Datainspektionen

Beslut
2014-06-02

Diarienr
137-2014

Landstingsstyrelsen
Landstinget i Uppsala län
Box 602
751 25 Uppsala

Tillsyn av Landstingsstyrelsen, Landstinget i Uppsala län, i anledning av ”Min journal via nätet”

Datainspektionen meddelar följande

BESLUT

Landstingsstyrelsen, Landstinget i Uppsala län har i strid med 5 kap. 4 och 5 §§ patientdatalagen (2008:355) gett ombud för enskilda direktåtkomst till landstingets personuppgifter om de enskilda.

Landstingsstyrelsen, Landstinget i Uppsala län har i strid med 31 § personuppgiftslagen underlåtit att föra behandlingshistorik (loggar) över den enskilde patientens åtkomst till uppgifter om sig själv.

Landstingsstyrelsen, Landstinget i Uppsala län föreläggs att:

1. Snarast upphöra med att ge ombud för en enskild direktåtkomst till landstingets personuppgifter om de enskilda.
2. Införa loggar över den enskilde patientens åtkomst till uppgifter om sig själv.

Ärendet avslutas.

Redogörelse för tillsynsärendet

I enlighet med beslutad tillsynsplan har Datainspektionen granskat personuppgiftshanteringen som sker i samband med att Landstingsstyrelsen, Landstinget i Uppsala län (härefter Landstinget) medger den enskilde

direktåtkomst till Landstingets personuppgifter om den enskilde via Internet efter inloggning genom Mina vårdkontakter. Syftet med inspektionen har varit att kontrollera efterlevnaden av bestämmelsen i 5 kap. 5 § patientdatalagen, 2 kap. 13-15 §§ SOSFS 2008:14 samt de säkerhetsåtgärder Landstinget ska vidta till skydd för personuppgifter enligt 31 § personuppgiftslagen.

Datainspektionen har upprättat protokoll över inspektionen. Landstinget, som beretts tillfälle att yttra sig över protokollet, har kommit in med yttrande och svar på en kompletterande fråga den 3 mars 2014.

I ärendet har fråga bland annat uppkommit om Landstinget har ett rättsligt stöd när Landstinget tillåter dels att den enskilde ges möjlighet att medge ombud direktåtkomst till landstingets personuppgifter om den enskilde, dels när vårdnadshavare får direktåtkomst till Landstingets personuppgifter om vårdnadshavarens barn.

Närmare uppgifter om vad som framkommit i ärendet och därmed legat till grund för Datainspektionens bedömning framgår nedan.

Skäl för beslutet

Landstinget har bland annat uppgett följande.

Om den enskildes direktåtkomst

Inga journaluppgifter lagras i e-tjänsten ”Min journal via nätet” utan dessa hämtas omedelbart från journalsystemet Cosmic. Uppgifterna är åtkomliga för den enskilde om denne otvetydigt, elektroniskt, lämnar en anmälan bestående av:

1. En godkänd elektronisk identifikation för e-tjänsten Mina vårdkontakter och har loggat in på denna tjänst,
2. Patientens val av tjänsten ”Min journal”,
3. Att denne intygar att han/hon har tagit del av den fullständiga informationen om vart man vänder sig i det fall det uppkommer medicinska frågor eller funderingar,
4. Att patienten väljer ett av två alternativ som villkor för visning av informationen.

Denna anmälan behandlas automatiskt efter vissa kriterier, vilket innebär att de fyra villkoren ovan måste vara uppfyllda. Dessutom ska sådana informationsmängder, som landstinget på förhand har bestämt att de får visas

för patienten vid direktåtkomst, finnas i journalsystemet. I annat fall avvisas patientens anmälan och patienten informeras om detta.

