JÄMTLANDS LÄNS LANDSTING

Landstingets revisorer

2009-02-03

Dnr REV/11/2009

Revisionschef Lennart Ledin 063-14 75 27
Certifierad revisor Ulf Rubensson, 063-14 75 29

Landstingsstyrelsen

IT-säkerhet och Logghantering

Revisionskontoret har på vårt uppdrag granskat IT-säkerhetsarbetet inom landstinget. Granskningen omfattar en uppföljning av om den beslutade basnivån för IT-säkerhet har uppnåtts samt hur loggkontroller görs och hanteras i de IT-system som hanterar patientuppgifter, d v s det vårdadministrativa systemet VAS och tandvårdssystemet T4.

Resultatet av granskningen framgår av bifogad granskningsrapport.

Resultatet av granskningen visar sammanfattningsvis att:

- Den beslutade basnivån för IT-säkerhet har ännu inte uppnåtts. Mycket återstår att göra. Vi anser att arbetet med att nå basnivån bör ges hög prioritet.
- Regler och anvisningar för hur inloggning skall ske och hur loggar skall kontrolleras och hanteras är ändamålsenliga men följs inte i väsentliga avseenden. Detta är en ledningsfråga som omedelbart behöver åtgärdas.
- Utöver de ovan nämnda systemen kan det finnas andra system med patientuppgifter som inte har anpassats till kraven i den nya Patientdatalagen. Det är också sannolikt att det kan uppstå problem om eller när det uppdagas att så är fallet. Konsekvensen kan bli att de längre inte får användas med betydande störningar för verksamheten som följd. Det är enligt vår mening också en viktig ledningsfråga att i tid se till att samtliga system som innehåller patientuppgifter uppfyller gällande lagar och förordningar.

Vi emotser senast den 5 juni 2009 landstingsstyrelsens yttrande över resultatet av granskningen med en redovisning av vilka åtgärder som styrelsen vidtar eller avser vidta med anledning av resultatet. Av redovisningen bör framgå närmast ansvariga för åtgärderna samt tidplan.

För Jämtlands läns landstings revisorer

Mona Nyberg
Ordförande

Jöns Broström
Vice ordförande

Bilaga
Revisionskontorets revisionsrapport "IT-säkerhet och Logghantering"

Kopia
Fullmäktiges presidium
Beredningen för vård och rehabilitering
Landstingsdirektören
Bitr. landstingsdirektören
Tandvårdschefen
Chefen ledningsstab IT
Systemansvarig VAS
Chefen ledningsstab Utveckling
Chefen ledningsstab sekretariat
Patientuppgiftsombudet

Jämtlands Läns Landsting

REVISIONSRAPPORT

IT-SÄKERHET OCH LOGGHANTERING

Ansvarig: Ulf Rubensson

Certifierad kommunal revisor

INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Den beslutade basnivån för IT-säkerhet har ännu inte uppnåtts. Mycket återstår att göra.

- Vi bedömer det som viktigt att det tas fram en långsiktig och beslutad genomförandeplan för IT-säkerhetsarbetet.

- Arbetet med att uppnå den beslutade basnivån bör ges hög prioritet.

Vi har närmare granskat hur uppföljningen av loggar sköts vad gäller det vårdadministrativa systemet VAS och tandvårdssystemet T4 som hanterar patientuppgifter.

Vår samlade bedömning är att de regler och anvisningar som finns huvudsakligen är ändamålsenliga, men att det finns ett utrymme för förbättringar.

Däremot har vi funnit att reglerna inte följs i några, enligt vår mening, väsentliga avseenden. Det gäller att man använder andras inloggning resp att det förekommer s.k. grupploggin i VAS. Detta sker med resp lednings kännedom. Enligt vår mening är det otillfredsställande med en ledning/styrning som inte

reagerar när uppsatta regler bryts. Att medvetet inte agera är också en form av beslut som kan medföra juridiska konsekvenser. T ex kan det bli svårt att utkräva något ansvar från den/de individer som bryter mot reglerna.

Patientdatalagen är ny och det är, enligt vår bedömning, sannolikt att det bland befintliga system kan finns sådana som ännu inte hunnit anpassas till den nya lagstiftningen. Det är dock också sannolikt att det kan komma att uppstå problem om eller när det uppdagas att ett system inte klarar de krav som finns i lagar och förordningar. Konsekvensen kan bli att något system därmed inte heller längre får användas. Är då systemet av avgörande betydelse för verksamheten kan en allvarlig störning uppstå.

Det är därför, enligt vår mening, en viktig ledningsfråga att i tid vidta åtgärder som säkerställer att samtliga system som innehåller patientuppgifter uppfyller gällande lagar och förordningar.

2 INLEDNING/BAKGRUND

Vid en tidigare granskning av det vårdadministrativa systemet VAS framkom att mycket av säkerheten för den personliga integriteten är beroende av att inloggningar i systemet görs med unika användaridentiteter och att uppföljning av loggar görs. Något som föreföll oklart om det fungerade helt tillfredsställande.

Landstingets revisorer har, bland annat mot bakgrund av ovanstående, i sin risk- och väsentlighetsanalys bedömt det angeläget att genomföra en granskning av landstingets IT-säkerhet.

3 SYFTE, REVISIONSFRÅGA OCH AVGRÄNSNING

Det övergripande kontrollmålet var att svara på om det finns en tillfredsställande säkerhetskultur, säkerhetsrutiner och säkerhetsarrangemang för att skydda landstingets IT-system från intrång, sabotage och obehörig åtkomst av information etc. För att få svar på detta hade vi för avsikt att kontrollera om landstinget lever upp till den beslutade säkerhetsnivån BITS (”Basnivå för IT-säkerhet) och om de delar av den som handlar om ”egenkontroll” (interna kontrollen) fungerar.

Då granskningen påbörjades framkom att landstinget ännu inte har uppnått den nivå för IT-säkerheten som fastläggs i BITS (se avsnitt 7.1), men också att ett arbete för att nå dit pågår. Granskningens inriktning avgränsades därför starkt och inriktades huvudsakligen mot kontrollen av loggarna. Revisionsfrågorna i detta avseende utgår från aktuell lagstiftning, Socialstyrelsens förordningar samt landstingets regler.

Granskningen är i huvudsak avgränsad till

- säkerhetsnivå BITS (”Basnivå för IT-säkerhet”)
- vårdadministrativa systemet (VAS) och tandvårdssystemet (T4).

4 REVISIONSKRITERIER

Revisionskriterierna utgår från:

1. **Patientdatalag** (2008:355)

2. **Socialstyrelsens föreskrifter** om informationshantering och journalföring i hälso- och sjukvården. SOSFS 2008:14

3. **IT-säkerhetsplanen**

   IT-säkerhetsplanen är en bilaga till landstingets IT-strategi och har godkänts av landstingsdirektören i december 2003 (Dnr: JLL 1097/2003).

   Utdrag ur IT-säkerhetsplanen, avsnitt ”Inledning”:

   ”I dokumentet Kvalitetshandbok för systemförvaltning definieras landstingets systemstruktur samt ansvarsroller för drift och förvaltning av landstingets IT-system. IT-säkerhetsplanen har upprättats som en bilaga till landstingets IT-strategi.

   Säkerhetsarbetet så som det här beskrivs har baserats på rekommendationer om basnivå för IT-säkerhet (BITS) utgivna av Krisberedskapsmyndigheten (KBM). BITS-rekommendationerna definierar en balanserad basnivå för säkerheten i IT-system. IT-system betraktas som samhällsviktiga och intar en central roll när det gäller olika samhällsfunktioners möjligheter att kontinuerligt kunna bedriva sin verksamhet. Detta är särskilt tydligt för landstinget som är huvudman for hälso- och sjukvården i länet. Därför har landstinget valt att följa BITS-rekommendationerna i sitt IT-säkerhetsarbete.”

