NR 6 - november 2020

Revisionskontoret

Sammanfattning av granskningsrapport

IT- och informationssäkerhet

Uppdrag och syfte

På uppdrag av Region Skånes revisorer har EY granskat IT- och informationssäkerhet i Region Skåne. Det övergripande syftet med granskningen har varit att bedöma om Region Skånes arbete med informationssäkerhet och IT-säkerhet, bedrivs på ett systematiskt och ändamålsenligt sätt.

Resultat av granskningen

Den sammanfattade bedömningen är att IT- och informationssäkerhetsarbetet till stora delar bedrivs systematiskt och ändamålsenligt men i vissa delar är otillräckligt.

I granskningen görs bedömningen att området utvecklats i positiv riktning under de senaste åren, framför allt inom styrning och ledning med tydliggörande av ansvar och framtagande och fastställande av relevanta styrande riktlinjer och instruktioner från centralt håll. Region Skåne har även utformat en organisation för regionalt dataskyddsarbete som bedöms möjliggöra ett strukturerat och målinriktat arbete för anpassning gentemot GDPR. Granskningen har dock påvisat brister inom:

- **Systematisk uppföljning, kontroll och utvärdering**
- **Utbildning**
- **Patientintegritet i journalsystem**

Regionstyrelsen och kollektivtrafiknämnden rekommenderas att:

- Genomföra en kartläggning av upprättade instruktioner inom området för informationssäkerhet och utvärdera om lämpliga instruktioner i enlighet med beslutade riktlinjer för informationssäkerhet har upprättats.
- Säkerställa att rutiner och ansvar för uppföljning av avtal med molntjänstleverantörer, personuppgiftsbiträden och andra tredjeparter med ansvar för IT-säkerhet, informationssäkerhet och dataskydd är tydligt definierade.
- Införa rutiner för regelbunden och systematisk uppföljning av informationssäkerhetsarbetet inom regionen för att utvärdera om beslutade riktlinjer efterlevs. I samband med detta utvärdera behov av resurser, systemstöd, metoder, eller instruktioner för att möjliggöra en effektiv uppföljning.
- Följa upp utbildningsinsatser för att dels kontrollera om samtliga medarbetare genomgår den grundläggande e-utbildningen i säker informationshantering och dels få insikt i hur många medarbetare som genomgått kompetenshöjande men ej obligatoriska utbildningar.

Regionstyrelsen rekommenderas även att

- Årligen genomföra uppföljning av beslutade kortsiktiga mål för informationssäkerhetsarbetet.
- Utvärdera behov och möjligheter för att tillsätta resurser med regionövergripande ansvar för ledning, kravställning, och uppföljning rörande IT-säkerhet.
- Tillse att regionövergripande process utarbetas för att tydliggöra dels hur krav på biträden som hanterar personuppgifter för Region Skånes räkning ska definieras och dels hur instruktioner för biträdenas behandling av personuppgifter ska utformas vid tecknande av avtal.
- Genomföra en översyn av nuvarande hantering av regionens registerförteckning av personuppgiftsbehandlingar i syfte att identifiera hur systemstöd kan utvecklas för att förbättra kvaliteten i registerförteckningen, samt underlätta uppföljning och kontroll av följsamheten gentemot GDPR.
- Följa upp projektet för införande av Skånes Digitala Vårdsystem avseende hur patientens integritet i det nya systemet kommer att säkerställas i enlighet med gällande lagstiftning genom exempelvis förbättrade behörighetsstrukturer eller automatiserad loggуppföljning.

Rapporten finns tillgänglig på www.skane.se/revisionen

REGION SKÅNE