2015-01-29 150432
Dnr: REV 72:2-2014

Landstingsstyrelsen
Hälso- och sjukvårdsnämnden

Informationssäkerhet och hantering av personuppgifter

Revisorerna genomförde år 2012 två granskningar av landstingets informationssäkerhet och hantering av personuppgifter. Vår uppföljande granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit åtgärder med anledning av de brister som framkom i 2012 års granskningar. Vi bedömer att styrelsen och nämnden för år 2014 inte säkerställt styrning, uppföljning och kontroll av att personuppgifter hanteras i enlighet med gällande lagstiftning. Bedömningen baserar vi på följande iakttagelser:

- Varken landstingsdirektören, landstingsstyrelsen eller hälso- och sjukvårdsnämnden har under de senaste åren fått rapportering om granskningar, riskanalyser, skyddsåtgärder m.m. av betydelse för informationssäkerhetsarbetet i landstinget.

- Det finns ingen uppföljning från landstingsstyrelsen, hälso- och sjukvårdsnämnden, landstingsdirektören eller staber som visar i vilken grad verksamheterna följer riktlinjer för informationssäkerhet och hantering av personuppgifter.

- Vi har genomfört ett stickprov i fem verksamheter som visar att det finns brister i tillämpningen av riktlinjer för loggkontroller och hantering av behörigheter i journalsystemet SySteam cross. Stickprovet visar bland annat att tre av fem verksamheter inte genomfört loggkontroller i enlighet med upprättade anvisningar.

- En iakttagelse i 2012 års granskningar var att landstingsdirektören utsett en av landstingets jurister till informationssäkerhetsansvarig och personuppgiftsombud. Sedan juristen avslutat sin anställning i juni 2013 har landstinget saknat dessa funktioner. Informationssäkerhetsansvarig ska enligt föreskrifter från Socialstyrelsen (SOSFS 2008:14) minst en gång om året rapportera till vårdgivaren om informationssäkerhetsarbetet. Personuppgiftsombud ska enligt personuppgiftslagen (1998:204) självständigt se till att verksamheten behandlar personuppgifter på ett lagligt sätt samt påpeka eventuella brister för den som är personuppgiftsansvarig.

Vi bedömer att avsaknad av uppföljning och väsentliga funktioner för arbete med informationssäkerhet medför risk att landstingsstyrelsen och hälso- och

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

sjukvårdsnämnden inte uppfyller sitt vårdgivaransvar inom informationssäkerhetsområdet.

Under arbetet med granskningen har vi fått information om att landstinget från och med februari 2015 anställt en jurist som ska få funktionen som informationssäkerhetsansvarig och personuppgiftsombud. Juristen ska enligt chefen för planeringsstaben se över informationssäkerhetsarbetet, utveckla rutiner för rapportering till landstingsstyrelsen och hälso- och sjukvårdsnämnden m.m.

Rekommendationer

Mot bakgrund av granskningens iakttagelser kvarstår rekommendationer från 2012 års granskningar. Landstingsstyrelsen och hälso- och sjukvårdsnämnden bör säkerställa:

- Att styrelsen och nämnden får rapporter om granskningar, riskanalyser, skyddsåtgärder m.m. av betydelse för informationssäkerhetsarbetet i landstinget.

- Att det finns informationssäkerhetsansvarig och personuppgiftsombud och att funktionerna har skriftliga uppdragsbeskrivningar.

- Att riktlinjer för informationssäkerhet och hantering av personuppgifter är kända bland verksamheterna och att verksamheterna följer riktlinjerna.

