VÄSTRA GÖTALANDSREGIONEN
REVISIONSENHETEN

Pressmeddelande

Från Revisionen 2008-02-28 14:00

Revisorerna synade hanteringen av personregister:

Glapp mellan SU och gällande lag - medan gymnasiestyrelsen får godkänt

- Det finns ett glapp mellan vad gällande rätt kräver och hur Sahlgrenska universitetssjukhuset hanterar patienters personuppgifter. Var god åtgärda!

Så kan man mycket kort sammanfatta en granskning som regionens revisorer låtit göra av hur sjukhuset skyddar patienternas integritet när det hanterar personuppgifter. Regionens gymnasiestyrelse innefattades också i granskningen. De brister man hittade där var små och av formell karaktär.

Syftet med granskningen var att se om organisationen för hantering av personuppgifter är ändamålsenlig och att de åtgärder som krävs för att säkerställa att personuppgifterna följer lagar och regionens egna riktlinjer. Nu var det inte så i alla delar. Granskarna hittade en del saker som man gärna ser att Sahlgrenska universitetssjukhuset åtgärdar.

För att ha bra kontroll på och god ordning i alla personregister har regionen utsett ett antal personuppgiftsombud, ett för varje nämnd eller styrelse. Ombuden har till uppgift att vid sidan om sina ordinarie befattningar bevaka att personuppgifter hanteras på rätt sätt

- **Ingen planerad kontroll eller uppföljning**

Någon planerad kontroll eller uppföljning av hur personuppgifter hanteras i regionen förekommer inte. Revisorerna menar att det kan medföra risk för att missförhållanden inte upptäcks eller för att ombuden inte anser sig ha mandat att undersöka misstänkta missförhållanden.

Personuppgiftsombuden bildar ett informellt nätverk som revisorerna vill se utvecklas till ett mer formaliserat samarbete med en formell instruktion som fastslår såväl samarbetsformer som mötesordning

Tillsammans med sjukhusets personuppgiftsombud och IT-chef fann man en del brister som

- många små register som är svåra att ha kontroll över
- onödigt många register med likartad funktion
- bristande behörighetshantering
- sekretessproblem i kommunikationen med primärvården
- tekniska problem med spärrade journaler

- sjukhusgemensamt krypteringsverktyg för känslig information saknas
- svårkontrollerad hantering av personuppgifter i samarbetet med universitet och läkemedelsföretag
- avståndet mellan informationssäkerhetschef och sjukhusdirektör för stort
- vårdspecialiserad jurist efterlyses

- **Stickprov**

Granskarna gjorde stickprov i tre känsliga personregister; en databas för borderline-patienter, ett digitalt bildarkiv och ett arkiv gällande urininkontinens.

Den information om borderline-registret som granskarna tog del av var ofullständig samtidigt som man bland annat fann

- att informationsinnehållet hade för låg säkerhetsklass,
- att patientinformation lagrats utan att forskningsprojektet påbörjats
- att patienternas samtycke inte inhämtats
- att personuppgifterna förvarades okrypterade
- att personuppgifterna inte var avidentifierade
- att säkerhetskopiering inte förekommit
- att personuppgifterna förvarades i ett USB-minne och på papper, båda i låst utrymme, samt i lösenordsskyddade en persondator

- **Bildarkiv raderat**

Ett bildarkiv vid ögonkliniken kunde inte kontrolleras eftersom det av misstag hade raderats sommaren 2006. En äldre persondator byttes ut mot en ny utan att innehållet i den gamla blev säkerhetskopierat. Forskningsmaterial som insamlats under 20 år gick förlorat.

Informationen om registret om urininkontinens var inte heller det fullständigt och granskarna fann att uppgifterna som skulle lagrats i Göteborgsuniversitets datacentral med hög säkerhet, behörighetskontroll och inloggningsregistrering i stället lagrades okrypterade i två persondatorer, en hos registeransvarig och en hos en extern statistiker. Säkerhetskopiering skötte de var för sig.

- **Hög hastighet och nya lagar**

Revisorerna anser att de regler som finns för hantering av personuppgifter inte följs fullt ut. En förklaring kan vara att sjukhuset infört ny teknik för snabbt, en annan kan vara att tidigare hårda krav på att få tillstånd från Datainspektionen försvann när datalagen ersattes med personuppgiftslagen och vårdregisterlagen.

Man anser vidare att personuppgiftsombudets avstånd till sjukhusdirektören lett till att dess kontrollverksamhet inte är effektiv nog

Vidare menar granskarna att de upptäckta bristerna visar att kunskapen om de regler och lagar som finns om personuppgifter och informationssäkerhet är för dåliga vid sjukhuset.

