Granskningsrapport – Hantering av personuppgifter

Projekt: **Granskning avseende hur den personliga integriteten skyddas vid behandling av personuppgifter**

Medverkande: Joakim Eriksson, Ernst & Young
Johan Dahlsjö, Ernst & Young
Staffan Gavel, Ernst & Young

Sammanfattning

Inom Västra Götalandsregionen (VGR) har vissa centrala åtgärder vidtagits för att säkerställa att personuppgifter hanteras korrekt även om ansvaret ligger på respektive nämnd eller styrelse. I ett beslut av regionstyrelsen 1999 (RS 9/2 -99, § 40) bestäms att nämnder och styrelser skall utse personuppgiftsombud. Personuppgiftsombuden, som samarbetar i ett informellt nätverk, har att självständigt se till att de ansvariga behandlar personuppgifter i enlighet med lag och god sed.

Av den genomförda granskningen framgår att personuppgiftsombudens verksamhet främst är stödjande. Personuppgiftsombuden bidrar med informationstexter och blanketter samt ledning i diverse frågor kring exempelvis utlämnande av uppgifter eller införande av nya informationssystem. Någon strukturerad granskning eller kontroll direkt inriktad på hantering av personuppgifter genomförs däremot inte, trots att granskning är en av personuppgiftsombudens huvuduppgifter.

När det gäller vår granskning av SU pekar de iakttagelser som gjorts på att det finns ett glapp mellan vad gällande rätt kräver och hur SU hanterar patienters personuppgifter. Det är rimligt att anta att det kommer att krävas relativt stora investeringar i kunskap, utbildning och ny teknik för att åtgärda glappet. Orsaken står sannolikt att finna i det relativt snabba införandet av ny teknik. En annan orsak kan vara att kravet på Datainspektionens tillstånd för personregister upphörde i och med att datalagen ersattes med personuppgiftslagen och vårdregisterlagen.

Vår granskning av Gymnasiestyrelsen gav tidigt vid handen att den hantering som sker centralt typiskt sett inte innebär några stora integritetsrisker. Anledningen är den relativt begränsade volymen och de relativt harmlösa personuppgifter som hanteras avseende elever. När det gäller hur uppgifter hanteras av enskilda lärare eller annan skolpersonal är det mer osäkert, men vi har inte funnit något som pekar på annat än mindre formella brister.

Innehållsförteckning

Bakgrund

Personuppgiftslagen (PuL) från 1998 bygger på EG-direktiv 46/95/EG och är den generella lagstiftning som reglerar behandling av personuppgifter och bland annat ställer krav på samtycke, information och säkerhet. Beroende på verksamhet regleras behandling av personuppgifter i ett stort antal mer eller mindre specifika lagar. Inom den offentliga vården regleras hanteringen av personuppgifter, utöver personuppgiftslagen, främst av vårdregisterlagen, sekretesslagen och patientjournallagen. Att personuppgiftslagen är generell innebär att för det fall en mer specifik lag inte reglerar hanteringen av personuppgifter på ett speciellt område så träder personuppgiftslagens regler in. Det innebär att en personuppgiftsbehandling/personregister i det enskilda fallet oftast regleras av flera lagar. Den splittrade regleringen kring personuppgifter rörande patienter har uppmärksammats och det ligger ett förslag (SOU 2006:82) om en ny "patientdatalag". Det är i dag oklart om, och i så fall när, den nya lagen kommer att träda i kraft. Tillsynsmyndigheter när det gäller hantering av personuppgifter enligt ovanstående lagar är Datainspektionen och Socialstyrelsen.

Inom VGR finns ca 1800 personregister och respektive nämnd eller styrelse är personuppgiftsansvarig. Av personuppgiftslagen följer vissa lättnader om ett personuppgiftsombud utses. I ombudets uppgifter ligger att hålla en förteckning över personuppgiftsbehandlingar samt att se till att personuppgifter behandlas på ett lagligt sätt. Det innebär bland annat att hantera förfrågningar från registrerade och personal samt att påpeka eventuella brister för ansvariga.

I en skrivelse från Regionstyrelsens kansli 2004-03-15 framgår att många av regionens ombud har svårt att hinna med sin uppgift och att den juridiska kompetensen är låg i förhållande till de frågeställningar som ska hanteras.

På det nationella planet har Datainspektionen i rapporterna "Ökad tillgänglighet till patientuppgifter (Rapport 2005:1)" och "Personuppgifter i vårdregister (Rapport 2003:4)" uppmärksammat generella brister inom vården rörande information till patienter, kunskap om ansvaret för personuppgifter samt behörighet till patientuppgifter.

Syfte

Uppdraget syftar till är att granska och analysera huruvida VGR har en ändamålsenlig organisation samt de tekniska och administrativa åtgärder som krävs för att säkerställa att personuppgifter hanteras i enlighet med lag och interna riktlinjer.

Avgränsning

Granskningen baseras på observationer, intervjuer och granskning av dokument. Avgränsning har gjorts till Sahlgrenska Universitetssjukhuset (SU) och Gymnasiestyrelsen samt till personuppgifter avseende patienter och elever.