Vid revisorernas överläggning den 29 januari 2015 beslöt revisorerna enhälligt att ställa sig bakom slutsatser och rekommendationer i detta missiv. Missiv och underliggande rapport (nr 22/2014) lämnar revisorerna för kännedom till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

För landstingets revisorer

Christer Fessé
Ordförande

Karl Gustav Abramsson

LANDSTINGSREVISIONEN

Granskning av informationssäkerhet och hantering av personuppgifter

Rapport nr 22/2014

VÄSTERBOTTENS LÄNS LANDSTING

Januari 2015
Susanne Hellqvist, revisor, revisionskontoret
Diarienummer: REV 72:2-2014

Innehåll

1. Sammanfattande analys

1.1 Bakgrund

Revisorerna granskade år 2012 landstingets informationssäkerhet (nr 20/2012). Revisorerna genomförde även en granskning av landstingets hantering av personuppgifter (nr 25/2012). Granskningarna visade att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte hade säkerställt styrning, uppföljning och kontroll som innebar att landstinget hanterade personuppgifter i enlighet med gällande lagstiftning.

I granskningsplanen för år 2014 beslutade revisorerna att följa upp iakttagelserna i 2012 års granskningar.

1.2 Iakttagelser i 2014 års granskning

Granskningen visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit åtgärder med anledning av de brister som framkom i 2012 års granskningar. Vi bedömer att styrelsen och nämnden för år 2014 inte säkerställt styrning, uppföljning och kontroll av att personuppgifter hanteras i enlighet med gällande lagstiftning. Bedömningen baserar vi på följande iakttagelser:

- Varken landstingsdirektören, landstingsstyrelsen eller hälso- och sjukvårdsnämnden har under de senaste åren fått rapportering om granskningar, riskanalyser, skyddsåtgärder m.m. av betydelse för informationssäkerhetsarbetet i landstinget.

- Det finns ingen uppföljning från landstingsstyrelsen, hälso- och sjukvårdsnämnden, landstingsdirektören eller staber som visar i vilken grad verksamheterna följer riktlinjer för informationssäkerhet och hantering av personuppgifter.

- Vi har genomfört ett stickprov i fem verksamheter som visar att det finns brister i tillämpningen av riktlinjer för loggkontroller och hantering av behörigheter i journalsystemet SySteam cross. Stickprovet visar bland annat att tre av fem verksamheter inte genomfört loggkontroller i enlighet med upprättade anvisningar.

- En iakttagelse i 2012 års granskningar var att landstingsdirektören utsett en av landstingets jurister till informationssäkerhetsansvarig och personuppgiftsombud. Sedan juristen avslutat sin anställning i juni 2013 har landstinget saknat dessa funktioner. Informationssäkerhetsansvarig ska enligt föreskrifter från Socialstyrelsen (SOSFS 2008:14) minst en gång om året rapportera till vårdgivaren om informationssäkerhetsarbetet. Personuppgiftsombud ska enligt personuppgiftslagen (1998:204) självständigt se till att verksamheten behandlar personuppgifter på ett lagligt sätt samt påpeka eventuella brister för den som är personuppgiftsansvarig.

Vi bedömer att avsaknad av uppföljning och väsentliga funktioner för arbete med informationssäkerhet medför risk att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte uppfyller sitt vårdgivaransvar inom informationssäkerhetsområdet.

Under arbetet med granskningen har vi fått information om att landstinget från och med februari 2015 anställt en jurist som ska få funktionen som informationssäkerhetsansvarig och personuppgiftsombud. Juristen ska enligt chefen för planeringsstaben se över informationssäkerhetsarbetet, utveckla rutiner för rapportering till landstingsstyrelsen och hälso- och sjukvårdsnämnden m.m.

1.3 Rekommendationer

Mot bakgrund av granskningens iakttagelser kvarstår rekommendationer från 2012 års granskningar. Landstingsstyrelsen och hälso- och sjukvårdsnämnden bör säkerställa:

- Att styrelsen och nämnden får rapporter om granskningar, riskanalyser, skyddsåtgärder m.m. av betydelse för informationssäkerhetsarbetet i landstinget.

- Att det finns informationssäkerhetsansvarig och personuppgiftsombud och att funktionerna har skriftliga uppdragsbeskrivningar.

- Att riktlinjer för informationssäkerhet och hantering av personuppgifter är kända bland verksamheterna och att verksamheterna följer riktlinjerna.

