

Landstingsstyrelsen
Landstinget i Värmland
651 82 Karlstad

(er beteckning LK/052693)

Beslut efter tillsyn enligt personuppgiftslagen (1998:204)

Datainspektionens beslut

Datainspektionen bedömer att Landstingsstyrelsen, Landstinget i Värmland (landstinget) kan tillgodose de krav som ställs i 8 § lagen om vårdregister (1998:544) rörande direktåtkomst.

Datainspektionen förutsätter dock att landstinget beaktar Datainspektionens påpekanden nedan (under Datainspektionens bedömning) rörande direktåtkomst till vårdregister, logguppföljning, information, samordnad vårdplanering och avtal med personuppgiftsbiträde.

Ärendet avslutas, men kan komma att följas upp.

Bakgrund

Datainspektionen genomförde en inspektion hos landstinget den 25 april 2005. I ett beslut den 8 juli 2005 förutsatte Datainspektionen att landstinget i det fortsatta arbetet med journalsystemet Cambio COSMIC (Cosmic) utformar regler för åtkomst till patientuppgifter med utgångspunkt från vilken information personalen behöver för att utföra sitt arbete. I samma beslut gav Datainspektionen ett föreläggande för landstinget att utarbeta rutiner för att följa upp loggarna och att försäkra sig om att regelbundna kontroller faktiskt genomförs i hela organisationen.

Redogörelse för det aktuella tillsynsärendet

I syfte att följa upp beslutet genomförde Datainspektionen en ny inspektion hos landstinget den 12 december 2005. Avsikten var att kontrollera IT-säkerheten, bl.a. rutiner för uppföljning av loggar i journalsystemet Cosmic, samt få information om personuppgiftsbehandlingen i Meddix som används för samordnad vårdplanering.

På inspektionen den 12 december 2005 framkom bl.a. följande. Cosmic hade 60-70 användare på onkologkliniken på Centralsjukhuset i Karlstad. Till sommaren 2006 beräknades Cosmic ha 1000 användare i bl.a. psykiatrin. Logg fördes i Cosmic men det fanns ingen organisation för att ta hand om resultatet. Landstinget hade påbörjat ett projekt för att se över logghanteringen. Det framkom att behörighetsadministrationen skulle förbättras i en ny version av Cosmic. Det fanns en skiss till en förvaltningsorganisation för Cosmic. Meddix testades en period under hösten 2005. Frågan om vem som ”äger” informationen i Meddix skulle utredas, liksom rutiner för bevarande och gallring inkluderande gallring av personuppgifter som behandlats under försöksperioden.

Datainspektionen har härfter inhämtat kompletterande upplysningar från landstinget. Av en redogörelse från landstinget som inkom den 26 september 2006 framgår bl.a. följande.

Allmänt om Cosmic

Idag finns cirka 1000 användare av Cosmic. I början av 2008 ska införandet av Cosmic på Centralsjukhuset i Karlstad vara klart. Det finns en ny IT-organisation i landstinget. En grupp om tio personer ansvarar för förvaltningen av Cosmic. I gruppen finns en förvaltningsledare och en person med ett uttalat ansvar för logghanteringen. Landstingets säkerhetskommitté har fastställt dokumentet *Riktlinjer för Logghantering i COSMIC*, daterat den 18 september 2006. På varje ny klinik som får Cosmic utgör riktlinjerna grund för information och utbildning. Då påtalas också det lokala ansvaret för logghantering och uppföljning som åvilar respektive verksamhetschef men i praktiken utförs av lokala administratörer. Alla användare av Cosmic ska underteckna en blankett som upplyser om att vårdrelation och behov är absoluta förutsättningar för att få ta del av vårdinformation. Vårdrelation och behov definieras i blanketten. Vårdrelation innebär att man deltar i eller ansvarar för vård som är pågående, dvs. planeras, genomförs eller utvärderas. Behov beskrivs som att den vårdinformation man tar del av är väsentlig för den fortsatta bedömningen eller handläggningen. Blanketten innehåller också upplysningar om att alla registreringar i Cosmic är spårbara och kopplas till användaridentiteten samt att händelser i Cosmic följs upp regelbundet.

Tekniska funktioner

Behörighetsprofilerna är fastställda centralt medan tilldelningen av åtkomstmöjlighet sker i varje verksamhet av lokala administratörer. En uppdelning har gjorts mellan psykiatri och övrig verksamhet så att en journal skriven inom psykiatrin endast är tillgänglig inom psykiatrin. För att användaren ska få tillgång till en journal tillhörande annan verksamhet måste man aktivt välja att få denna journal presenterad. Sådana aktiva val måste göras per verksamhet, det finns ingen direktåtkomst till fullständig journal. En funktion för informationsklassning gör det möjligt att ”märka” del av vårddata som känslig alternativt mycket känslig. Om en journal innehåller informationsklassad vårddata måste man aktivt välja att bryta informationsklassningen.

Uppföljning av loggar

Riktlinjer för Logghantering i COSMIC har anvisningar om både systematisk stickprovskontroll av loggar i COSMIC och kontroller vid misstanke om missbruk av behörigheten. Enligt riktlinjerna finns det en användarmanual till logganalysfunktionen i COSMIC. Riktlinjerna anger vilka olika aspekter som granskningen ska innehålla, t.ex. vilka arbetsuppgifter personalen har och om patienten har vårdats inom den aktuella verksamheten. Ett granskningsprotokoll ska upprättas och förvaras på arbetsplatsen. Vid förvaltningsorganisationens fortlöpande möten i verksamheterna är logghanteringsfrågan en stående uppföljningspunkt på dagordningen. Den årliga verksamhetsberättelsen ska innehålla en beskrivning av logguppföljningen.