Metod

Initialt intervjuades ett antal nyckelpersoner i syfte att inhämta information för att i samråd med VGR:s revisionsenhet besluta om inriktningen på den vidare granskningen. Efter dessa intervjuer beslöts att dela in den fortsatta granskningen i fyra delar:

1. Granskning av dokument
2. Intervjuer med verksamhetsföreträdare/personuppgiftsombud
3. Stickprov avseende känsliga personregister
4. Kontroll av fullständigheten i gällande förteckning

Granskning av dokument
Denna del innefattar en analys av de dokument som styr hur personuppgifter skyddas samt den förteckning som finns över pågående behandlingar. Analysen syftar till att avgöra i vilken mån dokumenten och förteckningen är ändamålsenliga och i enlighet med gällande lagstiftning.

Intervjuer med verksamhetsföreträdare/personuppgiftsombud
Intervjuerna har genomförts för att kartlägga och analysera hur arbetet är organiserat. Detta i syfte att bedöma förutsättningarna att säkerställa tillräckligt skydd och korrekt hantering av personuppgifter.

Stickprov avseende känsliga personregister - SU
Tre personregister inom olika kategorier har följts upp för att kontrollera att personuppgifter hanteras och skyddas på det sätt som beskrivs i registerförteckningen.

Kontroll av fullständigheten i gällande förteckning - SU
Tanken var att genom ett antal stickprov kontrollera huruvida system med patientinformation upptagna på SU IT:s systemlista även återfanns i förteckningen över personregister som förs av personuppgiftsombudet. Tillsammans med IT-chefen för SU valdes femton system/applikationer med patientuppgifter. Kontrollen fick dock utgå på grund av att det inte var möjligt att söka på systemnamn i systemet över personregister (Persreg) och att det saknas gemensam namnstandard inom SU, dvs. olika namn används för samma system/applikationer.

Granskning av dokument

Vi har begärt att få ta del av interna dokument som styr alternativt används i arbetet med att säkerställa tillräckligt skydd och korrekt hantering av personuppgifter.
Begäran har ställts till:

- Personuppgiftsombud för Regionstyrelsen m.fl. samt sammankallande för PUO-nätverket
- Personuppgiftsombud/informationssäkerhetschef vid Sahlgrenska Universitetssjukhuset
- Personuppgiftsombudet vid Gymnasiestyrelsen

Följande dokument har överlämnats:

- Ansökan om tillstånd för behandling av personuppgifter vid Västra Götalandsregionen
- Ansökan om tillstånd för behandling av personuppgifter vid Västra Götalandsregionen (Sahlgrenska Universitetssjukhuset)
- Brev Utdrag
- Miniflöde
- Infohandl nov-02
- Blankett för samtycke vid deltagande i studie
- Exempel på kallelse till centralt PUO-möte
- Exempel på anteckningar från centralt PUO-möte
- Information om samtycke i samband med publicering av personuppgifter på Internet (Naturbruksgymnasiet)
- Information om databehandling
- Skyddad identitet för personal
- Skyddad identitet
- Lista över personuppgiftsombud m fl
- Persreg 1.0 - Ärendehantering vid anmälan om behandling av personuppgifter vid Sahlgrenska Universitetssjukhuset
- Reglemente för informationssäkerhet
- Säkerhetspolicy för Västra Götalandsregionen
- Regional riktlinje för informationssäkerhet
- Regional anvisning för styrning av åtkomst och behörigheter
- Regional anvisning för klassificering och styrning av tillgångar
- Regional anvisning för styrning av kommunikation och drift
- Regional anvisning för styrning av systemutveckling och systemunderhåll
- Regional anvisning för kontinuitetsplanering
- Regional anvisning för fysisk och miljörelaterad säkerhet
- Anvisning "Regional IT incidentorganisation"
- Regler för informationssäkerhet vid Sahlgrenska Universitetssjukhuset
- Regionstyrelsens beslut (RS9/2 -99)

Vidare har vi beretts tillgång till det system för registerförteckning och ärendehantering som används inom SU.

Iakttagelser

VGR - Organisation
Inom VGR är respektive nämnd eller styrelse personuppgiftsansvarig i förhållande till de vars personuppgifter behandlas. Samtliga har utsett, och hos Datainspektionen registrerat, ett personuppgiftsombud med uppgift att bevaka att personuppgifter hanteras i enlighet med god sed och gällande lag. I ett beslut av regionstyrelsen 1999 (RS9/2 -99) bestäms att dessa ska utse personuppgiftsombud. Samtliga personuppgiftsombud har rollen som personuppgiftsombud utöver sina egentliga grundbefattningar.

Som stöd i arbetet har ett nätverk av personuppgiftsombud (PuO-nätverk) skapats som administreras av regionstyrelsens ombud. Något konstituerande dokument för PuO-nätverket finns inte. I nätverket, som träffas 6 till 8 halvdagar per år, ingår även två regionjurister. Under dessa möten utbyts erfarenheter och kunskap och flera ombud ingår även i en motsvarande gruppering som arbetar med informationssäkerhet.

I nätverkets regi har det arbetats fram gemensamma mallar och dokument. Nätverket diskuterar och kommunicerar även frågor mellan mötestillfällena. En frågeställning som ofta tas upp är om en viss typ av personrelaterad information får lämnas ut till någon som efterfrågar densamma.