2. Bakgrund

Revisorerna granskade år 2012 landstingets informationssäkerhet (nr 20/2012). Revisorerna genomförde även en granskning av landstingets hantering av personuppgifter (nr 25/2012).

En iakttagelse var att ansvarsfördelningen på politisk nivå inte var tydlig. Det var inte definierat hur personuppgiftsansvaret var fördelat mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden. En annan iakttagelse var att det saknades uppföljning och kontroll av om verksamheterna följde anvisningar för informationssäkerhet. Ett stickprov av fem verksamheter vid NUS visade att ingen av dessa genomförde kontroller av behörigheter till journalsystemet SySteam cross enligt upprättade anvisningar. Merparten av verksamheterna följde inte heller riktlinjer för kontroller av loggar i journalsystemet.

Av granskningarna framgick att landstingsdirektören hade utsett en av landstingets jurister som informationssäkerhetsansvarig och personuppgiftsombud. Juristen saknade dock en skriftlig arbetsbeskrivning och uppgav att han inte hade tillräckligt med tid att arbeta med frågorna. Det förekom ingen rapportering från juristen till landstingsdirektören eller styrelsen och nämnden om informationssäkerhetsarbetet i landstinget.

Rekommendationer i granskningarna var att landstingsstyrelsen och hälso- och sjukvårdsnämnden skulle säkerställa:

- Att styrelsens och nämndens personuppgiftsansvar blev tydligt definierat.
- Att styrelsen och nämnden fick rapporter om granskningar, riskanalyser, skyddsåtgärder m.m. av större betydelse för informationssäkerhetsarbetet i landstinget.
- Att informationssäkerhetsansvarig och personuppgiftsombud fick ett skriftligt uppdrag.
- Att riktlinjer för informationssäkerhet och behandling av personuppgifter blev kända bland verksamheterna och att verksamheterna följde riktlinjerna.

2.1 Revisionsfrågor

Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att:

- Det är definierat hur personuppgiftsansvaret är fördelat mellan styrelsen och nämnden?
- Det finns tydliga regler för informationssäkerhet och hantering av personuppgifter?
- Är reglerna kommunicerade till verksamheterna?
- Det finns en utsedd informationssäkerhetsansvarig och att denna har en dokumenterad arbetsbeskrivning?

- Det finns personuppgiftsombud för styrelsens och nämndens ansvarsområden och att ombudet eller ombuden har skriftliga uppdrag?
- Att verksamheterna följer riktlinjer för informationssäkerhet?
    - Finns central uppföljning av om verksamheterna följer anvisningar för loggkontroller m.m.?
    - Eget stickprov i syfte att kontrollera verksamheternas följsamhet till riktlinjer för informationssäkerhet (se mer under avsnittet Metod och genomförande nedan)
- Det finns rutiner för rapportering till landstingsdirektören, styrelsen och nämnden om informationssäkerhetsarbetet i landstinget?

2.2 Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar. Vi har utgått från nedanstående revisionskriterier:

- Kommunallagen 6 kap, 7§
- Patientdatalagen (2008:355) och Personuppgiftslagen (1998:204). Av rapporten framgår närmare vilka paragrafer som utgjort revisionskriterier i granskningen.
- Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Av rapporten framgår närmare vilka paragrafer som utgjort revisionskriterier i granskningen.
- Landstingsfullmäktiges reglemente för landstingsstyrelsen och hälso- och sjukvårdsnämnden
- Landstingsfullmäktiges säkerhetspolicy, beslutad 2011-06-21
- Landstingets regler för informationssäkerhet och hantering av personuppgifter

2.3 Ansvarig styrelse och nämnd

Landstingsstyrelsen och hälso- och sjukvårdsnämnden.

2.4 Metod och avgränsning

Granskningen är avgränsad till landstingets informationssäkerhetsarbete med avseende på hantering av personuppgifter och skydd mot obehörig intern åtkomst. Granskningen avser inte informationssäkerhetsarbete med avseende på fysisk säkerhet, exempelvis skydd av serverhallar, tekniskt skydd mot obehörig extern åtkomst etc.

