REGIONREVISORERNA

Rapport nr 1/2024

# Systematiskt arbete med informationssäkerhet och dataskydd på Karolinska universitetssjukhuset

# Kort om rapporten

Revisonen har granskat det systematiska arbetet med informationssäkerhet samt dataskydd. Revisonens bedömning är att Karolinskas styrning och kontroll av informationssäkerhetsarbetet inte är helt tillräcklig. Sjukhuset har ett ledningssystem som i all väsentlighet svarar mot kraven. Sjukhuset behöver se till att riskanalyser genomförs samt att uppföljningsrutiner implementeras. Karolinska bör även analysera hur sjukhuset ska efterleva kommande ytterligare lagkrav på informationssäkerhet.

Revisionens bedömning är att Karolinskas styrning och kontroll av arbetet med dataskydd är otillräcklig. Karolinska saknar ett samlat register över personuppgiftsbehandlingar, vilket innebär att Karolinska inte har kontroll över sjukhusets personuppgiftsbehandlingar och därmed svårt att efterleva kraven enligt GDPR. Revisionen bedömer även att sjukhuset behöver tydliggöra det operativa ansvaret för dataskydd.

Karolinska behöver enligt revisionens bedömning säkerställa att beslut avseende informationssäkerhet och dataskydd fattas i enlighet med kommunallagen.

Regionrevisorerna

2024-09-19

Diarienummer
RK 2023-0108

Karolinska universitetssjukhuset

# Projektrapport 1/2024
# Systematiskt arbete med informationssäkerhet och dataskydd på Karolinska universitetssjukhuset

Revisorerna i revisorsgrupp II beslutade vid sitt möte den 26 september 2024 att överlämna rapporten till Karolinska Universitetssjukhuset för yttrande senast 2024-12-31.

Revisonens samlade bedömning är att nämnden för Karolinska universitetssjukhusets styrning och kontroll av informationssäkerhetsarbetet inte är helt tillräcklig. Revisionen bedömer att nämnden behöver se till att riskanalyser genomförs samt att uppföljning implementeras. Nämnden bör även analysera hur sjukhuset ska efterleva kommande ytterligare lagkrav på informationssäkerhet.

Revisionens samlade bedömning är att nämnden för Karolinska universitetssjukhusets styrning och kontroll av arbetet med dataskydd är otillräcklig. Revisionen bedömer att nämnden måste säkerställa att nämnden har ett komplett och aktuellt register över personuppgiftsbehandlingar så att kraven enligt GDPR kan efterlevas.

Revisionen bedömer även att nämnden för Karolinska universitetssjukhuset måste säkerställa att nämndens beslut avseende informationssäkerhet och dataskydd fattas i enlighet med kommunallagen.

**Region Stockholm**
Regionrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08 123 100 00
E-post:
regionrevisorerna.rev@regionstockholm.se

Säte: Stockholm
Org.nr: 232100-0016
www.regionstockholm.se

*Besök oss: Hantverkargatan 25B, T-bana Rådhuset, se www.sl.se*

Revisorerna vill särskilt ha svar på hur nämnden för Karolinska universitetssjukhuset avser att:

- säkerställa ett systematiskt och långsiktigt arbete med regelefterlevnad avseende informationssäkerhet och dataskydd.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Annika Sandström
ordförande

Anna Peterson
samordnande administratör (sekr.)

# 1. Slutsatser och rekommendationer

## 1.1. Bakgrund

Karolinska universitetssjukhuset är regionens största vårdgivare. Sjukhuset hanterar betydande mängder känslig information, inklusive personuppgifter av högt skyddsvärde. Om Karolinska brister i sitt arbete med informationssäkerhet innebär det risk för att information förloras, att obehöriga kommer åt journaluppgifter, att verksamhetskritisk information inte finns tillgänglig när den behövs och att osäkerhet om informationens korrekthet kan uppstå. Negativa händelser kan leda till att patientsäkerheten inte kan upprätthållas och att både patienters och personalens integritet äventyras. I förlängningen kan även sjukhusets ekonomi och förtroende skadas.

Karolinska universitetssjukhuset har rekommendationer som revisionen lämnat med anledning av tidigare granskningar av informationssäkerhets- respektive dataskyddsarbete och som ännu inte åtgärdats fullt ut.[1] Bristerna har främst bestått i prioritering av riskanalyser, tydlighet i roller och ansvar, adekvat utbildning av samtliga anställda samt medvetenhet kring områdena inom samtliga verksamheter. Inom ramen för granskningen genomförs även en uppföljning av rekommendationer som avser införandet av det s.k. NIS-direktivet.[2] [3]

Revisionen bedömer att det finns risk för att problemen kvarstår och har mot denna bakgrund låtit granska om Karolinska universitetssjukhuset uppfyller kommunallagens krav på intern kontroll avseende informationssäkerhet och dataskydd, samt om arbetet bedrivs på ett systematiskt sätt och i enlighet med lagstiftning, interna mål och regelverk samt regionfullmäktiges mål.

Granskningen har, under ledning av revisionskontoret i Region Stockholm, genomförts av upphandlad konsult. Granskningen genomfördes under perioden december 2023 - maj 2024. Revisionen har nedan sammanfattat de slutsatser som kan dras och lämnar rekommendationer med anledning av granskningen. Ansvarig projektledare vid revisionskontoret har varit Charlotta Edholm. Konsultens iakttagelser och bedömningar i sin helhet framgår i bilaga. Ansvarig konsult har varit Charlotte Arnell, PwC AB.

## 1.2. Granskningens resultat – informationssäkerhet

Revisonens samlade bedömning är att Karolinskas styrning och kontroll av informationssäkerhetsarbetet inte är helt tillräcklig

Karolinska universitetssjukhuset har riktlinjer och vägledningar för ett systematiskt informationssäkerhetsarbete som i stort svarar mot krav i regionens riktlinjer. Revisionen bedömer att Karolinska skapat förutsättningar för ett effektivt arbete genom att sjukhuset utformat ett ledningssystem för informationssäkerhetsarbetet med beskrivningar av ansvar och processer. Nämnden har informerats om handlingsplanen för informationssäkerhet, men revisionen konstaterar att det är oklart hur den beslutats och att det inte framgår av delegationsordningen hur sådana beslut ska fattas. Revisionen bedömer att det innebär att det finns en risk för att informationssäkerhetsarbetet därmed inte blir en integrerad del av nämndens samlade styrning. Sjukhusledningen behöver vidare försäkra sig om att det i enlighet med regionens riktlinjer finns etablerade kanaler för ansvariga tjänstepersoner att lämna information om informationssäkerhetsavvikelser till ledningen.

[1] Grundläggande arbete med informationssäkerhet, Karolinska universitetssjukhuset samt SLSO, projektrapport 2018 nr 8, RK 2018-0021, 2019-01-29 (informationssäkerhet) samt Delrapport 2018 Karolinska universitetssjukhuset, RK 2018-0032, 2018-10-30 (dataskydd).
[2] Årsrapport 2022 Karolinska Universitetssjukhuset, RK 2022–0024, 2023-03-23.
[3] NIS-direktivet är en EU-förordning som ställer krav på säkerhet i nätverk och informationssystem. Det infördes i svensk lagstiftning 2018.

Ansvaret för informationssäkerhet på sjukhuset följer det delegerade verksamhetsansvaret. Varje person som har ansvar för en verksamhet har också ansvar för att skydda informationen i samma verksamhet. Granskningen visar dock att det bland ansvariga i verksamheten råder en osäkerhet både avseende vem som har det faktiska ansvaret och vad som konkret behöver göras. Det gäller exempelvis för riskanalyser, som i viss utsträckning genomförs, men där revisionens stickprov visar på brister. Revisonen konstaterar sammantaget att sjukhusets styrning inte fått tillräckligt genomslag i det praktiska informationssäkerhetsarbetet.

Revisionen bedömer att Karolinska har en hög genomförandegrad när det gäller informationssäkerhetsutbildningar, men det finns inget krav på upprepning av utbildningen eller fortsättningsutbildning för de roller där fördjupad kunskap behövs. Revisionen bedömer att sjukhuset behöver säkerställa att medarbetarna kan behålla och utveckla en tillräcklig kunskapsnivå över tid.

Granskningen visar att det finns brister i uppföljningen av informationssäkerhetsarbetet inom sjukhuset. Tyngdpunkten i sjukhusets arbete med informationssäkerhet har hittills främst legat på utformning av riktlinjer, snarare än på övervakning och uppföljning av arbetet. Uppföljning sker inom vissa delar av verksamheten, men sjukhuset har haft svårt att nå kontinuitet. Revisionen noterar att Karolinska uppger att det finns svagheter med det verktyg som tillhandahålls av regionen för uppföljning av enskilda system. Revisionen bedömer dock att sjukhuset har ett ansvar för att säkerställa att kontrollen är tillräcklig för att minimera risken för informationssäkerhetsbrister i befintliga system. Revisionen ser positivt på att sjukhuset har gjort en analys av brister i förhållande till NIS-direktivet. Ett nytt NIS-direktiv träder i kraft i början av 2025. Direktivet innebär ytterligare krav på informationssäkerheten.

Genom arbetet med riskanalys och internkontrollplan får nämnden information om bland annat informationssäkerhetsrisker. Nämnden bör dock enligt revisionen överväga behovet av mer systematisk uppföljningsinformation, utöver den kvartalsvisa rapportering som sker till nämnden utifrån internkontrollplanen, för att nämnden ska kunna säkerställa regelefterlevnad i enlighet med kommunallagens krav.

Tidigare lämnade rekommendationer inom informationssäkerhet ersätts av nya, se nedan. Rekommendationerna som rör NIS-direktivet kvarstår.

## 1.3. Granskningens resultat – dataskydd (GDPR)

Revisionens samlade bedömning är att Karolinskas styrning och kontroll av arbetet med dataskydd är otillräcklig.

Karolinska har en omfattande behandling av personuppgifter som en del av sjukhusets arbete med att utföra sitt uppdrag som vårdgivare, forskningshuvudman och myndighet. Eftersom det handlar om känsliga personuppgifter bedömer revisionen att risknivån inom sjukhuset är hög när det gäller dataskydd. Granskningen visar att sjukhuset har en riktlinje som utgör en god utgångspunkt för dataskyddsarbetet, men i övrigt är sjukhusets ramverk för styrning och vägledning begränsat. Riktlinjen är fastställd av chefen för rättskansliet.  Revisionen bedömer dock att riktlinjen bör beslutat av nämnden, eftersom nämnden har ett direkt ansvar för dataskydd.

Sjukhusets delegationsordning saknar beskrivning av hur ett flertal beslut inom dataskydd ska tas, såsom t.ex. riskanalys, konsekvensbedömning och avslag på beslut om utlämning av personuppgifter. Verksamhetschefers mandat att besluta i dataskyddsfrågor är otydligt formulerat och följer enligt revisionens bedömning inte kommunallagen. Granskningen visar att verksamhetschefer i praktiken inte uppfattar vilket ansvar man har. I styrdokumenten är det ofta otydligt vem som ska göra vad. Vidare bör Karolinska som personuppgiftsansvarig utse en företrädare, men revisionen har inte kunnat identifiera vem på Karolinska som har denna roll. Detta innebär att det råder oklarhet om vilken funktion som har det operativa ansvaret för dataskyddsarbetet. Sammantaget bedömer revisionen att roller och ansvar när det gäller dataskydd överlag är otydligt formulerade, vilket enligt revisionens bedömning bidrar till att styrningen inte får avsett genomslag.

Revisionen konstaterar att Karolinska saknar ett samlat register över personuppgiftsbehandlingar, vilket är ett krav enligt GDPR. Därutöver saknas stora delar av sjukhusets personuppgiftsbehandlingar i befintliga register. Personuppgiftsbehandlingar avseende den ordinarie hälso- och sjukvården saknas i princip helt i registren på sjukhuset, vilken även gäller för administrationen inklusive personalhantering. Bristerna i sjukhusets register över personuppgiftsbehandlingar medför att sjukhuset inte heller kan efterleva kraven på risk- och konsekvensbedömningar, även om sjukhuset delvis har riktlinjer på plats. Revisionen noterar att Karolinska har inlett ett arbete med att komplettera registret.

Vidare saknas det rutiner för att säkerställa att registren är korrekta över tid och att data används för rätt syfte. Karolinska saknar en tydlig process för att identifiera och analysera risker relaterade till personuppgiftshantering, vilket är särskilt viktigt när nya system införs. Revisionen noterar vidare en avsaknad av strukturerad dokumentation och rapportering av riskerna.

Revisionen bedömer sammantaget att Karolinska saknar kontroll över vilka personuppgiftsbehandlingar som sjukhuset ansvarar för. Det innebär svårigheter för sjukhuset att leva upp till kraven i GDPR om att kunna redovisa för de som registrerats vilka personuppgiftsbehandlingar de omfattas av, vilket i sin tur utgör en betydande verksamhetsmässig och ekonomisk risk för sjukhuset.

Nämnden erhåller en årsrapport om dataskyddsarbetet samt information vid allvarliga avvikelser, men revisionen bedömer att det inte är tillräckligt för att nämnden ska kunna försäkra sig om att sjukhuset efterlever lagkrav och riktlinjer.

Tidigare lämnade rekommendationer inom dataskydd ersätts av nya, se nedan.

## 1.4. Rekommendationer – informationssäkerhet

Nämnden för Karolinska universitetssjukhuset rekommenderas att:

- fastställa den årliga handlingsplanen på ett korrekt sätt.
- genomföra en analys av Karolinskas status i förhållande till det nya NIS-direktivet och den tillhörande lagstiftning som träder i kraft i början av 2025 i syfte att säkerställa efterlevnad av direktivet.

Ledningen för Karolinska universitetssjukhuset rekommenderas att:

- säkerställa att riskanalyser sker i enlighet med interna regelverk samt lagstiftning.

## 1.5. Rekommendationer – dataskydd

Nämnden för Karolinska universitetssjukhuset rekommenderas att:

- fastställa riktlinjen för behandling av personuppgifter på ett korrekt sätt.
- säkerställa att sjukhuset har ett komplett och aktuellt behandlingsregister.

Ledningen för Karolinska universitetssjukhuset rekommenderas att:

- tydliggöra roller, ansvar och arbetssätt avseende det operativa dataskyddsarbetet.
- komplettera befintlig riktlinje med obligatoriska avstämningspunkter, där riskanalyser och vid behov konsekvensbedömningar blir obligatoriska att genomföra för att exempelvis ett IT-system ska kunna köpas in eller driftsättas.
- säkerställa att riskanalyser och konsekvensbedömningar sker i enlighet med interna regelverk samt lagstiftning.

