NR 7 - Dec 2023

Revisionskontoret

Sammanfattning av granskningsrapport

Granskning av Informations- och IT-säkerhet fokus patientdata

Uppdrag och syfte

Revisorerna har genomfört en granskning av informations- och IT-säkerhet med fokus på patientdata inom Region Skåne. KPMG AB har biträtt i granskningsarbetet.

Syftet med denna granskning har varit att bedöma om arbetet med informations- och IT-säkerhet inom Region Skåne bedrivs på ett systematiskt och ändamålsenligt sätt.

Resultat av granskningen

Den samlade bedömningen utifrån granskningens syfte är att arbetet med IT- och informationssäkerhet inom Region Skåne inte är systematiskt och ändamålsenligt och att det finns risk att patientdata inte skyddas mot obehöriga.

Region Skåne har inte säkerställt medborgarens integritet då patientinformation i journalsystem endast delvis är skyddade mot obehöriga. Det informationssäkerhetsarbete som genomförts är inte i nivå med de krav som ställs i lag och i interna styrdokument. Region Skåne har delvis ett tillräckligt skydd för sina databaser och system. Däremot saknas en samlad bild avseende vilka skyddsbehov som finns för Region Skånes informationstillgångar då informationsklassning och riskbedömning inte genomförts i tillräcklig omfattning. Rutiner för incidenthantering finns men de saknar en tydlig beskrivning av ansvar, processer samt eskaleringsvägar i händelse av olika incidenttyper. Avvikelser och incidenter hanteras därför endast delvis i enlighet med gällande lagstiftning och regelverk.

Rekommendationer till regionstyrelsen:

- Stärka den interna kontrollen av samtliga nämnder och styrelser avseende efterlevnad av de styrande dokument som utgör Region Skånes ledningssystem för informationssäkerhet.
- Utvärdera om nuvarande resurser för informationssäkerhetsarbetet motsvarar omfattning av Region Skånes krav på informationssäkerhet mot bakgrund av lagkrav och interna beslut.
- Genom regelbunden uppföljning tillse att pågående arbete med riskhantering av Region Skånes informationssystem fortgår och slutförs, samt att säkerhetsåtgärder vidtas som analyser visat behov av i syfte att skydda patientinformation och andra skyddsvärda uppgifter.
- Säkerställa att Region Skånes process för åtkomst- och behörighetshantering stärks vad gäller tilldelning, förändring och avslut av behörigheter så att endast behöriga har tillgång till information.
- Utreda om det finns möjlighet att centralisera logghanteringen för att avlasta verksamheterna samt kvalitetssäkra och stärka Region Skånes förmåga att genomföra kontroller i tillräcklig omfattning.
- Säkerställa att Region Skånes medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att nuvarande rutiner för incidenthantering kompletteras med tydlig beskrivning avseende ansvar, processer och eskaleringsvägar i händelse av olika incidenttyper samt att rutinerna etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov på regionövergripande nivå.

Rekommendationer lämnades också till nämnden för operativ regiongemensam verksamhet, primärvårdsnämnden och sjukhusstyrelse Ystad.

Rapporten finns tillgänglig på www.skane.se/revisionen