Vi har genomfört granskningen genom dokumentstudier, intervjuer och stickprov. Vi har hämtat information från chef och jurist vid staben för planering och styrning samt systemägare för SySteam cross. I syfte att kontrollera följsamheten till riktlinjer för informationssäkerhet har vi även genomfört ett stickprov av fem verksamheter i landstinget.

Vi har kontrollerat om verksamheterna hanterar behörigheter och genomför loggkontroller i enlighet med upprättade anvisningar. I denna del har projektledaren bistått av revisor Jonas Hansson vid revisionskontoret.

Samtliga intervjuade har fått möjlighet att lämna synpunkter på rapportens innehåll. Granskningen har även kvalitetssäkrats genom att den granskats av annan sakkunnig vid revisionskontoret.

3. Riktlinjer och ansvar

3.1 Beslut om åtgärder

Revisorerna beslutade den 28 februari 2013 att lämna över skrivelser till landstingsstyrelsen och hälso- och sjukvårdsnämnden med information om iakttagelserna i 2012 års granskningar.

En genomgång av landstingsstyrelsens protokoll för år 2013 och 2014 visar att styrelsen inte beslutat om några åtgärder med anledning av granskningarna.

Hälso- och sjukvårdsnämnden uppdrog den 20 maj 2013 (§ 52-53) till landstingsdirektören att vid nämndens sammanträde i augusti 2013 återkomma med förslag till åtgärder. En genomgång av nämndens protokoll visar att landstingsdirektören inte presenterade några åtgärdsförslag hösten 2013. Vi har inte heller funnit att nämnden beslutat om några åtgärder under år 2014.

3.2 Lagar och föreskrifter

Hur landstinget ska hantera personuppgifter finns reglerat i Personuppgiftslagen (SFS 1998:204) och Patientdatalagen (SFS 2008:355). Patientdatalagen är tillämplig vid en vårdgivares behandling av personuppgifter i patientjournaler och nationella kvalitetsregister.

I Patientdatalagens fjärde kapitel finns bestämmelser om inre sekretess och elektronisk åtkomst inom en vårdgivares verksamhet. Vårdgivaren ska bestämma villkor för tilldelning av behörigheter till patientuppgifter och se till att åtkomst till sådana uppgifter dokumenteras och kan kontrolleras. Vårdgivare ska enligt lagen göra systematiska och återkommande kontroller av om någon obehörigen kommer åt patientuppgifter.

Enligt Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) ska vårdgivaren säkerställa att det i verksamhetens ledningssystem finns en dokumenterad informationssäkerhetspolicy. Informationssäkerhetspolicyn ska säkerställa att patientuppgifter är åtkomliga för den som är behörig (tillgänglighet), att patientuppgifterna är oförvanskade (riktighet), att obehöriga inte kan ta del av uppgifterna (sekretess) samt att det är möjligt att härleda förändringar och åtgärder till en specifik användare (spårbarhet).

Vårdgivaren ansvarar enligt föreskrifterna för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter.

Vårdgivaren ansvarar vidare för att det i ledningssystemet finns rutiner som säkerställer systematiska och återkommande stickprovskontroller av loggar i journalsystem.

3.3 Personuppgiftsansvar

Enligt patientdatalagen är varje myndighet i landsting som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Den personuppgiftsansvarige ska enligt personuppgiftslagen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som myndigheten behandlar. En iakttagelse i 2012 års granskning var att det inte var definierat hur personuppgiftsansvaret var fördelat mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden.

Landstingsfullmäktige beslutade den 18 februari 2014 om reviderade reglementen för landstingsstyrelsen och hälso- och sjukvårdsnämnden. Av reglementena framgår att landstingsstyrelsen och hälso- och sjukvårdsnämnden är personuppgiftsansvariga för de personuppgifter som nämnden och styrelsen behandlar. Vi har inte funnit några riktlinjer som tydliggör vad styrelsens och nämndens ansvar omfattar.