4. **Riktlinjer för tillgång till vårdinformation i landstingets vårdregister, logguppföljning samt åtgärder vid misstänkt olovligt användande.** Fastställda av landstingsdirektören 2008-03-28 (Dnr LS 323/2008)

5 GRANSKNINGSANSVARIG

Ansvarig för granskningen har varit Ulf Rubensson. Certifierad kommunal revisor, anställd av Jämtlands läns landstings revisorer.

6 METOD

Granskningen har genomförts genom studier av dokument, enkät till berörda verksamhetsområdeschefer samt intervjuer.

Granskningen har ansatsen att analysera om befintliga kontroller är ändamålsenliga och att lämna förbättringsförslag.

7 RESULTAT

7.1 BASNIVÅ FÖR IT-SÄKERHET (BITS)

Vid intervju med landstingets IT-säkerhetsansvarige framkom att man ännu inte har uppnått den beslutade basnivån för IT-säkerhet (BITS).

Ett arbete pågår för att ta reda på vad som behöver åtgärdas för att uppnå BITS. En hjälp i arbetet är programvaran ”BITS Pro 2”. Med hjälp av denna görs f.n. en genomgång av ett antal viktiga system. Genomgångarna görs i samråd med resp. systemansvarig

Pågår	**Planeras**
Samordning Internt IT-nätverk System - Flexlab - JLL Insidan - Master Befolkning - Platina - RIS - PACS - VAS	Heroma (”fd” Palett) - nov Raindance - dec

Programvaran BITS Pro ger rapporter med förteckningar över vilka åtgärder som behöver vidtas utifrån registrerade bedömningar. Landstingets IT-säkerhetsansvarige upplever att listade åtgärdsbehov tenderar att bli så många att det är svårt att göra prioriteringar.

Det har skett och sker även andra genomgångar och vidtas åtgärder inom IT-säkerhetsområdet.

- en extern konsult har gått igenom om man följer standarden för hur ledningssystem för IT bör byggas i en org.
- en extern konsult har gjort en säkerhetsrevision med avseende på de tjänster som köps från Tieto Enator
- ett arbete pågår med kontinuitetsplanering (ex brand i datorhall).
- man har nätverksträffar för systemansvariga där man har genomgångar och lär av varandra.
- det pågår ett arbete med en s.k. HSA-katalog som kommer att underlätta kontrollen över aktualiteten på användaridentiteter och behörigheter
- ”smarta kort” införs för förstärkt id-kontroll vid inloggning

Det fanns ingen dokumenterad plan för IT-säkerhetsarbetet på längre sikt än 5-6 månader.

Bedömning:
Med hänvisning till att BITS beslutades som en grund för IT-säkerheten i december 2003 (ca 5 år sedan) har förvånansvärt lite skett för att på ett strukturerat sätt se till att beslutet verkställts. Det arbete som nu pågår förefaller dock kunna åtgärda bristerna under förutsättning att samtliga väsentliga system och andra system, där säkerhetsproblem kan finnas, inventeras och att de brister som framkommer också åtgärdas.

Då säkerställandet av att BITS uppnås kan vara kritiskt för vissa verksamheter och då det även kan handla om att säkerställa att integritetskänslig information hanteras rätt, är det viktigt att den påbörjade genomgången och de åtgärdsbehov som framkommer ges hög prioritet.

Vi bedömer det som viktigt att det tas fram en långsiktig och beslutad genomförandeplan för IT-säkerhetsarbetet..

7.2 LOGGNING OCH IDENTIFIERING AV ANVÄNDARE MM.

Allmänt om hur det är tänkt att patientdata ska skyddas

På landstingets hemsida finns bl.a. följande text vad gäller journaler[1)]:

> *”Din journal är i första hand ett stöd för oss som arbetar i vården för att vi ska kunna ge en god och säker vård. Det är bara du själv och den personal som vårdar dig som har rätt att läsa din journal. Alla uppgifter skyddas för obehörig insyn och spridning.”*
>
> Vidare sägs bl.a.:
>
> *”Det är bara behörig personal som är delaktig i just din vård som får ta del av informationen i din journal. Personal i andra landsting kan inte se din journal om du söker vård hos dem. Journalen kan inte heller nås av anställda i andra myndigheter.*
>
> *Varje gång någon tar del av uppgifter om dig i journalen registreras det. Det betyder att det i efterhand går att spåra via en så kallad logg om någon har läst om dig. Vi är skyldiga att kontrollera vem som tagit*

[1] Sökväg: / Startsida / Hälso- och sjukvård / Patientinformation / Lagar, regler och rättigheter / Patienträttigheter / Din journal

del av dina uppgifter och du har själv rätt att ta del av den informationen.
Inom all hälso- och sjukvård råder sträng sekretess för uppgifter som rör hälsotillstånd och andra personliga uppgifter. Alla som arbetar inom landstingets hälso- och sjukvård har tystnadsplikt enligt sekretesslagen."

Landstinget har numera en patientjournal som är gemensam för hela landstinget. Tidigare var journalen uppdelad på de olika vårdenheter vilket medförde att de inte på ett enkelt sätt kunde ta del av varandras information. Syftet med förändringen var bl.a. att få en mer samlad bild av patientuppgifterna. Men förändringen innebär också att den personkrets som kan komma åt uppgifterna har utökats väsentligt. Att bara ha en journal innebär att uppgifterna som registreras kan läsas av personal oavsett var vården ges inom landstinget.

I landstingets riktlinjer för tillgång till vårdinformation står bl.a. följande:

"Landstingets hälso- och sjukvård är ett gemensamt sekretessområde inom vilket inre sekretess råder. Detta innebär att behörig vårdpersonal kan, utifrån eget ansvar, skaffa sig tillgång till den patientinformation i landstingets vårdregister som denne behöver för vård och behandling av sina patienter.

*Att en anställd har teknisk behörighet att skaffa sig tillgång till information om en viss patient i ett vårdregister är **inte** detsamma som att ha behov av - och rätt till - att ta del av den informationen. Rätten till tillgång baseras på att man i den aktuella situationen behöver åtkomst till informationen för att på ett riktigt och säkert sätt fullgöra sina uppgifter gentemot aktuell patient.*

För att ha rätt att ta del av vårdinformation krävs att det finns en vårdrelation till patienten.

En vårdrelation uppstår när en enskild befattningshavare planerar eller utför aktivitet i förhållande till patienten. En vårdrelation är begränsad i tid och innehåll till patientens vårdepisod."

Som framgår ovan bygger behörigheten på att det ska finnas en vårdrelation och att uppgifterna behövs för vården i den aktuella situationen. Uppfylls inte detta är man inte behörig och den som ändå tar del av patientuppgifter begår därmed en brottslig handling.

Det skydd som finns består både i att det sker en prövning av vilka som ska få ha åtkomst till system med patientuppgifter och i att det även regleras vem som får göra vad i systemen.

Enligt landstingets regler är det tänkt att varje användare ska tilldelas ett unikt användarnamn kopplat till ett lösenord som bara innehavaren känner till. För närvarande utgörs identitetskontrollen av om användaren kan ange rätt lösenord. Det pågår dock ett arbete inom landstinget med att införa s.k. smartcard och som kommer att i hög grad stärka identitetskontrollen eftersom det då även kommer att krävas att det finns något unikt som användaren har (kortet), förutom rätt lösenord.

