LANDSTINGSREVISIONEN

Granskning av vårdgivarens informationssäkerhet

Rapport nr 20/2012

VÄSTERBOTTENS LÄNS LANDSTING

Februari 2013

Tobias Hermansson, Ernst & Young

Granskning av vårdgivarens informationssäkerhet

Västerbottens läns landsting

20 februari 2013

Innehållsförteckning

Sammanfattning

Ernst & Young har på uppdrag av revisorerna i Västerbottens läns landsting (VLL) genomfört en granskning inriktad mot vårdgivarens informationssäkerhet. Syftet med uppdraget har varit att bedöma om ansvarig vårdgivare i VLL säkerställt att landstinget har rutiner och kontroller som innebär att patientdata hanteras på korrekt sätt i förhållande till socialstyrelsens föreskrifter (SOSFS 2008:14) och patientdatalagen (2008:355).

Vår bedömning är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte i tillräcklig utsträckning har säkerställt rutiner och kontroller som innebär att patientuppgifter behandlas på ett korrekt sätt i förhållande till socialstyrelsens föreskrifter och patientdatalagen. VLL har en organisation och struktur på plats för att i all väsentlighet kunna säkerställa att patientuppgifter behandlas på korrekt sätt, men utformade rutiner och kontroller avseende exempelvis loggkontroller är inte fullt ut implementerade i verksamheten. I vår granskning har vi identifierat förbättringsområden för i första hand styrning av informationssäkerhetsarbetet samt rutiner och kontroller avseende den inre sekretessen i SYSteam Cross såsom behörighetsstyrning och loggkontroller:

- VLL har en utpekad informationssäkerhetsansvarig och beslutade riktlinjer för informationssäkerhet. Informationssäkerhetsansvarig saknar dock arbetsbeskrivning och tid för att arbeta med informationssäkerhet och i arbetet med informationssäkerhet sker ingen årlig rapportering av vilka granskningar och skyddsåtgärder av större betydelse som gjorts, vilka riskanalyser som har utförts avseende informationssäkerhet och vilka förbättringsåtgärder som har vidtagits, varken till informationssäkerhetsansvarig eller till landstingsstyrelsen och hälso- och sjukvårdsnämnden.
- Periodisk granskning av behörigheter i SYSteam Cross utförs inte på samtliga enheter och hanteringen kring avslut av behörigheter skiljer sig mellan enheterna, vilket ökar risken för att användare som bytt befattning eller avslutat sin anställning fortfarande har åtkomst till patientinformation.
- På granskade enheter har ingen uppföljning av verksamhetens loggranskning utförts. Enligt befintliga anvisningar, *Anvisningar för loggkontroll*, ska uppföljning av verksamhetens loggranskning utföras av Staben för verksamhetsutveckling. Genomförs inte uppföljning av att loggkontroller utförts enligt definierade anvisningar ökar risken för att loggkontroller utförs på ett felaktigt sätt, vilket i sin tur kan medföra att felaktigheter eller avvikelser inte upptäcks. Vår granskning visar även att enheterna har olika rutiner för loggkontroller och att inte samtliga enheter har kännedom om befintliga anvisningar för loggkontroller. Majoriteten av enheterna kontrollerar inte tillräckligt många användare för att säkerställa att varje användare blir kontrollerad i snitt en gång per år.

Samtliga förbättringsområden som har identifierats i samband med granskningen har redovisats i rapporten och rekommendationer på åtgärder har presenterats (kapitel 3), som kan eliminera eller minimera bristerna. Landstingsstyrelsen och hälso- sjukvårdsnämnden bör säkerställa att rekommendationerna åtgärdas för att säkerställa att patientuppgifter hanteras på ett korrekt sätt i förhållande till socialstyrelsens föreskrifter och patientdatalagen.

Identifierade prioriterade rekommendationer

- Vi rekommenderar VLL att ta fram en arbetsbeskrivning för vilket ansvar som åligger rollen informationssäkerhetsansvarig. Säkerställ vidare att informationssäkerhetsansvarig har tillräckligt med arbetstid avsatt för att utföra arbete relaterat till sin roll och säkerställ att verksamheten informeras om vem som är informationssäkerhetsansvarig och dennes arbetsuppgifter och ansvar.
- Landstingsstyrelsen och hälso- och sjukvårdsnämnden är ytterst ansvarig för informationssäkerheten inom sina verksamhetsområden. Vi rekommenderar att rutiner införs för att kontinuerligt rapportera informationssäkerhetsarbetet till landstingsstyrelsen och hälso- och sjukvårdsnämnden. Vidare behöver rutiner skapas för vilken information verksamheten ska rapportera till informationssäkerhetsansvarig.
- Vi rekommenderar VLL att per enhet skapa rutiner för hur avslut av behörigheter ska hanteras, och implementera rutiner för periodisk granskning av behörigheter i SYSteam Cross. Den periodiska granskningen bör genomföras och rapporteras i enlighet med upprättad anvisning.
- Befintliga anvisningar för loggkontroller bör kommuniceras till samtliga enheter för att säkerställa att enheterna hanterar loggkontroller på samma sätt. Vi rekommenderar enheterna att särskilt gå igenom befintliga anvisningar för att säkerställa att loggkontroller genomförs i enlighet med anvisningarna. Vi rekommenderar VLL att kontinuerliga uppföljningar av loggkontroller genomförts. En rutin om återrapportering av loggkontroller bör upprättas för att säkerställa att uppföljning av loggkontroller genomförs.

