Tjänsteutlåtande

2025-08-21 K 2025-4576

Nämnden för Karolinska Universitetssjukhuset

P19. Remissvar gällande Riktlinje för informationssäkerhet samt dataskydd, RS 2025-0418

Ärendebeskrivning
Regionstyrelsen har skickat en remiss avseende uppdaterad riktlinje för informationssäkerhet samt dataskydd inom nämnder och bolag.

Beslutsunderlag
Karolinska Universitetssjukhusets tjänsteutlåtande.

Förslag till beslut
Nämnden för Karolinska Universitetssjukhuset beslutar
att som svar på regionstyrelsens remiss godkänna reviderat förslag till yttrande avseende Riktlinje för informationssäkerhet samt dataskydd, RS 2025-0418.

Förvaltningens motivering till förslaget

Detta utlåtande utgör Karolinska Universitetssjukhusets svar på remissen och innehåller en bedömning av dokumentets utveckling i förhållande till tidigare version.

Övergripande inriktning för uppdaterade riktlinjer för informationssäkerhet och dataskydd är att göra ansvarsfördelningen tydligare, stärka den juridiska grunden och förbättra språket så att det blir enklare att förstå och använda i praktiken.

En viktig förbättring är att begreppet riskbedömning har preciserats. I stället för att endast revidera riskanalyser vid "väsentliga förändringar", föreslås att revidering ska ske vid alla förändringar som kan påverka informationssäkerheten eller dataskyddet. Detta ger en mer proaktiv och riskbaserad styrning, i linje med NIS-lagens krav. Vidare förtydligas att riskanalysen ska omfatta både identifiering och bedömning av risker i relation till verksamhetens mål, vilket stärker kopplingen mellan informationssäkerhet och verksamhetsstyrning.

Ansvarsfördelningen inom nämnder och bolag har också förtydligats. Förvaltningschef eller VD ges ett tydligt övergripande ansvar, medan informationssäkerhetssamordnaren får ett mer definierat mandat att både samordna arbetet och rapportera allvarliga avvikelser direkt till högsta ledningen. Detta kompletterar den ordinarie rapporteringsstrukturen och säkerställer att viktig information når beslutsfattare i rätt tid. Dataskyddssamordnarens roll har också utvecklats till att innefatta stöd och uppföljning enligt GDPR och interna styrdokument, vilket stärker efterlevnaden av dataskyddsregelverket.

Språkbruket har förbättrats genom att använda juridiskt korrekta och tydliga formuleringar, exempelvis vid beskrivning av ansvarsförbindelser, incidentrapportering och upphandling. Det framgår nu att ansvarsförbindelsen ska vara undertecknad innan tillgång ges till IT-utrustning, och att regionstyrelsen ansvarar för både innehåll och rutiner.

Vid incidentrapportering har det förtydligats att regionen ska informeras parallellt med tillsynsmyndigheter, vilket stärker samordning och kontroll.

Vid upphandling av IT-tjänster eller extern drift har kraven på informationssäkerhet och dataskydd skärpts. Leverantören ska uppfylla dessa krav under hela avtalstiden, och en behovs- och riskanalys ska genomföras innan anskaffning. Detta säkerställer att rätt krav ställs från början och att de följs upp under hela leveransperioden.

Utbildningskravet har också förtydligats: grundläggande utbildning i informationssäkerhet och dataskydd ska genomföras av samtliga medarbetare, men nu med tillägget att utbildningen ska anpassas efter arbetsuppgifter. Detta ökar relevansen och stärker kompetensen i praktiken.

Slutligen har begreppslistan utökats med juridiskt definierade termer såsom personuppgift, riskanalys, skyddsåtgärd och revision. Detta bidrar till en mer enhetlig och korrekt tillämpning av riktlinjerna inom hela organisationen.

Sammanfattningsvis innebär de föreslagna förändringarna att riktlinjerna blir mer tydliga, juridiskt hållbara och praktiskt användbara. De stärker regionens förmåga att hantera informationssäkerhet och dataskydd på ett systematiskt och rättssäkert sätt, i enlighet med både nationell lagstiftning och EU:s dataskyddsförordning.

Ekonomiska konsekvenser
Ingen påverkan

Konsekvenser för patientsäkerhet
Ingen påverkan

Miljö-/arbetsmiljökonsekvenser
Ingen påverkan

Övriga konsekvenser
Ingen påverkan

Facklig samverkan
Ingen påverkan

Christophe Pedroletti
Sjukhusdirektör