

Handläggare  
Anders Nordmark

Datum  
2022-11-22

Diarienummer  
HSN/224556

Ert Datum  
2022-06-15

Er beteckning  
Rev/22002

Regionens revisorer

## **Svar på revisionsrapport om Granskning gällande hantering av skyddade personuppgifter**

Hälso- och sjukvårdsnämnden vill avge följande svar på rubricerad revisionsrapport.

Revisorerna bedömer sammanfattningsvis att styrelse och nämnder inte i tillräcklig omfattning säkerställt intern styrning och kontroll vid hantering av skyddade personuppgifter. Även om det finns ett antal styrande dokument som i huvudsak bedöms utförliga, behövs utförligare, regionövergripande och verksamhetsspecifika beskrivningar baserade på inventerade riskmoment. Riktlinjerna bör enligt revisorerna vara fastställda av regionstyrelse och nämnder – inte som idag av chefsfunktioner.

Det finns enligt revisorerna risker av allmän karaktär som gäller hela regionen, exempelvis extern kommunikation med myndigheter, ändamålsenliga systemstöd, telefonkontakt med privatpersoner, avvikelshantering, brister i informationsspridning av styrande dokument till medarbetare samt rutiner för hantering av medarbetare med skyddade personuppgifter. Vidare finns verksamhetsspecifika risker som är unika för varje situation.

Revisorerna uppmärksammar kompetens och kunskapsspridning som särskilda utvecklingsområden. Medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter bör stärkas genom obligatoriska utbildningar, eftersom den mänskliga faktorn identifierats som en stor risk i sammanhanget.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån genomförd risk- och konsekvensanalys. Regionstyrelsen och granskade nämnder har därmed inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontrollerar att rutinerna efterlevs. Avvikelse systematiseras och aggregeras inte för att åtgärda brister vid hantering av skyddade personuppgifter.

*Revisorerna rekommenderar regionstyrelsen att, utifrån sitt ansvarsområde, tillse att det genomförs risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov lyfta in bedömda risker i internkontrollplanen.*

Datum  
2022-11-22

Diarienummer  
HSN/224556

Även om det i praktiken till viss del har genomförts risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter, saknas systematiska och dokumenterade sådana analyser. Enligt regionens övergripande riktlinje för skyddade personuppgifter ska hälso- och sjukvården, kollektivtrafiken, kultur- och bildning, HR-avdelningen samt patientnämndens verksamhet göra en egen riskbedömning av de skyddade personuppgifter som behandlas; motsvarande gäller skyddade personuppgifter avseende förtroendevalda. Riktlinjen kan behöva kompletteras med tydligare rutiner för risk- och konsekvensanalyser. Redovisning av risker vid hantering av skyddade personuppgifter bör vara en del av internkontrollplanen för år 2023.

*Revisorerna rekommenderar regionstyrelsen att tillse att det genomförs en översyn av de styrande dokumentens klassificering och beslutshierarki avseende skyddade personuppgifter i syfte att säkerställa att styrelse och nämnder fastställer riktlinjerna.*

Regionstyrelsen ansvarar för strategiska frågor om informationssäkerhet samt för gemensam struktur och samordning av regionens ledningssystem. Styrelsen är vidare personuppgiftsansvarig för behandlingar av personuppgifter som sker i styrelsens verksamhet. Mot bakgrund av att riktlinjer som huvudregel enligt fullmäktigebeslut inte ska beslutas på chefsnivå i förvaltningen och att hanteringen av skyddade personuppgifter berör bland annat invånare, anser styrelsen det rimligt att riktlinjer på området fastställs av styrelse och nämnder. Rörande hälso- och sjukvårdsnämndens område så hanteras inom hälso- och sjukvården hela tiden känsliga personuppgifter där flertalet av dessa har motsvarande skyddsstatus som ”skyddade personuppgifter”. En konsekvens av detta vore att det blir stora svårigheter att dra gränsen för vilka dokument som ska fastställas politiskt och vilka som kan hanteras inom tjänstemannaorganisationen. Styrande dokument kring hantering av personuppgifter alla kategorier bör fortsatt hanteras inom tjänstemannaorganisationen.

*Revisorerna rekommenderar regionstyrelsen att tillse att det genomförs obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument avseende skyddade personuppgifter samt avvikelshantering, erfarenhetsanalys och i praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.*

Enligt regionens övergripande riktlinje för skyddade personuppgifter ska de medarbetare som hanterar sådana uppgifter årligen erbjudas internutbildning i dessa frågor. Kansliavdelningen ansvarar för utbildningen, som ska publiceras i Utbildningsplattformen. Eftersom en säker hantering av skyddade personuppgifter kräver att medarbetarna har goda kunskaper om regelverket, bör utbildningen bli obligatorisk för personal som hanterar skyddade personuppgifter. Specifikt gällande hälso- och sjukvårdens personal är hantering av personuppgifter, inklusive de skyddade, att betrakta

Datum  
2022-11-22

Diarienummer  
HSN/224556

som ett föreskrivet kompetensområde och alla medarbetare har en hög kunskapsnivå kring detta. Regelbunden upprepning årligen i samband med till exempel APT bör räcka som metod.