## 1.6. Rekommendationer – informationssäkerhet och dataskydd

Nämnden för Karolinska universitetssjukhuset rekommenderas att:

- revidera arbets- och delegationsordningen för att återspegla de beslut som är nödvändiga att fatta inom ramen för både informationssäkerhets- och dataskyddsarbetet samt för att säkerställa att nämndens beslutshantering sker i enlighet med kommunallagen.

Ledningen för Karolinska universitetssjukhuset rekommenderas att:

- säkerställa att det finns väl definierade rapporteringskanaler för både informationssäkerhetssamordnare och dataskyddsombud direkt till sjukhusdirektör.
- implementera standardiserade processer för regelbunden uppföljning och kontroll av informationssäkerhets- respektive dataskyddsarbetet.
- säkerställa att medarbetare med nyckelfunktioner genomgår fördjupade utbildningar avseende informationssäkerhet och dataskydd.
- säkerställa att medarbetare regelbundet genomför grundläggande informationssäkerhets- och dataskyddsutbildning för att upprätthålla och säkerställa kunskapsnivån över tid.

## Vad gör regionrevisorerna?

Regionrevisorerna granskar den verksamhet som bedrivs av regionens nämnder och bolagsstyrelser. Revisionsuppdraget är det största inom kommunal verksamhet.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, saklighet och integritet främja, granska och bedöma verksamheten. Den övergripande uppgiften för revisorerna är att granska hur nämnder och styrelser tar sitt ansvar. De förtroendevalda revisorerna är fullmäktiges och ytterst medborgarnas instrument för den demokratiska kontrollen. De har därmed en viktig funktion i den lokala självstyrelsen.

Ledamöter i nämnder och styrelser ansvarar inför fullmäktige för hur de själva, anställda och uppdragstagare genomför verksamheten. I ansvaret ingår att genomföra en ändamålsenlig verksamhet utifrån fullmäktiges mål, beslut och riktlinjer samt de föreskrifter som gäller för verksamheten, på ett ekonomiskt tillfredsställande sätt och med en tillräcklig intern kontroll samt att upprätta rättvisande räkenskaper.

I årsrapporter för nämnder och styrelser sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna finns på www.regionstockholm.se. Det går även att prenumerera på regionrevisorernas nyhetsbrev genom att anmäla intresse via e-postmeddelande till regionrevisorerna.rev@regionstockholm.se.

**Postadress:** Box 22230, 104 22 Stockholm
**Besöksadress:** Hantverkargatan 25 b (T-bana Rådhuset)
**Telefon:** 08-123 100 00
**E-post:** regionrevisorerna.rev@regionstockholm.se
**Hemsida:** www.regionstockholm.se

Region Stockholm

# Granskning av dataskyddsarbete och systematiskt informationssäkerhetsarbete på Karolinska universitetssjukhuset

**Region Stockholm**

Augusti 2024

*Charlotte Arnell, projektledare*
*Sara-Rosa Ageborg, projektmedarbetare*
*Markus Månsson, projektmedarbetare*
*Kristian Damlin, kvalitetssäkrare*

pwc

**Revisionsrapport**

# Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Stockholm genomfört en granskning. Granskningen syftar till att bedöma om Karolinska universitetssjukhuset uppfyller kommunallagens krav på intern kontroll avseende informationssäkerhet och dataskydd, samt om arbetet bedrivs på ett ändamålsenligt sätt och i enlighet med lagstiftning, interna mål och regelverk samt regionfullmäktiges mål.

Vidare syftar granskningen till att följa upp tidigare rekommendationer från regionrevisionen avseende bägge områdena.

Utifrån genomförd granskning är vår samlade bedömning att Karolinska sjukhuset inte helt bedriver ett ändamålsenligt arbete avseende systematiskt informationssäkerhetsarbete. Avseende dataskyddsarbetet är vår samlade bedömning att det inte bedrivs på ett ändamålsenligt sätt.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet “Sammanfattande bedömningar utifrån revisionsfrågor”.

Revisionsfråga 1-5 avser informationssäkerhet och revisionsfråga 6-12 avser dataskydd.

| Revisionsfrågor | Bedömning | |
|---|---|---|
| 1. Finns en ändamålsenlig styrning av informationssäkerhetsarbetet? | Inte helt |  |
| 2. Är roller och ansvar för informationssäkerheten tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller? | Inte helt |  |
| 3. Genomförs riskanalyser avseende informationssäkerhet på ett ändamålsenligt sätt? | Inte helt |  |
| 4. Genomförs utbildning för samtliga medarbetare på ett ändamålsenligt sätt? | Inte helt |  |
| 5. Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt? | Inte helt |  |
| 6. Finns en ändamålsenlig styrning av dataskyddsarbetet? | Inte helt |  |
| 7. Är roller och ansvar för dataskydd arbetet tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller? | Nej |  |
| 8. Är behandlingsregistret ändamålsenligt och hålls det aktuellt? | Nej |  |
| 9. Genomförs riskanalyser avseende personuppgiftshantering på ett ändamålsenligt sätt? | Nej |  |
| 10. Genomförs konsekvensbedömningar enligt GDPR på ett ändamålsenligt sätt? | Inte helt |  |
| 11. Hålls riskanalyser och konsekvensbedömningar aktuella på ett ändamålsenligt sätt? | Nej |  |
| 12. Genomförs uppföljningen av dataskyddsarbetet på ett ändamålsenligt sätt? | Nej |  |

# Innehållsförteckning

# Förkortningar och begrepp

| | |
|---|---|
| Complianceportalen | IT-stöd för egenkontroll och uppföljning av regelefterlevnad (i det här fallet efterlevnad av Region Stockholms riktlinjer för informationssäkerhet). Regionen ansvarar för portalen och kontrollernas utformning. |
| Dataskydd | Samlingsbegrepp som både har en formell mening genom dataskyddsförordningen, men är också ett samlingsbegrepp för åtgärder som syftar till att skydda personuppgifter. |
| GDPR | Den allmänna dataskyddsförordningen |
| HSL | Hälso- och sjukvårdslag |
| IMY | Integritetsskyddsmyndigheten |
| ITIL | Information Technology Infrastructure Library. ITIL-processer är ett samlingsbegrepp på olika typer av IT-processer, exempelvis incidenthantering eller ärendehantering. |
| Karolinska | Karolinska universitetssjukhuset |
| KL | Kommunallag |
| LIS | Ledningssystem för informationssäkerhet |
| NIS-direktiven | NIS 1- och 2-direktiven avser direktiven om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. I Sverige är NIS 1-direktivet implementerat genom lag om informationssäkerhet för digitala och samhällsviktiga tjänster. NIS 2-direktivet föreslås implementeras genom den nya cybersäkerhetslagen. |
| Nämnd(en) | Karolinska universitetssjukhusets styrelse är en nämnd som ansvarar för verksamheten inför regionfullmäktige och förvaltningen. |
| OSL | Offentlighet- och sekretesslag |
| Personuppgifts-behandling/ behandling | När personuppgifter hanteras på olika sätt är det formella begreppet för hanteringen ”behandling”. En behandling kan innebära exempelvis insamling, bearbetning, arkivering, spridning eller radering av personuppgifter. |

# Inledning

## Bakgrund

Karolinska universitetssjukhuset hanterar stora mängder känslig information i allmänhet, och starkt skyddsvärda personuppgifter i synnerhet. Det innebär att sjukhusets arbete med informationssäkerhet och dataskydd är avgörande för en säker hantering av personuppgifter och verksamhetskritisk information. Brister i arbetet med informationssäkerhet och dataskydd kan bland annat öka riskerna för förlust av information, att känsliga personuppgifter hamnar i orätta händer, att verksamhetskritisk information inte finns tillgänglig för personal och patienter eller att informationens korrekthet inte kan garanteras. I det fall någon eller flera av riskerna skulle realiseras, uppstår i sin tur nya risker. Dels för skador på Karolinskas förtroende, ekonomi och verksamhet, dels för personliga skador för drabbade personer.

Karolinska universitetssjukhuset är regionens största vårdgivare med en komplex organisation vilket ställer krav på ett systematiskt informationssäkerhetsarbete. I en tidigare granskning har revisionen bland annat konstaterat att det grundläggande systematiska informationssäkerhetsarbetet inte omfattade samtliga verksamheter på alla nivåer och att samtliga medarbetare inte genomgått regionens utbildning för informationssäkerhet. I tidigare granskningar har det även konstaterats brister i Karolinska universitetssjukhusets arbete med *både* informationssäkerhet och dataskydd. Bristerna har främst bestått i prioritering av genomförande av riskanalyser, tydlighet avseende roller och ansvar, adekvat utbildning av samtliga anställda samt medvetenhet kring områdena inom samtliga verksamheter.

Regionrevisorerna har bedömt att det finns risk för att problemen kvarstår och att planering och löpande uppföljning av informationssäkerheten inte följer gällande regelverk. Därför genomförs denna granskning.

## Varför är dataskydd och informationssäkerhet viktigt?

Informationssäkerhet beskrivs vanligtvis som en uppsättning administrativa och tekniska åtgärder för att bevara informationens konfidentialitet, riktighet och tillgänglighet.[1] Konfidentialitet innebär att informationen endast är tillgänglig för behöriga personer. Riktighet innebär att informationens innehåll är korrekt och inte kan ändras av obehöriga. Tillgänglighet innebär att informationen är tillgänglig när den behövs. Definitionen av behörighet, riktighet och tillgänglighet inom hälso- och sjukvårdsområdet styrs främst av lagstiftning, föreskrifter och praxis.

Patientuppgifter innehåller ofta både integritetskänslig information och sådana uppgifter som enligt GDPR klassas som känsliga personuppgifter och därmed har särskilt skydd enligt lag. Exempel på integritetskänslig information är uppgifter om sociala förhållanden, relationer, barn och vissa ekonomiska uppgifter. Patientuppgifter är också

[1] Det finns ingen legal eller formellt fastslagen definition av informationssäkerhet. Däremot speglar ovan beskrivning den i branschen och praxis vedertagna definitionen. Mer om innebörden kan exempelvis läsas här: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/om-informationssakerhet/.

sekretessbelagda enligt OSL, vilket innebär att de är extra skyddsvärda ur ett dataskyddsperspektiv. Exempel på känsliga uppgifter enligt GDPR är hälsouppgifter, uppgifter om sexualliv och politiska åsikter. Otillräckligt dataskydd kan leda till obehörig åtkomst och därmed riskera patientens integritet. Ett starkt dataskydd är därför avgörande för att upprätthålla förtroendet mellan patienter och vårdgivare. Om patienten inte känner att deras information är tillräckligt skyddad kan det påverka deras vilja att dela viktig information och söka vård, vilket i sin tur kan påverka patientsäkerheten.

Den ökade digitaliseringen innebär många möjligheter, men också ökade sårbarheter och hot mot dataskydd och informationssäkerhet. Detta kräver att organisationer ökar medvetenheten för att förstå vilken information som är mest kritisk för att upprätthålla verksamhetsprocesser och invånarnas förtroende. Organisationer som hanterar personuppgifter behöver kunna identifiera och skydda dessa samtidigt som de behöver kunna upptäcka och hantera incidenter och katastrofer. I detta avseende är det därför viktigt att organisationer har en ändamålsenlig styrning av och kontinuerligt arbete med informationssäkerhet och dataskydd.

## Syfte och revisionsfrågor

Granskningen syftar till att bedöma om Karolinska universitetssjukhuset uppfyller kommunallagens krav på intern kontroll avseende informationssäkerhet och dataskydd, samt om arbetet bedrivs på ett ändamålsenligt sätt och i enlighet med lagstiftning, interna mål och regelverk samt regionfullmäktiges mål. Vidare syftar granskningen till att följa upp tidigare rekommendationer från regionrevisorerna avseende båda områdena.

Bedömningen görs i huvudsak genom att nedanstående frågeställningar undersöks.

1. Finns en ändamålsenlig styrning av informationssäkerhetsarbetet?
2. Är roller och ansvar för informationssäkerheten tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller?
3. Genomförs riskanalyser avseende informationssäkerhet på ett ändamålsenligt sätt?
4. Genomförs utbildning för samtliga medarbetare på ett ändamålsenligt sätt?
5. Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?
6. Finns en ändamålsenlig styrning av dataskyddsarbetet?
7. Är roller och ansvar för dataskydd arbetet tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller?
8. Är behandlingsregistret ändamålsenligt och hålls det aktuellt?
9. Genomförs riskanalyser avseende personuppgiftshantering på ett ändamålsenligt sätt?
10. Genomförs konsekvensbedömningar enligt GDPR på ett ändamålsenligt sätt?
11. Hålls riskanalyser och konsekvensbedömningar aktuella på ett ändamålsenligt sätt?
12. Genomförs uppföljningen av dataskyddsarbetet på ett ändamålsenligt sätt?

## Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för granskningens analyser och bedömningar. I denna granskning utgör följande regelverk revisionskriterier:

- Kommunallag (2017:725)
- Förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, allmänt kallad GDPR
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174)
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

## Avgränsning

Granskningen avser Karolinska universitetssjukhuset och i huvudsak år 2023. Granskningen omfattar sjukhusledning, stabsnivå samt vissa utvalda verksamheter. Se vidare nedan.

## Metod

Granskningen har genomförts genom dokumentstudier, enkät och intervjuer. Olika typer av styrande dokument, mallar, vägledningar, beslut och liknande har analyserats. Intervjuer har hållits med följande funktioner:

- Sjukhusdirektör,
- Chef för rättskansliet,
- Informationssäkerhetssamordnare tillika tillförordnad enhetschef för myndighetsjuridik,
- Tillförordnad informationssäkerhetssamordnare,
- Säkerhetschef,
- IT-säkerhetssamordnare,
- Processägare för ITIL-process,
- Dataskyddsombud, och
- Dataskyddsjurist.

Samtliga intervjuade har fått möjlighet att faktagranska rapporten, undantaget sjukhusdirektör och informationssäkerhetssamordnare tillika tillförordnad enhetschef för myndighetsjuridik. Bägge dessa tjänstepersoner hade avslutat sina anställningar vid tiden för granskningens färdigställande. Vid faktagranskningen har även chef för intern kontroll och riskhantering deltagit.