3.4 Personuppgiftsombud

Ett personuppgiftsombud är en fysisk person som efter förordnande från den personuppgiftsansvarige självständigt ska se till att verksamheten behandlar personuppgifter på ett lagligt sätt (Personuppgiftslagen § 38). Ombudet ska bland annat föra en förteckning över pågående personuppgiftsbehandlingar samt ge råd och stöd till registrerade. Om det finns risk för att verksamheten bryter mot bestämmelser i lagstiftningen ska ombudet påpeka bristerna för den som är personuppgiftsansvarig. Ett ombud kan representera flera personuppgiftsansvariga.

En iakttagelse i 2012 års granskning var att landstingsdirektören på uppdrag av landstingsstyrelsen hade utsett en av landstingets jurister till personuppgiftsombud. Ombudet saknade ett skriftligt uppdrag som beskrev omfattningen av dennes arbete samt vilka nämnder ombudet företrädde. Det förekom ingen rapportering från ombudet till landstingsdirektören, landstingsstyrelsen eller hälso- och sjukvårdsnämnden om hanteringen av personuppgifter. Personuppgiftsombudets arbete bestod i att ge stöd och råd till verksamheterna och att kontrollera lagligheten i behandlingar av personuppgifter som verksamheterna anmälde.

Sedan juristen avslutat sin anställning i landstinget våren 2013 har landstingsdirektören inte utsett något nytt personuppgiftsombud för landstingsstyrelsens och hälso- och sjukvårdsnämndens ansvarsområden.

3.5 Riktlinjer

Landstingsfullmäktige beslutade i juni 2011 om en säkerhetspolicy för landstinget. Enligt policyn ska landstingsdirektören besluta om riktlinjer för informationssäkerhet.

Landstingsdirektören beslutade i juni 2012 om övergripande riktlinjer för informationssäkerhet. Riktlinjerna finns i landstingets ledningssystem på intranätet Linda. Av riktlinjerna framgår att dessa syftar till en säker hantering av information för att uppnå önskad tillgänglighet, riktighet, sekretess och spårbarhet.

I ledningssystemet finns även ytterligare anvisningar som i olika delar kompletterar och konkretiserar landstingsdirektörens riktlinjer för informationssäkerhet. I ledningssystemet finns bland annat riktlinjer för åtkomst till elektronisk information, anvisningar för loggkontroller, anvisningar för användning av patientuppgifter vid kvalitetssäkringsarbete och utbildning m.m.

3.6 Informationssäkerhetsansvarig

Enligt Socialstyrelsens föreskrifter för informationssäkerhet och journalföring i hälso- och sjukvården ska vårdgivaren utse en eller flera personer som ansvarar för informationssäkerhetsarbetet (3 §). Den eller de som har fått denna uppgift ska minst en gång om året till vårdgivaren rapportera om genomförda granskningar och skyddsåtgärder av större betydelse, genomförda riskanalyser och förbättringsåtgärder.

Vid tidpunkten för 2012 års granskningar hade landstingsdirektören utsett en jurist vid planeringsstaben till informationssäkerhetsansvarig. Sedan juristen avslutat sin anställning i juni 2013 har landstinget saknat en informationssäkerhetsansvarig.

3.7 Informationssäkerhetsarbetet

Enligt landstingsdirektörens riktlinjer för informationssäkerhet ska informationssäkerheten regelbundet följas upp, såväl på central nivå som inom respektive verksamhet. Granskningar, riskanalyser och åtgärder av större betydelse för informationssäkerheten ska rapporteras till landstingsstyrelsen. Landstingsdirektören ansvarar för att det finns rutiner för sådan rapportering.

Vi har inte funnit att landstingsdirektören, landstingsstyrelsen eller hälso- och sjukvårdsnämnden fått någon rapportering om informationssäkerhetsarbetet i landstinget.

I landstinget finns ett säkerhetsråd som enligt riktlinjer beslutade av landstingsstyrelsen årligen ska rapportera utvecklingen inom olika säkerhetsområden till landstingsdirektören. Eftersom landstinget sedan våren 2013 saknat en informationssäkerhetsansvarig har det inte funnits någon representant i rådet som lämnat rapport över utvecklingen inom säkerhetsområdet informationssäkerhet.

