Utdrag ur Regionstyrelsens svar 2024-04-10 § 84

Svar på revisionsrapport ”Granskning av informationssäkerhet - uppföljning och skyddade personuppgifter”

Regionens revisorer har i brev den 20 december 2023 bett om regionstyrelsens kommentarer och synpunkter på revisionsrapporten ”Granskning av informationssäkerhet – uppföljning och skyddade personuppgifter”.

Granskningen utgår från nio revisionsfrågor vilka berör rutiner, uppföljning och övrig hantering av skyddade personuppgifter. Revisionen redovisar även en bedömning om tillräckliga åtgärder har vidtagits med anledning av de rekommendationer som lämnades i en tidigare revisionsrapport (från 2019).

I det följande kommenteras i första hand de konkreta rekommendationer som lämnas till regionstyrelsen. I en avslutande del lämnas också några påpekanden och synpunkter när det gäller uppföljningen av den granskning som genomfördes 2019.

Den kan inledningsvis noteras att skyddade personuppgifter förekommer i ett stort antal system inom regionens verksamhet. Förekomsten av sådana uppgifter är inte begränsade till olika vårdstöds- och patientinformationssystem. Regionen har också anställda medarbetare med skyddade personuppgifter. Det innebär i sin tur att regionens styrning och kontroll av skyddade personuppgifter omfattar informationssystem för både patienter och egen personal.

Rapporten konstaterar att regionstyrelsen (och hälso- och sjukvårdsnämnden) har säkerställt att ändamålsenliga styrdokument har upprättats för hanteringen av skyddade personuppgifter. Rapporten rekommenderar här att en uppföljning ska göras av lokala rutiner och att dessa utgår från de regiongemensamma strukturerna. Regionstyrelsen har i huvudsak ingen annan uppfattning – det är centralt att regiongemensamma styrdokument följs och tillämpas på verksamhets- och enhetsnivå.

Regionen har, som nämnts ovan, ett stort antal system, där individer med skyddade personuppgifter förekommer, och det åligger samtliga så kallade förvaltningsobjekt att utfärda och se till att lokala rutiner tillämpas. Den långsiktiga ambitionen ska vara att alla sådana objekt ska föras in i en förvaltningsplan. Därutöver gäller att varje berörd linjechef i regionens organisation kan ta sitt ansvar för att vid behov upprätta lokalt anpassade rutiner.

Mot denna bakgrund behöver det finns ett ändamålsenligt stöd för att detta lokala ansvar ska kunna tas. Regionstyrelsen bedömer att flera initiativ har tagits och planeras för att understödja en sådan utveckling. Ett exempel gäller granskningens rekommendationen att säkerställa och följa upp en regiongemensam struktur för riskanalyser avseende hantering av skyddade personuppgifter. En ny rutin – med den inriktningen – har fastställts under 2023 (765501).

I granskningen anförs vidare att regionstyrelsen bör säkerställa en struktur för förankring av styrdokument och rutiner på området. Regionstyrelsen bedömer att det finns en ändamålsenlig struktur på plats för förankring av styrdokument inom ramen för systemen med Oktav och Platina. Det som kan förbättras är spridningen och kännedomen om förekommande styrdokument. I detta avseende är eventuella brister inte först och främst en ”strukturfråga”, utan mer av en tillämpningsfråga. Frågeställningen hänger därmed samman med nästa rekommendation som avser uppföljningen av personalens kunskap kring gällande regelverk och vem som ansvarar för att uppföljning genomförs. Regionstyrelsen uppfattar att dessa två rekommendationer till övervägande del i grunden handlar om utbildning.

Regionstyrelsen vill här, i likhet med granskningen, notera att utbildningsplattformen Kompass är under uppbyggnad. Avsikten under 2024 är att föra in utbildning i

informationssäkerhet i plattformen, vilket kommer ge förutsättningar för uppföljning av vilka enheter och medarbetare som har genomgått utbildning.

Rapporten rekommenderar att en utredning bör genomföras för att se över behovet av obligatorisk utbildning om informationssäkerhet och skyddade personuppgifter. Regionstyrelsen bedömer att ett obligatorium inte är ändamålsenligt, åtminstone inte i dagsläget.

Ett skäl är att det råder stora variationer mellan olika enheter inom regionens organisation, när det gäller i vilken utsträckning som skyddade personuppgifter hanteras. Inom delar av hälso- och sjukvårdsorganisationen förekommer sådan hantering relativt frekvent medan det inom andra enheter i stort sett inte förekommer alls. Lokala anpassningar ur utbildningssynpunkt är mot denna bakgrund nödvändigt.