Granskningen inkluderar även uppföljning genom stickprov. Stickproven har utgjorts av Karolinskas behandlingsregister, samt tre IT-system avseende röntgeninformationssystem, bildarkiv och kommunikationssystem samt regional mellanlagringstjänst. De granskade systemen har valts ut av Karolinska själva (genom dataskyddsjurist, dataskyddsombud samt informationssäkerhetssamordnare gemensamt). Alla systemen är sjukhusövergripande och innehåller stora mängder personuppgifter och känslig/sekretessbelagd information. Stickproven har tagits genom att behandlingsregistret har granskats och avseende systemen har riskanalyser,

protokoll från utförda egenkontroller i Complianceportalen och konsekvensbedömningar samlats in. Totalt har tolv dokument granskats.

De utvalda verksamheterna som granskats särskilt är:

- Tema Barn /Astrid Lindgrens Barnsjukhus,
- Tema Cancer,
- Tema Kvinnohälsa och Hälsoprofessioner, och
- Stab Teknik.

Samtliga verksamhetschefer och verksamhetsområdeschefer inom dessa verksamheter har fått möjlighet att besvara en enkät avseende informationssäkerhets- och dataskyddsarbetet. Sammantaget har 29 enkäter skickats ut, och 23 svar har inkommit. För tema barn och stab teknik har verksamhetscheferna valt att besvara enkäten gemensamt. För tema Kvinnohälsa och Hälsoprofessioner har två verksamheter svarat gemensamt. Fem verksamheter har inte inkommit med svar.

Granskningen har genomförts som en sammanhållen granskning och resulterat i en rapport. Däremot har respektive område (informationssäkerhet och dataskydd) analyserats och bedömts separat.

## Tidigare granskningar och rekommendationer

I tidigare granskningar har regionrevisorerna lämnat ett flertal rekommendationer. Följande granskning har, utöver ovan revisionsfrågor, även fokuserat på att följa upp dessa rekommendationer. De rekommendationer som har ingått i granskningen listas nedan:

- Nämnden bör säkerställa att det grundläggande systematiska informationssäkerhetsarbetet omfattar samtliga verksamheter på alla nivåer (id 29851).
- Nämnden bör säkerställa att samtliga anställda genomgår regionens utbildning för informationssäkerhet (id 29852).
- Nämnden bör säkerställa att en åtgärdsplan tas fram med nyckelkontroller (till exempel risk- och sårbarhetsarbetet, hantering och övervakning av informationssystem och nätverk, systemförvaltning och systemägaransvar) för att säkerställa efterlevnad av NIS-direktivet (id 97667).
- Ledningen bör vidta åtgärder så att genomförande av egenkontroller och riskanalyser prioriteras av verksamheterna när det gäller efterlevnad av GDPR (id 29845).
- Ledningen bör säkerställa att det finns en systematik så att kontinuitetsplaner övas regelbundet med avseende på informationssäkerhet (id 97669).
- Ledningen bör utveckla rutiner för systematisk uppföljning av att informationssäkerhetsutbildningar genomförs av alla anställda (id 97668).

Uppföljningen av rekommendationerna återfinns i slutet av rapporten.

# Granskningsresultat

## Organisation

### Informationssäkerhet

Vid tiden för denna granskning är arbetet med informationssäkerhet organiserat genom primärt tre roller; informationssäkerhetssamordnare, -handläggare och -koordinator. Informationssäkerhetssamordnare och -handläggare är placerade på rättskansliet och informationssäkerhetskoordinatorer är placerade i respektive tema, funktion eller stabsenhet. Informationssäkerhetsarbetet utförs i nära samarbete med IT-säkerhetsarbetet, och detta är organiserat inom stab teknik.[2]

Under granskningen informerades om en omorganisation där informationssäkerhetsfunktionerna avsågs att flyttas till stab teknik. Vid tiden för granskningen uppgavs att flera roller var vakanta, exempelvis informationssäkerhetshandläggare (tillsattes under granskningen) och flertalet tjänster som informationssäkerhetskoordinator.

### Dataskydd

Arbetet med dataskydd är främst organiserat inom rättskansliet genom dataskyddsombud och dataskyddsjurist. Även informationssäkerhetssamordnaren arbetar indirekt med dataskydd och vid tiden för denna granskning är den rollen placerad på rättskansliet.

Informationssäkerhetskoordinatorerna ansvarar för att koordinera arbetet med dataskydd inom respektive tema, funktion eller stab, och dessa ska finnas utsedda inom respektive tema, stab eller funktion. Vid tiden för granskningen uppgavs att flertalet tjänster som informationssäkerhetskoordinator var vakanta.[3]

## Revisionsfråga 1: Finns en ändamålsenlig styrning av informationssäkerhetsarbetet?

### Utgångspunkter

Utgångspunkten för en ändamålsenlig styrning av informationssäkerhetsarbetet är att kraven i kommunallagen avseende styrning och kontroll kan uppnås. Det innebär att styrningen behöver utformas så att nämnden kan säkerställa att verksamheten bedrivs i enlighet med regionens egna mål och riktlinjer, samt i enlighet med lagar och andra regelverk.[4] Nämnden ska också se till att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.[5] Ett exempel på vad som menas med “i övrigt tillfredsställande” är att en verksamhet eller uppgift bedrivs på ett kostnadseffektivt sätt.

Hur styrningen ska genomföras är generellt inte reglerat men i vissa fall finns regler för detta i speciallagstiftning, exempelvis att arbetet med informationssäkerhet ska vara

---

[2] Organisationen finns beskriven i Riktlinje för arbetsflöden, roller, organisation och mandat gällande informationssäkerhet och IT-säkerhet, dokumentnr K62392.

[3] Organisationen finns beskriven i Riktlinje för behandling av personuppgifter på Karolinska Universitetssjukhuset, dokumentnr K51961.

[4] KL 6 kap. 6 § 1 st.

[5] KL 6 kap. 6 § 2 st.

systematiskt och riskbaserat[6] eller att en vårdgivare ska ha ett ledningssystem som säkerställer en tillräcklig hög grad av informationssäkerhet.[7] Det är vanligt att någon form av standard (exempelvis ISO) används antingen som regelrätt system, eller som riktmärke för styrningen av informationssäkerhet.

Sammantaget innebär en ändamålsenlig styrning av informationssäkerhetsarbetet att styrningen ska tillförsäkra att mål uppfylls, regler följs och att det görs på ett sätt som är kostnadseffektivt. Om informationssäkerhetsarbetet inte styrs på ett ändamålsenligt sätt kan det leda till brister i säkerheten, samt att arbetet inte sker effektivt och utifrån överenskomna prioriteringar.

**Iakttagelser**

Region Stockholms riktlinjer för informationssäkerhet utgår från internationell standard avseende styrning och implementering av informationssäkerhet (ISO 27000-serien). Strukturen för styrdokumenten (ledningssystemet) består av Region Stockholms policy för verksamhetsskydd[8] samt Region Stockholms riktlinjer för informationssäkerhet.[9] I riktlinjen anges att alla nämnder och bolag ska ha en egen handlingsplan för informationssäkerhet och den ska årligen uppdateras. Handlingsplanen ska innehålla en plan över de mål och aktiviteter inom informationssäkerhetsområdet som nämnden avser att genomföra under året. I denna granskning har vi tagit del av sjukhusets handlingsplaner för 2023 respektive 2024. Av riktlinjerna framgår att det ska finnas en handlingsplan, men inte vem som ska fatta beslut om den.

Av handlingsplanen för 2023 framgår att det är en plan för verksamhetsåret. Motsvarande dokument för år 2024 innehåller både en sammanfattning av föregående år, samt en plan för verksamhetsåret. Av nämndens beslut för handlingsplanen 2023 framgår endast att "rapporten" är lagd till handlingarna.[10] Det innebär att formellt sett har inte nämnden beslutat om sjukhusets handlingsplan för informationssäkerhetsarbetet, utan endast delgivits informationen. Av beslutsunderlaget, det vill säga själva handlingsplanen framgår inte handläggare avseende planen 2023, och för 2024 är det informationssäkerhetssamordnaren. Beslut om handlingsplanen finns inte upptaget i arbets- och delegationsordningen, förutom det fall att nämnden menar att beslutet anses utgöra ett styrande dokument. I sådant fall kan handlingsplanen anses vara ett verkställighetsbeslut enligt p. 35 i arbets- och delegationsordningen.

Vi har tagit del av en mängd olika styrande dokument avseende det mer operativa informationssäkerhetsarbetet. Det finns mallar för exempelvis klassning av skyddsnivå för IT-system[11] samt en riktlinje för riskbedömning[12] med en riskmatris[13] och en mängd riktlinjer och vägledningar för verksamheterna att följa. Det finns även ett formulär i Complianceportalen som avser krav vid upphandling av IT-tjänst och -system där det

[6] Lag om informationssäkerhet för samhällsviktiga och digitala tjänster, 11 §.
[7] HSLF-FS 2016:40, 3 kap. 2 §.
[8] Verksamhetsskydd, dnr RS 2020-0147.
[9] Riktlinjer för informationssäkerhet, dnr RS 2020-0148.
[10] Justerat protokoll för sammanträde den 24 april 2023, p. 18. Avseende 2024 års handlingsplan har vi endast kunnat ta del av beslutsunderlag men inte det justerade styrelseprotokollet.
[11] Klassning av skyddsnivå för IT-system, dokumentnr K62150.
[12] Riktlinje riskbedömning, dokumentnr K61957.
[13] Riskbedömningsmall inkl. riskmatris ver. 2.0, dokumentnr K61958.

genom egenkontroll ges stöd i vilka krav som behöver ställas i upphandlingen. Under början av 2024 har även en vägledning gällande systematiskt informationssäkerhetsarbete med årshjul för verksamhetsansvariga upprättats.[14]

Av enkätsvaren framgår att regler, riktlinjer, rutiner och vägledningar tillgängliggörs för verksamheter och medarbetare genom intranätet Inuti, via dokumenthanteringssystemet Centuri, via verksamhetschefer i samband med arbetsplatsträffar, medarbetarsamtal, ledningsgruppsmöten, och genom informationssäkerhetsutbildning i DISA och det styrande dokumentet Vägvisaren.

Samtidigt är det övergripande intrycket av enkätsvaren att svar på frågor som relaterar till styrning av informationssäkerhetsarbetet, varierar och skiljer sig en del jämfört med de styrande dokumenten. Exempel på en sådan variation är hur olika verksamhetschefer beskriver roller och ansvar för informationssäkerhetsarbetet. Det förekommer svar som går i linje med styrdokumenten, vissa uppger att ansvaret inte ligger på verksamhetschefsnivå utan centralt och vissa uppger att ansvaret ligger på informationssäkerhetskoordinatorn. Ett annat exempel är avseende hur utbildning av medarbetare säkerställs. Där hänvisar flera till att det följs upp centralt och genomförs vid nyanställning, medan andra beskriver att det är respektive chefs ansvar att kontrollera att obligatorisk utbildning genomförs. Ytterligare exempel avser riskanalyser där det generellt förekommer få svar avseende vem som ser till att dessa görs och uppdateras. Det förekommer även svar som indikerar att man inte har kunskap om vad frågan avser eller att det ansvaras för centralt.

**Bedömning**

*Finns en ändamålsenlig styrning av informationssäkerhetsarbetet?*

Vår bedömning är att det delvis finns en ändamålsenlig styrning av informationssäkerhetsarbetet inom Karolinska. Strukturen med styrande dokument på en regionövergripande nivå, som bryts ner i konkreta mål och aktiviteter för Karolinska, och kompletteras med operativa stödjande och styrande dokument, ger goda förutsättningar för ett effektivt och framgångsrikt arbete.

Avseende handlingsplanen bedömer vi att beslutshanteringen brister. Vår bedömning är att nämnden inte kan anses ha fastställt handlingsplanen utifrån formuleringen i protokollet och faktumet att det inte har funnits ett förslag till beslut för nämnden att ta ställning till (exempelvis genom en tjänsteskrivelse). Vi bedömer inte heller att det kan vara fråga om ett verkställighetsbeslut. Ett beslut om nämndens samlade arbete, mål och prioriteringar kan svårligen anses vara verkställighet (och därigenom inte behöva beslutas om eller delegeras av nämnden) utifrån att det kräver både avvägning, bedömning och inte är av rent förberedande art. Och även om beslut om handlingsplanen hade varit delegerat, hade det enligt vår bedömning funnits risk för att ett sådant beslut omfattats av delegationsförbudet i kommunallagen, eftersom det är ett beslut som bestämmer nämndens mål, inriktning, och omfattning avseende informationssäkerhetsarbetet.[15]

[14] Vägledning gällande systematiskt informationssäkerhetsarbete med årshjul för verksamhetsansvariga.
[15] Se vidare avseende delegationsförbudet: KL 6 kap. 38 §.

Sammantaget innebär detta att vår bedömning är att Karolinska endast har tagit fram ett förslag till handlingsplan, men inte fastställt densamma. Det innebär i sin tur att Karolinska inte följer regionens riktlinje om att det ska finnas en handlingsplan.

De formella bristerna skapar en otydlighet på flera sätt. Dels är det direkt oklart vem som i realiteten styr nämndens arbete avseende informationssäkerhet. Dels innebär beslutshanteringen att informationssäkerhetsperspektivet inte blir en integrerad del av den sammanlagda styrningen (inklusive mål, prioriteringar och investeringar). Exempelvis hade utvärdering av informationssäkerhet och beslut om handlingsplan varit integrerat i budget- och uppföljningsarbetet, och beslutas om av nämnden. På så sätt hade utvärderingen kunnat kopplas till behovsidentifiering, prioritering och beslut om budget. På så sätt hade styrningseffekten blivit starkare och nämndens ansvarstagande hade blivit tydligare.

Avseende sjukhusets operativa styrning genom riktlinjer, vägledningar, instruktioner, handlingsplaner, mallar och liknande, är vår bedömning att dessa är omfattande, välskrivna och tillgängliga för den som söker efter dokumenten. Samtidigt är intrycket, genom intervjuer och enkätsvaren, att de olika styrande och stödjande dokumenten inte helt har fått ett betydande genomslag i den praktiska verksamheten.

## Revisionsfråga 2: Är roller och ansvar för informationssäkerheten tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller?

### Utgångspunkter

Om roller och ansvar för informationssäkerheten inte är tydliga, kända och kommunicerade kan det leda till brister i ansvarsfördelning, samordning, kompetens, kontroll och uppföljning av informationssäkerhetsarbetet. Det kan i sin tur öka risken för incidenter, avvikelser, klagomål och sanktioner som kan skada Karolinskas verksamhet, rykte och förtroende.