1. Inledning

1.1. Bakgrund

Vårdgivarens informationssäkerhet regleras i patientdatalagen (2008:355) och socialstyrelsens föreskrifter (SOSFS 2008:14). Informationssäkerhet handlar om tillgänglighet, sekretess och riktighet som för Västerbottens läns landsting (VLL) innebär att patientuppgifter är tillgängliga och användbara för den som är behörig, att patientuppgifterna är korrekta, att obehöriga inte har möjlighet att ta del av uppgifterna, samt att det är möjligt att härleda förändringar och åtgärder till en specifik användare.

Revisorerna i VLL har beslut att genomföra en granskning inriktad mot vårdgivarens informationssäkerhet. Revisorerna önskar att granskningen av vårdgivarens informationssäkerhet tar utgångspunkt i valda delar av den granskning av hur landstinget följer patientdatalagen (nr 13/2009) som Ernst & Young genomförde 2009, liksom den verksamhetstillsyn som Socialstyrelsen genomförde 2011 avseende vårdgivarens informationssäkerhet.

1.2. Syfte

Syftet med granskningen har varit att bedöma om ansvarig vårdgivare i VLL säkerställt att landstinget har rutiner och kontroller som innebär att patientdata hanteras på korrekt sätt i förhållande till socialstyrelsens föreskrifter (SOSFS 2008:14) och patientdatalagen (2008:355). Följande övergripande revisionsfråga kommer att besvaras:

- Har ansvarig vårdgivare i VLL säkerställt att landstinget har rutiner och kontroller som innebär att patientuppgifter hanteras på ett korrekt sätt i förhållande till socialstyrelsens föreskrifter och patientdatalagen?

För att besvara den övergripande revisionsfrågan har revisionsfrågan brutits ned i nio (9) underliggande revisionsfrågor som är utgångspunkten för denna granskning:

- Finns en ändamålsenlig informationssäkerhetspolicy upprättad, liksom är ansvar för informationssäkerhet definierat?
- Finns och tillämpas rutiner för att säkerställa att behörigheter i SYSteam Cross begränsas till vad som är nödvändigt för att ge en god och säker vård?
- Finns och tillämpas rutiner för att begränsa (spärra) åtkomst till patientuppgifter i SYSteam Cross?
- Finns och tillämpas rutiner för hantering av åtkomst till patientuppgifter i SYSteam Cross vid sammanhållen journalföring?
- Finns och tillämpas rutiner för uppföljning av SYSteam Cross användning genom regelbunden kontroll av loggarna avseende åtkomst till patientuppgifter?
- Finns och tillämpas rutiner för enskildas direktåtkomst till sina patientuppgifter i SYSteam Cross och till loggar avseende åtkomst till sina patientuppgifter?
- Finns och tillämpas rutiner för att säkerställa att patientuppgifter som överförs från SYSteam Cross i öppna nät skyddas?

- Finns och tillämpas rutiner för säkerhetskopiering av patientuppgifter i SYSteam Cross?
- Finns rutiner för signering och låsning av journalanteckningar för att säkerställa spårbarheten i genomförda förändringar?

1.3. Revisionskriterier

Patientdatalagen (2008:355) trädde i kraft juli 2008 och reglerar åtkomst och hantering av patientdata och vårdinformation. Revisionskriterier för granskningen har varit kapitel 4, "grundläggande bestämmelser om inre sekretess och elektronisk åtkomst inom en vårdgivares verksamhet" samt kapitel 6, "sammanhållen journalföring". Socialstyrelsens föreskrifter (SOSFS 2008:14) kompletterar patientdatalagen och granskningen har sin grund i kapitel 2, "ansvar för informationssäkerhet".

Utöver det har granskningen sin utgångspunkt i valda delar av den granskning av hur landstinget följer patientdatalagen (nr 13/2009) som Ernst & Young genomförde 2009, liksom den verksamhetstillsyn som Socialstyrelsen genomförde 2011 avseende vårdgivarens informationssäkerhet.

1.4. Avgränsningar

Granskningen är avgränsad till att omfatta journalsystemet SYSteam Cross på Norrlands Universitetssjukhus i Umeå (NUS).

Vår granskning har inte haft sådan omfattning eller inriktning att vi haft möjlighet att upptäcka alla brister eller avvikelser som kan förekomma.

1.5. Metod

Granskningen har genomförts genom att identifiera och testa implementerade kontroller i SYSteam Cross, liksom att identifiera och testa rutiner avseende informationssäkerhet för SYSteam Cross, där det varit möjligt.

Uppdraget har genomförts i följande steg:

- Uppstartsmöte och avstämning av projektplan för att få en enhetlig bild av hur granskningen ska genomföras.
- Upprättande av granskningsprogram och inläsning av material från tidigare granskningar av informationssäkerheten/patientdatalagen.
- Genomförande av intervjuer för identifiering och test av rutiner och kontroller.
- Sammanställning av rapport och iakttagelser.
- Faktagranskning utförd av samtliga respondenter.
- Slutrapportering till Revisionskontoret.

Uppdraget har genomförts genom intervjuer med representanter för fem enheter inom VLL, utvalda av Revisionskontoret. Utöver dessa har intervjuer genomförts med systemansvarig för SYSteam Cross informationssäkerhetsansvarig samt representanter från Informatikenheten.

2. Granskning

2.1. SYSteam Cross

SYSteam Cross är ett system specifikt framtaget för arbete inom vård. VLL använder SYSteam Cross för hantering av patientuppgifter och som journalsystem. Inom VLL finns ungefär 8000 användare i SYSteam Cross.