Någon formell skyldighet för ett enskilt ombud att delta i nätverket finns inte och alla ombud deltar inte heller aktivt. Varje ombud rapporterar direkt till respektive personuppgiftsansvarig. Det upprättas ingen plan över nätverkets arbete och inriktning utan det styrs av vilka frågor som från tid till annan aktualiseras.

Enligt sammankallande ombud är ansvariga inom VGR:s IT-organisation väl insatta i problematiken kring personuppgiftshantering och reagerar ifall omfattande personuppgiftsbehandling skulle påbörjas utan att det kommer till respektive ombuds kännedom. Någon skriftlig instruktion för anställda inom VGR:s IT-organisation som preciserar denna uppgift finns dock inte. Generellt genomför ombuden inga regelbundna kontroller eller revisioner. Enligt sammankallande ombud får respektive ombud en hel del information om vad som sker genom att de även har andra roller i respektive verksamhet.

Dokument
De dokument som tagits fram centralt i PUO-nätverket och används är:

- Blankett för ansökan om tillstånd för behandling av personuppgifter vid Västra Götalandsregionen
- Svarsbrev vid ansökan om registerutdrag enligt 26 § PuL
- Flödesschema för att ta beslut om enskilda behandlingar är förenliga med PuL
- Information om databehandling – Handikappförvaltningen
- Lista över personuppgiftsombud m.fl.
- Skyddad identitet

När det gäller informationssäkerhet finns ett antaget regelverk som bygger på den internationella standarden ISO/ICE 27002 (tidigare ISO/ICE 17799). Datainspektionen har utvecklat innebörden av personuppgiftslagens krav på informationssäkerhet i "Allmänna råd - Säkerhet för personuppgifter". Regionens regelverk täcker på ett övergripande plan samtliga områden som tas upp i de allmänna råden. För närvarande är regelverket föremål för en

omfattande omarbetning. Regionen har vidare ett säkerhetsråd, vars ansvar inkluderar informationssäkerhet, som leds av regionens säkerhetsdirektör.

Analys

Ansvaret för korrekt hantering och skydd av personuppgifter ligger på respektive nämnd eller styrelse. Genom att utse personuppgiftsombud uppmärksammas frågan och ansvaret för att bevaka området ges till en fysisk person. Denna åtgärd innebär förbättrade förutsättningar för korrekt hantering och skydd.

Det informella nätverk som i dag fungerar som ett stöd för enskilda ombud synes ge ett bra stöd när det gäller lagtolkning och praktisk hantering av uppkommande frågor. Däremot bedrivs ingen strukturerad kontroll eller revision av pågående personuppgiftsbehandlingar, varken direkt via personuppgiftsombuden eller via nätverket. Det finns därmed en risk att ombuden inte upptäcker missförhållanden alternativt inte tycker sig ha mandat att undersöka misstänkta missförhållanden.

På grund av nätverkets informella natur blir inriktningen och aktiviteten i nätverket starkt beroende av enskilda personers intresse och engagemang. Bristen på formell instruktion och obligatorisk närvaro innebär en risk att nätverket utvecklas på ett sätt som inte är optimalt eller att det upphör helt.

När det gäller de dokument som arbetats fram inom nätverket och används inom VGR är vår bedömning att de generellt är ändamålsenliga och i enlighet med gällande rätt. Undantag är ett flödesschema som inte uppdaterats med de ändringar i personuppgiftslagen som skett sedan 2000.

Vidare saknas centralt framtagna mallar för biträdesavtal att använda när tredje part behandlar personuppgifter för den ansvariges räkning. Att mall för biträdesavtal saknas leder till osäkerhet hur väl skyddet fungerar när personuppgifter hanteras av tredje part för VGR:s räkning.

Rekommendationer

Vi rekommenderar att respektive ombud tydligt påminns om åliggandet att genomföra återkommande revisioner och rapportera resultatet av dessa till personuppgiftsansvarig.

Vidare rekommenderas att en formell instruktion upprättas som formaliserar PuO-nätverkets arbete och möten.

Vi rekommenderar ytterligare granskning av skyddet kring personuppgifter som hanteras av tredje part (Personuppgiftsbiträden).

Slutligen bör flödesschemat uppdateras och mallar för biträdesavtal arbetas fram.

SU

Inledning

Inom vården ställs många gånger frågan om personlig integritet kontra säkerhet och effektivitet på sin spets. Både lagstiftning och tillgänglig teknik är under ständig förändring. Särskilt frågan om så kallad inre sekretess har uppmärksammats av tillsynsmyndigheter och media efter ett antal händelser rörande obehörig tillgång till journalinformation. SU har under våren anmälts till både Datainspektionen och Socialstyrelsen av denna anledning. Sannolikt är det inom detta och närliggande områden de största riskerna finns när det gäller kränkning av enskildas personliga integritet genom behandling av personuppgifter. Kränkningar som EG-direktivet och personuppgiftslagen syftar till att skydda.