Enbart användandet av s.k. smartcard löser dock inte sekretessproblematiken avseende åtkomsten till patientuppgifter. Vad avser patientuppgifter är VAS, när användarna väl är inloggade, ett mycket öppet system. Det finns få spärrar och de som finns kan vid nödlägen forceras.

Säkerheten bygger i stor utsträckning på prevention. All åtkomst av patientuppgifter (både läsning och förändring) ska loggas. Loggarna ska sedan kontrolleras. För att detta ska få en tillräckligt preventiv effekt måste det göras med en sådan frekvens och omfattning att användarna upplever en stor risk för upptäckt.

Landstingets personuppgiftsombud har tilldelats ett ansvar för att kontrollera att rutinerna fungerar.

Hur ser det då ut?

För att ta reda på om säkerheten fungerar på avsett sätt har vi ställt upp ett antal revisionsfrågor som vi sökt svar på genom

- att studera gällande regler,
- skriftliga frågor till verksamhetsområdescheferna,
- intervjuer med personal inom IT-staben, systemansvarig för VAS och landstingets personuppgiftsombud.

Revisionsfråga:

1. Finns dokumenterade rutiner för tilldelning av teknisk behörighet till system med vårdinformation?

Rutiner finns. Beslut av landstingsdirektör 2008-06-04 (LS/761/2008).

Bedömning

Införandet av den s.k. HSA-katalogen och införande av s.k. smartcards bör kunna ge förutsättningar att för uppnå en god säkerhet.

Revisionsfråga:

2. Är det säkerställt att s.k. grupploggin[2] inte användas?

Utdrag ur Socialstyrelsens föreskrift 2008:14:

> ***”Styrning av behörigheter***
>
> *6 § Vårdgivaren ska ansvara för att det i ledningssystemet finns rutiner som säkerställer att hälso- och sjukvårdspersonalens och andra befattningshavares behörighet begränsas till vad som är nödvändigt för att ge en god och säker vård.*
> *Vårdgivaren ska vidare ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till patientuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.*
> *Vårdgivaren ska även ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheterna ”*

[2] Med grupploggin avses att flera personer använder samma användaridentitet (samma användarnamn och lösenord)

VAS

Enligt de uppgifter vi fått används s.k. grupploggin på C-operation, som besvarade vår förfrågan om detta enligt följande:

> *"Vid c-op förekommer ett grupplogin i VAS. Personalen/användarna som använder VAS operationsmodul på c-op rör sig mellan många olika klientarbetsplatser under kort tid och behöver kunna arbeta effektivt men ändå säkert. Kontot får användas för att nå operationsmodulen i VAS. Genom att logga in till detta konto fås behörighetsrollen "O2" (roll för operationspersonal) i VAS. VAS-kontot 'opal' används för att kunna vara påloggad löpande via gemensamma klientarbetsplatser och nyttjas för att kunna sköta registrering och snabbt ha kontroll på patientliggaren i VAS operationsmodul. Via gruppkontot "opal" i VAS ges endast åtkomst till operationsplaneringen, ej till journaluppgifter eller remisser/svar för en patient. Gruppkontot ger rollbehörigheten "O2" i VAS."*

Vid diskussion med den systemansvarige för VAS framkom även att det finns ett grupplogin för personalen hos Tieto Enator som sköter driften av systemet. Med detta grupploggin följer en omfattande behörighet till systemets alla delar. Systemansvarige lämnade oss information om att detta omgående skulle förändras så att även de personer från driftleverantören som behöver åtkomst till VAS har en egen användaridentitet.

Vi har även fått uppgifter om att personal använder VAS under annan persons inloggning.
Det förekommer:

- då man har studenter. De skriver då under ansvarig ordinarie personals inloggning. Man uppger att ordinarie personal kontrollerar/signerar det som skrivits.
- på operationsavdelningen som anger som skäl:
  -: *eftersom de är många användare på samma klientarbetsplats, har någon loggat in används det som är öppet, men då är oftast den som är inloggad kvar på operationssalen. En förutsättning för att ändra arbetssättet är att införa s.k. smartcards.*
- på IVA som anger som skäl:
  -: *det förekommer oftast accidentellt när det är många som vill läsa journaler från samma dator samt när IVA har "dåliga" patienter, oroliga patienter, flera patienter. Det förkommer även att personalen "lånar" (efter överenskommelse) den andres inloggning för att ex. göra och/eller sända laboratorieremisser när andra datorer i närheten är upptagna. Detta beror på att inloggningsproceduren är för lång och att IVA:s datorer stundvis är hårt belastade och inte räcker till.*
- på BUP, som anger som skäl:
  -: *det händer i receptionen för att medarbetare snabbt ska kunna se vissa uppgifter.*
- i primärvården som anger som skäl:
  -: *Tyvärr händer det, då det kan ta lång tid att gå in och ur VAS för en enkel sak exempelvis i samband med ärenden i reception.*
- på ortopeden, som anger som skäl:
  -: *Alla har eget inlogg och målsättningen är att använda eget inlogg, men utifrån att vi har tre arbetsstationer på ortopedmottagningen så händer det ibland att läkare eller kollegor behöver ta del av patientinformation.*

T4

Från tandvårdsförvaltningen uppges att inga grupploggin förekommer.

Bedömning

Att använda landstingets system under annan persons inloggning får enligt landstingets regler inte förekomma. Det strider både mot patientdatalagen och mot Socialstyrelsens förordningar.

I landstingets riktlinjer för hur vårdinformation ska hanteras står bl.a. följande:

> *”Olovligt intrång och olovligt efterforskande i ett vårdregister kan vara straffbart enligt straffbestämmelserna om dataintrång i* ***brottsbalken*** *4 kap 9c § (böter eller fängelse i högst två år). Bestämmelsen är tillämplig då någon använder sig av sin behörighet till åtkomst till ett elektroniskt journalsystem för att läsa uppgifter utan att detta behövs för arbetet, t ex av nyfikenhet.”*

Användande av grupploggin strider mot Socialstyrelsens föreskrift SOSFS 2008:14 då det medför att logglistorna inte visar vilka individer som haft åtkomst till patientuppgifterna. Detta medför i sin tur en fara för loggarnas bevisvärde och att det preventiva skydd som logguppföljningen avses vara, mot att obehöriga ska ta del av patientuppgifter, sätt ur spel. Ur denna aspekt är grupplogin nästan lika illa som om någon olovligen tillskansar sig någon annans användaridentitet.

Att grupplogin ändå tillåts förekomma med arbetsledningens och, vad gäller C-operation, IT-stabens kännedom[3], tyder på att VAS ännu inte är tillräckligt anpassat till verksamhetens behov. Det kan också vara så att delar av organisationen har svårt att anpassa sitt arbetssätt till de verktyg som tillhandahålls och de regler som gäller.

Att studenter skriver under ordinarie personals övervakning gör att det inte går att se vem som tagit del av vilka patientuppgifter. För detta krävs att studenterna tilldelas egna användaridentiteter vilket dock kan kräva nya lösningar kring hur signering mm ska gå till. Vi förslår att därför att möjliga lösningar undersöks.

Här finns således en officiell regel som anger förbud och en intern praxis där den/de som upplever den t ex som ett hinder i arbetet, tillåts bryta mot den med ”tyst godkännande” från ledningen. Enligt vår mening är det otillfredsställande med en ledning/styrning som inte reagerar när uppsatta regler bryts. Att medvetet inte agera är också en form av beslut som kan medföra juridiska konsekvenser. T ex kan det bli svårt att utkräva något ansvar från den/de individer som bryter mot reglerna.

