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