Förvaltningsorganisationen för SYSteam Cross består av en systemägare (som också är vårdsystemägare, vilket innebär att han har en paraplyroll för samtliga vårdsystem inom VLL), en systemförvaltare och 12-13 systemhandläggare. Systemhandläggarna har olika specialistområden, men arbetar samtliga med support och hantering av behörigheter för SYSteam Cross. Utöver detta finns 50-60 så kallade LISA (Lokal Informatik System Ansvarig) som utses av verksamheten och som hanterar systemsupport inom sin enhet. Systemägaren, systemförvaltaren och utsedda LISA träffas en gång per månad för att diskutera problem och planerade förändringar för SYSteam Cross.

2.2. Informationssäkerhetspolicy

Underliggande revisionsfråga:

- Finns en ändamålsenlig informationssäkerhetspolicy upprättad, liksom är ansvar för informationssäkerhet definierat?

Identifierade starka sidor

- Det finns en utsedd informationssäkerhetsansvarig.
- Det finns riktlinjer för informationssäkerhet framtagna och publicerade.

Identifierade svaga sidor

- Informationssäkerhetsansvarig saknar arbetsbeskrivning och tid för att arbeta med informationssäkerhet.
- Riktlinjerna för informationssäkerhet är övergripande och anvisningar för hur arbetet ska omsättas i praktiken saknas.
- Riktlinjerna för informationssäkerhet har inte kommunicerats till samtliga medarbetare inom VLL. Flera respondenter saknar kännedom om riktlinjerna för informationssäkerhet och dess eget ansvar avseende informationssäkerhet.
- Det sker ingen årlig rapportering av vilka granskningar och skyddsåtgärder av större betydelse som har gjorts, vilka riskanalyser som har utförts avseende informationssäkerheten och vilka förbättringsåtgärder som har vidtagits, varken till informationssäkerhetsansvarig eller till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

I granskningarna 2009 samt 2011 påpekades att det saknas en informationssäkerhetspolicy, och i granskningen från 2009 påpekades att landstinget saknade en utsedd person för att arbeta med informationssäkerhet. Informatikenheten tillsatte 2010 en informationssäkerhetsansvarig, men på grund av olika omständigheter ville man flytta rollen utanför Informatikenheten. I maj 2012 tilldelades en av två jurister inom VLL rollen som informationssäkerhetsansvarig. I samband med tilldelningen av rollen som informationssäkerhetsansvarig skedde ingen formell överlämning och det fanns inte heller någon arbetsbeskrivning upprättad för rollen som

informationssäkerhetsansvarig. Detta, samtidigt som de juridiska arbetsuppgifterna markant ökade under 2012, leder till att endast omkring 2 h per vecka ägnas åt informationssäkerhetsarbetet.

Informationssäkerhetsansvarig har fortsatt ingen arbetsbeskrivning upprättad och anser att det inte är tydligt vilka hans arbetsuppgifter är, varför informationssäkerhetsarbetet bedrivs ad hoc.

Efter Socialstyrelsens granskning 2011 har *Riktlinjer för informationssäkerhet* upprättats. Den person, som idag har rollen som informationssäkerhetsansvarig, tog fram riktlinjerna under en period i slutet av 2011. Dokumenten godkändes av landstingsdirektören och hur eller om de sedan kommunicerats till verksamheten är inte känt. Dokumenten finns sedan 2012-06-08 att tillgå i landstingets ledningssystem som är ett system VLL använder för att lagra dokument och som finns tillgängligt för samtliga medarbetare via Intranätet. Riktlinjerna beskriver övergripande ansvar för personal, fysisk säkerhet, åtkomst till elektronisk information samt informationssystem. I riktlinjerna finns också beskrivet att verksamhetschefer är ansvariga för informationssäkerhet, men inte i vilken utsträckning eller vad det konkret betyder exempelvis för verksamhetschefernas arbete.

Informationssäkerhetsansvarig har ingen uppfattning om efterlevnaden av riktlinjerna, då det inte finns några uppfyllelsekrav i riktlinjerna eller görs någon uppföljning av informationssäkerhetsansvarig. Det sker inte någon rapportering till informationssäkerhetsansvarig kring incidenter som inträffat och informationssäkerhetsansvarig gör inte någon årlig rapportering till ledningen över informationssäkerhetsarbetet.

I våra intervjuer med respondenter från verksamheten har det framkommit att de flesta respondenter inte har kännedom om riktlinjerna för informationssäkerhet - endast respondenter från en enhet hade kännedom om riktlinjerna. Respondenterna framförde också att landstingets ledningssystem endast ses som ett dokumenthanteringssystem dit medarbetare vänder sig när de söker efter dokument de har kännedom om sedan tidigare. Uppfattningen bland respondenterna var att information som är viktig behöver kommuniceras via chefskanalen alternativt via e-post.

Sammanfattningsvis kan vi se att det finns en utsedd informationssäkerhetsansvarig, dock ser vi brister i form av att informationssäkerhetsansvarig inte har tillräckligt med tid avsatt för detta arbete samt att det inte finns någon arbetsbeskrivning över vilket ansvar som åligger denne. Verksamheten vet inte vart de finner informationen om informationssäkerhetsriktlinjerna och det är osäkert om informationssäkerhetsriktlinjerna kommunicerats ut till verksamheten. Det finns inte heller några rutiner för rapportering till informationssäkerhetsansvarig och likaså genomför informationssäkerhetsansvarig inte någon rapportering till landstingsstyrelsen och hälso- och sjukvårdsnämnden över informationssäkerhetsarbetet.