Iakttagelser

Organisation och ärendeprocess
Utförarstyrelsen för Sahlgrenska Sjukhuset är personuppgiftsansvarig och har utsett ett personuppgiftsombud som tillika är informationssäkerhetschef. Till sin hjälp har ombudet en person som arbetar närmare heltid med administration av personregister och därmed relaterade frågor. Inrättandet av nya personregister följer en fastlagd process "Ärendehantering vid anmälan om behandling av personuppgifter inom Sahlgrenska Universitetssjukhuset". Vidare finns ett IT-system (PersReg) där samtliga personregister kommer att lagras och som stöder de olika aktiviteterna i processen för anmälan och prövning av nya register. I dag finns även information om personregister inklusive bakgrundsinformation och beslut från Etikprövningsnämnden på papper i ett låst arkiv. Enligt personuppgiftsombudet är processen implementerad men IT-stödet är inte helt uppdaterat med aktuell information samt justerat efter den senaste omorganisationen inom SU.

Övergripande är IT-verksamheten inom SU organiserad så att VGR IT sköter driften av de nät och applikationer som används inom SU. IT-chef och ansvariga systemägare med förvaltningsorganisation är kravställare mot VGR IT. Vidare finns för varje område inom SU en person med rollen IT-samordnare med huvudsaklig uppgift att samordna IT-behoven.

Enligt processen för anmälan av personregister fungerar det så att den som önskar påbörja ett nytt register (behandling) registrerar detta i systemet som kan nås över intranätet. Därefter informeras områdeschefen, som inte godkänner men har möjlighet att stoppa inrättandet av det nya personregistret. Om ärendet inte stoppas av områdesansvarig granskas det vidare av personuppgiftsombud/informationssäkerhetschef och områdets IT-chef/samordnare. Respektive områdes IT-chef/samordnare har uppgiften att vid inrättandet av nya personregister granska säkerhetsnivån samt den tekniska lösningens lämplighet ur ett IT-driftsperspektiv, exempelvis se till att liknande register använder gemensamma plattformar. Från och med 2007 kommer det årligen skickas en fråga till samtliga registrerade kontaktpersoner som får bekräfta att registrerad information om personregistret är korrekt.

Etikprövningsnämnden
När det gäller forskningsprojekt prövas särskilt känsliga personregister/behandlingar innan de påbörjas av Etikprövningsnämnden. Nämndens prövning sker enligt Lag (2003:460) om etikprövning av forskning som avser människor. När prövning ska ske framgår av följande stycke:

3 § Denna lag skall tillämpas på forskning som innefattar behandling av
1. *känsliga personuppgifter enligt 13 § personuppgiftslagen (1998:204), eller*
2. *personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden enligt 21 § personuppgiftslagen, om forskningspersonen inte har lämnat sitt uttryckliga samtycke till behandlingen.*

Personuppgiftsombudet
Personuppgiftsombudets verksamhet är idag inriktad på att granska inkommande anmälningar om personuppgiftsbehandlingar/register samt att utbilda och informera verksamheten om gällande säkerhetsföreskrifter och lagkrav. Vid anställning genomgår samtliga chefer inom SU, samt en hel del övrig personal, en informationssäkerhetsutbildning som innefattar hantering av personuppgifter. När ett personregister anmäls informeras den som anmäler registret om personuppgiftslagens grundkrav för behandling. Slutligen finns information och ett interaktivt självtest tillgängligt för alla som har tillgång till SU:s intranät.

Enligt personuppgiftsombudet har respektive områdes IT- chef/samordnare kompetens kring hur personuppgifter ska hanteras och fångar upp felaktiga och icke anmälda personregister när det rör sig i verksamheten på respektive område. Personuppgiftsombudet befarar dock att IT-samordnarna, i och med att de kommer att centraliseras, tappar den lokala verksamhetsanknytning som krävs för att fullgöra denna uppgift fullt ut.

Information om nya riktlinjer och ny lagstiftning erhåller Personuppgiftsombudet främst via Datainspektionen, Socialstyrelsen och PuO-nätverket.

Någon reviderande verksamhet, som innebär att en viss verksamhet närmare granskas eller att ett visst personregister följs upp, förekommer i princip inte.

När det gäller information om personuppgiftshantering till patienter lämnas den muntligen, via anslag och via en blankett som finns tillgänglig på intranätet.

Förfrågningar enligt 26 § personuppgiftslagen att få ta del av alla personuppgifter som behandlas är inte särskilt vanligt förekommande och hanteras utan problem inom de av lagen angivna tidsramarna. Vanligare är förfrågningar om loggningsuppgifter rörande vilka som tagit del av den frågandes journalhandlingar.

När det gäller informationssäkerhet gäller regionens regelverk direkt för SU men ett dokument, "Regler för informationssäkerhet vid Sahlgrenska Sjukhuset", har upprättats som en sammanställning av redan gällande bestämmelser. Ansvaret för informationssäkerheten är delegerat enligt samma principer som verksamhetsansvaret. Någon central uppföljning avseende tillämpningen av regelverket sker enligt ombudet inte.

Områden som framhölls som problematiska under diskussion med SU personuppgiftsombud och IT-chef är:

- Det finns ett relativt stort antal små register ute i verksamheten som inte är anslutna till SU:s nätverk. Dessa är svåra att få kontroll över.

- Av historiska skäl finns i dag ett onödigt stort antal system där flera fyller liknande behov.