Ett sätt att skapa tydlighet kring roller och ansvar är att tydliggöra vem som får fatta olika typer av beslut. I en verksamhet som styrs av kommunallagen, såsom Karolinska universitetssjukhuset, är beslutanderätten i huvudsak placerad hos nämnden (förutom i de fall där annan lagstiftning än kommunallagen placerat den någon annanstans, exempelvis hos en läkare). Dessa beslut kallas också beslut i kommunallagens mening. Det innebär i sin tur att för Karolinskas administrativa verksamhet, det vill säga ej hälso- och sjukvård och forskning, ligger den huvudsakliga beslutanderätten hos nämnden. För att arbetet och den dagliga verksamheten ska kunna skötas på ett rationellt och effektivt sätt har det genom kommunallagen getts möjlighet till delegation av nämndens beslutanderätt.[16]

Den huvudsakliga mängden av delegationsbeslut förtecknas i det som vanligtvis kallas delegationsordning. Delegationsordningen blir då en form av förteckning av beslutsmandat, vilket i sin tur kan skapa en tydlighet även kring roller och ansvar. I detta sammanhang är det dock viktigt att notera att delegationsordningen inte är en beskrivning av ansvarsområden utan endast en beslutsförteckning (däremot kan beslut

[16] KL 6 kap. 37 § samt 7 kap. 5-6 §§.

om förvaltningens organisation inklusive roller och ansvarsområden vara ett beslut som delegeras till exempelvis förvaltningschef/sjukhusdirektör). Förteckningen (eller annat beslut) behöver också vara så pass specifik att det är tydligt vilka beslut som avses att delegeras och vem delegaten är.[17]

Det finns en kategori av beslut som anställda kan fatta utan delegation och dessa kallas verkställighet eller ibland verkställighetsbeslut. Det finns ingen lagstadgad definition av verkställighet utan den definitionen som finns har utvecklats genom kommunallagens förarbeten och praxis. Av förarbetena till kommunallagen sägs, vilket är den uppfattning som också stöds i praxis, att rent förberedande åtgärder eller rent verkställande åtgärder där det saknas utrymme för självständiga bedömningar inte är beslut i kommunallagens mening. Beslut där det föreligger alternativa lösningar och beslutsfattaren själv måste göra vissa överväganden eller bedömningar anses däremot utgöra beslut i kommunallagens mening.[18]

Det finns även ett antal beslut som inte är tillåtet att delegera, exempelvis ärenden som avser verksamhetens mål, inriktning, omfattning eller kvalitet, eller ärenden som inte får delegeras utifrån speciallagstiftning.[19] Detta innebär att exempelvis nämndens budget, verksamhetsplan, olika typer av riktlinjer eller beslut om strategiska vägval och liknande, behöver fattas av nämnden.

Sammantaget innebär detta att om ett beslut inte är reglerat i speciallagstiftning, inte finns upptaget i delegationsordning eller i annat beslut om delegation, eller kan anses vara verkställighetsbeslut, behöver det fattas av nämnden. Delegationsordningen ska i sin tur vara specifik och tydlig avseende vilka beslut som delegeras och till vilka funktioner delegationen ges. Detta innebär i sin tur att delegationsordningen kan användas som ett av flera verktyg för att strukturera och dokumentera ansvar och roller, eftersom beslutanderätten i de flesta fall är ett utfall av olika ansvarsområden.

**Iakttagelser**

Sjukhusdirektören är ytterst ansvarig tjänsteperson för informationssäkerhet på sjukhuset.[20] Ansvaret för informationssäkerhet är därefter kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet eller får ett delegerat verksamhetsansvar också är ansvarig för att skydda informationen i denna verksamhet.[21] Det innebär att ansvaret för informationssäkerheten hos Karolinska är kopplat till verksamhetsansvaret i samtliga led och ska följa den ordinarie linjeorganisationen.[22]

Informationssäkerhetssamordnaren är enligt ledningssystemet ansvarig för att samordna arbetet, och till sin hjälp ska samordnaren ha en handläggare och koordinatorer på respektive tema, funktion och stab. Enligt Region Stockholms riktlinjer

[17] Dalman, Lindblom, Persson, Wikell, Kommunallagen med kommentarer och praxis, 6 uppl., s. 342-346.
18 Se prop. 2016/2017:171, s. 206-209.
19 KL 6 kap. 38 §.
[20] Riktlinje för informationssäkerhet, RS 2020-0148.
[21] K Ledningssystem för informationssäkerhet samt Riktlinjer för informationssäkerhet RS 2020-0148.
[22] K Ledningssystem för informationssäkerhet samt Riktlinjer för informationssäkerhet RS 2020-0148.

ska informationssäkerhetssamordnaren, oavsett placering i organisationen, ha möjlighet att rapportera större avvikelser till högsta ledningen.[23]

Av intervjuer och dokumentation framgår att varje tema, funktion och stab kan ha en utsedd informationssäkerhetskoordinator, om inte är det verksamhetschefens ansvar att tillse att arbetet genomförs. Informationssäkerhetskoordinator för respektive tema, funktion eller stab är ansvarig för att koordinera och leda de nödvändiga aktiviteterna inom deras verksamhet med stöd från övriga informationssäkerhetsfunktioner såsom Karolinskas informationssäkerhetssamordnare och informationssäkerhetshandläggare. Det framgår dock av intervjuer att dessa roller har varit otydliga, har kombinerats med andra roller och varit varierande i kontinuitet. Flera av rollerna både har varit och är vakanta. Vid intervjuer uppges att det funnits vissa svårigheter att rapportera direkt till sjukhusledning avseende informationssäkerhet bland annat utifrån informationssäkerhetssamordnarens organisatoriska placering. Vi har inte kunnat identifiera en rutin eller annat styrande dokument avseende hur sådan rapportering ska gå till. Samtidigt uppges att det alltid är fritt att föra fram viktig information till både ledning och styrelse (nämnd). Det framgår av intervjuer att förändringar i roller och ansvar kommuniceras via Karolinskas intranät.

I sjukhusets arbets- och delegationsordning[24] finns endast ett fåtal beslut avseende informationssäkerhet utpekat. Ett exempel är delegationen till sjukhusdirektören att utse informationssäkerhetssamordnare. Det saknas däremot delegation avseende exempelvis riskanalyser.

Av enkäterna framgår att ett flertal av respondenterna är medvetna om sitt informationssäkerhetsansvar som verksamhetschefer, men vissa respondenter refererar till informationssäkerhetskoordinator som utpekad ansvarig för informationssäkerhetsarbetet alternativt svarar endast att alla medarbetare är enskilt ansvariga för informationssäkerhetsarbetet inom Karolinska.

**Bedömning**

*Är roller och ansvar för informationssäkerheten tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller?*

Vi bedömer att roller och ansvar för informationssäkerheten är delvis tydliga, kända och att medarbetarna blir informerade om förändringar i ansvar och roller. Enbart sett till styrande dokument är roller och ansvar beskrivna och dessa dokument finns tillgängliga på intranätet.

Avseende arbets- och delegationsordningen[25] bedömer vi den som bristfällig utifrån att den i princip saknar beslut som bör vara delegerade avseende informationssäkerhet. Sådana beslut är exempelvis beslut om fastställande av riskanalyser och accepterande av risker (alternativt ett tydliggörande av exempelvis beslut om avtal och vad sådana beslut måste innehålla). Vi bedömer inte att den typen av beslut är möjliga att betrakta som verkställighet i kommunallagens mening (eftersom de kräver analys, avvägning och bedömning), och därför behöver de fattas direkt av nämnden, eller delegeras.

[23] Riktlinjer för informationssäkerhet RS 2020-0148.
[24] Dnr K 2024-0963.
[25] Dnr K 2024-0963.

Sammantaget innebär avsaknaden av delegerade beslut avseende informationssäkerhet både en formell brist, och att en avsaknad i tydlighet avseende roller, uppgifter och beslutsmandat.

Även om verksamhetscheferna är generellt medvetna om att de har ett ansvar för informationssäkerhet och det finns riktlinjer för de olika rollerna har det dock funnits otydligheter och variationer inom dessa roller, där de har kombinerats med andra arbetsuppgifter och haft varierande kontinuitet (vakanser). Utifrån intervjuerna och svaren i enkäterna framstår det som att det finns oklarheter kring roller och ansvar och att arbetet i praktiken inte följer de roller och ansvar som pekas ut i styrande dokument. Sammantaget innebär detta en svårighet att i praktiken efterleva den struktur och den ansvarsfördelning som beskrivs i de styrande dokumenten.

## Revisionsfråga 3: Genomförs riskanalyser avseende informationssäkerhet på ett ändamålsenligt sätt?

### Utgångspunkter

Riskanalyser avseende informationssäkerhet är ett grundläggande verktyg för att identifiera och hantera de hot och sårbarheter som kan påverka Karolinskas informationstillgångar, såsom patientdata. Krav på att genomföra riskanalyser framgår av lagstiftning på olika sätt och de är också överlappande. Krav på genomförande och aktualitetshållande av riskanalys finns exempelvis i lag om informationssäkerhet för samhällsviktiga och digitala tjänster[26] och i Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.[27] Att utgå från riskanalyser avseende informationssäkerhet utgör också ett indirekt krav i GDPR eftersom utfallet av dessa styr hanteringen av personuppgifter.

Det är också viktigt att riskanalyser genomförs, och risker omhändertas innan exempelvis ett system tas i bruk. Det finns flera skäl till detta. Ett är att det är en följd av regelverken, även om det inte uttryckligen framgår av lagtext. Dock innebär ett användande av exempelvis ett system som innehåller personuppgifter, där det inte finns en riskanalys eller där det finns icke omhändertagna risker, att det inte kommer gå att visa att man följer GDPR. Ett annat skäl är att arbetet med riskhantering avseende IT-system och dessutom i en miljö som Karolinskas, är svårt och komplext. För att skapa så enkla och tydliga processer som möjligt, är det en stor fördel om det finns tydliga ”avstämningspunkter”. Exempelvis att det är tydligt vad som behöver finnas på plats innan ett system upphandlas, och det sker en avstämning av detta innan nästa steg kan tas. Risken annars är att det skapas en kultur där det inte upplevs spela någon roll om de interna reglerna följs eller ej.

Om riskanalyser inte genomförs på ett ändamålsenligt sätt kan det leda till att Karolinska inte uppfyller sina skyldigheter att skydda informationen, samt att sjukhuset utsätter sig för onödiga kostnader och störningar vilket kan skada Karolinskas verksamhet, rykte och förtroende. Riskanalyser är också grunden för effektiv planering, prioriteringar och kvalitativa underlag för handlingsplaner och investeringar.

[26] 11 §.
[27] 3 kap. 5 §.

**Iakttagelser**

I riktlinjer för informationssäkerhet[28] anges att nämnder och bolag ansvarar för att riskanalyser genomförs samt att dessa ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. I Karolinskas tillämpningsanvisningar för ovan nämnda riktlinje[29] anges att riskbedömning ska göras utifrån identifierade avvikelser, risker och sårbarheter. Det anges också att för varje risk ska det finnas en ägare samt att det ska fattas beslut om riskerna kan godtas eller ej. Om de inte kan godtas ska det tas fram en handlingsplan. Utöver detta har även Karolinska tagit fram en generell riktlinje[30] med tillhörande utvärderingsmatris avseende riskbedömning.[31] Ett riskområde som enligt denna riktlinje ska utvärderas är *data och integritetsskydd*. Karolinskas riktlinje för riskbedömning anger hur riskbedömningar ska genomföras, men däremot beskrivs inte *när* riskbedömningar ska göras. I övrigt finns ett antal mer specifika vägledningar avseende riskbedömningar och riskhantering. Dock har vi inte kunnat identifiera något styrande dokument (avseende informationssäkerhet) som anger ett obligatoriskt eller tvingande krav på riskanalys (inklusive åtgärdande av brister) innan driftsättning av system eller liknande.

I intervjuer beskrivs att hanteringen och genomförandet av riskanalyser kan vara utmanande. Det har övervägts att ta fram ytterligare dokument som vägledning. Tidsbrist och andra ansvarsområden har gjort det svårt att prioritera riskanalyser tidigare. Det uppges även vid intervjuer att det har varit svårt att styra och kommunicera hur man ska hantera risker i verksamheten. Uppföljning av riskanalyser är också en utmaning. Det planeras för[32] att arbeta mer riskbaserat, men under intervjuer uppges också att det i dagsläget saknas en systematisk metod för att genomföra och följa upp riskanalyser.

Det varierar även inom verksamheterna hur mycket man har arbetat med riskanalyser utifrån vilka resurser som har funnits tillgängliga. I enkäterna ges en mängd olika svar på frågan hur verksamheterna arbetar med riskanalyser. Några anger att de tar del av riskanalyser som görs på sjukhusövergripande nivå eller som utförs av informationssäkerhetskoordinator, vissa uppger att riskanalyser görs vid behov, andra att det är oklart när det görs, och ytterligare andra att det görs gemensamt med systemansvariga, eller att det görs när det sker genomgång av Complianceportalen. Vidare framgår även att några respondenter uppfattar att systemägare samt produktägare ska säkerställa att riskbedömningar görs och följs upp för sina ansvarsområden.

Avseende riskanalyser för informationssäkerhet har stickprov genomförts på tre IT-system som är i bruk. För två av systemen har vi inte kunnat få någon tidigare riskanalys utan endast tagit del av den analys som genomförts efter att den efterfrågats för denna granskning. Av den riskanalysen framgår att det inte finns någon rutin för att kontrollera behörigheter i systemet, att inloggning inte måste ske med e-tjänstekort samt

[28] Dnr RS 2020-0148
[29] Utdrag från intranätet, inget specifikt dokument.
[30] Riktlinje riskbedömning, dokumentnr K61957.
[31] Riskbedömningsmall inkl. riskmatris ver. 2.0, dokumentnr K61958.
[32] Se Handlingsplan för informationssäkerhet vid Karolinska Universitetssjukhuset 2024, dnr K 2024-2391, delmålsområde 1.

att kommunikation mellan dessa två system och andra inte är krypterad. Det uppges att det ena av dessa system ska tas ur bruk år 2026.

