Hälso- och sjukvårdsnämnden 2023-05-22 HSN 914-2023

Hälso- och sjukvårdsnämndens svar på revisionsrapport avseende arbetet med GDPR, informationssäkerhet och IT-säkerhet

Svar på revisionsrapport avseende granskning av Hälso- och sjukvårdsnämndens arbete med GDPR och informationssäkerhet och IT-säkerhet

Rapporten besvaras enligt följande.

Efterlevnad av GDPR

- *Revisorerna anser att styrelsen ska tydliggöra hur dataskyddsarbetet ska organiseras och genomföras i regionen. Dataskyddsarbetet bör utgå från ett övergripande styrdokument för GDPR, tydlig ansvarsfördelning och dokumenterade rollbeskrivningar. Tydliggör vilket stöd och vilka resurser som finns för informationssäkerhetsansvarig och dataskyddsombud.*

Regionen har tagit fram en ny struktur för dataskyddsarbetet som har fastställts i ledningssystemet, se riktlinjen Struktur för dataskyddsarbetet. Av den riktlinjen framgår rollerna inom dataskyddsarbetet där ansvarsområden tydliggörs. Dataskyddombudet arbetar deltid som dataskyddombud och deltid som regionjurist. Informationssäkerhetssamordnaren har en heltid på informationssäkerhetsområdet. Det finns ett internt nätverk för dataskydd- och informationssäkerhet med kompetenser inom informationssäkerhet, dataskydd, juridik och IT-säkerhet, cybersäkerhet och beredskap. Nätverket har återkommande träffar, syftet är att utgöra en expertgrupp och samordna frågor på området.

- *Revisorerna anser att styrelsen skall säkerställa att styrdokument är aktuella över tid och kända bland verksamheterna samt säkerställa att anställda har tillräcklig kunskap i dataskyddsarbetet genom regelbundna utbildningar.*

Utbildningar kommer att genomföras två gånger per år inom området GDPR. De utbildningarna som genomfördes under hösten 2022 riktade sig till personer med särskilt ansvar för personuppgifter samt personuppgiftshandläggare. Tanken är att personuppgiftshandläggaren skall ta tillbaka den kunskapen till enheten och sprida denna vidare. Verksamhetscheferna är ansvarig för att de styrande dokumenten är kända i verksamheten och att de anställda har tillräcklig utbildning.

- *Revisorerna anser att styrelsen ska säkerställa tillräcklig uppföljning och kontroll av verksamheternas hantering av personuppgifter och att policyer, riktlinjer och rutiner följs.*

Dataskyddsombudet har presenterat en kontrollplan för året 2023 samt en granskningsrapport för 2022. I kontrollplanen ingår bland annat att följa upp

styrande dokument och följsamhet till dessa. Syftet med detta är att verksamheterna själva skall systematiskt följa upp arbetet med GDPR.

Informations-och IT-säkerhet

- *Se över organisationen för arbetet med IT-och informationssäkerhet. Säkerställ en tydlig ansvarsfördelning.*

Arbetet med organisation för information, IT och cybersäkerhet samt dataskydd är ett pågående arbete då vi nu fått flera centrala roller på plats, det har fastställts ett nätverk för dataskydd- och informationssäkerhet. Regionen arbetar nu med att skapa ett gemensamt arbetssätt och struktur för arbetet. Informationssäkerhetssamordnarrollen har nu tillsatts och till skillnad från tidigare har denne inte rollen som Dataskyddsombud, vilket innebär utökade resurser. En central del är att beskriva och säkerställa en tydlig ansvarsfördelning för informationssäkerhetsarbetet, vilket delvis har påbörjats i och med framtagande av beskrivning av dataskyddsorganisationen och inom riktlinjen för informationssäkerhet – förvaltning och drift, men roller, ansvar och mandat avser regionen förtydliga.

I de övergripande riktlinjerna för informationssäkerhet finns informationssäkerhetsansvaret dokumenterat kopplat till linje och till objektsförvaltning. Verksamhetscheferna är ansvarig för informationssäkerheten inom sin verksamhet och objektägarna ansvarar för säkerheten i systemen och att det finns kontinuitetsplaner för dessa. Vad gäller information inom hälso- och sjukvården har hälso- och sjukvårdsförvaltningen utsett en informationsägare, som ansvarar för att säkerställa att information skyddas på avsett sätt.

- *Inför en standardiserad process för att identifiera risker inom IT-och informationssäkerhet.*

Framtagande av en standardiserad process för att genomföra riskanalyser inom information- IT och cybersäkerhet har utvecklats i arbetet med övergripande riskanalysen för informationssäkerhet där regionen tagit fram en grund för en process som ska utvecklas.

Regionstyrelsen har tagit fram en standardiserad process för övergripande riskanalys som bygger på befintliga genomföra riskanalyser i verksamheten. Regionstyrelsen planerar att ta fram ett stöd och struktur för att identifiera, hantera och aggregera informationssäkerhetsrisker för att förbättra säkerhetsåtgärderna för våra informationstillgångar. Här avses det implementeras informationssäkerhetsperspektiv i befintlig struktur för riskanalyser samt förtydliga styrande information kopplat till processen och

beslutsstrukturen för att vidta åtgärderna. Riskanalysen för 2022 är beslutad och åtgärdsplan för riskerna finns framtagen för arbetet framåt.

- *Säkerställ att styrdokument är aktuella över tid och kända bland verksamheterna. Säkerställ att anställda får tillräcklig utbildning inom IT-och informationssäkerhet*

Ansvar och roller är en del för att säkerställa ett systematiskt informationssäkerhetsarbete, en annan del handlar om vår överenskomna dokumenterade information, som fastställs, synliggörs, följs upp och utvecklas. Det pågår ett arbete med att följa upp vår dokumenterade information för att identifiera behov av utveckling och säkerställa att vi har den nivå av dokumenterad information som behövs. En del av ledningssystemet är att kommunicera gällande information till berörda personer genom exempelvis kommunikations- och utbildningssatsningar. Detta hänger också ihop med ovanstående rekommendation om att skapa en standardiserad process för att identifiera risker, då det är en del i att öka säkerhetsmedvetandet.

- *Säkerställ tillräcklig uppföljning och kontroll av verksamheternas arbete med IT och informationssäkerhet och att policyer, riktlinjer och rutiner följs.*

Årligen görs en informationssäkerhetsberättelse som följer upp verksamheternas arbete med informationssäkerhet på vissa områden.

Regionen ska fortsätta utveckla sitt ledningssystem för informationssäkerhet med dess komponenter, där kontroll och uppföljning av verksamheternas informationssäkerhetsarbete är en av delarna. Den ena delen av kontroll och uppföljning handlar om att följa upp verksamheternas kontinuerliga informationssäkerhetsarbete. Hur uppföljningsstrukturen ska utvecklas är i en pågående utredningsfas, och det planeras att ta fram en ännu tydligare struktur för detta. Den andra delen handlar om kontroll och uppföljning av implementationen av säkerhetsåtgärderna i objektens arbete, för att utgöra stöd och struktur för verksamheternas arbete. Detta kommer att kopplas till och följas upp i objektplanerna.