2.3. Behörigheter i SYSteam Cross

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för att säkerställa att behörigheter i SYSteam Cross begränsas till vad som är nödvändigt för att ge en god och säker vård?

Identifierade starka sidor

- Samtliga användare i SYSteam Cross har individuella användarkonton.
- Samtliga användare tilldelas behörighet utifrån sin roll och vilken enhet de ska arbeta på.

Identifierade svaga sidor

- Periodisk granskning av behörigheter utförs inte på samtliga enheter, och inte någon enhet följer upprättad anvisning som beskriver att användares behörigheter ska granskas 2-3 gånger per år.
- Borttag av behörigheter hanteras olika på enheterna.

Arbetet med behörigheter har delegerats till enheternas LISA, men verksamhets- eller enhetschef är ansvariga för att meddela LISA om nyanställda som har behov av behörigheter i systemet. Behörighet till SYSteam Cross tilldelas av systemhandläggare på Informatikenheten och detta utförs efter att ett ärende registrerats av enhetens LISA i webbportalen, Web-fasit. LISA beställer behörighet utifrån den nya medarbetarens roll och det finns fördefinierade roller från tidigare medarbetare som kopieras vid tilldelningen av behörigheten. Samtliga användare tilldelas individuell behörighet.

Även borttag av behörigheter hanteras av LISA. De flesta respondenter har förklarat att LISA erhåller information från verksamhets- eller enhetschef när personal ska sluta. När det gäller visstidsanställda eller studenter håller LISA själv ordning på slutdatumet och begär avslut från Informatikenheten via webbportalen, Web-fasit. Upplevelsen bland respondenterna är att information inte alltid når LISA när personer ska sluta eller byta anställning inom VLL, varför det finns en risk att behörigheter inte avslutas.

I granskningarna från 2009 och 2011 påpekades att landstinget inte genomför systematisk uppföljning av behörigheter. Enligt *Anvisningar från SYSteam Cross Systemägare*, 2011-09-02, ska användares behörigheter granskas 2-3 gånger per år och rapporteras till verksamhetschef.

Det finns möjlighet för LISA att ta ut en lista från SYSteam Cross över användare som har behörighet till dess enhet. Av fem granskade enheter sker en årlig granskning av behörigheter endast på en enhet. Två enheter granskar listor över registrerade användare när det finns tid – granskningarna dokumenteras alljämnt inte. Två enheter saknar helt rutiner för granskning av behörigheter.

SYSteam Cross kräver att lösenordet är 6 tecken långt, det måste bestå av siffror och bokstäver samt bytas årligen. De senaste 24 lösenorden kan inte återanvändas. VLL kommer under 2013 att införa SITHS-kort för säker autentisering av användare.

2.4. Spärr av patientuppgifter

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för att begränsa (spärra) åtkomst till patientuppgifter i SYSteam Cross?

Identifierade starka sidor

- Det finns möjlighet att spärra patientuppgifter.
- En varningsruta kommer upp när en användare försöker få åtkomst till information om en spärrad patient.

Identifierade svaga sidor

- En användare kan inte se vad spärren avser innan användaren har gått förbi varningen om att det finns spärrade patientuppgifter. Specifikation av vad spärren avser kan endast göras med hjälp av fritext på patientöversikten.

Patientuppgifter får, enligt patientdatalagen, inte göras tillgängliga genom elektronisk åtkomst för den som arbetar vid en annan vårdenhet hos samma vårdgivare eller hos en annan vårdgivare inom ramen för sammanhållen journalföring, om patienten motsätter sig det. I sådana fall ska patientuppgifter spärras. Uppgift om att det finns spärrade uppgifter får vara tillgänglig för andra vårdenheter eller vårdgivare. Vad avser en spärr vid en annan vårdenhet hos samma vårdgivare får denna hävas av en behörig befattningshavare hos vårdgivaren om patienten samtycker till det eller om patientens samtycke inte kan inhämtas och information kan antas ha betydelse för den vård som patienten behöver.

En patient som önskar spärra sina patientuppgifter måste skriftligen vända sig till diariet. När diariet hanterat begäran diarieförs begäran, diariet lägger ett ärende till Informatikenheten, och en spärr sätts på patienten. Likaså görs en notering i fritext på patientöversikten avseende vad spärren avser, exempelvis vilka vårdenheter som berörs.

Om det finns spärrade uppgifter hos den vårdenhet man väljer i systemet, så kommer en varningsruta upp. Det framgår inte i varningsrutan vad spärren avser utan varningsrutan meddelar endast att det finns en spärr på patienten och i vilka fall det är tillåtet att gå vidare. Om användaren väljer att gå förbi spärren nås vyn för patientöversikt, i vilken noteringen om vad spärren avser ska framgå.

Hanteringen är likadan vad gäller vårdenheter hos andra vårdgivare inom ramen för sammanhållen journalföring.

I granskningen från 2011 påpekades att landstinget bör införa en teknisk spärr i systemet, då nuvarande lösning mer är att betrakta som en markering. Med nästa version av SYSteam Cross, version 5, kommer spärren att göras om och patienter ska då inte kunna spärra patientuppgifter mot enskilda vårdenheter. Den nya versionen kommer införas under 2013/2014.

2.5. Sammanhållen journalföring

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för hantering av åtkomst till patientuppgifter i SYSteam Cross vid sammanhållen journalföring?