- Bristande behörighetshantering i sjukhusgemensamma journalsystem, exempelvis framhölls svårigheten att avgöra när en viss vårdgivare behöver tillgång till viss patientinformation.

- Fortfarande används i vissa fall gemensam inloggning till patientjournalsystem.

- Problem kring kommunikation med primärvården på grund av osäkerhet kring sekretess.

- Spärrade journaler kan av tekniska skäl inte "nödöppnas".

- Gemensam katalog över anställda saknas vilket är en förutsättning för en mer finmaskig behörighetskontroll.

- Det saknas ett gemensamt och sanktionerat verktyg för att kryptera känslig information

- SU har svårt att kontrollera hanteringen av personuppgifter som hanteras av enheter tillhörande Göteborgs Universitet (GU), trots att ansvaret mot den registrerade ligger hos SU. Problemet ligger bland annat i att ett stort antal personer har dubbel anställning.

- SU har svårt att kontrollera personuppgifter som hanteras av läkemedelsföretag i samband med kliniska studier, men där ansvaret mot den registrerade ligger hos SU. Grunden till problemet ligger i att SU har ansvar för informationen som lämnas av patienten men läkemedelsföretaget bestämmer ändamål och medel för behandlingen.

- Det saknas effektiva verktyg för uppföljning av systemloggar. Detta försvårar uppföljning av obehörigt tillträde till personuppgifter.

- Informationssäkerhetschefens organisatoriska placering är två rapporteringsnivåer under sjukhusdirektören kan innebära problem att få gehör för krav på efterlevnad av gällande regler.

- SU har ingen egen jurist inom organisationen som är specialiserad på vårdrelaterad juridik.

Dokument
De dokument som används är:

- Ansökan om tillstånd för behandling av personuppgifter vid Västra Götalandsregionen (Sahlgrenska Universitetssjukhuset)
- Blankett för samtycke vid deltagande i studie
- Skyddad identitet för personal
- Persreg 1.0 - Ärendehantering vid anmälan om behandling av personuppgifter vid Sahlgrenska Universitetssjukhuset

- Regler för informationssäkerhet vid Sahlgrenska Universitetssjukhuset

I dokument "Ansökan om tillstånd för behandling av personuppgifter vid Västra Götalandsregionen (Sahlgrenska Universitetssjukhuset)." så saknas rubriken "Kategori av personer vars personuppgifter behandlas".

Förteckningssystemet efterfrågar nödvändig information och innehåller genomarbetade informationstexter.

Stickprov avseende känsliga personregister

Tre personregister/behandlingar som finns registrerade i förteckningssystemet valdes ut för uppföljning. Registren valdes utifrån kriterierna att de skulle innehålla en relativt stor volym uppgifter samt att uppgifterna skulle vara av integritetskänslig karaktär. De register som valdes för uppföljning är 1. Databas för borderline patienter; 2. Digitalt bildarkiv (ögon); 3. Urininkontinens (ÖS).

1. Borderline patienter
Angivet syfte med registret är: *Uppföljning, utvärdering och metodutveckling av behandlingsinsatser på en psykiatrisk behandlingsenhet.*

Iakttagelser
Informationen om registret "Borderline patienter" var ofullständig och följande väsentliga omständigheter avvek från den information som anmälts till personuppgiftsombudet:

- Informationsklass var registrerad som "Hög" men skulle vara "Mycket Hög".

- Forskningsprojektet har ännu inte påbörjats. Däremot har projektet förberetts genom att patientinformation lagras på enheten (utöver sedvanlig arkivering av patientinformation).

- Patienternas samtycke har inte inhämtats avseende deltagande i forskningsprojektet.

- Personuppgifterna förvaras okrypterade, informationen är inte avidentifierad (t.ex. att namn och personnummer ersatts av ett löpnummer) och säkerhetskopiering utförs inte.

- Personuppgifterna förvaras på USB-minne i ett låst utrymme, på papper i låst utrymme samt på lokal PC i en särskild programvara som är lösenordsskyddad.

- Utöver vad som angivits tillförs personuppgifter via journalsystem och av utredningsteam.

- Automatiskt system för registrering av inloggningar saknas.

2. Digitalt bildarkiv (ögon)
Angivet syfte med personregistret är: *Inom ögonklinikens verksamhet finns många anledningar att fotografera ögats yttre och ögonlock för att dokumentera t.ex. tumörer och status före och efter operation av förändringar. Som förberedelse till att vi börjar med*

datajournal övergår jag till att fotografera med digital teknik så att bilderna skall finnas tillgängliga och kunna länkas till journalen.

Iakttagelser
Personregistret "Digital bildhantering" vid ögonkliniken raderades av misstag under sommaren 2006. All information fanns i en lokal PC som någon från IT-supportavdelningen hämtade i syfte att byta till en nyare dator när registeransvarig var på semester. Datorn togs utan att inhämta bekräftelse att all information var säkerhetskopierad. Efterforskningar har gjorts men informationen har inte varit möjlig att återskapa eftersom datorn skickats för destruktion. Enligt registeransvarig innebar detta att forskningsmaterial (personuppgifter) som samlats in under 20 år gick förlorat. Något nytt bildregister kommer inte att påbörjas förrän en central systemlösning för lagring av digitala bilder finns tillgänglig.

