

Regionens revisorer

För kännedom:

Regionfullmäktige

Regionstyrelsen**Granskning av införande av nytt vårdinformationssystem**

Vi har i egenskap av förtroendevalda revisorer i Region Norrbotten genomfört en granskning av införande av nytt vårdinformationssystem. Syftet med granskningen är att bedöma om regionstyrelsen säkerställt att implementering av nytt vård informationssystem sker i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt. Granskningsobjekt är regionstyrelsen. Granskningen är avgränsad till områdena informationssäkerhet, IT-säkerhet och personuppgiftshantering. Granskningen är också avgränsad till perspektivet om gällande regelverk och etablerad praxis efterlevts avseende processen för införandet av nytt vårdinformationssystem.

Vi har i vår granskning biträttats av sakkunniga från PwC.

Vår samlade revisionella bedömning är att:

- Regionstyrelsen **inte helt** säkerställt att implementering av nytt vårdinformationssystem skett i enlighet med gällande lagstiftning och på ett ändamålsenligt sätt avseende områdena informationssäkerhet, IT-säkerhet och personuppgiftshantering.

Granskningen bedömer att riskanalyser, konsekvensbedömningar och lämplighetsbedömningar följer lagkrav och branschstandard samt att de utförts och uppdaterats i takt med ändrade förutsättningar.

Vi bedömer det som **en brist** att konsekvens- och lämplighetsbedömning fastställdes efter driftsättning, och som problematiskt att det strukturerade riskarbetet påbörjades för sent. Granskningen bedömer vidare att ändamålsenliga risk- och behovsanalyser avseende behörighetstilldelning har genomförts. Däremot är det tydligt att frågan om den reella åtkomsten till patientuppgifter är ett orosmoment som inte fått en tillfredsställande lösning innan driftsättningen. Avseende riskanalyserna vill vi understryka att de är i grunden väl genomförda, och att det är tydligt att det finns en grundläggande systematik i arbetet som är positiv. Det är framförallt den sista delen som avser analys och motivering kring varför risker och brister trots allt accepteras som behöver förbättras.

Tjänsteavtalet och PUB-avtalet, exklusive instruktionen, bedöms i allt väsentligt följa branschstandard och innehålla relevanta villkor. Det är dock **en brist** att instruktionen initialt var varken fullständig eller korrekt. Granskningen visar att regionen har konstaterat att en överföring av personuppgifter kommer att ske till tredjeland, vilket det saknades stöd för i instruktionen och således är det en överföring som strider mot det ingångna avtalet. Den 6 december undertecknades en ny instruktion avseende peronuppgiftsbehandlingen

Regionens revisorer

som i allt väsentligt hanterar dessabrister. Dock är det fortsatt en brist att detta inte fanns på plats redan vid driftsättningen.

Avseende huruvida ändamålsenliga tester av systemet har genomförts bedömer vi att de krav som finns i allmänna råd och vägledningar är uppfyllda. Däremot är det **en brist** att test- och granskningsresultaten inte är tillfredsställande och inte heller åtgärdade innan systemet driftsattes. Avseende ändamålsenlig planering för uppföljning av leverantör och avtal har regionen, genom villkor i avtalen, skapat formella förutsättningar för att kunna följa upp leverantören och leveransen. Mot bakgrund av att uppföljningar genomförts redan innan driftsättning bedömer vi det som rimligt att det vid tiden för granskningen inte finns tidsatta planer för uppföljning.

Avslutningsvis bedömer vi att Region Norrbotten, genom relativt omfattande utbildningsinsatser, har skapat goda förutsättningar för att användarna ska ha kunskap om säker hantering av information. Det är också fördelaktigt att informationssäkerhet har integrerats i utbildningen. Granskningen visar att regler, rutiner och vägledningar har arbetats fram och godkänts av en för detta avsedd gruppering, och därefter kommunicerats inom verksamheten. Det är tydligt att det funnits en systematik för arbetssättet.

För att utveckla granskningsområdet lämnas följande **rekommendationer** till regionstyrelsen:

- Säkerställa att riskanalyser avseende informationssäkerhet, konsekvensbedömningar avseende dataskydd samt lämplighetsbedömningar avseende sekretess, påbörjas i ett tillräckligt tidigt skede i framtida upphandlingar och införanden av IT-system och -tjänster,
- Säkerställa att de höga risker som inte kunnat reduceras innan driftsättning, snarast följs upp och åtgärdas,
- Säkerställa att de handlingsplaner (inklusive ytterligare tester och fortsatta externa granskningar av leverantören) som överlämnas från projektet till förvaltningen av vårdinformationssystemet genomförs,
- Säkerställa att slutgiltiga beslut avseende beslut om driftsättning, fastställande av riskanalyser, lämplighetsbedömning och liknande motiveras skriftligt.

Revisorerna överlämnar härmed granskningen för kännedom och yttrande från regionstyrelsen senast 2025-09-24.

För Region Norrbottens revisorer

Krister Hammarbergh
Revisionens ordförande

Bjarne Hald
Förtroendevald revisor

Bilaga: Revisionsrapport ” Granskning av införande av nytt vårdinformationssystem”, PwC, Januari 2025.

Deltagare

KRISTER HAMMARBERGH Sverige

Signerat med Svenskt BankID

2025-02-18 12:46:51 UTC

Undertecknare

Datum

Namn returnerat från Svenskt BankID: Hans Krister Hammarberg

Krister Hammarbergh

Leveranskanal: E-post

BJARNE HALD Sverige

Signerat med Svenskt BankID

2025-02-20 09:01:27 UTC

Undertecknare

Datum

Namn returnerat från Svenskt BankID: BJARNE NIELSEN HALD

Bjarne Hald

Leveranskanal: E-post