För ett system finns ett protokoll från en egenkontroll från 2021. Som förklaring till att egenkontroll inte gjorts efter 2021 anges att en förändring i Complianceportalen medfört att det inte längre finns kriterier i Complianceportalen för detta system att kontrollera mot.  En åtgärdslista avseende kända brister lämnas också med anteckningen att det finns ingen riskanalys yngre än fem år. Det lämnas även en notering om att en ny klassning och egendeklaration bör genomföras. Av åtgärdslistan framgår också att det är oklart hur kommunikation till och från systemet skyddas och om lagringen sker krypterat. Däremot framgår att loggar går att kontrollera och att viss behörighetshantering sker trots att rutin för årlig behörighetskontroll saknas.

**Bedömning**

*Genomförs riskanalyser avseende informationssäkerhet på ett ändamålsenligt sätt?*

Vi bedömer att riskanalyser avseende informationssäkerhet delvis genomförs på ett ändamålsenligt sätt.

Det finns styrande och stödjande dokumentation tillgänglig för den som aktivt söker vägledning. Det innebär att det finns en tydlighet kring att riskanalyser ska göras och till viss del hur de ska göras. Vi uppfattar dock en otydlighet kring när, av vem och hur riskanalyserna ska genomföras. Vi har inte kunnat identifiera obligatoriska "avstämningspunkter" där det ställs krav på genomförd analys, att den håller en viss kvalitet, samt att den görs (och brister/risker åtgärdas) *innan* inköp, driftsättning eller liknande. Det försvårar regelefterlevnaden och skapar otydlighet och osäkerhet i det operativa arbetet. I sin tur skapar detta en risk för att risker och sårbarheter inte hanteras på ett tillräckligt genomgripande sätt eller tillräckligt snabbt. Det skapar också en risk för inlåsningseffekter, exempelvis genom att system köps in och sedan inte kan användas med mindre än betydande informationssäkerhetsrisker.

Utifrån resultaten av stickproven bedömer vi att genomförandet är bristfälligt vilket leder till att ett stort antal risker framstår som icke bedömda eller inte åtgärdade. Det framstår också som att riskanalyser inte görs regelbundet avseende informationssäkerhet. Eftersom de granskade systemen ändå används innebär det en risk för att sekretessbelagd information röjs eller att obehöriga får åtkomst till känsliga personuppgifter.

## Revisionsfråga 4: Genomförs utbildning för samtliga medarbetare på ett ändamålsenligt sätt?

**Utgångspunkter**

Den "mänskliga faktorn" brukar anses som den vanligaste orsaken till incidenter. Därför är utbildning för samtliga medarbetare en grundläggande åtgärd för att upprätthålla informationssäkerhet på ett sjukhus. Utbildningen behöver dessutom vara kontinuerlig för att kunskap och riskmedvetenhet ska hållas hög och uppdaterad utifrån omvärldsförändringar.

**Iakttagelser**

Regionens riktlinjer[33] ställer krav på att alla medarbetare får den utbildning som behövs för att säkerställa hanteringen av relevanta informationstillgångar, att utbildningen ska vara anpassad till respektive medarbetares befattning, samt att denna ska bibehållas under medarbetarens hela anställnings- eller uppdragstid. I samma riktlinjer anges också DISA-utbildningen (eller annan motsvarande utbildning) som den lägsta nivån av utbildning som alla medarbetare måste genomgå.

Datorstödd informationssäkerhetsutbildning för användare (DISA) är Region Stockholms grundutbildning i informationssäkerhet. DISA-utbildningen är ett led i att öka medvetenheten och kunskapen om informationssäkerhet. DISA beskrivs som en kort och enkel utbildning som snabbt kan öka medarbetarnas kunskapsnivå om informationssäkerhet och sprida medvetenhet om området. DISA är obligatoriskt för alla medarbetare att genomgå.[34] Vid intervjuer uppges att utbildningen tidigare var tvingande för att få tjänstelegitimation utlämnad vid anställning men att kravet avskaffades av sjukhuset under 2023. Det uppges vidare att utbildningen fortfarande är obligatorisk att genomföra men att det är svårt att följa upp genomförandet, bland annat på grund av brister i den digitala plattform som används.

Vidare framgår av intervjuer att det även finns utbildning avseende informationssäkerhet i Vägvisaren. Av intervjuerna framgår att det inte sker någon annan utbildning, exempelvis riktad fördjupande utbildning för specifika roller. Av enkäterna framkommer en hög medvetenhet avseende utbildningarna och det beskrivs att deltagande följs upp av verksamhetschefer under arbetsplatsträffar och att påminnelser skickas ut på mejl eller under medarbetarsamtal vid behov.

Genomförande av DISA ska återrapporteras två gånger per år och ansvaras för av verksamhetschefer vilket framgår av årshjulet för verksamhetsansvariga.[35] Enligt intervjuer och handlingsplanen[36] ligger den nuvarande genomförandegraden på ca 75 procent av alla anställda. Avsaknaden av datorer för varje medarbetare och att utbildningen i framförallt DISA ibland sker på arbetsplatsträffar har dock gjort det svårt att följa upp genomförandet av utbildningen på individnivå. Dessutom kan anställda ha gjort utbildningen tidigare vid annan anställning inom regionen. Sannolikt är därför genomförandegraden högre än 75 procent.

**Bedömning**

*Genomförs utbildning för samtliga medarbetare på ett ändamålsenligt sätt?*

Vår bedömning är att det delvis genomförs utbildning för samtliga medarbetare på ett ändamålsenligt sätt men att det inte går att säkerställa att samtliga medarbetare bibehåller en stadigvarande och aktuell kunskapsnivå avseende informationssäkerhet under en längre tid.

[33] Riktlinjer för informationssäkerhet, dnr RS 2020-0148.
[34] K Ledningssystem för informationssäkerhet.
[35] Vägledning gällande systematiskt informationssäkerhetsarbete med årshjul för verksamhetsansvariga (K63067_2).
[36] Handlingsplan informationssäkerhet uppföljning 2023.

Vår bedömning är att medvetenheten om utbildningarna och dess syfte är hög. Genomförandegraden bedömer vi också som hög, med viss reservation för osäkerheten i mätningen. Däremot är det en brist att upprepning/uppdatering av utbildningen inte genomförs eller är ett krav. Avsaknaden av detta innebär en klar risk för att kunskapsnivån avseende informationssäkerhet inte är stadigvarande eller i linje med förändringar i arbetssätt och gällande regelverk. Denna brist innebär också att vi bedömer att Karolinska inte följer riktlinjens krav om att säkerställa att lämplig kunskapsnivå bibehålls.

Vi bedömer det också som en brist att det inte genomförs mer än grundläggande utbildningar eftersom flera funktioner behöver fördjupade kunskaper inom området (exempelvis verksamhetschefer eller informationssäkerhetskoordinatorer). Det innebär också att vi bedömer det som tveksamt om regionens riktlinje följs eftersom utbildningen inte anpassas till olika befattningsnivåer/funktioner.

## Revisionsfråga 5: Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?

### Utgångspunkter

Uppföljning av informationssäkerhetsarbete är nödvändigt för att säkerställa att Karolinska följer både de lagar, regler och riktlinjer som gäller för hantering av känslig och skyddsvärd information, och intern kontroll. Lagkrav på uppföljning finns både direkt och indirekt. Exempel på ett direkt krav är det som finns i lag om informationssäkerhet i samhällsviktiga och digitala tjänster där krav på en årlig, övergripande uppföljning finns.[37] Exempel på ett indirekt krav är regeln i kommunallagen om att nämnden ska se till att verksamheten följer gällande regler och ha en tillräcklig intern kontroll. För att efterleva dessa krav i praktiken är uppföljning nödvändig.

Uppföljning innebär också att Karolinska kan identifiera och åtgärda eventuella brister, risker eller incidenter som kan hota informationssäkerheten, samt utvärdera och förbättra sina processer, rutiner och system.

### Iakttagelser

Informationssäkerhetsarbetet följs upp på olika sätt. I nämndens underlag för verksamhetsplan för 2023[38] och 2024[39],internkontrollplan för 2023[40] och 2024[41] samt fördjupad sammanställning av bland annat risker[42] finns flera risker kopplade till informationssäkerhet upptagna. Riskerna handlar om otydliga roller avseende IT-säkerhet (2023 och 2024), behörigheter (2023), roller och ansvar för informationssäkerhet (2023 och 2024), ägande av data (2023 och 2024), cyberhot och andra IT-säkerhetshändelser (2024).I Complianceprogrammet för 2023 som redovisades för nämnden på sammanträdet den 28 september 2022 finns även två riskområden med som avser informations- och IT-säkerhet. Dessa innehåller bland annat risk avseende vakanta nyckelfunktioner för området samt bristande interna

[37] 3 kap. 6 §
[38] Sjukhusövergripande risker 2022 Styrelsen 230217.
[39] Risker VP 2024 Styrelsen 231213.
[40] Plan för intern kontroll år 2023, dnr K 2024-0301.
[41] Plan för intern kontroll, 2024, dnr K 2023-9145.
[42] Fördjupad sammanställning av mål, risker, kontroller och åtgärder, plan 2024, dnr K2023-9145.

styrande dokument. I dokumentet som förelades nämnden är områdena inte markerade med en uppdaterad status. Däremot beskrivs kort vissa vidtagna åtgärder samt att riskområdet började arbetas med under kvartal ett 2021.

Vid nämndens sammanträde den 28 september 2023 redovisades en uppdatering av sjukhusets övergripande risker.[43] Beskrivningen av åtgärder/status är den samma i uppföljningen i september som i dokumentet från februari avseende roller och ansvar och ägare av data. Avseende behörigheter är åtgärderna för den risken mer utförligt beskrivna och beskriver några påbörjade förbättringsåtgärder. I motsvarande dokument, Risker VP 2024, som föredragits för nämnden vid sammanträde den 13 december 2023 återkommer riskerna avseende roller och ansvar, ägare av data samt cyberhot. Beskrivningarna avseende åtgärder/status är de samma som tidigare. I detta dokument är dock ett slutdatum för genomförande tillagt (2024-12-31).

I Karolinskas verksamhetsberättelse för 2023[44], antagen av nämnden den 16 februari 2024, beskrivs översiktligt att arbetet med intern kontroll fortskrider enligt plan och det hänvisas till internkontrollplanen för 2023 för mer detaljerad information.

Vid tiden för denna granskning har ännu inte någon uppföljning av internkontrollplanen för 2024 redogjorts för nämnden. Under denna granskning har vi inte kunnat identifiera att det har redovisats någon uppföljning av complianceprogrammet. Dock är de risker som beskrivs i complianceprogrammet snarlika risker i internkontrollplanen och därför följs de till viss del upp inom ramen för internkontrollarbetet.

Vid intervjuer uppges att informationssäkerheten i systemen följs upp årligen genom Complianceportalen. Det uppges samtidigt att egenkontrollerna i Complianceportalen inte uppfattas som helt relevanta uppföljningsverktyg eftersom frågorna anses vara något trubbiga och inte anpassade till sjukhusverksamhet. Egenkontrollerna inklusive dessa frågor är bestämda av Region Stockholm och kan inte påverkas av Karolinska. Det uppges också att det saknas ett effektivt sätt att följa upp genomförande och resultat i Complianceportalen på aggregerad nivå. Det innebär, enligt uppgift vid intervju, att det inte finns någon översikt över i vilken grad egenkontroller i Complianceportalen genomförs eller den aggregerade risknivån.

Det uppges vidare att Karolinska framfört till regionen att man inte anser att Complianceportalen, med dess nuvarande innehåll och struktur, är det mest optimala verktyget för uppföljning.

I Complianceportalen ska även en övergripande egenkontroll avseende nämndens informationssäkerhetsarbete göras årligen.[45] Informationssäkerhetssamordnaren ansvarar för att fylla i denna. Kontrollen är framtagen av regionledningskontoret och det uppges, med viss osäkerhet, att utfallet av planen lämnas vidare till regionstyrelsen för vidare uppföljning. Formuläret innehåller sex frågor som alla är av JA/NEJ-karaktär. Det ställs krav på översiktliga beskrivningar av exempelvis åtgärder men inga fördjupade resonemang eller detaljerade beskrivningar. Exempel på frågor är om avvikelser i de

[43] Sjukhusövergripande risker delår Styrelsen 230928, finns ej dnr.
[44] Verksamhetsberättelse, dnr K 2024-0301.
[45] Indikator Karolinska 2023(2880711) (0), utdrag från Complianceportalen som avser den årliga uppföljningen på nämndsnivå.

mest skyddsvärda IT-systemen är gjorda, om nämnden ställt krav på informationssäkerhet i upphandlingar samt om medarbetare informeras om sekretess och tystnadsplikt. Karolinska har svarat ja på samtliga frågor.

Det uppges också att planerade personalminskningar och omorganiseringar har påverkat informationssäkerhetsarbetet negativt. Trots detta har det gjorts ett arbete med att utveckla riktlinjer och implementera dessa i verksamheten. Arbetet med informationssäkerhet har hittills främst handlat om arbetssätt och kommunikationsvägar, men fokus håller på att skifta till uppföljning. Det finns ett årshjul för rapportering till nämnden, där man framförallt rapporterar om domstolsärenden och allvarliga avvikelser av regelefterlevnad (så kallade complianceavvikelser).

Av enkäterna framgår att uppföljning och tillvägagångssätt för uppföljning varierar inom de olika verksamheterna. Det framgår ingen enhetlig beskrivning av hur uppföljning går till men följande nämns: att man använder sig av årshjul som stöd, att man följer riktlinjer och vägledning, att uppföljning inte sker i dagsläget, att brister inrapporteras från olika håll och att avvikelserapportering sker, att uppföljning sker på arbetsplatsträffar, att otillåten tillkomst till journaler följs upp och rapporteras löpande, att uppföljning sker inom vissa delar av verksamheten men att det inte sker någon heltäckande uppföljning, att utbildning följs upp via Lärtorget och att brister och incidenter dokumenteras i Karolinskas avvikelsesystem händelsevis.

**Bedömning**

*Sker uppföljningen av informationssäkerhetsarbetet på ett ändamålsenligt sätt?*

Vår bedömning är att uppföljningen av informationssäkerhetsarbetet delvis är ändamålsenlig.

Karolinska har tydliga riktlinjer för att följa upp informationssäkerhetsarbetet och det finns utpekade personer som ansvarar för att övervaka och utvärdera säkerhetsåtgärder. Dessa funktioner har dock saknat kontinuitet och inte haft möjlighet eller resurser till att arbeta uppföljande med informationssäkerhet utan fokus har istället legat på att upprätta riktlinjer och vägledningar. Detta innebär att vi bedömer att övervakning och rapportering är bristfällig, vilket även bekräftas av de handlingsplaner och åtgärdsplaner vi har tagit del av. Det tydliggörs även av avsaknaden av enhetliga svar på hur informationssäkerhet följs upp inom de olika verksamheterna.

