

Distribution
Regionstyrelsen
Hälso- och sjukvårdsnämndenDelges:
Regionfullmäktige

Informationssäkerhet - skyddade personuppgifter

Vid överläggningar med Regionens revisorer den 19 november behandlades revisionsrapporten *Informationssäkerhet - skyddade personuppgifter*.

Vi vill med anledning av vår granskning få del av regionstyrelsens och hälso- och sjukvårdsnämndens kommentarer samt information om planerade åtgärder för respektive rekommendation i rapportens sammanfattning. Svaret bör vara oss tillhanda senast 19 februari 2026.

Bakgrund

Regionens revisorer genomförde 2023 en granskning av informationssäkerhet¹. Granskningen visade att regionstyrelsen och hälso- och sjukvårdsnämnden inte hade säkerställt en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter. Bland annat hade det inte säkerställts en tillräcklig uppföljning och rapportering av att rutinerna för skyddade personuppgifter efterlevdes. Styrelsens och nämndens svar på revisionsrapporten angav ett antal förbättringsområden.

Revisorerna bedömer att det finns en risk för att tillräckliga åtgärder inte har vidtagits utifrån den tidigare granskningen avseende skyddade personuppgifter. En granskning av området har därför beslutats ingå i 2025 års revisionsplan.

Iakttagelser och bedömning

Granskningen visar bland annat att riktlinjer för hantering av skyddade personuppgifter inte har upprättats. Granskningen visar även på brister avseende uppföljning av rutinefterlevnad och riskanalys.

Vi bedömer att det finns en bristande kontroll över hälso- och sjukvårdsnämndens utgivna uppdrag.

Vår sammantagna bedömning är att regionstyrelsen och hälso- och sjukvårdsnämnden i huvudsak inte tillsett att ändamålsenliga åtgärder har vidtagits utifrån 2023 års granskning.

¹ Granskning Informationssäkerhet - uppföljning och skyddade personuppgifter. Diarienummer 23REV41

Rekommendationerna från tidigare granskning kvarstår därmed i betydande utsträckning. Uppföljningen har även resulterat i att nya rekommendationer har tillkommit.

Rekommendationer

Vi lämnar följande rekommendationer till regionstyrelsen:

- Ta fram riktlinjer för hantering, uppföljning och rapportering av skyddade personuppgifter samt tillse att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.
- Tillse att lokala rutiner upprättas i enlighet med krav i den regiongemensamma rutinen.
- Följ upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- Säkerställ att en regiongemensam struktur för riskanalyser upprättas avseende hanteringen av skyddade personuppgifter.
- Säkerställ att rutinen för riskanalys implementeras samt att systemstödet för ändamålet förankras.
- Säkerställ efterlevnad till styrdokument för hantering av skyddade personuppgifter. Tillse vidare att det finns rutiner för att kunna följa upp planerade och genomförda utbildningar.
- Tydliggör processägarskap inom informationssäkerhetsområdet.

Vi lämnar följande rekommendationer till hälso- och sjukvårdsnämnden:

- Tillse att lokala rutiner upprättas i enlighet med krav i den regiongemensamma rutinen.
- Följ upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- Säkerställ kontroll över utgivna uppdrag.

REGIONENS REVISORER

Ingemar Wiklander
Ordförande

Birgitta Arnberg
Revisionsdirektör