3.8 Vår kommentar

Vi bedömer att avsaknad av uppföljning och väsentliga funktioner för arbete med informationssäkerhet medför risk att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte uppfyller sitt vårdgivaransvar inom informationssäkerhetsområdet.

Vi bedömer även att det inte är definierat hur personuppgiftsansvaret är fördelat mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden. Det är inte tydliggjort i vilket avseende styrelsen respektive nämnden ansvarar för att det finns ett tillfredsställande organisatoriskt och tekniskt skydd för de personuppgifter som verksamheterna hanterar.

Under arbetet med granskningen har vi fått information om att landstinget från och med februari 2015 anställt en jurist som ska få funktionen som informationssäkerhetsansvarig och personuppgiftsombud. Juristen ska enligt chefen för planeringsstaben se över informationssäkerhetsarbetet, utveckla rutiner för rapportering till landstingsstyrelsen och hälso- och sjukvårdsnämnden m.m.

4. Tillämpning av riktlinjer

4.1 Stickprov

I 2012 års granskning ingick ett stickprov av fem verksamheter vid NUS. Stickprovet visade att ingen av verksamheterna genomförde kontroller av behörigheter till journalsystemet SySteam cross enligt upprättade anvisningar. Merparten av verksamheterna följde inte heller riktlinjer för kontroller av loggar i journalsystemet.

Vi har i 2014 års granskning genomfört ett nytt stickprov för att kontrollera om verksamheter hanterar behörigheter och genomför loggkontroller i enlighet med upprättade anvisningar. Vi har genomfört kontroller och intervjuat verksamhetschef och lokalt systemansvarig (LISA) vid följande verksamheter:

- Mariehems hälsocentral
- Kvinnokliniken NUS
- Ersboda hälsocentral
- Lunggastroavdelningen NUS
- Neurocentrum NUS

4.2 Anvisningar för loggkontroller

Med loggning avses registrering av aktiviteter som utförs i ett elektroniskt system, exempelvis av vilken information som skapats, lästs eller överförts och vem som utfört aktiviteten. Landstingsdirektören har i *Riktlinjer för åtkomst till elektronisk information* (fastställda i juni 2012) beslutat att verksamheterna regelbundet ska genomföra loggkontroller enligt upprättade rutiner.

Systemägaren för SySteam cross har i januari 2014 fastställt mer detaljerade anvisningar för hur verksamheterna ska genomföra loggkontroller i journalsystemet. Enligt anvisningarna ska samtliga användare vara informerade om att loggning genomförs och att det pågår uppföljning i form av loggkontroller. Loggkontrollen ska genomföras av lokalt systemansvarig (LISA) och överlämnas till verksamhetschefen för bedömning.

Varje kalendermånad ska ett antal användare med läsbehörighet på vårdenheten slumpmässigt väljas ut. Loggar för dessa användare ska granskas för en 24-timmars period. Samtliga användare på enheten ska granskas minst en gång per år.

Den som genomför kontrollen ska upprätta ett protokoll över granskningen. Protokollet ska arkiveras och sparas minst två år på vårdenheten. Syftet är enligt anvisningarna att protokollet ska kunna visas upp vid den centrala uppföljning som landstinget ska genomföra. Om loggkontrollen inte visar på några avvikelser ska detta noteras i protokollet och de framtagna logglistorna kan makuleras. Om loggkontrollen visar på oklarheter ansvarar verksamhetschefen för att ta kontakt med berörd användare. Om ärendet ska hanteras som ett arbetsrättsligt ärende ska verksamhetschefen kontakta den centrala personalfunktionen. Utredning och beslut om åtgärd ska dokumenteras och diarieföras.