Avseende uppföljning på nämndnivå är det positivt att olika typer av informationssäkerhetsrisker finns upptagna i både riskdokument och internkontrollplan. I viss utsträckning är det också tydligt att det arbetats med riskerna och att en förbättring/minskning av risken har åstadkommits. Dock framstår det för vissa av riskerna som att det över tid inte har skett någon utveckling, alternativt att utvecklingen inte har redovisats för nämnden. Vi bedömer det som en brist att den uteblivna utvecklingen (eller redovisningen av densamma), inte har lett till åtgärder från vare sig förvaltning eller nämnd.

Det finns en medvetenhet om att de verktyg som finns för uppföljning på operativ nivå inte är helt adekvata, och försvårar en effektiv uppföljning. Samtidigt uppges att Karolinska inte kan påverka detta eftersom Complianceportalen styrs centralt av regionen. Det är självklart en komplicerande faktor att Karolinska inte har full rådighet

avseende Complianceportalen. Dock påverkas inte det lagstadgade ansvaret av detta. Det innebär att om sjukhuset själva noterar att de har bristande kontroll, behöver man vidta åtgärder för att kompensera detta. I detta fall skulle exempelvis stickprovskontroller kunna öka graden av kontroll avseende regelefterlevnad och om styrningen fungerar som avsett.

## Revisionsfråga 6: Finns en ändamålsenlig styrning av dataskyddsarbetet?

### Utgångspunkter

Utgångspunkten för en ändamålsenlig styrning av dataskyddsarbetet är detsamma som för informationssäkerhet (se revisionsfråga 1).

I likhet med informationssäkerhet finns det i lagstiftning inte någon omfattande reglering av hur styrningen ska gå till. De regler som gäller för informationssäkerhet påverkar indirekt även styrningen av dataskydd eftersom de två områdena är så tätt sammankopplade. GDPR innehåller inga explicita krav avseende styrning. Däremot innebär GDPR att en mängd krav som ska uppfyllas, speciellt för en verksamhet som Karolinskas. Det innebär i sin tur att det krävs en omfattande och effektiv styrning för att GDPR ska kunna efterlevas.

Sammantaget innebär en ändamålsenlig styrning av dataskyddsarbetet att styrningen ska tillförsäkra att mål uppfylls, regler följs och att det görs på ett sätt som utifrån omständigheterna är kostnadseffektivt. Det innebär att Karolinska behöver ha tydliga mål, roller, ansvar, processer, rutiner och kontroller för att säkerställa att dataskyddet uppfyller de krav som ställs av GDPR och annan relevant lagstiftning, samt att det finns en kontinuerlig uppföljning, utvärdering och successiv förbättring av dataskyddsarbetet. En sådan styrning bidrar till att skapa förtroende, kvalitet och effektivitet i Karolinskas verksamhet och relationer med de registrerade. Styrningen syftar också till arbetet sker utifrån beslutade prioriteringar och på ett ändamålsenligt och effektivt sätt.

### Iakttagelser

Karolinska behandlar personuppgifter inom ramen för sjukhusets uppdrag som vårdgivare, forskningshuvudman och myndighet. Personuppgiftsbehandlingarna styrs genom Riktlinje för behandling av personuppgifter på Karolinska universitetssjukhuset.[46] Den hierarkiskt strukturerade styrningen, som utgår från regionövergripande dokument, saknas för dataskydd. I stället finns Karolinskas riktlinje för behandling av personuppgifter som utgör ett relativt brett styrande dokument som täcker in både övergripande frågor, vissa operativa delar och ett kunskapsunderlag.

Riktlinjerna beskriver roller och ansvar för dataskyddsarbetet, olika definitioner, principer för personuppgiftsbehandling, grundläggande hanteringsregler och ett antal regler i samband med särskilda situationer. Exempelvis fastslås att Karolinska ska föra ett register över alla personuppgiftsbehandlingar och att det inför varje ny personuppgiftsbehandling ska göras en riskanalys. Riktlinjen är fastställd av chefen för rättskansliet och vi har inte kunnat verifiera att den antagits av nämnden.

[46] Dokumentnr K51961.

Utöver riktlinjen finns ett antal vägledningar, manualer och mallar, av både mer kunskapsfördjupande respektive operativ karaktär. Vi har inte kunnat identifiera några övriga styrande dokument utan endast dokument av stödjande karaktär. Exempel på sådana är vägledning avseende vilka personuppgifter som kan behandlas i molntjänster,[47] mall för bedömning av behov av konsekvensbedömning, och introduktion till systematiskt riskbaserat integritetsarbete. Övriga dokument avser att i huvudsak styra eller stödja en annan huvudfråga, exempelvis behörighetshantering eller IT-säkerhet. Dock påverkar dessa dokument hur personuppgiftsbehandlingar styrs och genomförs på sjukhuset eftersom hanteringen av personuppgifter påverkas av exempelvis hur behörigheter hanteras eller vilka IT-säkerhetsåtgärder som vidtas. Samtliga finns enligt uppgift tillgängliga på intranätet.

Av intervjuer framgår att styrdokument för dataskydd kommuniceras till berörda parter och medarbetare genom att de finns tillgängliga på intranätet. Det uppges också att det finns bristande kunskap, resurser och tid för att säkerställa en bra styrning av dataskydd inom Karolinska, men också att medvetenhet och mognad avseende synen på dataskydd och dess generella betydelse för Karolinskas verksamhet har ökat.

I enkäterna uppges att interna regler och rutiner för dataskydd når samtliga av verksamhetens medarbetare genom arbetsplatsträffar, ledningsmöten och exempelvis informationssäkerhetsutbildningen i DISA.

**Bedömning**

*Finns en ändamålsenlig styrning av dataskyddsarbetet?*

Vår bedömning av Karolinska universitetssjukhusets styrning av dataskyddsarbetet är att den är delvis ändamålsenlig.

Utifrån avsaknaden av regionövergripande styrning bedömer vi riktlinjen som ett väl fungerande dokument som täcker de väsentliga områdena. Riktlinjen kompletteras av vägledningar. Dessa är i flera fall (inte alltid) av en relativt teoretisk karaktär och på en relativt hög kunskapsnivå. I flera fall behöver den som ska tillgodogöra sig vägledningarna redan vara relativt insatt. I detta sammanhang bedömer vi att det saknas ett ”mellanled” där det operativa ansvaret tydliggörs, det vill säga. vem som ska göra vad, när och på vilket sätt. Ett exempel är hanteringen av behandlingsregister. Av riktlinjen framgår att det ska föras ett register och det finns en manual för själva registreringen. Däremot har vi inte kunnat identifiera några regler eller rutiner som pekar ut vem som ska se till att respektive personuppgiftsbehandling verkligen blir införd i registret, när detta ska göras, hur det ska hållas aktuellt eller hur förändringar ska hanteras.

Avsaknaden av ”mellanledet” gör att den beslutade styrningen och arbetssättet inte får den effekt som var avsett, vilket också avspeglas i brister i utförande och oklarheter kring ansvar, roller och utförande (se revisionsfråga 7-11).

Vi bedömer det också som en brist att ovan nämnda riktlinje inte beslutats av nämnden. Riktlinjen är beslutad i enlighet med delegationsordningen, men vi bedömer det som

[47] Dokumentnr K62394.

tveksamt om det alls är förenligt med kommunallagen att delegera ett beslut som bestämmer inriktningen på en så pass övergripande nivå. I och med att beslut om riktlinjen är delegerat saknas helt involvering av nämnden i styrningen av Karolinskas dataskyddsarbete, vilket vi bedömer som bristande eftersom nämnden har ett direkt ansvar för efterlevnaden av dataskyddsregler. Bristande styrning skapar också högre risk för bristande hantering, vilket i sin tur kan skada förtroendet för sjukhuset.

## Revisionsfråga 7: Är roller och ansvar för dataskyddsarbetet tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller?

### Utgångspunkter

Se bakgrundstexten under revisionsfråga 2.

### Iakttagelser

I Riktlinje för behandling av personuppgifter på Karolinska universitetssjukhuset[48] finns en översiktlig beskrivning av rollerna personuppgiftsansvarig, personuppgiftsbiträde, medarbetare, dataskyddsombud, informationssäkerhetssamordnare samt informationssäkerhetskoordinator. Det anges exempelvis att styrelsen (det vill säga nämnden) är ytterst ansvarig för sjukhusets behandling av personuppgifter, att medarbetare ansvarar för att följa regler och riktlinjer, att dataskyddsombudet ska övervaka att relevant lagstiftning följs och att informationssäkerhetskoordinator ska koordinera data- och integritetsskyddsarbete inom respektive verksamhet.

Vi har inte kunnat identifiera någon beskrivning eller beslut om vilken funktion inom sjukhuset som *operativt* är ansvarig för att se till att personuppgifter hanteras korrekt. I riktlinjen för personuppgiftsbehandling[49] beskrivs att nämnden har det yttersta ansvaret och informationssäkerhetskoordinatorn har ansvaret för att samordna arbetet. I flera andra sammanhang beskrivs att verksamhetschefen är ansvarig för att tillse att den information som används inom ramen för den verksamhet man ansvarar för, hanteras korrekt.[50] I den operativa vägledningen beskrivs följande:

“Varje tema, funktion och stab kan ha utsedda informationssäkerhetskoordinatorer, om inte är det verksamhetschefens ansvar att tillse att arbetet genomförs. Koordinatorns ansvar är att tillsammans med informationssäkerhetssamordnaren och data-skyddsombuden koordinera arbetet kring integritetskyddsfrågor och informationssäkerhetsarbete inom respektive verksamhet.”.[51]

Av vissa intervjuer framgår att den operativa vägledningen inte är framtaget som ett sjukhusövergripande styrande dokument. Av andra intervjuer framgår samtidigt att den ursprungliga avsikten med koordinatorernas uppdrag var att det skulle täcka både informationssäkerhet och dataskydd. Dock uppfattades det som ett för omfattande uppdrag av flera, och därför har rollerna delats. Det framgår vidare av intervjuer att i den delningen har framförallt informationssäkerhetsdelen beaktats och därmed har det

[48] Ibid.
[49] Ibid.
[50] Se iakttagelser under revisionsfråga 2 samt exempelvis dokumentet Integritetsskyddsfrågor och informationssäkerhetsarbete – en operativ vägledning för informationssäkerhetskoordinatorer vid Karolinska Universitetssjukhuset.
[51] Ibid., s. 4.

operativa dataskyddsarbetet blivit utan samordning. Detta har i sin tur inte kunnat åtgärdats på grund av personalminskning.

Av enkäterna framgår att majoriteten av verksamhetscheferna inte anser sig vara ansvariga för dataskyddsarbetet, alternativt inte har någon ansvarig medarbetare för dataskydd. Enkätsvaren ger också ett intryck av att verksamhetscheferna har en bild av att dataskyddsarbetet sker “på sjukhusnivå” eller på rättskansliet, samtidigt som det i styrdokument och intervjuer uppges att arbetet ska ske på verksamhetsnivå eller inom stab teknik.

Det finns en roll- och uppdragsbeskrivning som regionen har tagit fram för dataskyddsombud.[52] Motsvarande beskrivning finns även för rollen som företrädare för den personuppgiftsansvarige[53] framtagen av regionen. Enligt den senare beskrivningen är rollen som företrädare viktig att identifiera eftersom det är den funktion som ska se till att dataskyddslagstiftningen efterlevs i det operativa arbetet. Exempel på uppgifter som beskrivs i dokumentet är att tillse att riskanalyser och konsekvensbedömningar görs, ta ställning till risknivåer och att ett korrekt behandlingsregister finns. Det framgår tydligt av dokumentet att det inte ska vara dataskyddsombudet men chef eller annan verksamhetsansvarig lyfts fram som exempel på vem som skulle kunna ha rollen.

Båda dessa dokument är kategoriserade som PM och det uppges vid intervju att de utgör vägledning och inte är obligatoriska. Vid intervju uppges också att Karolinska valt att inte använda sig av begreppet ”företrädare för den personuppgiftsansvarige” eller att följa innehållet i PM:en.

I sjukhusets arbets- och delegationsordning[54] finns endast ett fåtal beslut avseende dataskydd utpekat. Ett exempel är delegationen till sjukhusdirektören att utse dataskyddsombud. Ett annat är delegationen till verksamhetschef, där denne i egenskap av lokalt arkivansvarig också har beslutanderätt (verkställighet) avseende hantering och utlämning av personuppgifter som är reglerat i ett avtal. Vid intervjuer förklaras att sjukhuset har gjort bedömningen att ansvar för personuppgiftshantering kan inrymmas i arkivansvarig och att alla beslut avseende dataskydd kan inrymmas i denna delegation (begränsat till det specifika arkivansvaret).

Respondenter uppger att roller och ansvar avseende dataskydd kommuniceras via Karolinskas intranät. Samtidigt beskrivs att en tydlig roll- och ansvarsfördelning för dataskyddsarbetet saknas och att det upplevs som svårt att nå ut till alla medarbetare med information och vägledning.

Avseende rollen som personuppgiftsansvarig noterar vi att det vid intervjuer flertalet gånger refereras till Karolinska universitetssjukhuset som ett bolag med en styrelse.

**Bedömning**

*Är roller och ansvar för dataskydd arbetet tydliga, kända och blir medarbetarna informerade om förändringar i ansvar och roller?*

[52] Roll- och uppdragsbeskrivning för dataskyddsombud (DSO), dnr RS 2022-0667.
[53] Dnr RS 2022-0667.
[54] Dnr K 2024-0963.

Vi bedömer att roller och ansvar för dataskyddsarbetet inte är tydliga och kända och att förändringar inte kommuniceras på ett sätt som gör att medarbetare blir informerade.

Utifrån de otydliga och motsägelsefulla uppgifterna i styrande dokument, intervjuer och enkäter bedömer vi att rollerna är otydligt beskrivna och inte kända. Vi bedömer att det saknas en tydlig beskrivning och utdelat ansvar för det operativa dataskyddsarbetet. Regionen har uppmärksammat behovet av ett tydligt utdelat ansvar i dessa frågor genom PM:en om företrädare för den personuppgiftsansvarige. Detta ansvar hade kunnat tydliggöras i Karolinskas riktlinje om behandling av personuppgifter men eftersom det saknas där, och inte beskrivs tydligt på annan plats, bedömer vi att det operativa ansvaret saknar en tydlig ägare (vilket också avspeglas i brister i utförandet, se revisionsfråga 8-11).