*Revisorerna rekommenderar regionstyrelsen att tillse att det övervägs att inrätta "compliancefunktion/-er", det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp. Detta för att hanteringen av skyddade personuppgifter ska vara prioriterat i regionens verksamheter.*

Enligt regionens övergripande riktlinje för skyddade personuppgifter ska kansliavdelningen utse en medarbetare med uppgift att följa upp att regionen arbetar strategiskt med hantering av skyddade personuppgifter i enlighet med kraven i riktlinjen angående IT-stöd, utbildning och riktlinjer inom verksamheterna. Hälso- och sjukvårdsnämnden noterar därmed att det alltså redan ska finnas en sådan funktion och ska överväga om funktionens roll och arbetsuppgifter behöver utvecklas och/eller tydliggöras.

*Revisorerna rekommenderar regionstyrelsen att tillse att det genomförs penetrationstester av IT-system och rutiner för att identifiera sårbarheter och skadeförlopp vid intrång.*

Regionstyrelsen ska överväga i vilken utsträckning penetrationstester av IT-system och rutiner bör genomföras och avser därefter att eventuellt komplettera styrande dokument med relevanta krav på sådana tester.

*Revisorerna rekommenderar regionstyrelsen att tillse att det genomförs systematiska loggkontroller i samtliga systemstöd i syfte att säkerställa att obehöriga inte kan få tillgång till skyddade personuppgifter.*

Systematiska loggkontroller kan inte säkerställa att obehöriga inte får tillgång till skyddade personuppgifter men bidrar till att sådana incidenter uppdagas och har också en avhållande effekt på personal som annars kan frestas ta del av personuppgifter utöver sin befogenhet. Inom hälso- och sjukvården finns lagkrav att vårdgivaren ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt patientuppgifter i systemen (4 kap. 3 § patientdatalagen). Styrelsen ska utreda vilka systemstöd i övrigt som ska prioriteras för genomförande av sådana loggkontroller. Inom hälso- och sjukvårdsnämndens ansvarsområde finns önskemål om utökad utveckling av befintligt systemstöd för "intelligent" logguppföljning. Resurs- och ekonomisk fråga årligen i verksamhetsplaneringen. Region-IT:s avsatta resurs för utökad stöd inom detta område behöver förstärkas.

*Revisorerna rekommenderar regionstyrelsen att tillse att det sker uppföljning av incidenter och avvikelser samt att avvikelshanteringen avseende skyddade personuppgifter stärks.*

Datum  
2022-11-22

Diarienummer  
HSN/224556

Regionstyrelsen noterar att det, enligt revisionsrapporten, inte finns några rapporterade avvikelser alls avseende skyddade personuppgifter. Det behöver givetvis inte innebära att avvikelser inte förekommit men tyder ändå på att avvikelser inte sker i större omfattning. Dock finns det anledning för styrelsen att följa upp att avvikelser avseende skyddade personuppgifter – liksom avvikelser generellt – rapporteras på korrekt sätt i regionens system för avvikelshantering. Inom hälso- och sjukvårdsnämndens ansvarsområde är avvikelssystemet väl implementerat och hanteringen systematiserad. Möjlighet att filtrera fram avvikelser kring skyddade personuppgifter bör finnas. Ingenting tyder på att avvikelser inom detta område inte skulle rapporteras.

Avslutningsvis konstaterar regionstyrelsen och hälso- och sjukvårdsnämndens att behandling av personuppgifter inom regionen till största delen avser uppgifter om patienter och patienters närstående inom hälso- och sjukvården. Även behandling av skyddade personuppgifter sker till övervägande del inom hälso- och sjukvården. Uppgifter om patienter och deras närstående skyddas alltid av stark sekretess enligt 25 kap. 1 § offentlighets- och sekretesslagen – det vill säga samma sekretess som gäller vid skyddad folkbokföring. Det innebär att IT-system och administrativa rutiner på detta område alltid måste uppfylla höga krav på säkerhet, oavsett om personuppgifterna är skyddade eller inte. Inom övriga delar av regionens verksamhet är offentlighet huvudprincip, vilket innebär en betydligt större risk för röjande av skyddade personuppgifter – ett förhållande som medför särskilda krav på åtgärder som ger en säker hantering av skyddade personuppgifter. Hälso- och sjukvårdens verksamheter är vana vid dessa kravställningar och försöker beakta som grundläggande krav vid upphandlingar att särskilt markera i systemen förekomst av skyddade personuppgifter, men många leverantörer har inte sådant stöd. Kraven på IT-system bör tydligare nationellt formuleras inom detta område om det ska kunna få genomslag.

Hälso- och sjukvårdsnämnden

Marianne Utterdahl  
Ordförande hälso- och sjukvårdsnämnden

Lena Gjevert  
Hälso- och sjukvårdsdirektör