Om ett ombuds direktåtkomst till den enskildes personuppgifter hos Landstinget (ombudsfunktionen)

Den enskilde kan välja att dela sin journal med ett så kallat ombud. Den enskilde går i sådana fall in i sin journal via Mina vårdkontakter och skriver in ombudets personnummer. Ombudets namn hämtas från e-tjänsten Master, och den enskilde kan sedan kontrollera att informationen är korrekt. Därefter väljer den enskilde vilka delar av journalen som ombudet ska få tillgång till och bekräftar delningen. Ombudet får då ett meddelande om delningen som denne kan acceptera och därmed få direktåtkomst till den enskildes uppgifter. Ombudet måste dock först logga in via Mina vårdkontakter. Om den enskilde har valt så kallat rådrum, dvs. att han eller hon endast vill ta del av uppgifter som är signerade och vidimerade, kan ombudet ändå välja att se allt direkt. Funktionen kan användas exempelvis när den enskilde ska in på sjukhus och vill att anhöriga ska kunna följa vad som händer. Hittills finns ett par hundra ombud.

Landstinget har, till stöd för sitt användande av ombudsfunktionen, i huvudsak uppgett följande. Den aktuella frågeställningen beträffande ombud berörs inte i propositionen till patientdatalagen. Ledning får därför sökas i personuppgiftslagen, hälso- och sjukvårdslagen samt offentlighets- och sekretesslagen. I SOU 2006:82, Patientdatalag m.m., s. 208, för utredningen ett resonemang om vad som enligt utredningen bör gälla när en registrerad har lämnat samtycke till en behandling av känsliga personuppgifter. I förarbetena till personuppgiftslagen anförs bland annat att ”Enligt regeringens uppfattning finns det, när någon har lämnat ett uttryckligt samtycke till en viss personuppgiftsbehandling, inte något integritetsskyddsintresse som gör det befogat att förbjuda den behandling som den registrerade och den personuppgiftsansvarige är överens om”.

Landstinget har vidare pekat på att enligt 2 kap. 3 § patientdatalagen får behandling av personuppgifter, som inte är tillåten enligt patientdatalagen, ändå ske om den enskilde lämnat ett uttryckligt samtycke till behandlingen, vilket Landstinget anser tyder på att en behandling av personuppgifterna på så sätt att ett ombud bereder sig tillgång till patientens journal via direktåtkomst, är laglig.

Landstinget har slutligen uppgett att ett uttryckligt lagstöd för en så kallad ombudsfunktion i ”Min journal via nätet” således saknas i patientdatalagen, men att det förda resonemanget visar att patientdatalagen ger utrymme för

den funktion som avses i ”Min journal via nätet”. Genom funktionen som den är utformad i ”Min journal via nätet” ger patienten ett uttryckligt samtycke till att efterge sekretess enligt definitionen av samtycke i personuppgiftslagen.

Om vårdnadshavares direktåtkomst till Landstingets personuppgifter om vårdgivarens barn

Vårdnadshavare har möjlighet att få direktåtkomst till sina barns journaler via Internet genom inloggning i e-tjänsten Mina vårdkontakter fram till och med att barnet är 12 år. Undantag från detta kan göras, men har ännu inte gjorts. Barn under 18 år har än så länge inte tillgång till sin egen journal, eftersom Landstinget inte vill att de ska bli tvingade till det av sina vårdnadshavare. Det finns tankar om att undantag kan göras motsvarande möjligheten för ungdomar att själva spärra sin journal, utifrån en bedömning av barnets ålder och mognad, men det finns ännu inga färdiga regler för detta.

Det så kallade barnskyddsteamet kan på egen hand, med omedelbar verkan, spärra direktåtkomsten till ett barns journal för den ena eller båda vårdnadshavarna.

Om loggar över patientens direktåtkomst

Den enskilde kan själv skriva in och sedan även ändra sina egna kontaktuppgifter och uppgifter om eventuella närstående. Den enskilde kan även skriva in information i en hälsodeklaration. Det syns därefter i loggen att det är patienten som själv har lämnat dessa uppgifter, i övrigt loggas inte patientens egen åtkomst.