Det ska också noteras att det redan finns utbildningsmöjligheter, material och kompetens att tillgå för verksamheter via informationssäkerhetsorganisationen. Införandet av Kompass kommer ge möjligheter – helt i enlighet med rapportens rekommendationer – att säkerställa att alla medarbetare genomgår utbildning med lämpliga intervall. Det blir mot denna bakgrund en viktig uppgift att säkerställa att utbildningsplattformen kan införas på ett bra sätt och fånga upp kvarvarande utbildningsbehov.

Regionstyrelsen delar rapportens rekommendation om att säkerställa att riktlinjer för hanteringen av skyddade personuppgifter tas fram och att efterlevnaden till sådan riktlinjer följs upp systematiskt. Den lokala anpassning och tillämpning som granskningen efterfrågar, kan understödjas av en sådan riktlinje. Ett uppdrag med denna innebörd ges därför till regiondirektören med återredovisning senast i september 2024.

Regionstyrelsen ser också – mot bakgrund av flera av granskningens rekommendationer – att det finns skäl att informera brett om den regiongemensamma struktur som finns, de krav som finns på linjechefer samt de utbildningsmöjligheter som finns. Regionstyrelsen kommer, mot denna bakgrund, att uppdra åt regiondirektören att under innevarande år genomföra en informationsinsats i linjeorganisationen.

Granskningen ställer och besvarar revisionsfrågan: har tillräckliga åtgärder vidtagits med anledning av de rekommendationer som lämnades i 2019 års revisionsrapport?

Regionstyrelsen bedömer att ett omfattande arbete med ledningssystem och organisation har genomförts sedan 2019. Processer för informationssäkerhet är dokumenterade inklusive ansvarsområden och arbetsuppgifter. När det gäller utbildning och främjande av en god säkerhetskultur ser regionstyrelsen ett behov av förbättringar. Införandet av utbildningsplattformen Kompass, är som nämnts ovan, ett viktigt utvecklingssteg, som behöver följas upp under kommande år.

I rapporten (avsnitt 5) behandlas frågan om tillräckliga åtgärder har vidtagits med anledning av de rekommendationer som lämnades i 2019 års revisionsrapport. I rapporten tabellförs rekommendationerna jämte bedömningar om rekommendationerna har åtgärdats i sin helhet, delvis eller inte alls.

Regionstyrelsen delar uppfattningen att flera av rekommendationerna är föremål för ett pågående arbete (varav ett urval har beskrivits närmare ovan – det gäller inte minst de rekommendationer som en koppling till utbildning och uppföljning). Frågan om central behörighetshantering är åtgärdad via utvecklingen av det nya journalsystemet Cosmic. Ett IGA-verktyg för central behörighetsanskaffning är införskaffat och IT-verksamheten bedriver ett införandeprojekt.

I rapporten påpekas särskilt att det saknas ett aggregerat riskregister. Här uppfattar regionstyrelsen att organisationen arbetar mer riskbaserat än tidigare. Risker och incidenthändelser dokumenteras och lagras – delar av det arbete som efterfrågas har utförts och pågår också inom ramen för utveckling och implementering av IMS, som är systemet som ska hantera risker. För närvarande har piloter med ett urval av förvaltningsobjekt utförts – bedömningen är här att systemet kommer tillgängliggöras för alla verksamheter som har behov under innevarande år (2024). Utbildning och användarhandledning kommer att erbjudas.

Rekommendationen att införskaffa en Siem-lösning bedöms i rapporten som ej åtgärdad. En sådan lösning ger kapacitet att samla in och aggregera ett stort antal säkerhetsloggar. Behov och förslag finns utredda och rekommenderade dels inom ramen för två externa utredningar och dels via en internt genomförd utredning 2020. Regionstyrelsen ser det som angeläget att frågan kan ges en lösning som medger att lagstiftningens krav kan tillgodoses genom en central logghanteringslösning. Regionstyrelsen avser att besluta om ett uppdrag med den innebörden.

Slutligen rekommenderas att den geografiska spridningen av regionens serverhallar utökas för att säkerställa redundans. Regionledningsförvaltningens IT-verksamhet kommer prioritera en förstudie kring frågan under 2024. Regionstyrelsen ser, mot den bakgrunden, ingen anledning att vidta ytterligare åtgärder.

REGIONSTYRELSEN

Glenn Nordlund
Ordförande

Åsa Bellander
Regiondirektör