Identifierade starka sidor

- Det finns rutiner för sammanhållen journalföring i SYSteam Cross och samtliga respondenter är medvetna om att patienten måste ge sitt medgivande för att enheten ska få söka information om patienten hos andra vårdgivare inom länet.

En vårdgivare är, enligt patientdatalagen, behörig att ta del av en annan vårdgivares patientuppgifter om följande kriterier är uppfyllda:

- Patienten har en aktuell patientrelation till vårdgivaren
- Patientuppgifterna kan antas ha betydelse för att förebygga, utreda och behandla sjukdomar eller skador hos patienten
- Patienten samtycker till att vårdgivaren tar del av patientuppgifterna

Om patientens samtycke inte kan inhämtas på grund av sjukdom eller liknande, och det föreligger en fara för patientens liv, kan under vissa omständigheter en vårdgivare ta del av en annan vårdgivares patientuppgifter/journalhandlingar utan patientens uttryckliga medgivande.

VLL tillämpar idag sammanhållen journalföring inom länet. Om vårdgivaren vill hämta patientuppgifter från en annan vårdgivare inom SYSteam Cross ska patienten tillfrågas om patienten godkänner det och vårdpersonalen ska notera patientens medgivande i fritext i patientöversikten.

För NPÖ (Nationell Patientöversikt) så är VLL idag anslutna som producenter och kommer att införa NPÖ som konsumenter under januari till och med april 2013. Det kommer inte finnas någon koppling mellan SYSteam Cross och NPÖ och för åtkomst till patientuppgifter via NPÖ kommer separat autentisering ske med SITHS-kort.

2.6. Loggkontroller

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för uppföljning av SYSteam Cross användning genom regelbunden kontroll av loggarna avseende åtkomst till patientuppgifter?

Identifierade starka sidor

- Det finns framtagna anvisningar för loggkontroller.
- Det genomförs kompletterande kontroller vid konkret misstanke om överträdelse.

Identifierade svaga sidor

- Enheterna tillämpar loggkontroller på olika sätt och samtliga enheter har inte kännedom om upprättade anvisningar för loggkontroller.
- Majoriteten av enheterna kontrollerar inte tillräckligt många användare för att säkerställa att varje användare blir kontrollerad i snitt en gång per år.
- Några enheter använder inte slumpgeneratorn vid loggkontroll, vilket medför att användare från andra enheter inte kontrolleras.
- Vid loggkontroller framgår det inte tydligt vilka åtgärder som vidtagits med patientuppgifterna, varför det är svårt för utförarna av loggkontroller att göra en bedömning huruvida åtkomsten är befogad.
- Dokumentationen av genomförda loggkontroller är inte enhetligt upprättad och i vissa fall väldigt översiktlig det där enbart framgår antalet anställda som kontrollerats och datum för kontrollen.
- På granskade enheter har ingen uppföljning av verksamhetens loggranskning utförts.
- Det finns ingen möjlighet för utförarna av loggkontroller att se vilka patientuppgifter som är spärrade, vilket omöjliggör särskild uppföljning av anställda som har haft åtkomst till dessa patientuppgifter.

VLL skapade 2006 anvisningar för hur loggkontroller ska utföras. I anvisningarna beskrivs:

- Att verksamhetschefen har ansvar för att loggkontroller sker för journalerna inom sitt verksamhetsområde
- Att antalet användare som kontrolleras varje månad ska motsvara att varje användare blir kontrollerad i snitt en gång per år
- Att användare ska väljas ut slumpmässigt
- Att loggkontroller ska genomföras vid misstanke om intrång, som för kända personer eller kända släktförhållanden
- Att protokoll på loggkontroller ska upprättas och arkiveras på vårdenheten i två år

Samtliga intervjuade verksamhetschefer har delegerat arbetet med loggkontroller, i alla fall utom ett till LISA. Hanteringen av loggkontroller skiljer sig åt mellan enheterna både i omfattning och i utförande, vilket är i enlighet med det påpekande som framfördes i granskningen 2011 att det är osäkert i vilken omfattning loggkontroller genomförs. Vi noterade också att inte samtliga enheter har kännedom om upprättade anvisningar för loggkontroller.

Det finns en slumpgenerator inbyggd i SYSteam Cross. Slumpgeneratorn slumpar fram en användare och redovisar då de journaler som användaren haft åtkomst till under en 24-timmarsperiod. Vissa enheter använder slumpgeneratorn medan andra har manuella listor som de följer upp för att säkerställa att alla anställda inom enheten blir kontrollerade minst en gång årligen. Majoriteten av enheterna når inte upp till målet, angivet i landstingets anvisningar, att samtliga användare ska granskas i snitt en gång per år.

Informationen som framgår när en användare kontrolleras är vilka patienter användaren haft åtkomst till, samt vid vilken tidpunkt patientjournalerna öppnades och stängdes - ingen information om vilken åtgärd som vidtagits är tillgänglig vid loggkontrollen, vilket också framfördes som ett påpekande vid granskningen 2011. Samtliga respondenter har beskrivit att enhetens LISA, eller utföraren av loggkontrollen, använder sin erfarenhet när de bedömer om användaren borde haft åtkomst till journalen. Utföraren av loggkontrollen vet ofta vilka patienter som är återkommande på enheterna, i annat fall kontrollerar de om patienten varit inskriven på enheten och om den granskade användaren är anställd på enheten. Om så är fallet görs ingen ytterligare kontroll, men om misstanke om felaktigheter kvarstår så går de in i patientjournalen för att följa upp om det finns någon signerad anteckning eller om det finns någon annan rimlig anledning till att användaren haft åtkomst till patientjournalen. Om det saknas uppenbar anledning rapporteras användaren vidare till verksamhetschefen.