Åtgärder måste omgående vidtas så att förbudet mot användande av annans inloggning och gruppinloggning kan efterlevas och efterlevs. Om s.k. smartcards löser problemet, som C-op. anger, så bör införandet av sådana kort ges högsta möjliga prioritet.

[3] Dnr:LS/776:1/2006. Brev från verksamhetsområdeschefen för akutområdet till IT-chefen, vari det framgår att man avser att frångå de rutiner som finns för inloggning i VAS

Revisionsfråga:

3. Går det att utläsa minst följande ur loggarna: Vem som haft tillgång till en uppgift och tidpunkt för åtkomsten.

VAS
Ja, till den del personal inte använt sig av grupploggin eller använt annans användaridentitet.

T4
Ja

Revisionsfråga:

4. Finns det för resp system dokumenterade regler för vad som skall loggas?

Ja, det finns angivet vad som skall loggas. Detta sker också i både VAS och T4

Förutom VAS och T4 finns det dock en mängd andra system inom landstinget som hanterar patientuppgifter. Då vår granskning i huvudsak har varit avgränsad till VAS och T4, har vi inte gjort någon djupare genomgång av hur andra system hanterar patientuppgifter med avseende på behörigheter och loggning. Vi vill dock ändå peka på några förhållanden:

Vid ett möte med personal från landstingets IT-stab framkom att man egentligen inte har något samlat grepp om vilka system som innehåller patientuppgifter, än mindre om patientdatalagen och socialstyrelsens förordningar kan sägas vara uppfyllda vad gäller t ex åtkomst och loggning. Vid mötet gjordes en genomgången av landstingets systemförteckning varvid det framkom att det finns en lång rad system som innehåller, eller ”möjligen innehåller”, patientuppgifter och därmed kan omfattas av patientdatalagen och Socialstyrelsen förordning SOSFS 2008:14 . IT-staben hänvisade till resp systemägare för svar på i vilken utsträckning patientuppgifter finns lagrade i systemen.

I BITS, som landstinget beslutat ska gälla, står bl.a. följande:

> *”Informationssystem som hanterar personuppgifter ska vara förtecknat och anmält till personuppgiftsombud (om sådant utsetts).”*

Peronuppgiftsombudet uppger att uppgifter om system som innehåller personuppgifter också erhålls. Enligt uppgift är det dock inte säkert att allt har rapporterats. Det ankommer på respektive systemägare att själv göra en anmälan till personuppgiftsombudet och alla är kanske inte tillräckligt informerade om detta.

Vi har erhållit en sammanställning över vilka register som anmälts till personuppgiftsombudet och dennes bedömning av om de innehåller patientuppgifter. Resultatet, enligt sammanställningen, visar på att det fanns ca 90 ej anmälda register varav 51 eventuellt kan innehålla patientuppgifter, enligt personuppgiftsombudets bedömning. Anmälda register med personuppgifter uppgår till 85 vara 64 bedöms kunna innehålla patientuppgifter.

Vi vill betona att uppgifterna i många fall bygger på kvalificerade gissningar. I några fall finns det tvivel på om registren fortfarande finns. Ovanstående uppgifter visar dock, även om de är osäkra, på att det finns en stor mängd system inom landstinget som hanterar personuppgifter och även patientuppgifter.

Bedömning

En kvalitetssäkrad förteckning över vilka system som hanterar personuppgifter bör upprättas i enligt med BITS. Lämpligen görs detta i samråd mellan IT-staben, resp systemägare och personuppgiftsombudet, varvid det även kan vara lämpligt att notera vilka som även innehåller patientuppgifter.

Alla systemägare bör informeras om anmälningsplikten och om vilka regler som gäller för person- och patientuppgifter och vilka krav detta medför på deras system. .

Patientdatalagen är ny och det är, enligt vår bedömning, sannolikt att det bland befintliga system kan finns sådana som ännu inte hunnit anpassas till den nya lagstiftningen. Det är dock också sannolikt att det kan komma att uppstå problem om eller när det uppdagas att ett system inte klarar de krav som finns i lagar och förordningar. Konsekvensen kan bli att något system därmed inte heller längre får användas. Är då systemet av avgörande betydelse för verksamheten kan en allvarlig störning uppstå.

Det är därför, enligt vår mening, en viktig ledningsfråga att i tid vidta åtgärder som säkerställer att samtliga system som innehåller patientuppgift uppfyller gällande lagar och förordningar.

Revisionsfråga:

5. Är loggarna skyddade mot obehörig förändring och borttagning?

Enligt uppgift kan bara TietoEnator, som svarar för driften av VAS och T4, göra ändringar.

Revisionsfråga:

6. Har systemägaren beslutat om hur länge loggdata skall sparas?

I landstingets ”Riktlinjer för tillgång till vårdinformation” (LS 323/2008) sägs:

> ”Systemägaren har att besluta om hur länge loggdata skall sparas, en kortaste bevarandetid på två år gäller dock.”

Kravet enligt Socialstyrelsens föreskrift SOSF 2008:14 11 § p6. är dock 10 år

VAS
Den anvisning som systemansvarig upprättat överensstämmer med riktlinjerna d v s att loggdata ska sparas i 2 år.

Bedömning:

Interna riktlinjer och anvisningar, avseende hur länge loggdata ska sparas, måste korrigeras.

7.3 UPPFÖLJNING/LOGGKONTROLL

Revisionsfråga:

7. Finns ändamålsenliga och dokumenterade rutiner för logguppföljningen.

VAS
Regler (bilaga 1) och anvisningar (bilaga 2) finns och förefaller, av de svar vi fått, som ändamålsenliga. Några har dock framfört önskemål om de skulle kunna utvecklas i fråga om hur urvalet ska göras.

Bedömning:

Vår bedömning är att reglerna huvudsakligen är ändamålsenliga. Förbättringar kan dock ske i några avseenden som beskriv på annan plats i denna rapport.

Revisionsfråga:

8. Granskas loggarna av *verksamhetschefen* eller av den i resp område som verksamhetschefen utsett.

VAS
Enligt den blankett (bilaga 3) som tagits fram av systemansvarig skall resultatet lämnas till områdeschef/verksamhetschef som sedan ska redovisa resultatet i områdeskommittén.

Enligt riktlinjerna (bilaga 1) och rutinbeskrivningen (anvisningen) (bilaga 2) för kontroll av journalloggar skall resultatet av kontrollerna bedömas och därefter lämnas till områdes-/verksamhetschef.

Enligt de uppgifter vi erhållit, utförs granskningen av loggarna i VAS av resp områdes ”VAS-ansvariga”, förutom vid en hälsocentral där den VAS-ansvarige tar fram listor som överlämnas till verksamhetschefen och medicinskt ansvarig läkare för kontroll.

Vi har också fått uppgift om att det inte gjorts några kontroller alls vid en hälsocentral sedan VAS infördes, men också uppgift om att man nu kommer att återuppta kontrollerna.

Det finns flera varianter på hur man i praktiken rapporterar resultatet av kontrollerna. Allt ifrån att man endast lämnar rapport vid misstänkt intrång till att man alltid lämnar rapport. Inom de flesta verksamhetsområden går en rapport till VO-chef, medan rapporterna inom några områden stannar hos avd/enhetschef. Tre områden uppger att resultatet redovisas för områdeskommittéerna.

T4

Granskningen görs av resp klinikchef.

