Bilaga Regionstyrelsens svar på fördjupad granskning nr 20/2023 Regionens hantering av skyddade personuppgifter

Regionstyrelsen har tagit del av revisorernas rapport och rekommendationer gällande hantering av skyddade personuppgifter.

Rapporten besvaras enligt följande

1.Upprätta ett regionövergripande styrdokument som är specifikt inriktat på hanteringen av skyddade personuppgifter. Ett sådant styrdokument, exempelvis i form av en riktlinje, bör omfatta inriktningen för arbetet av både regionens vårdtagare och dess medarbetare på en strategisk nivå.

Styrande information inom specifika verksamheter och system finns framtaget. Övergripande styrning för skyddade personuppgifter är under framtagande. Detta samordnas av informationssäkerhetsfunktionen.

2. Säkerställa att verksamheterna genomför risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.

Idag finns styrning gällande risk- och konsekvensanalyser inom olika områden, bland annat informationssäkerhet. Där beskrivs att riskanalysen ska ta hänsyn till den informationssäkerhetsklassning som genomförts. Handlingsplan utifrån informationssäkerhetsklassning berör patienter med skyddade personuppgifter samt att personuppgifter ska skyddas i enlighet med gällande författningar.

Övergripande behovs- och riskanalys för behörighetstilldelning lyfter specifikt fram skyddade personuppgifter som ett område att analysera. Den övergripande behovs- och riskanalysen kommer att ärvas ner till de specifika behovs- och riskanalyser som då också ska genomföras inom vårdverksamheterna.

Regionstyrelsen avser att förtydliga styrningen för risk- och konsekvensanalyser för att säkerställa att perspektivet beaktas där området behöver analyseras, detta implementeras i styrning avseende riskanalyser kopplat till informationssäkerhet och dataskydd. Om och på vilket sätt detta ska följas upp i internkontrollplanerna är något som utreds i nästa steg.

3. Säkerställa att verksamheterna utifrån ovanstående analys upprättar egna rutiner för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Säkerställ också att verksamheternas arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.

När behov finns att skapa verksamhetsspecifika dokument ska dessa implementeras i enlighet med principerna för regionens kvalitetsledningssystem, vilket inkluderar

implementering, kommunikation och uppföljning, som en del av den ordinarie ledningen och styrningen.

4. Säkerställa att verksamheterna genomför obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument och arbetsrutiner regelbundet.

Idag utbildas personal i arbetsmoment inom deras arbetsområden. För att möjliggöra stöd för uppföljning av utbildning ger Regionstyrelsen informationssäkerhetsfunktionen i uppdrag att ta fram särskilt avsnitt om skyddade personuppgifter i regionens övergripande utbildning om säkerhetsmedvetenhet och säkert beteende. Det är en utbildning som riktar sig till alla inom Region Västerbotten, och uppföljning kan då genomföras i regionens lärplattform.

5. Säkerställa att verksamheterna genomför kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.

Rutiner för systematiska loggkontroller finns för vårdsystem och detta följs årligen upp i patientsäkerhetsberättelsen. Egenkontrollsfrågor om systematiska loggkontroller har skickats ut till berörda verksamhetschefer.

I övrigt finns styrning kring loggning i alla våra systemstöd, där åtkomst till känslig information, inklusive ändring och radering ska loggas. Även beskrivning för hur hantering av kontroll av tekniska loggar för enskilda användare genomförs framgår.

6. Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.
I samband med dataskyddsombudets granskningar och rapporter har information om status inom fokusområden såsom bland annat personuppgiftsincidenter inhämtats och följts upp.

Regionstyrelsen avser förtydliga styrning avseende hantering av personuppgiftsincidenter för specifikt skyddade personuppgifter genom att komplettera befintligt stöd med att specifikt lyfta fram hantering av incidenter kopplat till skyddade personuppgifter. Detta samordnas av informationssäkerhetsfunktionen.

Regionstyrelsen följer upp alla beskrivna åtgärder om ett år.