3. Urininkontinens
Angivet syftet med personregistret är: *Att inhämta information som på sikt kan leda till en förbättrad utredning och behandling av kvinnor med urininkontinens. Studien gäller kvinnor över 15 år inom ett primärvårdsområde i Göteborg.*

Iakttagelser
Informationen om registret "Urininkontinens" var ofullständig och följande väsentliga omständigheter avvek från den information som anmälts till personuppgiftsombudet:

Inhämtade uppgifter lagras inte på GU Datacentral med dokumenterad säkerhetsorganisation, behörighetskontroll och registrering av inloggningar. Istället lagrades uppgifterna okrypterat på lokal PC hos registeransvarig och hos en extern statistiker. Säkerhetskopiering hanteras av respektive användare.

Relevant är dock att personuppgifterna lagras och bearbetas avidentifierade, d.v.s. namn och personnummer har ersatts av ett löpnummer. Enligt registeransvarig är vidare den tabell (kodnyckel) som gör det möjligt att koppla ihop uppgiftslämnare och uppgifter förvarad i ett låst och brandsäkert skåp som endast ansvarig för studien har tillgång till.

Analys

Översikt rättslig reglering
För att sätta analysen i sitt sammanhang lämnas en kort översikt över den rättsliga regleringen kring personuppgifter i vården.

Personuppgiftslagen och vårdregisterlagen ger de övergripande reglerna kring hantering av personuppgifter inom vården. Exempel på andra lagar som innehåller viktiga bestämmelser kring hur patientrelaterade personuppgifter ska hanteras återfinns i hälso- och sjukvårdslagen, patientjournallagen, sekretesslagen, lagen om yrkesverksamhet på hälso- och sjukvårdens område och arkivlagen.

Enligt hälso- och sjukvårdslagens 2 § framgår att verksamheten skall bygga på respekt för patientens självbestämmande och integritet och så långt det är möjligt utföras och genomföras i samråd med patienten.

Personuppgifter i patientjournaler och andra handlingar/register som hanteras av SU är allmänna handlingar och rätten att ta del av dessa begränsas av sekretesslagens bestämmelser i 7 kap 1 c §:

"Sekretess gäller, om inte annat följer av 2a §, inom hälso- och sjukvården för uppgift om enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider men."

Denna reglering gäller alltså avseende utlämnande av information till enskilda eller andra myndigheter.

Vem som överhuvudtaget har rätt till åtkomst till personuppgifter/information i en patientjournal regleras enligt nedan:

Av patientjournallagens 7 § framgår att:

"Varje journalhandling skall hanteras och förvaras så, att obehöriga inte får tillgång till den. Om en journalhandling eller en avskrift eller kopia av handlingen har lämnats ut till någon, skall det antecknas i patientjournalen vem som har fått handlingen, avskriften eller kopian och när denna har lämnats ut."

Vidare följer av vårdregisterlagens 8 § att:

"Endast den som för de ändamål som anges i 3 och 4 §§ behöver tillgång till uppgifterna för att kunna utföra sitt arbete får ha direktåtkomst till uppgifter i ett vårdregister. Åtkomsten får endast avse de uppgifter som behövs för arbetets utförande."

Att reglerna kring hanteringen av personuppgifter, särskilt rörande patienter, inom vården är splittrade och delvis oklara har uppmärksammats och en ny samlad lagstiftning har föreslagits. Den 18 oktober 2006 presenterades SOU 2006: 82 som föreslår en ny patientdatalag med följande reglering kring personuppgifter i patientjournaler:

Utredningens bedömningar och förslag:

"1. Nuvarande reglering i 7 § första stycket patientjournallagen om att varje journalhandling skall hanteras och förvaras så att obehöriga inte får tillgång till den bör behållas men
a) dels vidgas till att omfatta alla dokumenterade personuppgifter om patienter eller andra enskilda registrerade, dvs. även annan vårddokumentation, kvalitetsregisteruppgifter m.m. som behandlas enligt patientdatalagen,
b) dels förtydligas genom tillägget att den som arbetar hos en vårdgivare får ta del av sådana uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården. Bestämmelsen omfattar både manuellt och elektroniskt behandlade patientuppgifter, även uppgifter om avlidna.

2. När det gäller elektronisk patientjournalföring och övrig elektronisk patientdokumentation införs en ny bestämmelse om tillåten elektronisk åtkomst som delvis motsvarar nuvarande reglering i 8 § vårdregisterlagen men som ställer tydligare krav på vårdgivaren i fråga om behörighetssystem m.m. Närmare bestämmelser meddelas av regeringen eller, efter bemyndigande, av Socialstyrelsen efter samråd med Datainspektionen.

3. En ny bestämmelse införs som innebär en skyldighet för vårdgivaren att dokumentera elektronisk åtkomst samt att systematiskt och fortlöpande kontrollera om obehörig åtkomst till uppgifter om patienter förekommer. Närmare bestämmelser meddelas av regeringen eller, efter bemyndigande, av Socialstyrelsen efter samråd med Datainspektionen.