Tidigare var det LISA på respektive enhet som administrerade spärr av patientuppgifter på begäran av patienterna. När nu diariet administrerar spärr av patientuppgifter har LISA inte längre kännedom om vilka patienter som är spärrade och kan inte göra specifika kontroller för dessa patienter, vilket vi noterade att några av enheterna tidigare utfört.

Samtliga granskade enheter dokumenterar utförda loggkontroller och sparar dokumentationen i 10 år. Dokumentationen är dock inte enhetligt upprättad och i vissa fall väldigt översiktlig det där enbart framgår antalet anställda som kontrollerats och datum för kontrollen. På granskade enheter har ingen uppföljning av verksamhetens loggranskning utförts. Enligt befintliga anvisningar, *Anvisningar för loggkontroll*, ska uppföljning av verksamhetens loggranskning utföras av Staben för verksamhetsutveckling.

2.7. Patienters åtkomst till patientuppgifter

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för enskildas direktåtkomst till sina patientuppgifter i SYSteam Cross och till loggar avseende åtkomst till sina patientuppgifter?

Identifierade starka sidor

- Samtliga enheter har rutiner för hur patienter får åtkomst till information i sina journaler och samtliga enheter uppfyller patientdatalagens krav på att vårdgivaren på begäran från patienten ska informera om den åtkomst till patientens uppgifter som förekommit.
- Samtliga enheter försöker i möjligaste mån få patienten att ta ett möte med ansvarig läkare för att muntligen förklara vad som är angivet i patientjournalen om patienten begärt ut denna information.

Identifierade svaga sidor

- Det finns inga rutiner som beskriver hur utdrag ur patientjournalen ska delges patienten, vilket medför att enheterna har olika rutiner för att lämna ut patientuppgifter.

VLL saknar lösning där patienter kan få direktåtkomst till sina patientuppgifter, istället får patienter tillgång till patientuppgifter genom att patienten begär ut informationen från berörd enhet. 2/5 enheter kräver en skriftlig begäran, medan de övriga enheterna anser att det räcker med en muntlig begäran. Av fem granskade enheter går begäran om utdrag från patientregistret för tre enheter alltid via verksamhetschefen eller ansvarig läkare för godkännande. Övriga enheter kanaliserar begäran om tillgång till patientuppgifter till enhetens LISA som själv gör en bedömning om läkaren eller verksamhetschefen behöver konsulteras. Alla enheter beskriver att någon anställd gör en bedömning för att se om det finns skadlig eller svårtolkad information i patientjournalen innan informationen skickas till patienten. Om så är fallet försöker de se till att informationen lämnas över i samband med en muntlig avstämning, där en läkare har möjlighet att förklara informationen som är angiven i patientjournalen.

När en patient begär ut information över vilka användare som har varit inne i patientens journal måste en bestämd tidsperiod specificeras. Utformningen av den information som skickas till patienterna kan se olika ut mellan enheterna, men generellt redovisas namnet på användaren, dess befattning samt tidpunkten då användaren hade åtkomst till patientens journal.

2.8. Skydd av överföring av patientuppgifter i öppna nät

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för att säkerställa att patientuppgifter som överförs från SYSteam Cross i öppna nät skyddas?

Identifierade starka sidor

- Alla överföringar till/från SYSteam Cross till/från mottagare/avsändare utanför nätverket är krypterade med SSL-kryptering.
- Alla interna överföringar till/från SYSteam Cross är krypterade med SSL-kryptering, utom en överföring.

I granskningen från 2011 påpekades att VLL inte krypterar all data som skickades över öppna nät. VLL även ser sitt interna nätverk som ett öppet nätverk eftersom landstinget har fler än 13 000 individuella användare.

All information som skickas till/från SYSteam Cross till/från mottagare/avsändare utanför landstingets interna nätverk var redan 2011 krypterad, men sedan slutet av 2011 har VLL sett över samtliga interna överföringar till/från SYSteam Cross och i samtliga fall, utom ett, säkerställt att överföringarna är krypterade via SSL-kryptering.

Den förbindelse som inte är krypterad är den interna överföringen av informationen om läkemedel och patientuppgifter som överförs från SYSteam Cross till Pascal, som är ett system som verksamheten använder för ordination av dospaketerade läkemedel. Den externa förbindelsen mellan VLL och Apotekens Service AB är krypterad med SSL-kryptering.

2.9. Säkerhetskopiering

Underliggande revisionsfråga:

- Finns och tillämpas rutiner för säkerhetskopiering av patientuppgifter i SYSteam Cross?

Identifierade starka sidor

- SYSteam Cross finns i två i realtid speglade datahallar.
- Säkerhetskopiering genomförs kontinuerligt och rutin för genomförande av återläsningstester har införts.

SYSteam Cross finns i två i realtid speglade datahallar. I samband med normal drift körs SYSteam Cross i de båda datahallarna men kan vid problem köras från enbart en av datahallarna. Datahallarna är belägna ungefär 500 meter från varandra, i olika byggnader och olika brandzoner. Säkerhetskopiering av systemets databas genomförs en gång per dygn. Säkerhetskopian sparas till disk i den ena datahallen och till band i den andra datahallen. Säkerhetskopian förs månatligen till plats utanför VLL för lagring. Transaktionsloggar sparas var 30:e minut på disk som inte ingår i landstingets centrala SAN. Driften på Informatikenheten är ansvarig för att övervaka att säkerhetskopiering utförs som planerat.