Datainspektionens bedömning

Den enskildes direktåtkomst

Av 5 kap. 5 § patientdatalagen framgår att en vårdgivare får medge en enskild direktåtkomst till sådana uppgifter om den enskilde själv som får lämnas ut till honom eller henne och som behandlas för ändamål som anges i 2 kap. 4 § första stycket 1 och 2 (dvs. vårddokumentation). Den enskilde får under samma förutsättningar medges direktåtkomst till sådan dokumentation som avses i 4 kap. 3 § första stycket första meningen.

Av förarbetena till 5 kap. 5 § patientdatalagen framgår att bestämmelsen syftar till att en vårdgivare ska kunna medge enskild direktåtkomst till sin vårddokumentation. Däremot innebär bestämmelsen inte ett åliggande för en vårdgivare att tillhandahålla sådan åtkomst (prop. 2007/08:126, s. 245).

I förarbetena uttalas vidare följande (prop. 2007/08:126, s. 159).

Ett skäl som har anförts mot att ge patienter direktåtkomst till sina patientuppgifter är risken för att patienterna utsätts för påtryckningar från t.ex. anhöriga eller blivande arbetsgivare att visa dem uppgifterna. Ett sätt att begränsa denna risk är att göra uppgifterna inte alltför lätt tillgängliga. Uppgifter om en patient behöver inte med automatik finnas tillgängliga för denne via Internet enbart därför att en vårdgivare erbjuder sina patienter möjlighet att få direktåtkomst till uppgifterna. Tillgängligheten bör istället förutsätta att patienten inledningsvis på något sätt framfört önskemål till vårdgivaren om att få direktåtkomst till sina uppgifter. Denna förutsättning kommer sannolikt även innebära att det framför allt är de lite mer intresserade patienterna som kommer att ha direktåtkomst till sina patientuppgifter. En framställan om ett önskemål förutsätter ju överväganden från den enskildes sida och ett aktivt handlande. Det ger även vårdgivaren tillfälle att informera patienten om t.ex. vart han eller hon kan vända sig för att få hjälp att tyda uppgifterna. För tydlighetens skull kan tilläggas att det inte är regeringens mening att det ska krävas en formell ansökan från patienten som utmynnar i ett slags tillstånd. Alla patienter som framför önskemål till en vårdgivare som erbjuder sina patienter möjlighet att få direktåtkomst till patientuppgifter ska alltså kunna få sådan åtkomst.

Av förarbetena framgår således bland annat att uppgifterna inte ska göras ”alltför lätt tillgängliga”. Tillgängligheten bör i stället förutsätta att patienten inledningsvis på något sätt framfört önskemål till vårdgivaren om att få direktåtkomst till sina uppgifter.

När det gäller enskilda som har framfört önskemål till Landstinget om direktåtkomst, har Datainspektionen inget att erinra mot den valda lösningen. Datainspektionen förutsätter att endast sådana uppgifter som får lämnas till den enskilde görs åtkomliga via direktåtkomst.

En enskild som inte önskar någon direktåtkomst måste, som inspektionen uppfattat det, antingen själv gå in i e-tjänsten Mina vårdkontakter och där trycka på en förseglingsknapp alternativt kontakta Landstinget och be Landstinget att ”försegla” möjligheten till direktåtkomst. Den enskilde måste således själv agera för att stänga möjligheten till direktåtkomst via Mina vårdkontakter. Datainspektionen anser att en lösning där direktåtkomsten är förseglad till dess den enskilde begär att få direktåtkomst är att föredra. Mot bakgrund av hur Landstinget utformat direktåtkomsten samt att den enskilde själv kan ”försegla” direktåtkomsten, bedömer dock Datainspektionen att Landstinget inte har gjort uppgifterna ”alltför lätt tillgängliga”.

Ombuds direktåtkomst till Landstingets personuppgifter om den enskilde (ombudsfunktionen)

Av 5 kap. 4 § patientdatalagen framgår att utlämnande genom direktåtkomst till personuppgifter endast är tillåten i den utsträckning som anges i lag eller förordning. Enligt 5 kap. 5 § patientdatalagen får en enskild medges direktåtkomst till uppgifter om sig själv.