Bedömning:

Rutinbeskrivningen och blanketten/anvisningen bör ses över så att det blir tydligt om resultatet av kontrollerna ska redovisas i resp. områdeskommitté eller inte.

Revisionsfråga:

9. Görs logguppföljning genom regelbundna slumpmässiga urval av loggregistreringarna för personal resp patienter i tillräcklig omfattning?

VAS
Enligt rutinbeskrivningen (anvisningen) för kontroll av journalloggar (bilaga 2)skall

- Stickprovskontroller göras minst fyra gånger/år samt när behov uppstår.
- Kontrollerna bör göras i sådan omfattning att i genomsnitt minst en tiondel av användarna blir föremål för uppföljning varje år.
- Forceringar kontrolleras dagligen

Enligt den blankett/anvisning (bilaga 3) som tagits fram av systemansvarig ska kontroller göras minst tre gånger/år. Av blanketten/anvisningen framgår inte hur många patienter eller personal respektive kontroll bör omfatta.

På vår förfrågan har de flesta verksamhetsområdena svarat att kontroller görs 3-4 ggr per år.

De svar vi fått från verksamhetsområdena varierar i detaljeringsgrad. Vad gäller omfattningen av kontrollerna i form av antal patienter vars journaler kontrollerats resp hur många i personalen som omfattats av kontrollerna vill vi, av säkerhetsskäl, inte ange några uppgifter som gör att omfattningen hos någon viss enhet kan identifieras. Vi kan dock konstatera att omfattningen i form av antal kontrollerade patientjournaler resp personal inom vissa delar av organisationen är mycket få och i något fall saknas helt, utifrån de uppgifter vi fått.

Endast ett par verksamhetsområden har lämnat uppgifter som anger en sådan omfattning på kontrollen att de uppnår föreskrivna 10 procent av användarna. För några områden finns uppgift om antal kontroller, men det saknas uppgift om hur många som har behörighet att ta del av patientuppgifter. Vi har också fått uppgifter som tyder på att omfattningen av kontrollerna kan skilja betydligt mellan enheterna inom ett och samma verksamhetsområde.

Primärvården har inte kunnat precisera hur många kontroller som gjorts avseende patienter eller personal. Man hänvisade till att någon sammanställning ännu inte fanns klar.

Forceringar
Av ”Rutin för kontroll av journalloggar VAS”, (bilaga 2), framgår att en användare i VAS kan forcera sin behörighet och få åtkomst till journaler han/hon normalt inte har behörighet till om vederbörande bedömer att det finns sekretessbelagd journalinformation som kan vara värdefull att ta del av för vård av patienten.

Forceringar skall kontrolleras dagligen (enl. rutinbeskrivning för kontroll av loggar). Det är verksamhetens ansvar att gjorda forceringar kontrolleras. Om orsaken inte angivits tillräckligt tydligt ska kontakt tas med den användare som gjort forceringen. Efter denna kontroll skall markering att forceringen är kontrollerad göras i VAS.

Tyvärr kom frågan, om hur ofta kontroll av forceringar görs, inte med i vår enkät. Ett flertal har ändå kommenterat detta i sina svar och intrycket är att detta görs. Några anger dagligen, medan ett område anger 1-2 grr/vecka.

Från område ortopedi har vi däremot fått ta del av en lokal rutinbeskrivning varav det framgår: *”Daglig kontroll av ”forceringar” behöver ej utföras på område ortopedi. (endast kliniker med specifika sekretessregler ex. psykiatri)*”.

T4

Kontroller görs 3 ggr/år. Omfattningen av de utförda kontrollerna bedöms som tillräcklig.

Bedömning:

VAS
Blanketten/anvisningen bör ses över så att den överensstämmer med rutinbeskrivningen om hur ofta kontroller ska göras, dvs. minst 4 ggr/år.

Kontrollernas omfattning måste ökas kraftigt inom många enheter för att dessa ska nå upp till den nivå som anges i landstingets rutinbeskrivning och därmed ge den prevention som åsyftats.

Ortopedklinikens lokala rutinbeskrivning överensstämmer inte med den rutin som systemansvarig lagt fast om daglig kontroll av forceringar. En översyn av den lokala rutinbeskrivningen rekommenderas.

T4
Enligt de uppgifter vi erhållit bedömer vi omfattningen, i form av såväl antal kontrollerade patienter som personal, som tillräcklig. Kontrollernas frekvens bör dock kunna vara densamma som inom sjukvården, dvs. minst 4 ggr/år.

Revisionsfråga:

10. Dokumenteras och sparas dokumentationen från logguppföljning?

Enligt Socialstyrelsens föreskrift SOSFS 2008:14, 11 § p 5, ska vårdgivaren ansvara för att det i ledningssystemet finns rutiner som säkerställer att systematiska och återkommande stickprovskontroller av loggarna görs och att genomförda kontroller dokumenteras.

VAS
Utifrån de svar vi fått kan vi konstatera att de flesta verksamhetsområden sparat dokumentationen från utförda kontroller. Några svarar att dokumentationen sparas i 10 år, andra har svarat ”oändligt” eller ”löpande”. Vi har också fått uppgifter från två verksamhetsområden att ingen dokumentation sparats. I det ena fallet med argumentet att ”*Där vi kontrollerat har det inte varit några misstankar*”.

T4
Tandvårdsförvaltningen uppger att dokumentationen sparas i 2 år.

Bedömning:

VAS
Lämpligen bör rutinbeskrivningen kompletteras med att dokumentation om utförda kontroller skall sparas, oavsett kontrollernas resultat, och att de ska sparas lika länge som loggarna, dvs. 10 år.

T4
Dokumentation om utförda kontroller bör sparas lika länge som loggarna, dvs.. 10 år.

Revisionsfråga:

11. Kontrollerar personuppgiftsombudet på ett ändamålsenligt sätt att föreliggande riktlinjer efterlevs?

Personuppgiftsansvarig är den nämnd eller den styrelse (det politiska organet) som ansvarar för verksamheten där vårdregistret förs. För Jämtlands läns landsting är landstingsstyrelsen personuppgiftsansvarig.

Det yttersta ansvaret för behandling av personuppgifter ligger på personuppgiftsansvarig. Personuppgiftsansvarig skall se till att behandling av personuppgifter utförs på ett korrekt sätt.

Ett personuppgiftsombud kan utses för att hjälpa den personuppgiftsansvarige att uppfylla lagens krav. Landstinget har utsett ett sådant personuppgiftsombud.

I BITS, som landstinget beslutat ska gälla, står bl.a. följande:

”Informationssystem som hanterar personuppgifter ska vara förtecknat och anmält till personuppgiftsombud (om sådant utsetts).”

”Bearbetning av personuppgifter samt information om respektive samtycke till bearbetningen ska ske i enlighet med vad som överenskommits med personuppgiftsombud eller i enlighet med PUL.”

I prop. 2007/08:126 sägs bl.a.

”I den utsträckning den som är personuppgiftsansvarig utser ett personuppgiftsombud blir bestämmelserna i personuppgiftslagen om sådana ombud tillämpliga även på patientdatalagens område.”

I ”Riktlinjer för tillgång till vårdinformation” (Dnr LS 323/2008) har landstingets personuppgiftsombud tilldelats en uppgift enligt följande:

”Att logguppföljning gjorts, och resultatet därav, skall dokumenteras och dokumentationen skall sparas och kunna visas upp på begäran från JLL:s personuppgiftsombud som har att följa upp att föreliggande riktlinjer efterlevs.”