Datainspektionens bedömning

För att skyddet för patientuppgifter ska vara godtagbart ur integritetssynpunkt krävs en kombination av väl avvägda rutiner för behörighetstilldelning, administrativa rutiner och tydliga riktlinjer för när det är tillåtet att ta del av patientuppgifter. Vidare behövs funktioner i journalsystemet som exempelvis kan ställa krav på aktiva val för att nå viss information. Dessutom behövs uppföljningar av loggar och kontroller i efterhand av eventuella intrång. En annan viktig del av integritetsskyddet är att vårdpersonalen känner till reglerna för direktåtkomst och att loggen i praktiken följs upp.

Direktåtkomst till vårdregister

Enligt 8 § lag om vårdregister ska bara den som behöver tillgång till uppgifterna för att kunna utföra sitt arbete ha direktåtkomst till uppgifter i ett vårdregister. Vidare får åtkomsten endast avse de uppgifter som behövs för arbetets utförande. Bestämmelsen kan sägas motsvara vad som stadgas i 7 § patientjournalagen (1985:565) om s.k. inre sekretess, nämligen att varje journalhandling hanteras och förvaras så att obehöriga inte får tillgång till den (prop. 1997/98:108, Hälsodata- och vårdregister, s. 99).

Avgörande för hur vidsträckt behörighet en viss anställd ska ha är följaktligen behovet av uppgifter. Den personuppgiftsansvarige/vårdgivaren måste därför ordna behörighetstilldelningen på ett sådant sätt att sjukvårdsanställda inte får tillgång till fler uppgifter än vad som behövs för arbetet. Det krävs att en vårdgivare analyserar och aktivt tar ställning till vilken information som är nödvändig för en viss tjänst och utifrån detta tilldelar användaren behörighet till ett vårdregister. Det bör också finnas funktioner i journalsystemet som ställer krav på att användaren måste göra ett aktivt val för att kunna ta del av uppgifter utanför sitt ordinarie verksamhetsområde, dvs. information som kan finnas om en patient i vårdgivarens olika verksamheter ska inte vara omedelbart tillgänglig för läsning. Användarnas aktiva val kan också utgöra underlag för urval och granskning i samband med uppföljning av loggarna.

Det har framkommit i ärendet att landstinget bl.a. har rutiner för behörighetstilldelning, skriftliga riktlinjer för när det är tillåtet att ta del av patientuppgifter, funktioner i journalsystemet för aktiva val, möjlighet till

informationsklassning samt dessutom uppföljning och kontroller i efterhand av eventuella intrång. Sjukvårdspersonalen i landstinget får genom utbildning och skriftlig information kännedom om landstingets regler för direktåtkomst och att uppföljning av händelser sker regelbundet i COSMIC. Den skriftliga informationen innehåller dock inte någon hänvisning till 8 § lagen om vårdregister.

Mot bakgrund av vad som framkommit när det gäller åtkomst till vårdregistret bedömer Datainspektionen att det finns förutsättningar för att landstinget ska kunna tillgodose kraven rörande direktåtkomst i 8 § lagen om vårdregister. Datainspektionen vill dock lämna följande påpekanden.

Datainspektionen utgår från att användargränssnittet i journalsystemet har ett utgångsläge som innebär att användaren inte kan se om patienten är aktuell i någon annan verksamhet än den där användaren själv är verksam.

Det är lämpligt att landstinget, i den takt som åtkomst möjliggörs för fler användare, tar ställning till om omfattningen av eller urvalskriterierna för uppföljningen av loggarna behöver revideras. Landstinget bör också uppmärksamma mönster i åtkomsten som innebär att behörighetsprofilerna eller möjligheter till aktiva val behöver ändras.

Det är också lämpligt att informationen till användarna innehåller en hänvisning till bestämmelsen om direktåtkomst i 8 § lagen om vårdregister.

Logguppföljning

I dokumentet *Riktlinjer för Logghantering i COSMIC* har landstinget anvisningar för logghantering och kontroller av loggen.

Datainspektionen förutsätter att landstingets rutiner för granskning av loggarna också innebär att landstinget i praktiken försäkras sig om att regelbundna kontroller utförs enligt nämnda dokument.

Datainspektionen vill också framhålla betydelsen av att urvalet för logguppföljningen också omfattar aktiva val, dvs. när vårdpersonalen använder funktionen för att ta del av patientuppgifter i en annan verksamhet än den egna.

Övriga frågor

Datainspektionen anser att landstinget bör överväga att i sin information enligt 11 § lagen om vårdregister tydliggöra att vårdpersonalens åtkomst till patientuppgifter inte är begränsad till viss klinik/avdelning/– utom psykiatri – om personalen behöver ta del av patientuppgifterna för att utföra sitt arbete.

När det gäller ett meddelarsystem för samordnad vårdplanering mellan landstinget och kommunerna utgår Datainspektionen från att landstinget tar

ställning till sitt personuppgiftsansvar i förhållande till kommunernas samt att rutiner för bevarande och gallring införs för såväl försöksperioden som permanent drift.

Datainspektionen förutsätter att landstinget har ett skriftligt avtal med personuppgiftsbiträde enligt 30 § andra stycket personuppgiftslagen för distanssupporten av Cosmic.

Detta beslut har fattats av datarådet Katja Isberg Amnäs i närvaro av avdelningsdirektören Suzanne Carlsson Isberg, föredragande.

Katja Isberg Amnäs

Suzanne Carlsson Isberg

Kopia till:

Hans Ramstedt (personuppgiftsombud), Landstingshuset, 651 82 Karlstad
Cambio+ Healthcare Systems, Ågatan 40, 582 22 Linköping