I granskningen från 2011 påpekades att landstinget inte genomför återläsningstester för att verifiera att landstinget kan återläsa data från säkerhetskopior. Säkerhetskopian av systemets databas återläses fortsatt en gång per vecka, medan återläsning av hela systemet numera genomförs en gång per år.

2.10. Signering

Underliggande revisionsfråga:

- Finns rutiner för signering och låsning av journalanteckningar för att säkerställa spårbarheten i genomförda förändringar?

Identifierade starka sidor

- Sedan signering infördes som ett kvalitetsmått som påverkar budgeten så har samtliga enheter upplevt förbättringar i rutinerna för att signera och låsa journalanteckningar.
- Samtliga enheter arbetar löpande med uppföljning och förbättring av signeringsrutinen.

Signering har historiskt sett varit ett problem på flera enheter då gamla journalanteckningar legat osignerade i vissa fall i flera månader. Samtliga enheter har upplevt en stor förändring i signeringsrutiner efter att signering infördes som ett kvalitetsmått som påverkar enheternas budget. Enheterna har en minskande trend och förutom den centrala mätningen genomför majoriteten av enheternas LISA egna mätningar och följer upp osignerade journalanteckningar.

3. Slutsatser

3.1. Svar på övergripande revisionsfrågan

Vår bedömning är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte i tillräcklig utsträckning har säkerställt rutiner och kontroller som innebär att patientuppgifter behandlas på ett korrekt sätt i förhållande till socialstyrelsens föreskrifter och patientdatalagen. VLL har en organisation och struktur på plats för att i all väsentlighet kunna säkerställa att patientuppgifter behandlas på korrekt sätt, men utformade rutiner och kontroller avseende exempelvis loggkontroller är inte fullt ut implementerade i verksamheten. I vår granskning har vi identifierat förbättringsområden för i första hand styrning av informationssäkerhetsarbetet samt rutiner och kontroller avseende den inre sekretessen i SYSteam Cross såsom behörighetsstyrning och loggkontroller.

3.2. Iakttagelser och rekommendationer

Ernst & Young har identifierat ett antal förbättringsområden i samband med granskningen. Samtliga rekommendationer har klassificerats i tre kategorier utifrån följande skala:

Prioritet 1 – Rekommendationen bör hanteras snarast.

Prioritet 2 – Rekommendationen bör hanteras inom en snar framtid.

Prioritet 3 – Rekommendation som bör hanteras på sikt.

Landstingsstyrelsen och hälso- sjukvårdsnämnden bör säkerställa att rekommendationerna åtgärdas för att säkerställa att patientuppgifter hanteras på ett korrekt sätt i förhållande till socialstyrelsens föreskrifter och patientdatalagen.

3.1.1 Informationssäkerhet

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: Informationssäkerhetsansvarig saknar arbetsbeskrivning och tid för att arbeta med informationssäkerhet. **Rekommendation:** Vi rekommenderar VLL att ta fram en arbetsbeskrivning för vilket ansvar som åligger rollen informationssäkerhetsansvarig. Säkerställ att informationssäkerhetsansvarig har tillräckligt med arbetstid avsatt för att utföra arbete relaterat till sin roll och säkerställ att verksamheten informeras om vem som är informationssäkerhetsansvarig och dennes arbetsuppgifter och ansvar.	1

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: Det sker ingen årlig rapportering av vilka granskningar och skyddsåtgärder av större betydelse som har gjorts, vilka riskanalyser som har utförts avseende informationssäkerheten och vilka förbättringsåtgärder som har vidtagits, varken till informationssäkerhetsansvarig eller till landstingsstyrelsen och hälso- och sjukvårdsnämnden. **Rekommendation:** Landstingsstyrelsen och hälso- och sjukvårdsnämnden är ytterst ansvarig för informationssäkerheten inom sina verksamhetsområden. Vi rekommenderar att rutiner införs för att kontinuerligt rapportera informationssäkerhetsarbetet till landstingsstyrelsen och hälso- och sjukvårdsnämnden. Vidare behöver tydliga rutiner skapas för vilken information verksamheten ska rapportera till informationssäkerhetsansvarig.	1
Iakttagelse: Riktlinjerna för informationssäkerhet är övergripande och anvisningar för hur arbetet ska omsättas i praktiken saknas. **Rekommendation:** Komplettera riktlinjerna för informationssäkerhet med anvisningar som tydliggör på vilket sätt verksamheten ska arbeta med informationssäkerhet i vardagen.	2

3.1.2 Behörigheter i SYSteam Cross

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: Periodisk granskning av behörigheter i SYSteam Cross utförs inte på samtliga enheter och hanteringen kring avslut av behörigheter skiljer sig mellan enheterna, vilket ökar risken för att användare som bytt befattning eller avslutat sin anställning fortfarande har åtkomst till patientuppgifter. Enligt *Anvisningar från SYSteam Cross Systemägare*, ska användares behörigheter granskas 2-3 gånger per år och rapporteras till verksamhetschef. **Rekommendation:** En utgångspunkt för den inre sekretessen, integritetsskyddet, är att en användare endast ska få ta del av patientuppgifter som behövs för att han eller hon ska kunna fullgöra sina arbetsuppgifter. Vårdgivaren ska fortlöpande följa upp och korrigera behörigheter utifrån eventuella förändringar i användarens arbetsuppgifter. För att säkerställa den inre sekretessen rekommenderar vi VLL att per enhet säkerställa att det finns rutiner för hur avslut av behörigheter ska hanteras, och implementera rutiner för periodisk granskning av behörigheter i SYSteam Cross. Den periodiska granskningen bör genomföras och rapporteras i enlighet med upprättad anvisning.	1