Vid intervju framkom att landstingets personuppgiftsombud ännu inte hade kommit igång med att göra några kontroller. Arbetsuppgiften, som följde med att den nya patientdatalagen började gälla, var relativt ny och vederbörande hade ännu inte hunnit organisera och utforma rutiner för uppgiften.

Personuppgiftombudet anser att det kan behöva tas fram rutiner som medför möjligheter, att se över loggar och kontrollrutiner för dessa, innan nya system tas i bruk, framför allt om de innehåller integritetskänslig information.

Bedömning:

Enligt vår mening är personuppgiftsombudets kontrollfunktion av stor vikt för att landstinget med trovärdighet ska kunna hävda att patientuppgifterna hanteras på ett sådant sätt att patienternas personliga integritet är tryggad i enlighet med lagar och föreskrifter. Det är därför också av stor vikt att säkerställa att personuppgiftsombudet ges förutsättningar att utföra uppgiften samt att det finns tydliga befogenheter och/eller rapporteringsvägar om brister upptäcks.

Det viktigt att personuppgiftsombudets tillsyn snarast påbörjas.

Revisionsfråga:

12. Finns det ändamålsenliga rutiner som gör att det går att, på begäran, lämna sådana uppgifter till en patient om åtkomsten till dennes patientuppgifter som är utformad så att:
    - det framgår från vilken vårdenhet och vid vilken tidpunkt någon har tagit del av uppgifterna?
    - patienten kan göra en bedömning av om åtkomsten har varit befogad eller inte?

I Socialstyrelsens föreskrift SOSFS 2008:14, 12 § sägs:

”*Av informationen som vårdgivaren ska lämna till en patient om åtkomsten till dennes patientuppgifter ska det framgå från vilken vårdenhet och vid vilken tidpunkt någon har tagit del av uppgifterna. Informationen ska vara utformad på ett sådant sätt att patienten kan göra en bedömning av om åtkomsten har varit befogad eller inte.*”

Som framgår, av ovanstående föreskrift, anges bl a att det ska framgå från vilken vårdenhet någon haft åtkomst till patentuppgifterna och att uppgift ska lämnas så att patienten kan göra en bedömning av om åtkomsten varit befogad eller inte.

Vad vi kunnat se finns det ingen enhetlig nationell definition av begreppet vårdenhet[4]. Varje landsting bestämmer själv. Inom Jämtlands läns landsting har vi uppfattat att vårdenhet har tolkats som t.ex. hälsocentral, klinik, basenhet.

VAS

De flesta verksamhetsområdena har svarat att det finns ändamålsenliga rutiner för att, på begäran, lämna patienten en uppgift om från vilken vårdenhet och när någon tagit del av dennes patientuppgifter. Ett av de verksamhetsområden som anser att det finns ändamålsenliga rutiner har ändock lagt till att man inte är helt klar över vad som skall lämnas ut.

Ett verksamhetsområde bedömer att rutinerna inte är utformade så att patienten kan ta del av uppgifterna och inte heller bedöma om åtkomsten varit befogad eller inte.

I svaret från primärvården uppges att det inte finns några dokumenterade regler som man känner till, men man säger samtidigt att uppgifterna kan tas fram.

Vad gäller frågan om patienten har möjlighet att göra en bedömning av om åtkomsten varit befogad eller inte, har de flesta svarat att de inte tror att patienterna kan det eller att personal måste bistå för att detta ska vara möjligt. Från ett verksamhetsområde ställs frågan: *”Är detta patientens uppgift?”*.

Ett område uppger att man upplever de centrala riktlinjerna som oklara och exemplifierar med att man inte är riktigt säker på vad som får lämnas ut till patienten.

T4

Tandvården uppger att det går att ta fram uppgifter som visar från vilken vårdenhet och vid vilken tidpunkt någon har tagit del av uppgifterna, men svarar ”förhoppningsvis” på frågan om patienterna kan bedöma om åtkomsten varit befogad eller inte.

Bedömning:

För att ge patienterna en bedömningsmöjlighet, av om åtkomsten varit befogad eller inte, bör begreppet ”vårdenhet” ges en generös tolkning och uppgifter lämnas med så hög detaljeringsgrad som möjligt. T ex arbetsställe.

Rutinen för utlämnande av uppgift och hur den på ett pedagogiskt sätt ska kunna presenteras för de patienter som begär en sådan, behöver utvecklas.

[4] Vårdenhet: Definition enl Socialstyrelsens termbank. ″Organisatorisk enhet som tillhandahåller hälso- och sjukvård. Bedömningen av vad som anses vara en vårdenhet sker idag inte med enhetliga nationella principer utan varje huvudman avgör avgränsningen i det enskilda fallet. Vårdenhet kan vara t.ex. vårdcentral, sjukhus, klinik, basenhet, mottagning, vårdavdelning eller motsvarande.″

7.4 ÅTGÄRDER VID MISSTÄNKTA ELLER KONSTATERADE ÖVERTRÄDELSER

Revisionsfråga:

13. Görs uppföljning snarast vid misstänkt intrång eller överträdelse?

I de fall misstankar om intrång funnits finns det inget, i de uppgifter som lämnats till oss, som tyder på att uppföljning inte görs med skyndsamhet.

Revisionsfråga:

14. Utreds ev. misstankar om att någon berett sig tillgång till information utan att ha rätt till det av den misstänktes arbetsledning?

Av de svar vi fått på vår fråga, om det någon gång uppstått misstanke om intrång eller överträdelser, uppger de flesta att det aldrig uppstått några sådana misstankar. Ett område har dock svarat att ”*misstanke uppstår inte så sällan, men har hittills inte vid något tillfälle visat sig vara grundat på överträdelse, utan vi har funnit naturliga förklaringar vid genomgång av journalen*”.

Bedömning
Av detta skulle man eventuellt kunna dra slutsatsen att misstankar om överträdelse uppstår mycket sällan, men å andra sidan har vi också kunnat konstatera att omfattningen av antal utförda kontroller inte når upp till den beslutade nivån inom ett flertal områden.

De misstankar som ändå uppstår förefaller, enligt de svar vi fått, utredas i enlighet med landstingets anvisningar.

Östersund den 3 februari 2009

Ulf Rubensson
Certifierad kommunal revisor

8 BILAGOR

8.1 BILAGA: RIKTLINJER FÖR TILLGÅNG TILL VÅRDINFORMATION I LANDSTINGETS VÅRDREGISTER, LOGGUPPFÖLJNING SAMT ÅTGÄRDER VID MISSTÄNKT OLOVLIGT ANVÄNDANDE.

(Fastställda av landstingsdirektören 2008-03-28 (Dnr LS 323/2008)

Lagringen av landstingets datoriserade vårdinformation sker nu alltmera gemensamt och patientorienterat och i allt mindre utsträckning per organisatorisk enhet.

Vården av en patient sker idag ofta i en vårdkedja där alla de olika aktörerna behöver ta del av varandras information. För att patienten skall få bästa möjliga vård krävs att man har en helhetsbild av patientens sjukdomsbild och –historia. Många patienter utgår också från att vårdpersonalen på en enhet har information om patientens kontakter vid andra enheter inom landstinget.

Den patientorienterade lagringen möjliggör att relevant vårdinformation snabbt och enkelt kan göras tillgänglig för behörig vårdpersonal där och när den behövs – och det oavsett om den härrör från den egna organisatoriska enheten eller från någon annan enhet som patienten varit i kontakt med.

För att få tillgång till vårdinformation krävs att man behöver den för vård- och behandlingsändamål

Landstingets hälso- och sjukvård är ett gemensamt sekretessområde inom vilket inre sekretess råder. Detta innebär att behörig vårdpersonal kan, utifrån eget ansvar, skaffa sig tillgång till den patientinformation i landstingets vårdregister som denne behöver för vård och behandling av sina patienter.