4.3 Resultat stickprov loggkontroller

I tabellen nedan redovisar vi resultatet av stickprovet av loggkontroller:

Frågor	Mariehem HC	Kvinnoklinik NUS	Ersboda HC	Lunggastroavdelning NUS	Neurocentrum NUS
Verksamhetschef och LISA känner till riktlinjer för loggkontroller?	Ja	Nej	Ja	Ja	Ja
Verksamheten genomför kontroller varje månad?	Ja	Nej	Ja	Ja	Nej
Verksamheten kontrollerar alla anställda minst en gång per år?	Ja	Nej	Nej	Ja	Nej
Verksamheten upprättar protokoll över loggkontrollerna?	Ja	Nej	Ja	Ja	Ja
Verksamheten sparar protokollen minst två år?	Ja	Nej	Ja	Ja	Ja

Tre av fem verksamheter hade inte genomfört loggkontroller i enlighet med upprättade anvisningar. En av verksamheterna hade inte genomfört några loggkontroller alls. Vid tidpunkten för vårt stickprov kände verksamhetschefen vid enheten inte till anvisningarna för loggkontroller. Företrädare för övriga verksamheter uppgav att de kände till riktlinjerna. Två av verksamheterna hade dock inte genomfört kontroller i sådan omfattning att samtliga anställda kontrollerades minst en gång per år. Vid intervjuerna framkom att dessa verksamheter upplevde problem i tillämpningen av riktlinjerna. Verk-

samhetsföreträdare uppgav att det av resursmässiga eller tekniska skäl inte varit möjligt att genomföra kontroller i den omfattning som anvisningarna kräver.

Det förekommer ingen central uppföljning av om verksamheterna genomför loggkontroller i journalsystemet SySteam cross. Systemägaren för SySteam cross hänvisar till funktionen som informationssäkerhetsansvarig. Det är enligt systemägaren den informationssäkerhetsansvariges uppgift att genomföra kontroller av verksamheter, fånga upp synpunkter och problem kring riktlinjernas tillämpning m.m. Systemägaren ser problem med att tillämpa riktlinjerna i stora verksamheter med få lokalt systemansvariga. Det tar enligt systemägaren mycket tid i anspråk att genomföra loggkontroller.

Systemförvaltaren för Systeam cross har enligt uppgift regelbundna möten med lokalt systemansvariga i verksamheterna. I samband med dessa möten kan systemförvaltaren informera om nya riktlinjer, förändringar i rutiner m.m.

4.4 Anvisningar för hantering av behörigheter

Av landstingsdirektörens riktlinjer, *Informationssäkerhet – riktlinjer för åtkomst till elektronisk information*, framgår att respektive verksamhetschef ansvarar för att dess personal har rätt behörighet. Användarnas behörighet ska begränsas till vad som är nödvändigt för att ge en god och säker vård. Det ska finnas dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter. Förutom regelbunden kontroll av användarnas behörighetsbehov ska verksamheten genomföra översyn av behörigheter vid förändrade arbetsuppgifter samt efter organisations- eller systemförändring.

4.5 Resultat stickprov behörigheter

Vi har kontrollerat om verksamheterna tagit bort behörigheter för personal som avslutat sin anställning under perioden 1 januari-december 2014. Stickprovet är genomfört den 9 december 2014. Resultatet sammanfattas i tabellen nedan:

Vårdenhet	Avslutade anställningar år 2014	Behörigheter som inte var avslutade vid stickprovstillfället
Mariehems hälsocentral	9	1
Kvinnokliniken NUS	27	5
Ersboda hälsocentral	2	0
Lunggastroavdelning NUS	6	3
Neurocentrum NUS	28	4

Kontrollen visade att fyra av fem verksamheter hade oavslutade behörigheter för personal som slutat sina anställningar.

Vid tidpunkten för våra intervjuer hade ingen av verksamheterna dokumenterade rutiner för behörighetsadministration i enlighet med lands-

tingsdirektörens riktlinjer. Samtliga verksamhetsföreträdare uppgav att de arbetade utifrån informella rutiner och att det fanns en informell ansvarsfördelning för administration av behörigheter. Vi har i samband med kvalitetssäkringen av granskningen fått information om att två av verksamheterna nu tagit fram dokumenterade rutiner för administration av behörigheter.