4. Den enskilde patienten ges rätt att på begäran få information om vilken direktåtkomst och elektroniska åtkomst som förekommit till elektroniskt behandlade uppgifter om honom eller henne. Närmare bestämmelser om den information som skall ges till patienten meddelas av regeringen eller, efter bemyndigande, Socialstyrelsen efter samråd med Datainspektionen.

5. Den enskilde patienten ges rätt att begära att vårddokumentation spärras från tillgänglighet för andra vårdenheter alternativt vårdprocesser utanför den till vilken uppgifterna hör. Rätten motsvarar opt out-möjligheten i skede 1 vid sammanhållen journalföring.[1] Spärren skall med patientens samtycke kunna hävas helt eller delvis, t.ex. i en enstaka vårdsituation. Spärren skall också kunna forceras, om informationen kan antas ha betydelse för den vård som patienten oundgängligen behöver. Uppgift om att det finns spärrade uppgifter får vara tillgänglig för andra vårdenheter eller vårdprocesser liksom även uppgift om vilken vårdenhet eller vårdprocess som spärrat uppgifterna.

6. I patientdatalagen införs ett särskilt kapitel om inre sekretess och elektronisk åtkomst i en vårdgivares verksamhet, vari bestämmelserna enligt punkterna 1 b)–3 och 5 tas in. Bestämmelsen i punkten 1 a) tas in i patientdatalagens inledande kapitel. Bestämmelsen i punkten 4 om patientens rätt att få information om direktåtkomst och elektronisk åtkomst som förekommit hos en vårdgivare, tas in i ett kapitel om rättigheter för den enskilde."

Ansvar och styrning

Ansvaret för att personuppgifter avseende patienter hanteras korrekt ligger på utförarstyrelsen men är delegerat i linjen till de personer som arbetar i verksamheten. Personuppgiftsombudet ska självständigt kontrollera att personuppgiftsansvarig hanterar personuppgifter i enlighet med lag och god sed. När det gäller forskning är Etikprövningsnämndens verksamhet en viktig komponent i det samlade skyddet mot att felaktiga behandlingar/register påbörjas.

Avseende Ärendehantering, "Ärendehantering vid anmälan om behandling av personuppgifter inom Sahlgrenska Universitetssjukhuset", så finns en oklarhet kring vem som har ansvar för behandlingar som påbörjas.

Gjorda iakttagelser pekar på brister i tillämpningen av de regelverk som finns kring personuppgifter och informationssäkerhet. Orsaken till bristerna står sannolikt att finna i det relativt snabba införandet av ny teknik. En annan orsak kan vara att kravet på Datainspektionens tillstånd för personregister upphörde i och med att datalagen ersattes med personuppgiftslagen och vårdregisterlagen. Sannolikt innebar Datainspektionens tidigare förhandsgranskning att området prioriterades något hårdare än i dag.

Vidare är personuppgiftsombudets kontrollerande verksamhet inte effektiv. Anledningen till detta kan vara personuppgiftsombudets organisatoriska placering med rapportering till säkerhetschefen, det vill säga två rapporteringsnivåer under sjukhusdirektören. En annan kan vara den dubbla rollen som både personuppgiftsombud och informationssäkerhetschef.

[1] **Opt-out** innebär att om patienten själv agerar och begär begränsningar av tillgången till egna personuppgifter så respekteras detta, **Opt-in** innebär att patienten tillfrågas om vilken tillgång till egna personuppgifter denne accepterar och begränsning sker därefter i enlighet med detta, (författarens anmärkning).

Kompetens, informationsmaterial och förteckning
Gjorda iakttagelser pekar på brister inom verksamheten vad gäller kunskap om de regelverk som finns kring personuppgifter och informationssäkerhet.

Personuppgiftsombudet och dennes assistent ger intryck av att ha god kunskap om gällande regelverk och det finns material och systemstöd för att:

1. administrera en central förteckning över pågående personuppgiftsbehandlingar
2. informera de som avser att påbörja nya behandlingar
3. stödja verksamheten med informationstexter och blanketter för samtycke m.m.

Behörighet till patientjournaler
SU har under våren 2007 anmälts till Datainspektionen och Socialstyrelsen av en juridikstudent som i sitt uppsatsarbete noggrant analyserat huruvida SU:s hantering av behörighet till patientjournaler står i överensstämmelse med gällande rätt. Datainspektionen har för närvarande valt att inte öppna ett tillsynsärende med motiveringen att de nyligen utfärdat tydliga riktlinjer samt inväntar ny lagstiftning. Anmälan kan dock komma att ligga till grund för tillsynsärende längre fram. Socialstyrelsen har inte avslutat ärendet ännu och ansvarig handläggare meddelade per telefon att de saknar kompetens för att avgöra frågan inom den närmaste tiden.

SU tillämpar en princip som, med något undantag, går ut på att alla som arbetar med vård ska ha möjlighet att nå all information som finns i gemensamma patientjournalsystem. Vidare används i vissa fall gemensamma inloggningsuppgifter något som omöjliggör uppföljning av vem som har loggat in. Normalt finns alltså inte någon teknisk begränsning av tillgången till patientinformation. Det skydd som finns, när det gäller obehörig vårdpersonal, är stickprovskontroller av inloggningar när det är möjligt (effektivt verktyg saknas) samt förlitan på att anställda följer lagstiftning och interna regler.

