

Informationssäkerhet och hantering av personuppgifter

Iakttagelser

2014 års uppföljande granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit åtgärder med anledning av brister som framkom i två granskningar år 2012. Revisorerna 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 revisorerna 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.
- Landstinget har sedan juni 2013 saknat informationssäkerhetsansvarig och personuppgiftsombud. 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.

Revisorerna 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 uppgift över informationssäkerhetsarbetet, utveckla rutiner för rapportering m.m.

Rekommendationer

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.

Rapport: "Granskning av informationssäkerhet och hantering av personuppgifter". För ytterligare information kontakta Susanne Hellqvist, tel. 090-7857087. Den kompletta rapporten finns på landstingets hemsida www.vll.se men kan även beställas från landstingets revisionskontor.