Att en anställd har teknisk behörighet att skaffa sig tillgång till information om en viss patient i ett vårdregister är *inte* detsamma som att ha behov av - och rätt till - att ta del av den informationen. Rätten till tillgång baseras på att man i den aktuella situationen behöver åtkomst till informationen för att på ett riktigt och säkert sätt fullgöra sina uppgifter gentemot aktuell patient.

För att ha rätt att ta del av vårdinformation krävs att det finns en vårdrelation till patienten.

En vårdrelation uppstår när en enskild befattningshavare planerar eller utför aktivitet i förhållande till patienten. En vårdrelation är begränsad i tid och innehåll till patientens vårdepisod.

Tilldelning av teknisk behörighet till system med vårdinformationen

Respektive *systemägare* ansvarar för att ändamålsenliga och dokumenterade rutiner finns för tilldelning (och inaktivering) av teknisk behörighet till system med vårdinformation.

Verksamhetscheferna ansvarar sedan för att bedöma och besluta vilka behörigheter som resp användare i dennes verksamhet skall ha utifrån användarens arbetsuppgifter och utifrån de behörighetsprinciper som gäller för resp system. Det gäller även eventuella behov av *läs*behörigheter till vårdinformation hos andra enheter inom landstinget.
Vid tilldelning av behörighet skall utgångspunkten vara att behörighet skall ges till den information som kan behövas för den anställdes arbetsuppgifter, varken mer eller mindre.

Vid förändrade arbetsuppgifter eller byte av arbetsplats skall tilldelad behörighet omprövas. Vid anställningens upphörande skall behörigheten tas bort.

Säker identifiering

Behörigheten skall vara kopplad till en unik personlig användaridentitet. Grupplogin skall inte användas för tillgång till vårdinformation.

Loggning

Landstingets strategi för behörighetstilldelning och strävan mot en patientorienterad gemensam lagring av vårdinformationen ställer höga krav på uppföljning av hur åtkomstmöjligheterna används.

Åtkomst skall kunna följas upp i efterhand genom maskinell logg. Loggen skall vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning. Ur loggarna skall **minst** gå att utläsa
- vem som haft tillgång till en uppgift och
- tidpunkt för åtkomsten.

Respektive systemägare ansvarar för att systemets loggningsfunktioner är tillräckliga i förhållande till de uppgifter som behandlas i systemet. Systemägaren ansvarar också för att det finns dokumenterade regler för vad som skall loggas.

Loggarna skall vara skyddade mot obehörig förändring och borttag. Systemägaren har att besluta om hur länge loggdata skall sparas, en kortaste bevarandetid på två år gäller dock.

Uppföljning/loggkontroll

Respektive *systemägare* ansvarar för att det finns ändamålsenliga och dokumenterade rutiner för logguppföljningen. Granskningsansvaret följer sedan linjorganisationen. Loggarna skall granskas av *verksamhetschefen* eller av den i resp område som verksamhetschefen utsett.

Logguppföljning skall göras genom regelbundna slumpmässiga urval av logg-registreringarna för visst antal patienter och visst antal personal. När patient är s k kändis eller anställd görs större urval, eller totalkontroll om så anses motiverat. Sådana regelbundna uppföljningar skall göras minst en gång var 3:e månad. Dessutom skall uppföljning göras snarast vid misstänkt intrång eller överträdelse. Loggkontrollerna bör göras i en sådan omfattning att i genomsnitt minst en tiondel av användarna blir föremål för uppföljning varje år.

Att logguppföljning gjorts, och resultatet därav, skall dokumenteras och dokumentationen skall sparas och kunna visas upp på begäran från JLL:s personuppgiftsombud som har att följa upp att föreliggande riktlinjer efterlevs.

Åtgärder vid misstänkta eller konstaterade överträdelser

Vid misstanke om att någon berett sig tillgång till information utan att ha rätt till det skall detta utredas av den misstänktes arbetsledning. Landstingets personalchef skall informeras redan när utredningen påbörjas.. Verksamhetschefen där den misstänkte är anställd ansvarar för utredningen och det gäller även i de fall de misstänkta överträdelserna skett till vårdinformation från annat verksamhetsområde. Om utredningen inte kan skingra misstankarna skall samråd ske med landstingets personalchef för fortsatt handläggning och ev beslut om arbetsrättsliga åtgärder och om polisanmälan skall göras, se bifogad handläggningsrutin.

Verksamhetschefen har då även att ta ställning till om, och hur, berörd/a patient/er skall informeras om vad som skett. Patient kan få hjälp att kontakta patientnämnd när en överträdelse har ägt rum.

Juridiska förutsättningar för tillgång till vårdinformation

Sekretess och tystnadsplikt i offentlig verksamhet gäller enligt **sekretesslagen** i hälso- och sjukvården för uppgifter om enskild persons hälsotillstånd eller andra personliga förhållanden.

I **patientjournallagen** regleras att varje journalhandling ska hanteras och förvaras så att obehöriga inte får tillgång till den. Endast de som behöver få tillgång till journaluppgifter för att kunna utföra sitt arbete, har rätt att ta del av journalen.

I **vårdregisterlagens** 3 och 4 §§ regleras automatiserad behandling av personuppgifter inom hälso- och sjukvården för vissa i lagen närmare angivna ändamål, bl.a. dokumentationen av vården av patienten eller för sådan administration som rör patienter och som syftar till att bereda vård eller föranleds av vård i enskilda fall.

I § 8 vårdregisterlagen sägs 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.

Med direktåtkomst enligt vårdregisterlagen, menas att befattningshavaren har en behörighet till vårdinformationssystem som medger att befattningshavaren utan mellanled direkt kan komma åt lagrad information i vårdinformationssystemet.

Olovligt intrång och olovligt efterforskande i ett vårdregister kan vara straffbart enligt straffbestämmelserna om dataintrång i **brottsbalken** 4 kap 9c § (böter eller fängelse i högst två år). Bestämmelsen är tillämplig då någon använder sig av sin behörighet till åtkomst till ett elektroniskt journalsystem för att läsa uppgifter utan att detta behövs för arbetet, t ex av nyfikenhet.

Information till anställda, studerande och praktikanter

Verksamhetsansvariga har att informera sina anställda om förutsättningarna för tillgång till vårdinformation, att och hur loggning och logguppföljning sker samt om hur vid logguppföljning funna misstänkta eller konstaterade överträdelser hanteras. Av informationen skall framgå att det kan vara straffbart att bereda sig tillgång till information om en patient som man inte har en vårdrelation till.

Vid introduktion av nyanställd vårdpersonal samt personal från bemanningsföretag skall information om dessa förutsättningar ingå. Det gäller även vid introduktion av studerande och praktikanter som skall verka inom landstingets hälso- och sjukvård.

8.2 BILAGA: RUTIN FÖR KONTROLL AV JOURNALLOGGAR VAS

Ledningsstab utveckling, hälso- och sjukvård
Lena Persson, systemansvarig VAS
Telefon: 063-142472

2008-07-17

FK: VAS-kontaktpersoner

Verksamhetsområdeschef motsv

RUTIN FÖR KONTROLL AV JOURNALLOGGAR VAS

Bakgrund

I oktober 1998 fastställde dåvarande Data-etiska kommittén i Jämtlands läns landsting en rekommendation av regler för kontroll av otillbörligt utnyttjande av journalinformation, se bilaga 1. Utifrån den rekommendationen skrevs då en rutin för hur kontroll kunde göras i VANIA. Nedanstående beskrivning av kontroll i VAS är densamma som gällt för VANIA dock med komplettering av rutin för det som i VAS heter forcering av behörighet.