Avseende arbets- och delegationsordningen[55] bedömer vi den som bristfällig utifrån att den i princip saknar beslut som bör vara delegerade avseende dataskydd. Sådana beslut är exempelvis beslut om riskanalys, konsekvensbedömning och avslag på utlämning av personuppgifter. Vi bedömer inte att den typen av beslut är möjliga att betrakta som verkställighet i kommunallagens mening (eftersom de kräver analys, avvägning och bedömning), och därför behöver de fattas direkt av nämnden, eller delegeras.

Den beslutspunkt som finns upptagen avseende “hantering och utlämning av personuppgifter” bedömer vi som felaktig av flera skäl. Dels för att beslut av den typen som avses bedömer vi som delegationsbeslut utifrån att de kräver avvägning och bedömning. Dels för att beslutspunkten är konstruerad på ett felaktigt sätt. Att en och samma funktion kan ha beslut både avseende arkiv och dataskydd delegerat till sig (så som vi tolkar att tanken i Karolinskas delegationsordning är), är i sig inte felaktigt. Däremot behöver delegationen specificeras så att det framgår vilket beslut som avses. Det är därför inte möjligt att delegera en odefinierad mängd beslut. Risken med en hantering såsom Karolinskas, förutom att den inte bedöms vara förenlig med gällande lagstiftning, är att den skapar en otydlighet kring beslutsmandaten i organisationen.

Vi anser också att lämpligheten i att likställa arkivområdet och dataskyddsområdet är tveksamt. Det är två områden som i vissa delar har gemensamma beröringspunkter (exempelvis gäller GDPR även arkiv) men i övrigt är det två områden som skiljer sig mycket åt. De har fundamentalt olika regelverk, det behöver fattas helt olika beslut, ansvarsutkrävandet skiljer sig åt och den operativa verksamheten görs utifrån helt olika principer och syften. Utifrån det perspektivet ser vi inte att den lösningen som Karolinska har valt bidrar till tydlighet och transparens i roller och ansvar. Det är heller inte en lösning som vi känner igen från liknande verksamheter.

Vi bedömer också att det operativa arbetet med dataskydd har eftersatts i och med oklarheterna kring om arbetet ingår i koordinatorrollen eller ej. I kombination med att roller och ansvar är otydliga skapas en betydande risk för att det operativa dataskyddsarbetet blir bristfälligt.

[55] Dnr K 2024-0963.

Vi bedömer det också som problematiskt att det verkar råda oklarheter bland de anställda om sjukhuset är ett bolag eller en nämnd. Råder det oklarheter kring vilken associationsform sjukhuset har, innebär det risk för att dataskyddsregelverket tillämpas felaktigt. Anledningen är att dataskyddsregelverket skiljer sig åt i viss utsträckning beroende på om den personuppgiftsansvarige är ett bolag eller en myndighet (exempelvis en nämnd som lyder under kommunallagen såsom Karolinska).

## Revisionsfråga 8: Är behandlingsregistret ändamålsenligt och hålls det aktuellt?

### Utgångspunkter

Som personuppgiftsansvarig organisation ska Karolinska föra ett behandlingsregister eftersom det är ett krav enligt GDPR.[56] Registret ska innehålla alla personuppgiftsbehandlingar som organisationen ansvarar för, och beskriva bland annat ändamålet med den specifika personuppgiftsbehandlingen, vilka personuppgifter som behandlas och hur länge uppgifterna sparas. Syftet med behandlingsregistret är att den personuppgiftsansvariga organisationen ska ha en tydlig och detaljerad översikt över de behandlingar man ansvarar för, kunna säkerställa de registrerades rättigheter avseende användningen av deras personuppgifter, samt underlätta förutsättningarna för tillsyn.

Utöver de formella kraven är också ett fullständigt och uppdaterat behandlingsregister första steget mot ett ändamålsenligt dataskyddsarbete. Anledningen är att personuppgiftsbehandlingar i de flesta fall är mer eller mindre riskfyllda, och för hälso- och sjukvård och forskning kan brister avseende dataskydd leda till stora verksamhets- och förtroendeskador. Genom ett korrekt behandlingsregister skapas förutsättningar för översikt och kontroll över behandlingarna, och därmed kan arbetet prioriteras utifrån risknivåer och risker systematiskt sänkas och till och med elimineras.

### Iakttagelser

Riktlinje för behandling av personuppgifter på Karolinska universitetssjukhuset[57] anger att sjukhuset ska föra ett skriftligt och elektroniskt register över all behandling av personuppgifter. Riktlinjen hänvisar även till en användarmanual för detta ändamål.[58]

Av både intervjuer och genom kontroll av registret framgår att informationen om hur och varför personuppgifter behandlas inte är sammanställt i ett komplett och uppdaterat behandlingsregister. Det framgår även att majoriteten av de registrerade behandlingarna är relaterade till forskningsverksamhet och inte till övrig sjukhusverksamhet (exempelvis journalföring, bilddiagnostik, remisshantering, personaladministration och rekrytering). Inget av de styrdokument vi tagit del av innehåller rutiner för att säkerställa att behandlingsregistret är korrekt över tid och att de behandlade personuppgifterna används för det syftet de samlades in för (vilket är en av de grundläggande principerna i GDPR).

Svaren i enkäterna indikerar stora osäkerheter kring hur behandlingsregistret hanteras. Några svar antyder att man inte vet vilket register som avses eller vet vad ett

[56] Artikel 30.
[57] Dokumentnr K51961.
[58] Användarmanual för registrering av personuppgiftsbehandling i Privacy Record, K05470.

behandlingsregister är för något, några svarar att någon annan funktion på sjukhuset är ansvarig för registret (verksamhetschef, dataskyddsombud, systemförvaltare) och några svarar att man inte för register. Några svarar att de fyller i behandlingsregistret men det är inget som vi har kunnat verifiera förutom inom forskningsverksamheten (se nedan). Några uppger också att registret hålls på "sjukhusnivå" och att det kontrolleras av dataskyddsombudet.

Under granskningen har vi tagit del av Karolinskas behandlingsregister. Det innehåller 468 behandlingar, och de allra flesta av dessa avser forskning.[59] Det befintliga behandlingsregistret innehåller omfattande informationspunkter för de behandlingar som har registrerats och användarmanual finns för att underlätta hantering. Dock är inte registret komplett ifyllt/färdigställt utan de flesta behandlingar saknar viss information.

Under tiden för granskningen behandlas dataskyddsombudets årliga rapport[60] av nämnden, och denna bekräftar att det trots tidigare ansträngningar och informationsinsatser, finns ett betydande antal personuppgiftsbehandlingar som inte anmälts till registret ännu.

I slutskedet av arbetet med denna rapport påbörjades ett arbete med att komplettera behandlingsregistret och det uppgavs vid intervjuer att det hade mycket hög prioritet.

**Bedömning**

*Är behandlingsregistret ändamålsenligt och hålls det aktuellt?*

Vår bedömning att behandlingsregistret inte är ändamålsenligt och det hålls inte aktuellt.

Vår bedömning att stora delar av Karolinskas personuppgiftsbehandlingar saknas i behandlingsregistret eftersom behandlingar avseende den ordinarie hälso- och sjukvården i princip saknas, samt även administrativa områden såsom ekonomi, HR och övergripande IT. Det innebär att det finns risk för att Karolinska inte följer GDPR avseende skyldigheten att hålla register över personuppgiftsbehandlingar.[61] Att inte ha kontroll och översikt över vilka behandlingar organisationen ansvarar för innebär också svårigheter att leva upp till kraven i GDPR avseende att kunna lämna information och ge tillgång till de registrerade avseende de behandlingar de omfattas av.[62]

Intervjuer och enkätsvar visar att vissa respondenter har uppfattningen att någon annan ansvarar för behandlingsregistret, trots att så inte är fallet, tyder också på ett bristfälligt arbetssätt och otydligt kommunicerade roller och ansvar.

Utifrån ett strategiskt riskhanteringsperspektiv är det att betrakta som en betydande verksamhetsrisk att inte ha kontroll över vilka personuppgiftsbehandlingar organisationen ansvarar för. Personuppgiftsbehandlingar innebär generellt alltid risker, och för hälso- och sjukvård och forskning kan brister avseende dataskydd arbetet leda till skador både för verksamheten (exempelvis sanktionsavgifter, skadestånd,

[59] Utdrag registerförteckning mottaget: 2024-04-23.
[60] Dataskyddsombudens årsrapport till Karolinska Universitetssjukhusets styrelse 2024-04-23, K 2024-3369.
[61] Art. 30 GDPR.
[62] Art. 12-15 GDPR.

förtroendeskador och försämrade förutsättningar att bedriva verksamhet). Första steget för ett adekvat dataskyddsarbete är att ha kontroll över vilka behandlingar organisationen ansvarar för. På det sättet kan arbetet prioriteras utifrån risknivåer och därmed kan risker systematiskt sänkas och till och med elimineras.

## Revisionsfråga 9: Genomförs riskanalyser avseende personuppgiftshantering på ett ändamålsenligt sätt?

### Utgångspunkter

Riskanalyser avseende dataskydd är ett grundläggande verktyg för att en personuppgiftsansvarig organisation ska kunna bedöma och hantera risker för att förhindra dataintrång, förlust, och andra säkerhetsincidenter som kan äventyra personuppgifter. Resultatet av en riskanalys används för att implementera lämpliga tekniska och organisatoriska åtgärder, vilket bidrar till att säkerställa att personuppgiftshanteringen är förenlig med GDPR och andra relevanta lagar och regler avseende personuppgiftsbehandling.

Att arbeta systematiskt med riskanalyser, och dokumentera genomförandet av dem, är också ett sätt att uppfylla principen om ansvarsskyldighet.[63] Den innebär att den personuppgiftsansvarige ska kunna visa att behandlingen är förenlig med GDPR och att lämpliga tekniska och organisatoriska åtgärder har vidtagits för att skydda de registrerades rättigheter och friheter (det vill säga kunna visa hur detta går till). Det finns också andra lagstadgade krav som mer eller mindre direkt innebär krav på riskanalyser avseende personuppgiftsbehandling. Exempel på ett sådant krav återfinns i Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.[64]

### Iakttagelser

Det finns flera vägledningar från Region Stockholm som beskriver olika delar av dataskyddsarbetet. Ett av dessa är Introduktion till systematiskt riskbaserat integritetsskyddsarbete.[65] I detta dokument framgår att när en personuppgiftsbehandling inleds eller förändras ska det alltid genomföras en grundläggande bedömning (inte detsamma som konsekvensbedömning utan endast en inledande analys) som bland annat inkluderar en riskbedömning.

Av Karolinskas egen riktlinje för personuppgiftsbehandling[66] framgår att det inför varje ny personuppgiftbehandling ska göras en analys av vilka risker behandlingen kan innebära och vilka säkerhetsåtgärder som därmed behövs. I riktlinjen framgår däremot inte hur förändrade risker ska hanteras (exempelvis vid förändring i ett IT-system eller en förändring avseende vilka personuppgifter som behandlas). Riktlinjen innehåller ingen hänvisning till vägledning eller mall avseende en sådan analys, och vi har inte under granskningen kunnat identifiera någon specifik vägledning, mall eller liknande för detta.

---

[63] GDPR, art. 6 p. 2.
[64] 3 kap. 5 §.
[65] Dnr RS 2020-0935.
[66] Riktlinje för behandling av personuppgifter på Karolinska Universitetssjukhuset, dokumentnr K51961.

Det finns även en sjukhusövergripande riktlinje[67] med tillhörande mall[68] för bedömning, hantering och eventuellt åtgärdande av risker utifrån ett generellt perspektiv. Ett av riskområdena som rubriceras i mallen är ”Data- och integritetsskydd – risk för data- och integritetsintrång”, vilket är begrepp som inte generellt används i andra sammanhang. Det saknas förklaring till rubriken, eller hänvisning till stödjande dokument (både i riktlinjen och mallen).

Det finns ett metodstöd för arbetet med konsekvensbedömningar framtaget av Region Stockholm.[69] Det innehåller även vägledning avseende riskanalysen eftersom den är en förutsättning för konsekvensbedömningens genomförande. Dock bygger vägledningen i metodstödet på regionens egen mall avseende konsekvensbedömning, som innehåller ett frågebatteri för att identifiera risker och risknivå. I denna granskning har vi inte kunnat se att varken frågebatteriet avseende risker eller regionens mall för konsekvensbedömning används (Karolinska har en egen mall för konsekvensbedömning), varför metodstödet inte blir helt användningsbart avseende riskanalysen.

Av intervjuer framgår att det finns brister i metoder och kriterier för att genomföra riskanalyser inom Karolinska. Det uppges att det saknas en systematisk och strukturerad process för att bedöma och hantera risker avseende dataskydd, både avseende styrande dokument och efterlevnad av dessa. Det är även oklart hur ofta och vid vilka tillfällen riskanalyser avseende personuppgiftshantering genomförs eftersom det inte finns någon samlad översikt av riskanalyser avseende personuppgiftshantering. Det lyfts också att det tidigare inom verksamheterna funnits en bristande förståelse för konsekvenserna av att inte riskbedöma behandlingar och att därmed inte följa regler och riktlinjer. Vidare lyfts i intervjuer att mycket arbete har lagts ner på att utveckla den generella processen kopplat till riskhantering och internkontroll på sjukhuset samt att processen är relativt ny. Därför framhålls det vid intervjuer att det förväntas en förbättring inom området.

I enkäterna framkommer varierande svar på om verksamheterna upprättar riskanalyser avseende personuppgiftsbehandlingar eller ej. Vissa anger att riskanalyser inte görs på verksamhetsnivå utan sjukhusnivå, att riskanalyser görs vid behov eller vid nya processer, att riskanalyser inte görs alls, eller att man inte vet om det görs riskanalyser samt att riskanalys görs vid personuppgiftshantering i forskningssyfte inom ramen för etikprövningen. Endast två av respondenterna besvarar frågan hur riskerna rapporteras.

Av stickprov tagna vid denna granskning framgår att dataskyddsrisker inte är inkluderade i de riskanalyser som utförts på de system som kontrollerats. Vissa informationssäkerhetsrisker har bäring på dataskydd och finns med i det material som ingått i stickproven. Eftersom dataskydd inte ingår i egenkontrollen via Complianceportalen finns heller inga risker analyserade genom dessa formulär.