Skälet till bestämmelsen i 5 kap. 4 § är att direktåtkomst är en särskilt integritetskänslig form av elektroniskt utlämnande av personuppgifter. Enligt förarbetena finns det därför anledning att genom reglering i patientdatalagen klargöra i vilka fall direktåtkomst får förekomma till personuppgifter som behandlas enligt lagen. Sådant utlämnande bör bara få ske i den utsträckning som medges i lag eller förordning (prop. 2007/08:126, s. 76).

Frågan är om det finns rättsligt stöd för att ge ett ombud direktåtkomst till Landstingets personuppgifter om en enskild.

Till stöd för att direktåtkomst för ett ombud får ske har Landstinget anfört att det av 2 kap. 3 § patientdatalagen följer att behandling av personuppgifter som inte är tillåten enligt denna lag ändå får ske, om den enskilde lämnat ett uttryckligt samtycke till behandlingen.

Av förarbetena framgår att bestämmelsen i 2 kap. 3 § patientdatalagen ”kan sägas ge uttryck för principen att en enskilds uttryckliga samtycke till en viss personuppgiftsbehandling normalt ska respekteras. Huvudregeln i förevarande paragraf innebär således exempelvis att personuppgifter kan samlas in och behandlas för ett ändamål som inte anges i patientdatalagens ändamålsbestämning, se 4 §, om den enskilde har lämnat ett uttryckligt samtycke till detta. Något skriftligt samtycke från den enskilde fordras i och för sig inte, men det kan många gånger vara lämpligt att ha ett sådant för att förebygga eventuella framtida tvister. Huvudregeln gäller dock inte om annat framgår av patientdatalagen, annan lag eller förordning” (prop. 2007/08:126, s. 227).

Enligt Datainspektionens mening syftar bestämmelsen i 2 kap. 3 § på när en behandling av personuppgifter är *tillåten* och för *vilka ändamål* personuppgifter får behandlas.

Av förarbetena till ändamålsbestämmelserna i 2 kap. 4 § patientdatalagen framgår följande (prop. 2007/08:126, s. 227).

I paragrafens första stycke anges de primära ändamålen, alltså sådana ändamål som tar sikte på den egentliga kärnverksamheten inom hälso- och sjukvården. De primära ändamålen beskriver personuppgiftsbehandlingar som normalt äger rum i varje sjukvårdshuvudmans verksamhet. De angivna ändamålen avser inte bara den individinriktade hälso- och sjukvårdsverksamheten utan också sådana särskilda ändamål som faller vid sidan av den individinriktade verksamheten. Syftet med att ange ändamål är att slå fast en yttersta ram för när personuppgifter får samlas in och fortsättningsvis behandlas. Utgångspunkten är således att endast sådan personuppgiftsbehandling får äga rum som inryms i något eller några av de uppräknade ändamålen, se dock 5 §. Inom denna ram måste vårdgivaren i allmänhet bestämma mer konkreta och preciserade ändamål.

Inspektionen anser inte att frågan om på vilket sätt ett utlämnande kan ske utgör ett ändamål för behandlingen på så sätt att 2 kap. 3 § är tillämplig.

Datainspektionen anser att man måste skilja på sättet (hur) personuppgifterna behandlas, t.ex. utlämnande via direktåtkomst, och varför man behandlar personuppgifterna, dvs. ändamålet med behandlingen av personuppgifterna.

Vidare regleras uttömmande i 5 kap. 4 § patientdatalagen i vilka fall direktåtkomst får ske, och i den bestämmelsen saknas det stöd för den nu aktuella direktåtkomsten.

Att den enskilde lämnar ett uttryckligt samtycke till att Landstinget får medge ett ombud direktåtkomst till personuppgifter om den enskilde innebär således inte att direktåtkomsten har rättsligt stöd.

Mot bakgrund av ovanstående konstaterar Datainspektionen att Landstinget i strid med 5 kap. 4 och 5 §§ patientdatalagen medger ombud för en enskild direktåtkomst till Landstingets personuppgifter om den enskilde.

Landstinget föreläggs att snarast upphöra med att ge ombud för en enskild direktåtkomst till Landstingets personuppgifter om den enskilde.