- **Rekommendationer**

Granskningen har resulterat i ett antal rekommendationer:

- Återkommande kontroller borde sättas i system och avrapporteras till ledningen
- Utred och åtgärda där sjukhusets personuppgiftshantering inte uppfyller lagens krav
- Utred sjukhusets ansvar när det gäller andra aktörers hantering av personuppgifter som kommer från SU
- Personuppgiftsombudet borde ha en friare organisatorisk placering med ökade resurser på områdena juridik och informationssäkerhet
- Överväg om personuppgiftsombudet ska ha roll som både ombud och informationssäkerhetschef
- Säkra skyddet och hanteringen av personuppgifter som hanteras av tredje part

- **OK för gymnasiestyrelsen**

Man tittade även på hur regionens gymnasiestyrelse och dess skolor skötte samma uppgifter, och konstaterade att få personer var berörda och att de uppgifter som förekom var förhållandevis harmlösa samt att de brister som noterades var av formell karaktär.

Läs rapporten här.

KOMMENTARER:

Kerstin Brunnström, ordförande Sahlgrenska universitetssjukhuset:

- De iakttagelser som revisionen har gjort visar att det krävs förbättringar för att SU ska hantera personuppgifter på ett sätt som är korrekt från patientsäkerhetssynpunkt.

- Det är viktigt att så sker, och styrelsen kommer att försäkra sig om att bristerna rättas till och att sjukhuset följer gällande regler.

Jan Eriksson, sjukhusdirektör Sahlgrenska universitetssjukhuset:

- Vi har tagit del av revisionsrapporten. Den visar bland annat på att personalen inom Sahlgrenska universitetssjukhuset får utbildning i hanteringen av personuppgifter men att det krävs ytterligare vaksamhet, främst vid införande av ny teknik.

- Vi tar rapporten på starkt allvar och kommer systematiskt att gå igenom revisionens synpunkter.

- Patienterna skall alltid kunna lita på att personuppgifterna hanteras på bästa sätt.

Johnny Magnusson, vice ordförande regionstyrelsen:

- Jag vet att det varit bekymmer med regionens dataverksamhet, men det verkar vara sämre än jag trott. Det krävs ett större arbete med att få ordning på vår IT och IS och tycks mig som att vi inte haft tillräckligt politiskt fokus på de här frågorna.

Lars Hansson, chef VGR IT:

- VGR IT tar inte driftansvar för information som är lokalt lagrad i persondator om vi inte tecknat separat avtal om detta. Så har inte skett i det specifika fall som

nämns i rapporten.

- Innan byte av utrustning sker har information lämnats om att information i datorn måste säkras av den enskilda användaren. Om användaren inte kan närvara vid bytet skall man påtala detta i samband med beställningen av den nya utrustningen.

- I övrigt tycker jag att dokumentet på ett mycket bra sätt beskriver de informationssäkerhetsbrister som råder och vad man måste arbeta med för att säkra framtida eventuella händelser.

Ulrik Nilsson, ordförande revisorskollegiet:

- Det här är ett viktigt område. Det handlar om både patientsäkerhet och patientintegritet. En pikant detalj i rapporten är det raderade bildarkivet vid ögonkliniken.

Bernt Sabel, förtroendevald revisor, Västra Götalandsregionen:

- Granskningen visar att regionen måste ta frågorna om it-säkerhet på större allvar. Säkerheten måste prioriteras av ledningen och byggas in i systemen från början

- Det finns ett regelverk för it-säkerhet som förmodligen behöver uppdateras, men framförallt måste det efterlevas. De personuppgiftsombud som nämnder/styrelser har till sitt förfogande behöver få en tydligare arbetsordning och ombuden måste bevaka att patienternas integritet och säkerhet skyddas. Rollen som personuppgiftsombud bör därför vara skild från rollen som ansvarig för it-säkerheten.

- Informationstekniken är i dag ett viktigt hjälpmedel för vården. De stickprov som gjorts i ett par register på SU visar dock att det kan finnas allvarliga brister i säkerheten när känsliga personuppgifter hanteras. Det är därför viktigt att bland annat kunna spåra och säkra att endast de som behöver ha tillgång till uppgifterna för att vårda patienterna får det och att uppgifterna lagras på ett säkert sätt.

- Granskningen menar, att det finns brister i verksamheten vad gäller kunskapen om, men framförallt tillämpningen av, regelverken kring personuppgifter och informationssäkerhet. Kunskapen om hur tekniken kan eller bör användas för att göra hanteringen säkrare är också dålig. För att SU ska hantera patienternas personuppgifter på ett bättre sätt krävs därför förmodligen en hel del investeringar i kunskap, utbildning och ny teknik.

- Vi förväntar oss att SU tämligen omgående åtgärdar en del av bristerna, medan andra är av mer långsiktig karaktär.

Kontaktperson: Stellan Larsson, yrkesrevisor, 0708 - 55 24 53
Bernt Sabel, förtroendevald revisor, 0705 - 85 29 14

Skapat av: Håkan Johansson Epost: hakan.johansson@vgregion.se