4.6 Vår kommentar

Vi bedömer att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt att verksamheterna följer anvisningar för informationssäkerhet. Det finns ingen central uppföljning av om verksamheterna följer anvisningar för loggkontroller m.m. Vårt stickprov visar att det finns brister i tillämpningen av riktlinjer för loggkontroller och hantering av behörigheter i journalsystemet SySteam cross.

5. Svar på revisionsfrågor

Granskningen visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit åtgärder med anledning av de brister som framkom i 2012 års granskningar. Vi bedömer att styrelsen och nämnden för år 2014 inte säkerställt styrning, uppföljning och kontroll av att personuppgifter hanteras i enlighet med gällande lagstiftning.

I tabellen nedan sammanfattar vi svaret på revisionsfrågorna i granskningen:

Revisionsfråga	Bedömning	Kommentar
Är det definierat hur personuppgiftsansvaret är fördelat mellan landstingsstyrelsen och hälso- och sjukvårdsnämnden?	Nej	Av fullmäktiges reglemente framgår att landstingsstyrelsen och hälso- och sjukvårdsnämnden är personuppgiftsansvariga för de personuppgifter som styrelsen och nämnden behandlar. Vi har dock inte funnit några riktlinjer som tydliggör vad styrelsens och nämndens ansvar omfattar.
Finns tydliga regler för informationssäkerhet och hantering av personuppgifter?	Ja	Landstingsdirektören har beslutat om riktlinjer för informationssäkerhet och hantering av patientuppgifter.
Är reglerna kommunicerade till verksamheterna?	Ja	Riktlinjer för informationssäkerhet finns i ledningssystemet på intranätet. Enligt uppgift har lokalt systemansvariga i verksamheterna regelbundna möten med systemförvaltaren för journalsystemet SySteam cross. I samband med dessa möten lämnar förvaltaren information om nya rutiner o.s.v.

Finns utsedd informationssäkerhetsansvarig och har denne ett skriftligt uppdrag?	Nej	Funktionen som informationssäkerhetsansvarig har varit vakant sedan juni 2013. Från och med februari 2015 har landstinget anställt en jurist som enligt uppgift ska inneha funktionen.
Finns utsedda personuppgiftsombud för styrelsens och nämndens ansvarsområden och har ombudet eller ombuden skriftliga uppdrag?	Nej	Funktionen som personuppgiftsombud har varit vakant sedan juni 2013. Från och med februari 2015 har landstinget anställt en jurist som enligt uppgift ska inneha funktionen.
Har styrelsen och nämnden säkerställt att verksamheterna följer riktlinjer för informationssäkerhet?	Nej	Det finns ingen central uppföljning av om verksamheterna följer anvisningar för loggkontroller m.m. Vårt stickprov visar att det finns brister i tillämpningen av riktlinjer för loggkontroller och hantering av behörigheter i journalsystemet SySteam cross.
Finns rutiner för rapportering till landstingsdirektören, styrelsen och nämnden om informationssäkerhetsarbetet i landstinget?	Nej	Vi har inte funnit att landstingsdirektören, landstingsstyrelsen eller hälso- och sjukvårdsnämnden under de senaste åren fått rapportering om informationssäkerhetsarbetet i landstinget.

Landstingsstyrelsen och hälso- och sjukvårdsnämnden bör säkerställa:

- Att styrelsen och nämnden får rapporter om granskningar, riskanalyser, skyddsåtgärder m.m. av betydelse för informationssäkerhetsarbetet i landstinget.
- Att det finns informationssäkerhetsansvarig och personuppgiftsombud och att funktionerna har skriftliga uppdragsbeskrivningar.
- Att riktlinjer för informationssäkerhet och hantering av personuppgifter är kända bland verksamheterna och att verksamheterna följer riktlinjerna.

Umeå den 29 januari 2015

Susanne Hellqvist
Revisor
Västerbottens läns landsting