Det kan konstateras att SU:s hantering, avseende behörighet till patientjournaler, inte följer lagens bokstav och inte heller de riktlinjer som utfärdats av Datainspektionen. Hanteringen står inte heller i överensstämmelse med, de ovan nämnda, reglerna i förslaget om ny lagstiftning.

Ansvarsfördelningen mellan SU, GU och läkemedelsbolag m.fl.
Iakttagelser pekar på att SU i olika situationer har ansvaret för hantering av patienters personuppgifter utan att ha kontroll över hur dessa behandlas. Det gäller exempelvis när personuppgifter inhämtas i samband med vård men senare används för forskningsändamål. Har uppgifterna inhämtats i samband med att en patient söker sig till SU för vård och i den situationen lämnar information har SU ett ansvar för uppgifterna, även om andra aktörer bestämmer ändamål och medel kring den fortsatta behandlingen av personuppgifterna.

Rekommendationer

Vi rekommenderar att SU:

Ålägger personuppgiftsombudet att genomföra återkommande revisioner och rapportera resultatet av dessa till personuppgiftsansvarig.

Närmare utreder glappet mellan gällande lagkrav och framför allt SU:s hantering av personuppgifter i gemensamma journalsystem, och vidtar nödvändiga åtgärder.

Närmare utreder vilket ansvar SU har när det gäller andra aktörers hantering av personuppgifter, som inhämtats av vårdgivare inom SU, och vidtar nödvändiga åtgärder.

Överväger att ge personuppgiftsombudet en mer självständig organisatorisk placering samt ökade resurser inom juridik och informationssäkerhet.

Överväger den dubbla roll personuppgiftsombudet har som både personuppgiftsombud och informationssäkerhetschef med rapportering till säkerhetschef.

Säkerställer skydd och korrekt hantering av personuppgifter som hanteras av tredje part (Personuppgiftsbiträden).

Gymnasiestyrelsen

Inledning
Uppskattningsvis 1250 elever genomgår årligen utbildningar på 7 st gymnasieskolor som ligger under Gymnasiestyrelsens ansvar.

Iakttagelser
Ansvaret för att elevers personuppgifter hanteras korrekt är delegerat till rektorn på respektive skola. Några återkommande kontroller sker inte från Gymnasiestyrelsens sida men principiella frågor diskuteras centralt, t.ex. hantering av elever med sekretessmarkerade personuppgifter eller regler för Internetanvändning.

Personuppgiftsombudet för Gymnasiestyrelsen har inte deltagit aktivt i PuO-nätverkets möten de senaste två åren. Den person som enligt PuO-nätverketslista över ombud var ombud för Gymnasiestyrelsen hade ersatts av en ny person 2007 som även är medlem i säkerhetsrådet.

En säkerhetshandbok har tagits fram som gäller alla anställda. Särskild utbildning kring innehållet i säkerhetshandboken genomförs med systemadministratörer, IT-ansvariga, och rektorer. Säkerhetshandboken innehåller avsnitt om hantering av personuppgifter.

Det tidigare ombudet var sällan med på PUO-nätverkets möten (senast var under 2005) men tar del av utsänd information. Frågorna som diskuteras i nätverket har, enligt det tidigare ombudet, till stor del inte relevans för Gymnasiestyrelsen utan är ofta vårdrelaterade.

Det finns endast ett centralt system för hantering av personuppgifter och det heter ADELA. Detta system överför vissa uppgifter till ett system för schemaläggning samt till ekonomisystemet. Elever med sekretessmarkerade personuppgifter är "flaggade" i systemet så att uppgifterna erhåller särskilt skydd.

Dokumentation finns kring vilka personuppgifter som finns i ADELA samt hur den hanteras. Någon formell förteckning i enlighet med Datainspektionens riktlinjer (blankett) kunde däremot inte visas upp.

Särskild samtyckesblankett används för att inhämta elevers samtycke innan publicering av personuppgifter på skolornas hemsidor. Vidare lämnas information om personuppgiftshantering på antagningsbesked och i vissa skolor lämnas även information via anslag.

Inga förfrågningar enligt 26 § personuppgiftslagen har inkommit från elever till PuO.

Ett fall har inträffat då identiteten på en elev med skyddad identitet efterforskades. Skolans rutiner fungerade och information om eleven med skyddad identitet lämnades inte av skolans personal.

Gymnasiestyrelsen använder inte några system som efterfrågar den typ av personuppgifter som i PuL kategoriseras som känsliga.

Analys

Någon integritetskänslig hantering av elevernas personuppgifter sker inte i något centralt system. Vi kunde konstatera vissa brister gällande formalia. Risken för brister i hanteringen av elevers personuppgifter ligger sannolikt främst i den hantering som utförs av enskilda lärare. Några återkommande revisioner förekommer inte för att säkerställa korrekt hantering.

Rekommendationer

Vi rekommenderar att PuO åläggs att genomföra återkommande revisioner och rapportera resultatet av dessa till personuppgiftsansvarig.

Vi rekommenderar att PuO deltar i PuO-nätverkets möten.

Vi rekommenderar att utbildning kring personuppgifter och informationssäkerhet som hålls för rektorer, systemadministratörer och IT-ansvariga utvidgas till att även omfatta lärare.