Patientnämndsenheten
Lena Bäckman

Datum	**Vår beteckning**
2022-10-0512-20	PN/220941
Ert Datum	**Er beteckning**
2022-12-08	Rev/22002

Regionens revisorer

Svar på revisionsrapport om Granskning gällande hantering av skyddade personuppgifter

Patientnämnden 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, avvikelsehanteringen, 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. Avvikelser 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.

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.

Särskilt om patientnämndens arbete

Patientnämnden har utifrån Region Värmlands riktlinje arbetat fram en rutin (Skyddade personuppgifter RUT 23577). Inför framtagandet har varje steg i ärendehanteringen av inkomna ärenden till patientnämndsenheten identifierats och riskbedömts och skapar därmed ett underlag till rutinen. Rutinen har nu även kunnat testas i skarpt läge då tre ärenden där patienten har skyddad identitet inkommit till patientnämndsenheten, två små justeringar har identifierats och därmed ändrats.

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.

Revisorerna rekommenderar regionstyrelsen att tillse att det genomförs obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument avseende skyddade personuppgifter samt avvikelsehantering,

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. Styrelsen anser det dock inte motiverat att göra utbildningen obligatorisk för samtliga anställda, utan bedömer att det är tillräckligt att övriga erbjuds utbildningen.

Särskilt om patientnämndens arbete

Patientnämndsenheten är en liten enhet med få personer som hanterar ärenden, färre personer bidrar ökad säkerhet i hanteringen. Hantering av skyddade personuppgifter ingår i introduktionen av nya medarbetare och är därefter en fråga som tas upp i samband med genomgång av ärenden samt uppföljning av enhetens rutiner.

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. Styrelsen 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 skadekonsekvenser 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.

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

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 avvikelsehantering.

Avslutningsvis konstaterar regionstyrelsen 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.

Region Värmland

Datum	Diarienummer
2022-12-08	PN/220941

Särskilt om patientnämndens arbete

Patientnämnden har till dags dato inga klagomål från patienter och anhöriga som gäller röjda skyddade personuppgifter inom hälso – och sjukvård samt tandvård.

Patientnämndsenhetens ärendehanteringssystem Platina möjliggör kategorisering av olika ärendetyper Klagomål gällande röjda skyddade personuppgifter ska kategoriseras under kategorin bruten sekretess. Dessa ärenden är på så sätt sökbara och kan tas fram ur systemet. Systemet möjliggör även fritextsökning. Patientnämnden har i uppdrag att analysera inkomna klagomål för att identifiera brister inom hälso – och sjukvården samt tandvården. I arbetet med analyser och rapporter läser handläggaren klagomålen från patienter och närstående vilket i sig ytterligare ökar vetskapen om de ärenden som inkommer till patientnämndsenheten.

Patientnämnden

Håkan Axelsson
Ordförande patientnämnden

Lena Bäckman
Enhetschef patientnämndsenheten