppgifter dokumenteras utan att spärras har personuppgiftsansvaret för att det sker på ett lagligt sätt. I ansvaret ingår att patienten i skede ett ges information om den sammanhållna journalföringen. Personuppgiftsansvaret

omfattar även den fortsatta lagringen och det tillgängliggörande som sker därefter."

Sammantaget innebär detta att en vårdgivares personuppgiftsansvar vid sammanhållen journalföring åtminstone omfattar följande.

- Att vårdgivarens eget tillgängliggörande av patientuppgifter sker enligt patientdatalagen. Exempelvis ställs krav på att patienten ska informeras och ges möjlighet att motsätta sig ett tillgängliggörande innan uppgifterna görs tillgängliga för andra vårdgivare.
- Att vårdgivarens åtkomst till patientuppgifter som andra vårdgivare tillgängliggjort sker enligt patientdatalagen. Exempelvis ställs krav på inhämtande av patientens samtycke för åtkomsten, styrning av användarnas behörigheter samt kontroll av den åtkomst som skett till uppgifter andra vårdgivare gjort tillgängliga.

Skäl för beslutet

I ärendet har framkommit att Landstingsstyrelsen tillgängliggjort patientuppgifter rörande ca 270 000 patienter för Vård- och omsorgsnämnderna, Attendo Care samt Landstinget i Östergötland. Vid inspektionstillfället hade dessa utnyttjat sin möjlighet till direktåtkomst beträffande ca 600 patienter. Vidare har Landstingsstyrelsen möjlighet att bereda sig åtkomst till patientuppgifter rörande ca 450 000 patienter som Landstinget i Östergötland successivt tillgängliggör.

Sammanhållen journalföring – krav på information innan tillgängliggörandet

Regeringens uppfattning är att tillgängliggörandet av patientuppgifter inte ska få ske innan information lämnats till patienten (prop. 2007/08:126 Patientdatalag s. 113). I 6 kap. 2 § 3st. patientdatalagen ställs därför krav på vårdgivaren att, innan uppgifter görs tillgängliga genom sammanhållen journalföring, informera patienten om vad den sammanhållna journalföringen innebär och om att patienten kan motsätta sig att uppgifter görs tillgängliga för andra vårdgivare. Även om det inte är fråga om att inhämta patientens samtycke har patienten således en rätt att motsätta sig att uppgifter tillgängliggörs (s.k. opt-out). Därmed är patientens inställning avgörande för om uppgifter över huvud taget får tillgängliggöras i den sammanhållna journalföringen.

I patientdatalagen anges inte uttryckligen vad informationen enligt ovan ska innehålla eller hur den ska ges till patienten. Utgångspunkten är dock att information ska ges om vad den sammanhållna journalföringen innebär. I propositionen förutsätter regeringen att hälso- och sjukvårdens aktörer hittar lämpliga former som är väl avvägda och anpassade till olika verksamhetsområden och till olika slags samarbeten mellan vårdgivare genom

sammanhållen journalföring samt till den enskilde patientens förmåga att ta till sig informationen. Det är Datainspektionens uppfattning att en vårdgivare, för att leva upp till informationskravet i 6 kap. 2 § 3 st. patientdatalagen, åtminstone måste lämna information om följande.

- Ändamålet med den sammanhållna journalföringen,
- vilka uppgifter, om vilka kategorier av patienter, vårdgivaren avser att tillgängliggöra,
- för vilka andra vårdgivare uppgifterna tillgängliggörs,
- vilka förutsättningar som gäller för andra vårdgivares åtkomst till uppgifterna,
- patientens rätt att spärra uppgifter, samt
- hur spärrar får hävas.

Hur information ska lämnas till patienten får den enskilde vårdgivaren avgöra utifrån omständigheterna i det enskilda fallet. I propositionen uttalar regeringen följande av intresse i sammanhanget (prop. 2007/08:126 s. 249).

> ”Något krav på att informationen ska ges i viss form – muntligt eller skriftligt – finns inte. Det är dock viktigt att den personuppgiftsansvarige utarbetar rutiner för hur informationsskyldigheten ska fullgöras. Säkra rutiner ligger i den personuppgiftsansvariges eget intresse, eftersom denne – då det gäller information till en registrerad vid personuppgiftsbehandling – anses ha bevisbördan för att obligatorisk information faktiskt har lämnats till patienten. När det gäller t.ex. patienter som inte talar svenska bör den personuppgiftsansvarige se till att någon översätter informationen eller att det finns skriftliga informationsblanketter på flera språk.”

Vidare anför regeringen att det inte är nödvändigt att informationen lämnas vid varje kontakttillfälle med en patient, under förutsättning att *inget tvivel* råder om att patienten är införstådd med vad den sammanhållna journalföringen innebär. Regeringen konstaterar även att patientdatalagen inte innehåller några särskilda bestämmelser om hur icke beslutskompetenta personer ska informeras om sammanhållen journalföring. Det innebär att information kan behöva lämnas till någon behörig ställföreträdare eller någon nära anhörig (prop. 2007/08:126 s. 250).

Sammantaget kan konstateras att det ankommer på vårdgivaren att visa att samtliga patienter som omfattas av den sammanhållna journalföringen har fått information enligt ovan, innan tillgängliggörandet. Vidare är Datainspektionens uppfattning att informationskravet bl.a. innebär att en vårdgivare behöver lämna ny, kompletterande, information till patienterna för

det fall att den sammanhållna journalföringen förändrats sedan den ursprungliga informationen lämnades. Som exempel kan nämnas att nya vårdgivare anslutit sig till den sammanhållna journalföringen och därmed fått möjlighet att ta del av patientuppgifterna.

I ärendet har Landstingsstyrelsen redogjort för hur information lämnats om sammanhållen journalföring. Det har, förutom den information som bifogas kallelser till patienter, i huvudsak utgjorts av mediala inslag i tidningar och radio. Dessa inslag, som varit fokuserade på äldreomsorg, har inte innehållit uppgifter om vilka vårdgivare som kommer att kunna ta del av patientuppgifterna. Det saknas således information om att den sammanhållna journalföringen innebär att Landstingsstyrelsen tillgängliggjort vårddokumentation om ca 270 000 patienter för Vård- och omsorgsnämnderna, Attendo Care samt Landstinget i Östergötland. Det har inte heller framgått av informationen vilka uppgifter (om vilka kategorier av patienter) Landstingsstyrelsen tillgängliggjort eller att vårddokumentationen sträcker sig tre år tillbaka i tiden. Inte heller har Landstingsstyrelsen visat att man har tagit särskild hänsyn till den enskilde patientens förmåga att ta till sig information om vad den sammanhållna journalföringen innebär.

Det framgår tydligt av patientdatalagen att det är patienten själv som avgör om patientens vårddokumentation ska vara tillgänglig för andra vårdgivare. Patientens rätt i detta avseende härrör även från hälso- och sjukvårdslagens grundläggande principbestämmelse om respekt för patientens självbestämmande och integritet samt att vården så långt möjligt ska utföras i samråd med patienten. En förutsättning för att patienten ska ha reella möjligheter att ta tillvara sin självbestämmanderätt och sitt behov av integritetsskydd, t.ex. genom att motsätta sig ett tillgängliggörande, är naturligtvis att patienten får fullständig och aktuell information. Det ska, som framgår av regeringens uttalande ovan, inte råda något tvivel om att patienten är införstådd med vad den sammanhållna journalföringen innebär. Sett mot dessa utgångspunkter är det enligt Datainspektionen anmärkningsvärt att Landstingsstyrelsen tillgängliggjort uppgifter om länets i princip samtliga patienter (ca 270 000 st.) utan att lämna information om vilka vårdgivare som kommer att ha tillgång till uppgifter, vilka uppgifter det rör samt om varje patients rätt att motsätta sig detta. Behovet av en tydlig och riktad information gör sig även starkt gällande eftersom den största delen av de patienter som omfattas av Landstingsstyrelsens tillgängliggörande inte är föremål för de andra vårdgivarnas hälso- och sjukvård. Det torde i själva verket dröja åtskilliga årtionden innan Vård- och omsorgsnämnderna eller Attendo Care ens får ett potentiellt behov av ta del av patientuppgifter rörande t.ex. de personer som idag är i tjugo-, trettio- eller fyrtioårsåldern.

Det stöds även av det faktum att det vid inspektionstillfället endast hade förekommit direktåtkomst till 600 av de 270 000 patienterna.

Mot bakgrund av ovanstående konstaterar Datainspektionen att Landstingsstyrelsen i strid med 6 kap. 2 § 3 st. patientdatalagen tillgängliggör patientuppgifter för andra vårdgivare. Datainspektionen förelägger Landstingsstyrelsen att upphöra att tillgängliggöra patientuppgifter för andra vårdgivare till dess att berörda patienter fått information om vad den sammanhållna journalföringen innebär samt haft möjlighet att utnyttja sin rätt att motsätta sig tillängliggörandet. Ett tillgängliggörande av uppgifter får sedan ske rörande de patienter som, efter att ha fått information enligt ovan, inte motsatt sig tillgängliggörandet.

Behörighetsstyrning
Av 6 kap. 7 § patientdatalagen följer att bestämmelserna om behörighetstilldelning i 4 kap. 2 § gäller även vid sammanhållen journalföring. Enligt 4 kap. 2 § patientdatalagen ska vårdgivaren begränsa en användares behörigheter till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Bestämmelsen kompletteras sedan av 2 kap. 6 § SOSFS 2008:14, där det bl.a. framgår att varje användare ska tilldelas en individuell behörighet och att vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Enligt samma föreskrift ska vårdgivaren även ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheterna.

I prop. 2007/08:126 s. 149 anför regeringen följande av intresse i sammanhanget.

> ”Generellt 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.”

I ärendet har Landstingsstyrelsen redogjort bl.a. för den behovs- och riskanalys som ska göras i samband med tilldelning av behörighet till NPÖ.

För behörighetstilldelning till NPÖ gör verksamhetschefen en bedömning om personen i sin yrkesutövning kan träffa patienter från annan vårdgivare eller vid patientkontakt kan ha behov av att ta del av medicinsk information om behandling utförts vid annan vårdgivare. Behörigheten kan emellertid inte avgränsas till att avse vissa patienter eller verksamheter. En tilldelad behörighet innebär således en möjlighet till direktåtkomst beträffande alla patienter vars patientuppgifter tillgängliggörs i den sammanhållna journalföringen. I praktiken innebär detta att en användare som tilldelas behörighet till patientuppgifter som t.ex. Landstinget i Östergötland tillgängliggjort, automatiskt får tillgång till uppgifter om samtliga 450 000 patienter.

Datainspektionen konstaterar att Landstingsstyrelsen på ett övergripande plan gör en behovs- och riskanalys och bl.a. bedömer om en enskild användare i sin yrkesutövning kan träffa patienter från annan vårdgivare. Enligt Datainspektionen är denna analys bristfällig och behöver göras på en mer detaljerad nivå. Det innebär att vårdgivaren inte endast har att bedöma om användaren i sin yrkesutövning kan träffa patienter från annan vårdgivare, utan även vilka patienter eller kategorier av patienter från andra vårdgivare det kan vara fråga om. En inriktning bör, enligt Datainspektionen, vara att en användare inte ska ha en mer vidsträckt tillgång till patientuppgifter hos andra vårdgivare än vad användaren har i sin egen verksamhet. Det faktum att en patient inte motsatt sig ett tillgängliggörande i sammanhållen journalföring medför heller inte att en användare får tilldelas vidare behörigheter än vad som behövs med hänsyn till användarens behov. En användare som endast kommer i kontakt med t.ex. patienter i en viss åldersgrupp ska således inte ha tillgång till vårddokumentation som andra vårdgivare tillgängliggjort om patienter i helt andra åldersgrupper. Sett mot denna bakgrund måste det faktum att Landstingsstyrelsen saknar möjlighet att begränsa användarnas behörigheter till vad som behövs med hänsyn till varje användares behov, enligt vår bedömning, anses som en obefogad spridning av vårddokumentation. Landstingsstyrelsen saknar därmed sammanfattningsvis både de rutiner och den tekniska funktionalitet som krävs för att leva upp till patientdatalagens bestämmelser om behörighetsstyrning.

Mot bakgrund av ovanstående konstaterar Datainspektionen att Landstingsstyrelsen, genom att ha en alltför vidsträckt behörighetstilldelning, inte lever upp till kraven på behörighetsstyrning i 6 kap. 7 § och 4 kap. 2 § patientdatalagen samt 2 kap. 6 § SOSFS 2008:14. Datainspektionen förelägger därför Landstingsstyrelsen att ta fram såväl rutiner som en teknisk funktionalitet som möjliggör att behörigheterna kan begränsas till vad som

behövs för att användaren ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Åtkomstkontroll
Av 6 kap. 7 § patientdatalagen följer att bestämmelserna om åtkomstkontroll i 4 kap. 3 § gäller även vid sammanhållen journalföring. Enligt 4 kap. 3 § patientdatalagen ska vårdgivare göra systematiska och återkommande kontroller av om någon obehörigen kommer åt patientuppgifter. Detta kompletteras sedan av 2 kap. 11 § SOSFS 2008:14, där det bl.a. framgår att vårdgivaren ska ansvara för att det finns rutiner som säkerställer att

1. det av dokumentationen av åtkomsten (loggarna) framgår vilka åtgärder som har vidtagits med patientuppgifterna,
2. det av loggarna framgår vid vilken vårdenhet och vid vilken tidpunkt åtgärderna har vidtagits,
3. användarens och patientens identitet framgår av loggarna, och
4. systematiska och återkommande stickprovskontroller av loggarna görs.

Av regeringens proposition 2007/080:126 s. 149 f framgår bl.a. följande avseende åtkomstkontroll. För att främja patientsäkerheten bör vårdgivarna åläggas att systematiskt och fortlöpande företa kontroller av om obehörig åtkomst till uppgifter om patienter förekommer. Regeringen föreslår att detta uttryckligen föreskrivs som ett krav i patientdatalagen. En sådan bestämmelse innebär inte bara att faktiska dataintrång med större säkerhet kommer att kunna beivras. Bestämmelsen bör även få en starkt avhållande verkan på personal som, om risken för upptäckt är liten, kan frestas att olovligen läsa uppgifter.

Datainspektionen anser att rutinerna för åtkomstkontroll ska vara utformade på sådant sätt att de blir verkningsfulla i förhållande till den behandling av personuppgifter som sker hos vårdgivaren. En förutsättning för detta är bl.a. att berörd personal får tydlig information om logguppföljningarna och deras syfte. Vårdgivaren måste även kontinuerligt utvärdera rutinerna för åtkomstkontroll för att säkerställa att rutinerna är verkningsfulla.

I ärendet har framkommit att åtkomst till uppgifter i den sammanhållna journalföringen loggas samt att Landstingsstyrelsen har en rutin för åtkomstkontroll. Datainspektionen bedömer att Landstingsstyrelsen har förutsättningar att leva upp till kraven på åtkomstkontroll enligt 6 kap. 7 § och 4 kap. 3 § patientdatalagen samt 2 kap. 11 § SOSFS 2008:14. Datainspektionen förutsätter dock att Landstingsstyrelsen utvärderar och kontinuerligt utvecklar logguppföljningarna för att uppnå en verkningsfull åtkomstkontroll i enlighet med kraven i 4 kap. 3 patientdatalagen. Behovet av

en kontinuerlig utveckling av åtkomstkontrollen är särskilt stort med tanke på att nya användare tilldelas behörighet och nya vårdgivare ansluter sig till NPÖ.

Personuppgiftsansvar och personuppgiftsbiträde
I ärendet har bl.a. framkommit att Inera AB (f.d. Sjukvårdsrådgivningen SVR AB) mellanlagrar Landstingsstyrelsens vårddokumentation i form av ett index över de ca 270 000 patienterna och de vårdsystem patienterna förekommer i. Inera AB anlitar en extern IT-leverantör, Tieto, för driften av systemet.

Samarbetet mellan Inera AB och Landstingsstyrelsen regleras i ett anslutningsavtal, där det bl.a. framgår att Inera AB är personuppgiftsansvarig för de uppgifter som mellanlagras i NPÖ. Vid sidan om anslutningsavtalet finns ett personuppgiftsbiträdesavtal där Inera AB benämns personuppgiftsansvarig och respektive vårdgivare, t.ex. Landstingsstyrelsen, personuppgiftsbiträde.

Av den grundläggande definitionen i 3 § personuppgiftslagen följer att med personuppgiftsansvarig avses ”den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter”. Vidare följer av 2 kap. 6 § patientdatalagen att en vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. Personuppgiftsansvaret omfattar även den behandling av personuppgifter vårdgivaren utför när denne tillgängliggör egna personuppgifter eller tar del av uppgifter som en annan vårdgivare har gjort tillgängliga i den sammanhållna journalföringen.

Med personuppgiftsbiträde avses enligt 3 § personuppgiftslagen ”den som behandlar personuppgifter för den personuppgiftsansvariges räkning”.

Mot bakgrund av ovanstående bedömer Datainspektionen att Landstingsstyrelsen, inte Inera AB, är personuppgiftsansvarig för tillgängliggörandet, inklusive mellanlagringen, av patientuppgifter som härrör från den egna verksamheten. Om Landstingsstyrelsen anlitar en extern IT-leverantör för driften av ett system, inklusive hantering av personuppgifter, är denne att betrakta som ett personuppgiftsbiträde. Datainspektionen förutsätter därför att Landstingsstyrelsen klargör detta i förhållande till Inera AB och Tieto samt vidtar relevanta korrigeringar i anslutningsavtal och personuppgiftsbiträdesavtal.

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

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, teamledaren Suzanne Isberg, IT-säkerhetsspecialisten Magnus Bergström och juristen Patrik Sundström, föredragande.

Göran Gräslund

Patrik Sundström

Kopia till:
Personuppgiftsombudet Mikael Eriksson, Örebro läns landsting, Box 1613, 701 16 Örebro

Projektledaren Ulrika Landström, e-post Ulrika.landstrom@orebroll.se

Regionala tillsynsenheten, Socialstyrelsen, Box 423, 701 48 Örebro

Samtliga landsting och regioner samt Gotlands kommun, enligt lista på http://www.skl.se/web/Landsting.aspx (se bilaga)