Landstingsstyrelsen
Hälso- och sjukvårdsnämnden

**Granskning av informationssäkerhet**
Vi bedömer att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt rutiner och kontroller som innebär att patientuppgifter blir hanterade på korrekt sätt i förhållande till Patientdatalagen (2008:355) och Socialstyrelsens föreskrifter (2008:14). Vår bedömning bygger på följande iakttagelser:

- Landstingsstyrelsen och hälso- och sjukvårdsnämnden saknar rutiner som säkerställer att de får rapporter om informationssäkerhetsarbetet i landstinget. Varken landstingsstyrelsen eller nämnden har fått rapporter om vilka granskningar, riskanalyser, skyddsåtgärder m.m. av större betydelse som är gjorda inom området för informationssäkerhet.

- Landstingsdirektörens riktlinjer för informationssäkerhet är inte tillräckligt kända bland verksamheterna. Det finns ingen uppföljning om verksamheterna följer riktlinjerna för informationssäkerhet.

- Landstingsdirektörens riktlinjer för informationssäkerhet är övergripande. Det saknas detaljerade anvisningar för hur verksamheterna ska arbeta med informationssäkerhetsfrågorna i praktiken.

- Landstingsdirektören har utsett en informationssäkerhetsansvarig. Det saknas dock en arbetsbeskrivning över dennes uppgifter och ansvar.

- Ingen av de granskade enheterna följer upprättade anvisningar som anger att behörigheter till journalsystemet SYSteam Cross ska granskas 2-3 gånger per år och rapporteras till verksamhetschefen. Granskningen visar också att basenheterna hanterar hur användares behörigheter till journalsystemen ska avslutas på olika sätt.

- Det saknas landstingsövergripande uppföljning av om verksamheterna genomför loggkontroller enligt angivna anvisningar. Granskningen visar att verksamheter inte känner till anvisningarna och att man genomför kontroller på olika sätt.

**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

Med utgångspunkt av iakttagelserna lämnar vi följande rekommendationer till landstingsstyrelsen och hälso- och sjukvårdsnämnden. Säkerställ att:

- Styrelsen och nämnden får rapporter som är av större betydelse för informationssäkerheten inom sina verksamhetsområden.

- Landstingsdirektörens riktlinjer för informationssäkerhet blir tillräckligt kända bland verksamheterna. Se till att landstingsdirektören följer upp efterlevnaden av riktlinjerna.

- Landstingets informationssäkerhetsansvarige får en arbetsbeskrivning. I detta ligger att det blir tydligt vilket ansvar och vilka arbetsuppgifter som ingår i rollen som informationssäkerhetsansvarig.

- Verksamheterna följer upprättade anvisningar som innebär att användares behörigheter till journalsystemet blir granskade 2-3 gånger per år. Säkerställ också att det på basenhetsnivå finns dokumenterade rutiner som beskriver hur användares behörigheter till journalsystemet ska avslutas.

- Verksamheterna känner till och följer angivna anvisningar för loggkontroller. Säkerställ också att det finns rutiner om att minst en gång per år följa upp att verksamheterna genomför loggkontroller i enlighet med fastställda anvisningar.

Vid revisorernas överläggning den 28 februari 2013 beslöt revisorerna enhälligt att ställa sig bakom iakttagelser och slutsatser i detta missiv. Missiv och underliggande rapport (20/2012) bifogar revisorerna för kännedom till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

För landstingets revisorer

Rob Eriksson
Ordförande

Sven-Olov Södermark
Vice Ordförande