3.1.3 Spärr av patientuppgifter

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: En användare kan inte se vad spärren av patientuppgifter avser innan användaren har gått förbi varningen om att det finns spärrade patientuppgifter. Specifikation av vad spärren avser kan endast göras med hjälp av fritext på patientöversikten. **Rekommendation:** Spärrar innebär att åtkomsten till patientuppgifter i journalsystemet har begränsats. Vi rekommenderar VLL att skapa effektivare spärrar i SYSteam Cross, för att säkerställa att den begränsade åtkomsten till patientuppgifter säkerställs.	2

3.1.4 Sammanhållen journalföring

Inga väsentliga brister identifierade.

3.1.5 Loggkontroller

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: Enheterna har olika rutiner för loggkontroller. Exempelvis använder några enheter inte slumpgeneratorn vid loggkontroller, vilket medför att anställda från andra enheter, som varit inne i patientjournaler för den aktuella enheten, inte inkluderas i loggkontrollen. Majoriteten av enheterna kontrollerar inte tillräckligt många användare för att säkerställa att varje användare blir kontrollerad i snitt en gång per år. VLL har anvisningar för loggkontroller som inte samtliga enheter har kännedom om. **Rekommendation:** Vårdgivaren ska systematiskt och återkommande kontrollera åtkomsten till patientuppgifterna. Befintliga anvisningar för loggkontroller bör kommuniceras till samtliga enheter för att säkerställa att enheterna hanterar loggkontroller och dokumentering av utförda loggkontroller på samma sätt. Vi rekommenderar enheterna att särskilt gå igenom befintliga anvisningar för att säkerställa att loggkontroller genomförs i enlighet med anvisningarna.	1
Iakttagelse: På granskade enheter har ingen uppföljning av verksamhetens loggranskning utförts. Enligt befintliga anvisningar, *Anvisningar för loggkontroll*, ska uppföljning av verksamhetens loggranskning utföras av Staben för verksamhetsutveckling. Avsaknad av kontinuerlig uppföljning av att loggkontroller utförs enligt befintliga anvisningar ökar risken för att loggkontroller utförs på ett felaktigt sätt, vilket i sin tur kan medföra att felaktigheter eller avvikelser inte upptäcks. **Rekommendation:** Vi rekommenderar VLL att genomföra kontinuerliga uppföljningar av att loggkontroller genomförts. En rutin om återrapportering av loggkontroller bör upprättas för att säkerställa att uppföljning av loggkontroller genomförs.	1

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: Vid loggkontroller framgår det inte tydligt vilka åtgärder som vidtagits med patientuppgifterna, varför det är svårt för utförarna av loggkontroller att göra en bedömning huruvida åtkomsten är befogad. **Rekommendation:** VLL bör säkerställa att det tydligare framgår vilka åtgärder som vidtagits med patientuppgifterna, till exempel om användare har läst, ändrat, kopierat, upprättat eller skrivit ut vårddokumentation.	2
Iakttagelse: Det finns ingen möjlighet för utförarna av loggkontrollerna att se vilka patientuppgifter som är spärrade i SYSteam Cross, vilket omöjliggör särskild uppföljning av vilka användare som haft åtkomst till dessa patientuppgifter. **Rekommendation:** Om det finns möjlighet rekommenderar vi att utförarna av loggkontrollerna informeras om vilka patientuppgifter som är spärrade för att särskilt kunna följa upp att ingen obehörig haft åtkomst till dessa patientuppgifter.	3

3.1.6 Patienters åtkomst till patientuppgifter

Iakttagelser/rekommendationer	Prioritet
Iakttagelse: Samtliga enheter uppfyller patientdatalagens krav på att vårdgivaren på begäran från patienten ska informera om den åtkomst till patientens uppgifter som förekommit. Det finns dock ingen rutin som beskriver hur utdrag ur patientjournaler ska delges patienter, vilket medför att enheterna har olika rutiner för att lämna ut patientuppgifter. **Rekommendation:** Vi rekommenderar att rutiner skapas för hur verksamheten ska hantera begäran från patienter om tillgång till patientuppgifter.	3

3.1.7 Skydd av överföring av patientuppgifter i öppna nät

Inga väsentliga brister identifierade.

3.1.8 Säkerhetskopiering

Inga väsentliga brister identifierade.

3.1.9 Signering

Inga väsentliga brister identifierade.

Göteborg 2013-02-19

Tobias Hermansson
Ernst & Young

Bilaga 1. Respondenter

Befattning	Enhet
Verksamhetschef och LISA	Cancercentrum
Verksamhetschef, biträdande verksamhetschef och LISA	Barn och Ungdomsmedicin
Verksamhetschef och LISA	Hjärtcentrum
Biträdande verksamhetschef och LISA	Psykiatrin
Verksamhetschef	Reumatologi
Enhetschef samt Driftsansvarig	Informatikenheten
Informationssäkerhetsansvarig	Staben för planering och styrning
Systemägare SYSteam Cross	Staben för verksamhetsutveckling