Vårdnadshavares direktåtkomst till Landstingets personuppgifter om vårdnadshavarens barn

Av förarbetena framgår inte tydligt om ett barn har rätt att genom direktåtkomst via Mina vårdkontakter ta del av sina patientuppgifter. Där uttalas endast att den enskilde har en möjlighet att via direktåtkomst ta del av sin journal, inte från vilken ålder den enskilde ska ha denna möjlighet (prop. 2007/08:126, s. 159).

I avsaknad av uttryckliga förarbetsuttalanden anser Datainspektionen att det är rimligt att en vårdnadshavare har möjlighet att få direktåtkomst till sitt barns journaler via Mina vårdkontakter fram till dess att barnet har fyllt 12 år. Det är dock av största vikt att Landstinget, innan vårdnadshavaren medges direktåtkomst, beaktar den sekretess som kan gälla i förhållande till vårdnadshavaren.

Loggar över enskildas direktåtkomst

Av 1 kap. 4 § patientdatalagen framgår att personuppgiftslagen gäller vid behandling av personuppgifter inom Hälso- och sjukvården om inte annat följer av patientdatalagen.

Datainspektionens uppfattning är att patientdatalagens bestämmelser endast omfattar vårdgivarens skyldighet att kontrollera vårdpersonalens åtkomst, inte den enskildes egen åtkomst enligt 5 kap. 5 § patientdatalagen. I detta fall blir således personuppgiftslagen tillämplig eftersom patientdatalagen inte reglerar den aktuella personuppgiftshanteringen.

Av 31 § personuppgiftslagen framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, kostnaden för åtgärderna, särskilda risker med behandlingen och hur pass känsliga uppgifterna är.

Av författningskommentaren till 31 § personuppgiftslagen framgår att paragrafen ska ha samma innebörd som artikel 17.1 och 17.2 i EG direktivet (prop. 1997/98:44, s. 136). Av artikel 17.1 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter framgår att säkerhetsåtgärderna ska skydda personuppgifter från bland annat otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling.

Överföring av personuppgifter över ett öppet nät, till exempel internet eller sjunet, innebär enligt Datainspektionen en särskild risk för otillåten spridning av eller otillåten tillgång till uppgifterna.

Vid bedömning av hur pass känsliga uppgifterna är ska särskilt beaktas om personuppgifterna definieras som känsliga i personuppgiftslagen, om de omfattas av tystnadsplikt eller sekretess enligt offentlighets- och

sekretesslagen (2009:400) eller annan lagstiftning samt om behandlingen av dem omfattas av särreglering och vad den i så fall innebär.

Att upprätta behandlingshistorik för att dokumentera åtkomst till personuppgifter är en säkerhetsåtgärd enligt 31 § personuppgiftslagen. I fråga om behandlingshistorik (loggar) anges i Datainspektionens Allmänna råd Säkerhet för personuppgifter bland annat följande.

För att åtkomsten ska kunna kontrolleras bör det, beroende på känsligheten hos personuppgifterna, finnas en behandlingshistorik som sparas en viss tid. En behandlingshistorik bör följas upp och skyddas mot otillåtna ändringar. En behandlingshistorik bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Behandlingshistoriken bör, beroende på känsligheten hos personuppgifterna, ange till exempel läsning, ändring, utplåning eller kopiering av personuppgifter.

För att det ska gå att utreda obehörig användning av Landstingets personuppgifter om den enskilde som är tillgängliga genom direktåtkomst, har Landstinget en skyldighet enligt 31 § personuppgiftslagen att föra behandlingshistorik (loggar) över enskildas direktåtkomst.

Landstinget har i strid med 31 § personuppgiftslagen underlåtit att föra behandlingshistorik (loggar) över den enskilde patientens åtkomst till uppgifter om sig själv.

Landstinget föreläggs därför att upprätta behandlingshistorik (införa loggar) över enskildas direktåtkomst.

Övrigt

I en tjänst där Landstinget öppnar upp för direktåtkomst till patientuppgifter är det utomordentligt viktigt att säkerheten för uppgifterna som behandlas är hög.

Den information som har framkommit i ärendet föranleder inte Datainspektionen att rikta kritik mot Landstinget avseende säkerheten rörande ”Min journal via nätet”.

Inspektionen vill dock, med anledning av de höga krav på säkerhet som ställs när en vårdgivare ger den enskilde direktåtkomst till Landstingets personuppgifter om enskilda, lämna nedanstående allmänna rekommendationer på följande områden: signerade servercertifikat,

trafikövervakning, säkerhetsgranskningar samt behovet av ett strukturerat informationssäkerhetsarbete.

Signerade servercertifikat

Det har i ärendet framkommit att kommunikationen mellan patientens dator och e-tjänsten Min journal via nätet krypteringsskyddas med SSL med serverautentisering utifrån ett icke verifierbart, det vill säga av tredje part signerat, servercertifikat. Det innebär att patienter inte har någon möjlighet att kontrollera att det verkligen är Landstingets e-tjänst de kommunicerar med. Datainspektionen rekommenderar att patienter ges sådan möjlighet i situationer där patienten kan lämna in uppgifter till Landstinget via e-tjänsten.

Ett exempel på hur detta kan göras är att använda servercertifikat som signerats av en så kallad betrodd tredje part som använder en utökad valideringsfunktion för utgivningen av Landstingets certifikat, en så kallad extended validation. Ett alternativ är att publicera tillräcklig information och ge patienterna tydliga anvisningar om hur patienterna annars kan gå till väga för att kunna verifiera att det är Landstingets e-tjänst de kommunicerar med.

Trafikövervakning

Det har i ärendet framkommit att det finns funktioner för övervakning av misslyckade inloggningar och onormala trafikmönster, men att dessa endast används på förekommen anledning. Datainspektionen anser att sådana funktioner kan utgöra en del av intrångsskyddet och kan användas som ett led i skyldigheten att skydda personuppgifter från otillåten spridning av eller otillåten tillgång till uppgifterna.

Säkerhetsgranskningar

Det har i ärendet framkommit att Landstinget har genomfört tekniska säkerhetsgranskningar av infrastruktur och systemmiljö. Granskningarna har bestått av bland annat så kallad Whitebox-testning av källkod och systemarkitektur och granskning av produktionsmiljön utifrån en konsolidering av standardiserade ”security best practices” och senast rapporterade attackvektorer samt övergripande penetrationstest. Datainspektionen rekommenderar att sådana granskningar genomförs med viss regelbundenhet, till exempel i samband med större förändringar eller uppgraderingar av mjuk- eller hårdvara i anslutning till eller i kring e-tjänsten.

Behovet av ett strukturerat informationssäkerhetsarbete

Det har i ärendet framkommit att Landstinget har en strukturerad leveransprocess med kontinuerliga tester i testmiljö och acceptanstester innan driftssättning i produktionsmiljön, att det finns rutiner för avvikelsehantering och felanmälan, funktioner för trafikanalys och skydd mot överbelastningsattacker samt funktioner för kontroll av indata. Det har vidare framkommit att driften och administrationen av e-tjänsten hittills bedrivits i projektform, men att dessa uppgifter kommer att övertas av förvaltnings-organisationen. Datainspektionen vill i sammanhanget understryka behovet av ett fortsatt strukturerat informationssäkerhetsarbete hos förvaltnings-organisationen som innefattar rutiner för risk- och sårbarhetsanalyser, intrångsskydd, incidenthantering och kontinuitetsplanering för e-tjänsten.

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 för att kunna prövas. 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 generaldirektören Kristina Svahn Starrsjö efter föredragning av juristen Maria Bergdahl. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, t.f. enhetschefen Anna Hörnlund och IT-säkerhetsspecialisten Magnus Bergström deltagit.

Kristina Svahn Starrsjö

Maria Bergdahl

Kopia till:

1. Projektägare, Landstinget i Uppsala län (per e-post)
2. Informationssäkerhetsansvarig, Landstinget i Uppsala län (per e-post)