Kontroller

Stickprovskontroll av hur informationen i VAS används sker genom uttag av logglistor i formuläret SY26. Datum skall vara minst två dagar bakåt i tiden.

Skriv in aktuellt personnummer i SY26, hämtas från ”Förslag på kontroller” (se nedan).

Stickprovskontrollerna skall göras minst fyra gånger/år samt när behov uppstår.

Kontrollerna bör göras i sådan omfattning att i genomsnitt minst en tiondel av användarna blir föremål för uppföljning varje år.

Forceringar skall kontrolleras dagligen, se vidare ”Kontroll av forceringar”.

Bedöm resultatet som därefter skall lämnas till områdes-/verksamhetschef.

Förslag på kontroller

Det finns olika metoder för kontroll och nedan redovisas några förslag:

1. Inneliggandelistan (SV54). Välj den sista patienten som visas på bildskärmen.
2. Dagens patienter (AN1). Välj den sista patienten som visas på bildskärmen.
3. För övrigt kan kontroller göras vid misstanke om otillbörligt utnyttjande.
4. Om intressant/känd person har varit patient.
5. Om egen personal blir patient.

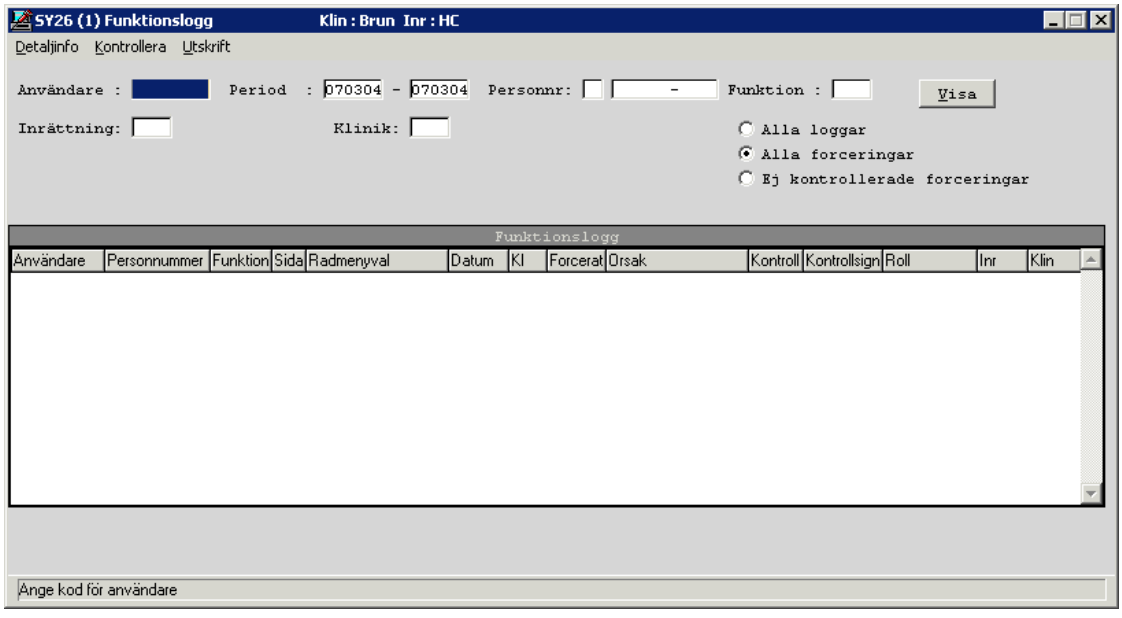
Forcering av behörighet

I VAS kan en användare forcera sin behörighet och få åtkomst till journaler han/hon normalt inte har behörighet till. Det är därför viktigt att det finns rutiner för dagliga kontroller om någon forcerat och tagit del av era journaler. Funktionen forcera skall användas när vårdgivaren bedömer att sekretessbelagd journalinformation kan vara värdefull att ta del av för vård av patienten.

För att användaren skall kunna forcera journaler så måste han/hon öppna formuläret SY74 ”Forcering - på” och där ange sitt lösenord samt orsak till forceringen. För att återgå till normalläge öppnar användaren formuläret SY75 ”Forcering - av” och därmed avlutas forceringen.

Kontroll av forceringar

Alla loggar kontrolleras i SY26 ”Funktionslogg”. Som tidsperiod kan valfri tid anges men till och med datum måste vara två dagar bakåt i tiden. Markera ”Ej kontrollerade forceringar”. I radmenyvalet Detaljinfo visas orsaken till forceringen, det finns också möjlighet att skriva ut logglistan och då skrivs även orsaken till forceringen ut. Det är verksamhetens ansvar att gjorda forceringar kontrolleras. Eventuellt måste kontakt tas med den användare som forcerat om orsaken till forceringen inte är tillräckligt tydlig. Efter denna kontroll skall markering att forceringen är kontrollerad göras i VAS. Radmenyvalet Kontrollera väljs och på frågan ”Forcering kontrollerad?” svaras Ja och därefter bekräftas med OK.



Bilaga 1

Data-etiska kommitténs rekommendation oktober 1998:

”Patienten ska aldrig behöva tvivla på att den information som lämnas i förtroende till hälso- och sjukvården hanteras korrekt och lagligt och att den bara är tillgänglig för behöriga personer. Både patienter och personal ska kunna lita på att systemen är tillgängliga när de behövs och att den information som hämtas ur dem är felfri och aktuell.

Sekretess innebär att bara auktoriserade användare äger rätt att bearbeta, läsa och skriva data. Sekretessbelagd data ställer mycket höga krav på åtkomstkontroll. Åtkomsten får endast avse de uppgifter som behövs för arbetets utförande.

Verksamhetschefen har ansvar för att säkerheten upprätthålls och för att kontroll sker med viss regelbundenhet.

Det finns olika metoder för kontroll och var och en väljer givetvis den som passar bäst. Man kan t ex slumpmässigt välja ut en viss användare eller särskild patientjournal. Särskild observans vad gäller ”kända eller intressanta personer”.

8.3 BILAGA: KONTROLL AV JOURNALLOGGAR VAS

JÄMTLANDS LÄNS LANDSTING

KONTROLL AV JOURNALLOGGAR VAS

Bakgrund

Människor som söker sjukvård skall aldrig behöva tvivla på att den information som lämnas i förtroende till hälso- och sjukvården hanteras korrekt och lagligt, samt att den bara är till- gänglig för behöriga personer.

Sekretess

Sekretess innebär att endast behöriga användare har rätt att läsa, skriva och bearbeta sekretessbelagd data.

Åtkomsten får endast avse uppgifter som behövs för arbetets utförande.

Kontroller

- Kontroll av hur informationen i VAS-systemet används sker genom uttag av logglistor.
- Kontrollerna skall göras minst tre gånger/år.
- Resultatet skall lämnas till områdeschef/verksamhetsschef som redovisar resultatet i områdeskommittén.

Förslag på kontroller

1. Inneliggandelistan (SV54). Välj den sista patienten som visas på bildskärmen.
2. Dagens patienter (AN1) Välj den sista patienten som visas på bildskärmen.
3. För övrigt kan kontroller göras vid misstanke om otillbörligt utnyttjande.
4. Om intressant/känd person varit patient.
5. Om egen personal blir patient.

Datum för kontroll:
Avd/mottagning:
Kontroller utförd av:
Kommentar: