Landstingsstyrelsen
Hälso- och sjukvårdsnämnden
Nämnden för funktionshinder och habilitering

Uppföljande granskning av sekretess i leverantörs och faktureringsrutinen

Revisorerna har i granskningar åren 2012-2014 uppmärksammat brister när det gäller sekretessmarkering av personuppgifter i landstingets system för leverantörsfakturor och kundfakturering. Denna uppföljande granskning visar att styrelsen och nämnderna inte har vidtagit tillräckliga åtgärder med anledning av iakttagelser och rekommendationer i tidigare granskningar.

Det har visserligen blivit bättre när det gäller sekretessmarkering av fakturor för köpt vård. Ett uppföljande stickprov visar att 5 procent saknar sekretessmarkering jämfört med 11 procent år 2014. Vid kontroll av konton för laboratorieprov och hjälpmedel är dock siffran betydligt högre, 70 respektive 93 procent av fakturorna saknar sekretessmarkering.

Enligt patientdatalagen får bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården ta del av patientuppgifter. Det är verksamhetschefen som ansvarar för att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med befattningshavarens aktuella uppgifter. För att sekretessmarkera en faktura i landstingets fakturasystem eller för att titta på en sådan faktura måste användaren ha en speciell behörighet som kallas sekretess. För att få sekretessbehörighet räcker det att användaren själv meddelar enheten för leverantörsfakturor. Ansökan behöver inte gå via verksamhetschefen.

Rekommendationer

Utifrån resultatet av granskningen rekommenderar vi landstingsstyrelsen, hälso- och sjukvårdsnämnden samt nämnden för funktionshinder och habilitering att säkerställa att:

- Det skyndsamt utförs kontroller i systemet för att se till att fakturor med integritetskänslig information blir sekretessmarkerade.
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen.
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i kundfaktureringsprocessen.

Västerbottens läns landsting
Landstingshuset, Köksvägen 11, 901 89 Umeå
Telefon: 090-785 00 00, telefax: 090-13 68 82
E-post: landstinget@vll.se Org.nr: 232100-0222
VAT-nr: SE232100022201 Bankgiro 5728-3061

- Det utförs löpande kontroller i systemet att fakturor med integritetskänslig information blir sekretessmarkerade.
- Personal som hanterar fakturor med integritetskänslig information har tillräcklig utbildning om lagstiftningen kring inre sekretess. Utbildningen bör ha en tydlig koppling till leverantörsfakturor.
- Det löpande utförs kontroller att sekretessbehörigheter i Agresso är aktuella.
- Ansökan om sekretessbehörighet i Agresso går via verksamhetschef.

Vid revisorernas överläggning den 28 januari 2016 beslöt revisorerna enhälligt att ställa sig bakom slutsatser och rekommendationer i detta missiv. Missiv och underliggande rapport (nr 13/2015) lämnar revisorerna för yttrande till landstingsstyrelsen, hälso- och sjukvårdsnämnden och nämnden för funktionshinder och habilitering. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 8 april 2016.

För landstingets revisorer

Christer Fessé
Ordförande

Bert Öhlund
Vice Ordförande

LANDSTINGSREVISIONEN

Uppföljande granskning av sekretess i leverantörs- och faktureringsrutinen

Rapport nr 13/2015

VÄSTERBOTTENS LÄNS LANDSTING

Januari 2016
Ingrid Lindberg, revisor, revisionskontoret
Diarienummer: REV 57:3-2015

Innehåll

1. Sammanfattande analys

Reglerna om tystnadsplikt och sekretess i hälso- och sjukvård finns för att skydda patientens personliga integritet. Patientdatalagen (2008:355) reglerar den inre sekretessen. Det innebär att inom en myndighet får en användare bara ta del av patientuppgifter om det krävs för att fullgöra sina arbetsuppgifter. Genom tilldelning av olika behörigheter begränsas åtkomsten till vad en användare behöver för att kunna slutföra sina arbetsuppgifter. En faktura som innehåller patientuppgifter omfattas av reglerna kring den inre sekretessen. Endast användare med sekretessbehörighet ska kunna se denna typ av fakturor.

Revisorerna har vid upprepade tillfällen uppmärksammat brister när det gäller hanteringen av sekretessuppgifter i landstingets system för leverantörsfakturor och kundfakturering.

Denna uppföljande granskning visar att problemet med att känslig information inte är spärrad kvarstår. Ett stickprov visar att det blivit bättre när det gäller sekretessmarkering av vårdfakturor. Fem procent saknar sekretessmarkering jämfört med 11 procent i föregående granskning. Det kan dock inte anses acceptabelt att integritetskänsliga fakturor saknar sekretessmarkering. Vi har i denna granskning också granskat fakturor för laboratorieprover och hjälpmedelskostnader. Laboratoriefakturorna saknar sekretessmarkering i 70 procent av fallen och fakturor för hjälpmedelskostnader saknar sekretessmarkering i 93 procent av fallen. Detta tyder på en låg kunskapsnivå av reglerna kring inre sekretess ute i verksamheterna.

Det är den som mottagningsattesterar en faktura som har till uppgift att sekretessmarkera den i Agresso. Användaren behöver ha en speciell behörighet för att sekretessmarkera en faktura i systemet eller för att kunna titta på eller godkänna en sekretessmarkerad faktura. För att få sekretessbehörighet räcker det med att användaren meddelar enheten på ekonomistaben för leverantörsfakturor. Enligt chefen för ekonomistaben leverantörsfakturor behöver inte begäran gå via verksamhetschef eller via en formell ansökningsprocess. I både Socialstyrelsens föreskrifter och landstingets riktlinjer för informationssäkerhet fastställs att det är verksamhetschefens ansvar att utdelade behörigheter är ändamålsenliga och motsvarar aktuella arbetsuppgifter.

När det gäller inre sekretess och kundfakturor är problemet att samlingsfakturor på genomförda insatser skickas till patientens hemlandsting. Därefter sprids samlingsfakturan till de enheter som har betalningsansvar. Följden av detta är att alla befattningshavare i kedjan kan läsa sekretessmarkerade uppgifter, även för de patienter som de inte har ansvar för. Med anledning av detta har landstinget gjort en översyn tillsammans med övriga landsting i norra regionen. Detta ledde till en överenskommelse att landstinget ska skicka alla akutfakturor på en separat faktura eftersom det hos våra regiongrannar är samma person som hanterar alla fakturor för akutsjukvård. Detta är en förbättring jämfört med tidigare, men berör endast en mindre del av alla fakturor som skickas. I övrigt avvaktar landstinget ett arbete som SKL driver för att få till stånd en lagändring samt införandet av e-faktura som planeras under år 2016.

Mot bakgrund av redovisade iakttagelser ovan bedömer vi att landstingsstyrelsen, hälso- och sjukvårdsnämnden och nämnden för funktionshinder och habilitering inte har en tillräcklig kontroll (KL 6 kap 7§) över hur verksamheterna hanterar känsliga patientuppgifter (PDL 4 kap 1-3 §§, SOSFS 2008:14 2 kap 19§). Styrelsen och nämnderna har inte vidtagit tillräckliga åtgärder med anledning av iakttagelser och rekommendationer i tidigare granskningar.

1.1. Rekommendationer

Vi rekommenderar styrelsen och nämnderna att säkerställa att:

- Det skyndsamt utförs kontroller i systemet för att se till att fakturor med integritetskänslig information blir sekretessmarkerade.
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen.
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i kundfaktureringsprocessen.
- Det utförs löpande kontroller i systemet att fakturor med integritetskänslig information blir sekretessmarkerade.
- Personal som hanterar fakturor med integritetskänslig information har tillräcklig utbildning om lagstiftningen kring inre sekretess. Utbildningen bör ha en tydlig koppling till leverantörsfakturor.
- Det löpande utförs kontroller att sekretessbehörigheter i Agresso är aktuella.
- Ansökan om sekretessbehörighet i Agresso går via verksamhetschef.

2. Bakgrund

Revisorerna har i upprepade granskningar mellan år 2012-2014 uppmärksammat brister när det gäller sekretessuppgifter i landstingets system för leverantörsfakturor och kundfakturering. Det har också framkommit kritik från andra landsting över att de samlingsfakturor som skickas från Västerbottens läns landsting innebär sekretessrisker (revisionsrapport Regionvård, intern kontroll NLL, november 2013).

Ett stickprov i en promemoria (Rev 3:1 2014) visade att 11 procent av de granskade fakturorna avseende köpt vård innehöll ospärrade sekretessuppgifter. Rekommendationer i granskningen var att landstingsstyrelsen och hälso- och sjukvårdsnämnden skulle säkerställa att:

- Det skyndsamt skulle genomföras kontroller i systemen för att se till att sekretessuppgifter endast var tillgängliga för behörig personal.
- Det upprättades specifika regler kring sekretess för landstingets alla system för debitering och leverantörsbetalning.
- Det utfördes systematiska kontroller i systemen för att försäkra sig om att endast behörig personal hade tillgång till sekretessuppgifter.

I yttranden till revisorerna hösten 2014 uppgav landstingsstyrelsen och hälso- och sjukvårdsnämnden att ett arbete hade påbörjats för att stärka landstingets hantering av sekretessmarkerade uppgifter.

En felaktig hantering av integritetskänsliga uppgifter kan orsaka patienter skada och förtroendeskada för landstinget samt ekonomiska skada. Utifrån tidigare iakttagelser har revisorerna beslutat att genomföra en uppföljande granskning.

2.1. Revisionsfrågor

Har landstingsstyrelsen, hälso- och sjukvårdsnämnden samt nämnden för funktionshinder och habilitering vidtagit tillräckliga åtgärder med anledning av revisorernas iakttagelser i 2014 års granskning?

Den övergripande revisionsfrågan ska vi besvara med hjälp av följande underliggande revisionsfrågor:

Har styrelsen och nämnderna säkerställt att:

- Det utfördes kontroller i systemen efter föregående granskning för att se till att sekretessuppgifter endast var tillgängliga för behörig personal?
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen?

- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i kundfaktureringsprocessen?
- Verksamheterna följer riktlinjerna för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen?
- Verksamheterna följer riktlinjerna för hanteringen av sekretessuppgifter i kundfaktureringsprocessen?
- Det utförs löpande kontroller för att säkerställa att enbart behörig personal har tillgång till sekretessuppgifter?

2.2. Avgränsning

Granskningen omfattar landstingsstyrelsens, hälso- och sjukvårdsnämndens samt nämnden för funktionshinder och habiliterings områden. Vi har granskat fakturor avseende perioden januari – oktober 2015. Granskningen är avgränsad till Agresso EFH när det gäller leverantörsfakturaprocessen. Eftersom all kundfakturering i landstinget utförs via ekonomisystemet Agresso ligger fokus på ekonomisystemet och gränssnittet mot landstingets system för fakturering.

3. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

- Kommunallagen (6 kap. 7 § om nämndernas ansvar för intern kontroll)
- Landstingets riktlinjer för informationssäkerhet
- Patientdatalagen (2008:355) (4 kap. 1-3 §§ om inre sekretess)
- SOSFS 2008:14 (2 kap 19§ om verksamhetschefens ansvar)

3.1. Metod

För att kontrollera hur processerna för hanteringen av sekretessmarkerade uppgifter fungerar har vi genomfört intervjuer med processansvarig för regionavtal och vårdfakturering samt enhetschef för ekonomistaben leverantörsfakturor. Vi har också gjort ett stickprov för att undersöka förekomsten av fakturor med integritetskänslig information som inte är sekretessmarkerad. Stickprovet har omfattat konton för köpt utomlänsvård (konto 5011-5026). Vi har kontrollerat samtliga fakturor som bokförts under september månad vilket motsvarar ca 10 procent av alla fakturor under perioden januari-oktober. Vi har också gjort ett stickprov av konton där det finns risk att personuppgifter kan förekomma, exempelvis konton för hjälpmedel (konto 5740-5748) och laboratorieprover (konto 5521). I detta fall har vi kontrollerat samtliga fakturor under oktober månad. I stickprovet ingår enbart fakturor som innehåller integritetskänslig information. Vi har dessutom gjort dokumentstudier av de regler som är aktuella.

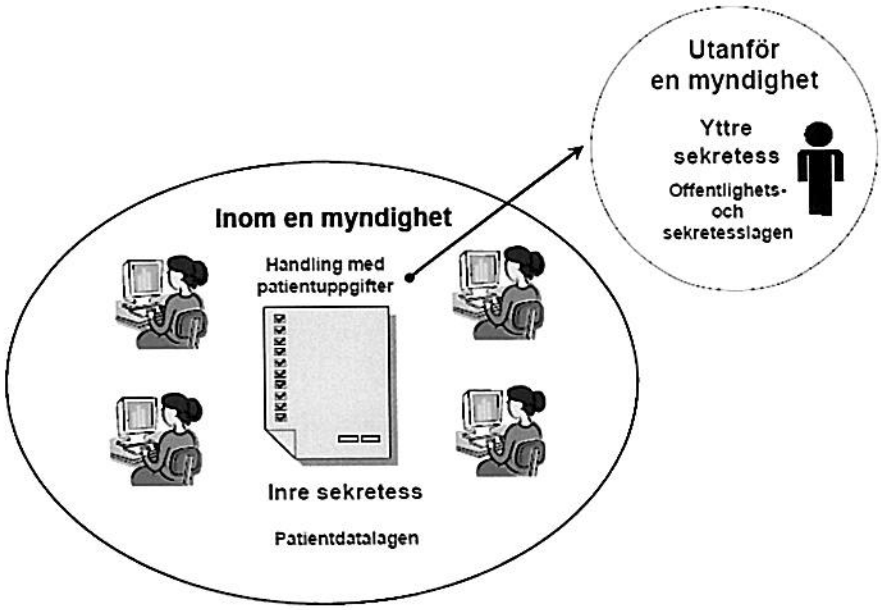
4. Resultat av granskningen

4.1. Rutiner och regelverk

Reglerna om tystnadsplikt och sekretess i hälso- och sjukvård finns för att skydda patientens personliga integritet. Att inte lämna ut uppgifter om patienter till utomstående är en viktig förutsättning för förtroendet för vården.

Regelverket om sekretess i vården är omfattande och det kan vara svårt att få en överblick över vad som gäller.

Lagstiftningen skiljer på den inre och den yttre sekretessen. Den inre sekretessen handlar om informationshantering inom en myndighets eller vårdgivares verksamhet och regleras av patientdatalagen (2008:355). Den yttre sekretessen gäller mellan olika myndigheter eller vårdgivare. Den regleras av offentlighets- och sekretesslagen (2009:400).



4.1.1. Offentlighets- och sekretesslagen (2009:400)

Offentlighets- och sekretesslagen behandlar den yttre sekretessen och innehåller bestämmelser om myndigheters handläggning vid registrering, utlämnande och övrig hantering av allmänna handlingar. Sekretessregleringen innebär att det finns en sekretessgräns runt en myndighet. Sekretessgränsen gäller i förhållande till alla som är utanför.

Sekretess innebär enligt offentlighets och sekretesslagen ett förbud att röja en uppgift som rör patientens personliga förhållanden, t.ex. sjukdom eller behandling, vare sig det sker muntligen, skriftligen eller på annat sätt.

4.1.2. Patientdatalagen (2008:355)

Patientdatalagen innehåller en samlad reglering av informationshanteringen inom hälso- och sjukvården. Syftet med lagen är att respektera patienters

integritet genom att hantera och förvara personuppgifter på ett sådant sätt att obehöriga inte får tillgång till dem.

Inom en myndighet eller verksamhet gäller inre sekretess vilket innebär att bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården får ta del av patientuppgifter.

Den inre sekretessen gäller för alla dokumenterade personuppgifter om patienter det vill säga att även administrativ dokumentation innefattas. Den inre sekretessen tydliggörs genom regler om behörighetsstyrning och kontroll av elektronisk åtkomst. Vårdgivaren ska se till att behörigheten för åtkomst till patientuppgifter begränsas till vad en användare behöver för att kunna utföra sina arbetsuppgifter inom hälso- och sjukvården. Vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter. En sådan kontroll främjar integritetsskyddet och gör det möjligt att förebygga, konstatera och beivra otillåten eller obefogad åtkomst till uppgifter. Kraven på säkerhetsåtgärder förtydligas i Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården.

Datainspektionen har tillsyn över att vårdgivarna hanterar personuppgifter med ett gott integritetsskydd för patienterna.

4.1.3. SOSFS 2008:14

Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården innehåller bland annat regler om styrning av behörigheter, åtkomst till patientuppgifter och kontroll av åtkomst.

Vårdgivaren har ansvar för att det finns en dokumenterad informationssäkerhetspolicy. Informationssäkerhetspolicyn ska bland annat säkerställa att obehöriga inte ska kunna ta del av patientuppgifterna. Verksamhetschefen har ansvar att hälso- och sjukvårdspersonalen och andra befattningshavare är informerade om de bestämmelser som gäller för hantering av patientuppgifter. Verksamhetschefen ansvarar för att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med hälso- och sjukvårdspersonalens och andra befattningshavares aktuella uppgifter.

Hälso- och sjukvårdspersonal och andra befattningshavare ska ansvara för personliga lösenord, för att datorer inte lämnas utan att patientuppgifter är skyddade från åtkomst samt endast ta del av patientuppgifter om han eller hon deltar i vården av patienten.

4.1.4. Personuppgiftslagen (1998:204)

Lagens syfte är att skydda den personliga integriteten och främja utvecklingen och iakttagandet av god informationshantering. Som känsliga personuppgifter enligt personuppgiftslagen betecknas exempelvis uppgifter som avslöjar personuppgifter som rör hälsa.

4.1.5. Landstingets regelverk

På landstingets intranät Linda finns en hänvisning till sekretesslagen (1980:100). Denna lag upphävdes genom offentlighets- och sekretesslagens tillkomst SFS (2009:400). På intranätet beskrivs mycket kortfattat vad sekretessreglerna innebär. Det nämns bland annat att hantering av personuppgifter ska följa patientdatalagen. Enligt en av landstingets jurister pågår ett arbete med att göra en sammanställning av de lagar och regler som rör sekretess. Resultatet av detta arbete kommer att läggas ut som en information på landstingets intranät när det är klart.

I november 2015 beslutade landstingsstyrelsen om nya riktlinjer för informationssäkerhet. Dessa riktlinjer ersätter de gamla riktlinjerna från år 2012. Riktlinjerna innefattar bland annat inre sekretess och behörighetsadministration och är ett utvecklande av de gamla riktlinjerna. Enligt riktlinjerna innebär den inre sekretessen att den berörde bara får ta del av den information som denne behöver för att kunna utföra sina arbetsuppgifter. Informationen får inte spridas utanför arbetsplatsen. Detta gäller även efter avslutad anställning.

Vad gäller behörighetsadministration säger riktlinjerna att respektive verksamhetschef ansvarar för att dess personal har rätt behörighet. Verksamhetschefen har ett ansvar att begränsa behörigheter i journalsystem och i andra system med känsliga personuppgifter till vad som behövs för att fullgöra sina arbetsuppgifter. Behörigheten ska vara tillräcklig men samtidigt inte mer omfattande än vad som är nödvändigt. Detta gäller även externa personer som tilldelas behörigheter till IT-system. Om en användare får nya arbetsuppgifter ska behörigheten följas upp och förändras så att den stämmer överens med de nya arbetsuppgifterna.

Behörighet skall enligt riktlinjerna tilldelas efter en analys av vilken information olika personalkategorier i olika verksamheter behöver. Riskanalysen ska ta hänsyn till vilka risker det kan innebära om personalen har för lite eller för mycket tillgång till olika patientuppgifter. Vissa patientuppgifter kan kräva särskilda riskbedömningar, till exempel personuppgifter som är sekretessmarkerade, uppgifter om allmänt kända personer samt uppgifter från vissa mottagningar eller vissa medicinska specialiteter. Då behoven varierar mellan olika typer av verksamheter ansvarar verksamhetschefen för att en behovs- och riskanalys genomförs på enhetsnivå. Dokumentation av genomförd behovs- och riskanalys arkiveras på enheten.

4.2. Granskningens resultat

4.2.1. Sekretess i leverantörsfakturarutinen

Alla fakturor som hanteras via landstingets inskanningscentral skannas in i ekonomisystemet Agresso som en öppen faktura. Alla som har användarbehörighet till Agresso har tillgång till öppna fakturor. Det är sedan upp till den som ska mottagningsattestera en faktura att bedöma om fakturan ska sekretessmarkeras eller inte. Att en faktura är sekretessmarkerad i Agresso innebär att endast de som har rättighet i systemet att se sekretessmarkerade

fakturor har tillgång. Övriga användare kan inte öppna fakturan utan får upp en bild som det står sekretess på istället.

En faktura sekretessmarkeras i systemet genom att byta dokumenttyp till sekretessbelagda leverantörsfakturor. För att kunna göra detta måste användaren ha en speciell behörighet i Agresso som kallas sekretess. Sekretessbehörigheten behövs också för att kunna se en sekretessmarkerad faktura. Även den som ska beslutsattestera fakturan behöver alltså sekretessbehörighet. För att få sekretessbehörighet i Agresso räcker det att användaren meddelar ekonomistaben leverantörsfakturor. Enligt chefen för ekonomistaben leverantörsfakturor finns i dagsläget ingen rutin att begäran måste gå via verksamhetschef eller via någon formell ansökningsprocess.

Vårdfakturor från andra landsting går direkt till medarbetare på ekonomistaben leverantörsfakturor. De mottagningsattesterar, sekretessmarkerar och bokför fakturorna. Fakturan skickas sedan vidare till respektive beslutsattestant. Eftersom fakturorna oftast är samlingsfakturor som gäller ett flertal verksamheter innebär det att vårdpersonal kommer att kunna se uppgifter om andra patienter än de som de själva har ansvar för. Enligt chefen för ekonomistaben leverantörsfakturor är det upp till avsändande landsting att ändra sina rutiner. Det går inte att skicka en del av en faktura vidare i systemet eller att maskera vissa uppgifter.

För laboratorieprover från andra landsting och fakturor för hjälpmedel är rutinen en annan. Dessa fakturor går direkt till respektive beställande verksamhet som attesterar och bedömer om fakturan ska sekretessmarkeras.

I samband med utbildningar i ekonomisystemet Agresso berör ekonomistaben leverantörsfakturor frågan om sekretess. De lär ut hur man sekretesmarkerar en faktura i systemet och talar om att när det finns personnummer på en vårdfaktura så ska den sekretessmarkeras. Ekonomistaben leverantörsfakturor har också lagt ut en information på landstingets intranät under sektionen för Agresso EFH. Där uppmanas användarna att inte skriva namn eller personnummer i kommentarsfältet eftersom det inte går att sekretesmarkera kommentarsfältet. Enligt chefen för ekonomistaben leverantörsfakturor finns ingen skriftlig handledning för vilken typ av information som kan behöva sekretessmarkeras. De förutsätter att verksamheterna utbildar sin egen personal i sekretessfrågor.

4.2.2. Vår kommentar

Enligt lagstiftning och landstingets regler är det verksamhetschefens ansvar för att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med hälso- och sjukvårdspersonalens och andra befattningshavares aktuella uppgifter. Därför är det rimligt att förfrågningar om behörighet till rollen sekretess i Agresso går via verksamhetschef.

4.2.3. Sekretess i kundfakturarutinen

När landstinget ska fakturera vård gällande patienter utanför länet går informationen via faktureringssystemet Epok till ekonomisystemet Agresso. Samlingsfakturor skickas en gång i månaden från Agresso till det remitte-

rande sjukhuset. Detta innebär att fakturauppgifter som rör flera olika kliniker kan hamna på samma faktura. När det gäller akutvård så skickar landstinget en separat faktura på detta. Detta är resultatet av ett arbete som utfördes år 2014 tillsammans med landstingen i norra regionen där man såg över faktureringsprocessen. I samband med detta gjordes en överenskommelse att VLL ska skicka akutfakturorna separat, eftersom det hos våra regiongrannar är samma person som tar emot alla fakturor avseende akutvård. Detta minskar risken för att obehöriga får tillgång till patientuppgifter när det gäller akutfakturor. Akutfakturorna utgör ca en femtedel av alla vårdfakturor.

Ekonomidirektörerna i landstingen har beslutat att from den 1 juni 2016 ska alla landsting e-fakturera vård. Just nu görs en förstudie över hur en kommunikationsplattform skulle kunna fungera. E-fakturering skulle innebära att det blir en faktura per patient. Enligt processansvarig för regionvård minskar detta risken att en faktura hamnar hos någon som inte har arbetat med patienten. E-fakturor kan dock ha andra juridiska aspekter än inskannade fakturor.

Enligt processansvarig för vårdfakturering har landstinget inga riktlinjer för sekretess vid debitering av utomlänsvård. I riksavtalet för utomlänsvård görs en uppmaning att observera att både fakturerande och betalande landsting har att beakta gällande säkerhetsbestämmelser.

4.2.4. Åtgärder med anledning av föregående granskning

Ett stickprov i föregående granskning (Rev 3:1 2014) visade att 11 procent av de granskade leverantörsfakturorna innehöll ospärrade personuppgifter. Det fanns också sekretessproblem kopplade till hanteringen av samlingsfakturor.

I det efterföljande yttrandet skrev både landstingsstyrelsen och hälso- och sjukvårdsnämnden att de avvaktade resultatet av ett arbete som Sveriges Kommuner och Landsting (SKL) drev. SKL hade gjort bedömningen att det saknades tillräckliga rättsliga förutsättningar för en elektronisk masshantering av vårdinformation enligt patientdatalagen och offentlighets- och sekretesslagen. SKL hade därför skrivit till Socialdepartementet för att få till stånd en lagändring. Någon lagändring eller rekommendation har inte kommit i ärendet ännu och arbetet pågår fortfarande. Enligt processansvarig för vårdfakturering håller juristerna på SKL på med att göra en bedömning av hur e-fakturor kan hanteras ur sekretesshänseende.

Vidare hänvisade landstingsstyrelsen och hälso- och sjukvårdsnämnden i sina yttranden till ett arbete som pågick inom landstinget för att stärka landstingets hantering av sekretessmarkerade uppgifter. Syftet var att säkerställa att offentlighetsprincipen och sekretesslagstiftningen skulle hanteras lagenligt i landstingets faktureringsprocesser. I november 2015 beslutade landstingsstyrelsen om nya informationssäkerhetsriktlinjer som berör sekretess och behörighetsstyrning kopplat till det lagstöd som finns.

Några uppdrag att utföra kontroller i systemet för att se till att sekretessuppgifter endast är tillgänglig för behörig personal lämnades inte i samband

med något av yttrandena. I styrelsens och nämndernas internkontrollplaner finns inga risker upptagna med anknytning till sekretess eller informationssäkerhet.

Enligt chefen för ekonomistaben leverantörsfakturor har inga förfrågningar kommit till dem rörande sekretessbehörigheter. Detta tyder på att inga kontroller av behörigheter har utförts, varken efter granskningen eller löpande. I de nya informationsriktlinjerna finns riktlinjer för att behörighetskontroller bör utföras regelbundet. I styrelsens och nämndernas internkontrollplaner finns inga risker upptagna med anknytning till sekretess eller informationssäkerhet.

Vi har inte kunnat kontrollera om styrelsen och nämnderna säkerställt att de fakturor som vid föregående granskning innehöll patientuppgifter som inte var spärrade blev sekretessmarkerade. Landstinget bytte år 2014 system för hantering av leverantörsfakturor. Det gamla systemet Invoice Manager har stängts ner. De inskannade fakturorna har förts över till databasen Diver, men det går inte längre att se vilka fakturor som varit sekretessmarkerade i Invoice Manager. Samtliga fakturor är sekretessmarkerade i Diver. Det är i dagsläget endast en person på ekonomistaben som kan se fakturorna.

4.2.5. Stickprov

Fakturor som bokförs på konton för köpt utomlänsvård (konto 5011-5026) innehåller i de flesta fall personuppgifter tillsammans med uppgifter om vilken vård som utförts. Detta innebär att de ska sekretessmarkeras för att förhindra att obehörig personal ska kunna se dem. Ett stickprov visar att en förbättring har skett jämfört med föregående granskning. 5 procent av fakturorna i stickprovet är inte sekretessmarkerade. Vid föregående granskning var motsvarande siffra 11 procent. Det kan inte anses acceptabelt att integritetskänsliga fakturor saknar sekretessmarkering.

	2015	2014
Antal med personuppgifter	**905**	**836**
Antal ej sekretessmarkerade	44	96
Andel ej sekretessmarkerade	5%	11%

Andelen integritetskänsliga vårdfakturor som saknar sekretessmarkering

I vårt stickprov har vi också kontrollerat fakturor för laboratorieprover och hjälpmedel av olika slag, exempelvis diabeteshjälpmedel, peruker, kompressionsstöd och proteser.

Typ av faktura	Antal innehållande personuppgifter	Antal ej sekretessmarkerade	Andel ej sekretessmarkerade
Vårdfakturor	905	44	5%
Laboratorieprov	202	142	70%
Hjälpmedel	268	248	93%
TOTALT	**1375**	**434**	**32%**

Resultat av stickprov av fakturor bokförda i september och oktober 2015

När det gäller konton för hjälpmedel varierar det om fakturorna innehåller patientuppgifter eller inte. Det beror exempelvis på om varan har beställts för att användas på kliniken eller om den beställts till en specifik patient. I stickprovet ingår bara de fakturor som innehåller patientinformation. Stickprovet visar att 93 procent av fakturorna saknar sekretessmarkering. För vissa hjälpmedelskostnader exempelvis diabeteshjälpmedel och kompressionshjälpmedel framgår det oftast inte direkt av fakturaspecifikationen vilken patient det avser. Av leveransadressen kan man dock i många fall utläsa namnet på patienten, adressen och i vissa fall även telefonnummer. Dessa fakturor härrör från ett vårdtillfälle i grunden och bör därför klassificeras som sekretessfakturor. Till fakturor avseende exempelvis peruker eller proteser bifogas ofta remissen som en fakturaspecifikation. Av remissen framgår personnummer och vem som remitterat patienten. Även i dessa fall är det vanligt att fakturan saknar sekretessmarkering. Fakturor på laboratorieprover från andra landsting innehåller i de flesta fall uppgift om personnummer och vilka prov som tagits och ska därmed sekretessmarkeras. I stickprovet saknar 70 procent av laboratoriefakturorna sekretessmarkering.

Av samtliga 1375 kontrollerade fakturor saknade 32 procent sekretessmarkering.

4.2.6. Vår kommentar

Resultatet av stickprovet visar att hanteringen av sekretessfakturor skiljer sig åt inom landstinget. När det gäller vårdfakturor som initialt hanteras av ekonomistaben är personuppgifter sekretessmarkerade i betydligt högre grad än när fakturan går direkt till klinikerna. Ute i verksamheten görs olika bedömningar om en faktura ska sekretessmarkeras eller inte. Detta tyder på att kunskapsnivån angående den inre sekretessen generellt sett är låg bland verksamheterna i landstinget och att en utbildningsinsats behövs. Utbildningsinsatsen bör vara specifikt inriktad på inre sekretess och hantering av fakturor med personuppgifter.

5. Svar på revisionsfrågor

Vi bedömer att landstingsstyrelsen, hälso- och sjukvårdsnämnden och nämnden för funktionshinder och habilitering inte har en tillräcklig kontroll över hur verksamheterna hanterar känsliga patientuppgifter. Granskningen visar att styrelsen och nämnderna inte har vidtagit tillräckliga åtgärder med anledning av iakttagelser och rekommendationer i tidigare granskningar.

I tabellen nedan sammanfattar vi svaren på de underliggande revisionsfrågorna i granskningen.

Har styrelsen och nämnderna säkerställt att?	Bedömning	Kommentar
Det utfördes kontroller i systemen efter föregående granskning för att se till att sekretessuppgifter endast var tillgängliga för behörig personal?	Går ej kontrollera	Landstinget har bytt leverantörsfakturasystem. Det gamla systemet har stängts ner. Det går inte längre att se om en faktura var sekretessmarkerad eller inte.
Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen?	Delvis	Det finns riktlinjer för informationssäkerhet som innefattar inre sekretess. Det finns ingen specifik handledning för hantering av sekretess i samband med leverantörsfakturor.
Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i kundfaktureringsprocessen?	Delvis	Det finns riktlinjer för informationssäkerhet som innefattar inre sekretess. Riksavtalet för utomlänsvård specificerar vad en faktura ska innehålla och att både säljande och köpande landsting ska beakta gällande sekretesslagstiftning. Osäkerhet råder dock kring vad som gäller för elektronisk masshantering av vårdinformation.
Verksamheterna följer riktlinjerna för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen?	Nej	Stickprovet visar att en stor andel av fakturor innehållande personuppgifter inte är sekretessmarkerade.
Verksamheterna följer riktlinjerna för hanteringen av sekretessuppgifter i kundfaktureringsprocessen?	Nej	Eftersom det är oklart vad som gäller kring elektronisk masshantering av vårdinformation avvaktar man resultatet av SKLs utredning.

Det utförs löpande kontroller för att säkerställa att enbart behörig personal har tillgång till sekretessuppgifter?	Nej	Stickprovet visar att en stor andel av fakturorna som innehåller integritetskänsliga uppgifter inte är sekretessmarkerade. Det krävs inte något formellt godkännande från verksamhetschef för att få rättigheter att se sekretessmarkerade fakturor.

6. Rekommendationer

Utifrån granskningens resultat ger vi följande rekommendationer till landstingsstyrelsen, hälso- och sjukvårdsnämnden samt nämnden för funktionshinder och habilitering.

Vi rekommenderar styrelsen och nämnderna att säkerställa att:

- Det skyndsamt utförs kontroller i systemet för att se till att fakturor med integritetskänslig information blir sekretessmarkerade.
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i leverantörsfakturaprocessen.
- Det finns dokumenterade riktlinjer för hanteringen av sekretessuppgifter i kundfaktureringsprocessen.
- Det utförs löpande kontroller i systemet att fakturor med integritetskänslig information blir sekretessmarkerade.
- Personal som hanterar fakturor med integritetskänslig information har tillräcklig utbildning om lagstiftningen kring inre sekretess. Utbildningen bör ha en tydlig koppling till leverantörsfakturor.
- Det löpande utförs kontroller att sekretessbehörigheter i Agresso är aktuella.
- Ansökan om sekretessbehörighet i Agresso går via verksamhetschef.

Umeå den 20 januari 2016

Ingrid Lindberg
Revisor
Västerbottens läns landsting