[67] Riktlinje riskbedömning, dokumentnr K61957.
[68] Riskbedömningsmall inkl. riskmatris ver. 2.0, dokumentnr K61958.
[69] Metodstöd inför och under genomförande av konsekvensbedömning avseende dataskydd (DPIA), dnr saknas.

**Bedömning**

*Genomförs riskanalyser avseende personuppgiftshantering på ett ändamålsenligt sätt?*

Vår bedömning är att sjukhuset inte genomför riskanalyser avseende personuppgiftshantering på ett ändamålsenligt sätt.

Vår bedömning är att Karolinska saknar en tydlig process för att identifiera och analysera risker relaterade till personuppgiftshantering. Även om det finns riktlinjer för att bedöma vilka risker som kan uppstå och hur de kan påverka patienternas integritet och säkerhet, utmynnar detta inte i tydliga processer och tillvägagångssätt eller krav på dokumentation. Övergripande framgår inte tydligt hur riskerna som identifierats i riskanalyser dokumenteras, rapporteras och prioriteras. Det finns en brist på strukturerad dokumentation och rapportering av riskerna.

Vidare indikerar intervjuer, enkäter och stickprov att verksamheterna inte är medvetna om vikten av att genomföra riskanalyser och inte har tillräcklig kunskap om hur man gör det.

Det är positivt att det i riktlinjen för personuppgiftsbehandling är tydligt angivet att riskanalyser ska genomföras innan personuppgiftsbehandling påbörjas. I praktiken innebär dock “innan” ett långt eller till och med mycket långt tidsspann (det kan handla om flera års tid). Ofta består också den tidsperioden av ett antal olika moment såsom förstudie, upphandling, anpassning och implementering. Om en riskanalys exempelvis görs i samband med implementering, men innan driftsättning, är risken stor att det uppdagas risker som i realiteten inte går att åtgärda med mindre än att systemet inte tas i bruk. Vilket i sin tur ofta får olyckliga konsekvenser för verksamheten. Därför behövs en tydlig process, där risker analyseras kontinuerligt för att minimera risken för inlåsningseffekter. Ofta innebär detta att det behöver tydliggöras explicit vid vilka tillfällen i exempelvis en upphandlingsprocess som riskanalyser behöver göras och/eller stämmas av, vilket saknas i Karolinskas fall.

Eftersom Karolinska saknar ett fullständigt register över de personuppgifter som behandlas och vilka risker som är förknippade med dem, saknas systematisk dokumentation av vilka personuppgifter som samlas in, hur de används och vilka åtgärder som vidtas för att skydda dessa. Det saknas även kontinuerlig övervakning eller utvärdering av riskerna relaterade till personuppgiftshantering på Karolinska. Det innebär att eventuella nya risker eller förändringar i befintliga risker potentiellt inte upptäcks eller åtgärdas i tid. Avsaknaden av processer för riskanalyser innebär även att Karolinska inte kan bedöma om tillräckliga tekniska och organisatoriska åtgärder är på plats för att skydda personuppgifterna, vilket innebär en risk för att GDPR inte kan efterlevas.

## Revisionsfråga 10: Genomförs konsekvensbedömningar enligt GDPR på ett ändamålsenligt sätt?

### Utgångspunkter

Konsekvensbedömningar enligt GDPR är obligatoriska när en typ av behandling sannolikt leder till en hög risk för de registrerades rättigheter och friheter.[70] Huvudregeln är också att konsekvensbedömningen ska göras innan en personuppgiftsbehandling påbörjas (exempelvis när ett IT-system tas i bruk), och god praxis är att bedömningen kontinuerligt ses över och utvärderas.[71] Bedömning av vad som sannolikt innebär en hög risk ska göras utifrån den förteckning som är framtagen av IMY i enlighet med GDPR.[72] Exempel på sådana behandlingar kan vara när stora mängder av personuppgifter behandlas, när känsliga personuppgifter behandlas, när de registrerade är i beroendeställning till den personuppgiftsansvarige eller när ny teknik används.[73]

Konsekvensbedömningen ska enligt GDPR åtminstone innehålla en systematisk beskrivning av personuppgiftsbehandlingen, bedömning av behovet och proportionaliteten, bedömning av riskerna för de registrerades rättigheter och friheter, samt de planerade skydds- och säkerhetsåtgärderna.[74] Det är också obligatoriskt att konsultera dataskyddsombudet.[75]

Sammantaget betyder detta att ett ändamålsenligt genomförande av konsekvensbedömningar innebär att dessa sker i relativt stor utsträckning i en verksamhet som Karolinskas (IMY lyfter i sin vägledning avseende konsekvensbedömningar särskilt fram vårdgivares behandling av personuppgifter som ett exempel på när konsekvensbedömning behövs), att dess innehåll följer de regler och rekommendationer som finns, samt att bedömningarna hålls aktuella och vid behov ändras.

Eftersom konsekvensbedömningarna enligt GDPR har många gemensamma nämnare med exempelvis informationsklassning, riskanalyser och analyser avseende IT-säkerhet, går det även att skapa ett arbetssätt som innebär en resurseffektiv hantering av arbetet där synergieffekterna tas om hand. Ett systematiskt arbete med behandlingsregistret är också ett verktyg för att samordna arbetet och bygga ett effektivt arbetssätt avseende konsekvensbedömningarna.

### Iakttagelser

Av riktlinjen för personuppgiftsbehandling[76] framgår att det inför varje ny personuppgiftsbehandling ska analyseras vilka risker personuppgiftsbehandlingen kan innebära och föreslås lämpliga säkerhetsåtgärder. Det framgår inte tydligt av riktlinjen

---

[70] GDPR, art. 35 p.1.
[71] Se exempelvis https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/forteckning-over-nar-en-konsekvensbedomning-ska-goras/, 2024-06-02.
[72] Art. 35 p. 4.
[73] GDPR. art. 35 p. 3.
[74] Art. 35 p. 7.
[75] GDPR, art. 35 p. 2.
[76] Riktlinje för behandling av personuppgifter på Karolinska Universitetssjukhuset, dokumentnr K51961.

vem som är ansvarig för att utföra konsekvensbedömningen eller den initiala riskbedömningen.

Vid intervjuer uppges att det finns brister i genomförandet av konsekvensbedömningar enligt GDPR inom Karolinska. Respondenterna beskriver att det finns brister avseende både kunskap och medvetenhet samt att konsekvensbedömningar sannolikt inte görs i den utsträckning som det borde ske. Vidare anger respondenterna också att aktualitetshållande och revidering av genomförda konsekvensbedömningar sannolikt brister ännu mer. Det uppges att de funktioner som behöver involveras som specialister i konsekvensbedömningarna endast vid enstaka tillfällen har sett konsekvensbedömningar eller blivit involverade i arbetet.

I enkäterna besvaras frågan om hur man arbetar med konsekvensbedömningar på olika och ibland något svårtolkade sätt. Två av svaren beskriver på ett tydligt sätt att man känner till sjukhusets riktlinjer och beskriver hur arbetet går till. Övriga svar beskriver övergripande att riktlinjerna följs (utan att besvara frågan om hur det arbetet går till), att konsekvensbedömningar inte görs regelbundet alternativt att verksamheterna inte vet om konsekvensbedömningar upprättas överhuvudtaget.

I den årliga rapporten av dataskyddsombudet anges både för år 2023[77] och 2024[78] att genomförande av konsekvensbedömning inte sker av någon utpekad funktion eller person inom verksamheterna men att dataskyddsombudet har som långsiktigt mål att verka för en översyn av vilken funktion som ska/bör genomföra en konsekvensbedömning.

Av stickproven tagna i denna granskning framgår att konsekvensbedömning utförts som en bedömning som avser två av de tre kontrollerade systemen (bilddiagnostik). Dock omfattas inte båda systemens totala personuppgiftsbehandlingar av konsekvensbedömningen, utan endast en avgränsad del. Vi har inte kunnat återfinna något av de tre kontrollerade systemen i behandlingsregistret, och därför kan vi inte inom ramen för denna granskning verifiera vilka personuppgifter som förekommer i de kontrollerade systemen. Det innebär i sin tur att vi inte med säkerhet kan bedöma om samtliga kontrollerade system bör genomgå konsekvensbedömning.

**Bedömning**

*Genomförs konsekvensbedömningar enligt GDPR på ett ändamålsenligt sätt?*

Vår bedömning är att konsekvensbedömningar enligt GDPR delvis genomförs på ett ändamålsenligt sätt, utifrån de brister vi kan konstatera i stickproven (både avseende genomförande och innehåll), uppgifterna i enkäten samt de redogörelser som lämnats vid intervjuer. Vår bedömning ligger även i linje med den bedömning som dataskyddsombudet gjort i de senaste årens årsrapporter.

Även om vi inte med säkerhet kan konstatera att samtliga genom stickprov kontrollerade system borde ha genomgått en konsekvensbedömning avseende GDPR, borde åtminstone en första analys/bedömning avseende personuppgiftsbehandlingen ha

[77] Dataskyddsombudens årsrapport till Karolinska Universitetssjukhusets styrelse 2024-04-23, K 2024-3369.
[78] Dataskyddsombudens årsrapport till styrelse 2023-04-24, K 2023-3784.

genomförts i enlighet med Karolinskas egen riktlinje.[79] Utifrån systemens funktion samt volymen och naturen avseende de personuppgifter som mest sannolikt behandlas i systemen, bedömer vi det som troligt att samtliga tre kontrollerade system hade behövt genomgå varsin eller en sammanhållen konsekvensbedömning.[80]

Den konsekvensbedömning som vi tagit del av är skriven i vad som framstår som en mall framtagen för sjukhuset och den är genomförd 2020. Det framgår också att den avser en begränsad del av systemet och att resten av systemet ska bedömas vid ett senare tillfälle. Någon sådan bedömning har vi inte fått ta del av. Vi har inte heller kunnat se att samråd avseende innehållet i bedömningen har skett med dataskyddsombudet, vilket krävs enligt GDPR.[81] Samtliga fält/frågor i mallen/formuläret är ifyllda, men vi bedömer att mallen/formuläret inte innehåller alla områden som en konsekvensbedömning behöver göra för att uppfylla kraven i GDPR. Det framgår exempelvis inte vilka personuppgifter som ska behandlas eller hur behandlingen ska gå till[82] eller proportionaliteten i behandlingen.[83] Analysen av risker och de planerade skyddsåtgärderna är endast översiktlig eftersom den är utformad i huvudsak som ikryssade av rutor med förskriven text. Konsekvensbedömningen innehåller endast ett antal föreslagna riskreducerande åtgärder, men det framgår inte om dessa i realiteten därefter har blivit genomförda.

I och med att det av riktlinjen inte tydligt är utpekat vilka funktioner som är ansvariga för att se till att konsekvensbedömningar görs och hålls uppdaterade, riskerar dessa att inte bli genomförda.

I sammanhanget vill vi tydliggöra att vi uppfattar att den ansvariga för det kontrollerade systemet har följt den framtagna mallen. Däremot är mallen missvisande och riskerar att inte ge förutsättningar för genomförande av en konsekvensbedömning i enlighet med lagkraven.

## Revisionsfråga 11: Hålls riskanalyser och konsekvensbedömningar aktuella på ett ändamålsenligt sätt?

### Utgångspunkter

Det finns både direkta och indirekta krav avseende att hålla riskanalyser och konsekvensbedömningar aktuella och uppdaterade. Dessa redogörs för under revisionsfråga tre och tio.

Grunden för att hålla riskanalyser och konsekvensbedömningar aktuella är den översiktliga kontrollen av både IT-system och personuppgiftsbehandlingar. Utifrån den kan en systematik byggas för regelbundna avstämningar, kontrollsystem vid förändringar av system eller arbetssätt, samt kontrollsystem vid upphandling och implementering av nya system. Systematiken kan se olika ut beroende på de specifika

[79] Riktlinje för behandling av personuppgifter på Karolinska Universitetssjukhuset, dokumentnr K51961.
[80] Även med hänsyn tagen till art. 35 p. 10 GDPR.
[81] Art. 35 p. 2 GDPR.
[82] Art. 35 p. 7a GDPR.
[83] Art. 35 p. 7b GDPR.

förutsättningarna, men täcks ovan beskrivna tre områden in brukar normalt en tillräcklig grad av aktualitetshållande uppnås.

Om riskanalyser och konsekvensbedömningar inte hålls aktuella på ett ändamålsenligt sätt kan det leda till att den personuppgiftsansvarige inte vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt genomförande av grundläggande dataskyddsprinciper eller integrerar de nödvändiga skyddsåtgärderna i behandlingen när förutsättningar förändras.

**Iakttagelser**

Av intervjuer framgår det att det är oklart hur ofta och vid vilka tillfällen konsekvensbedömningar genomförs eftersom det saknas en översiktlig kontroll på genomförandet. Konsekvensbedömningarna finns inte samlade, det förs ingen statistik över antalet genomförda bedömningar och de intervjuade uppger att de involveras i bedömningarna endast vid sporadiska tillfällen.

Vidare uppges vid intervjuer att verksamhetschefer är ansvariga för att uppdatera riskanalyser och konsekvensbedömningar. Eftersom det saknas en övergripande kontroll på i vilken omfattning riskanalyser görs, och hur ofta de uppdateras, saknas kunskap om hur ofta riskanalyser görs och hur de hålls aktuella. Det beskrivs att okunskap bidrar till att konsekvens- och riskbedömningar inte utformas på ett korrekt sätt, inte uppdateras och därmed att verksamheterna inte kan ta välgrundade beslut. De styrande dokumenten innehåller inte tydlig information om vem som ansvarar för att riskanalyser och konsekvensbedömningar. Riktlinjen för informationssäkerhet anger verksamhetsansvariga som ansvariga för informationssäkerhet i den aktuella verksamheten, i riktlinjen för personuppgiftsbehandling tas detta inte upp alls och i riktlinjen för arbetsflöden, roller, organisation och mandat gällande informationssäkerhet och IT-säkerhet[84] beskrivs att informationssäkerhetskoordinatorn har ansvaret för att samordna och stödja vid bland annat riskanalyser.

Av enkäterna framgår att de flesta verksamhetschefen uppfattar sig som ansvariga för arbetet med riskanalyser och att detta sker enligt Karolinskas rutiner alternativt att arbetet görs på olika nivåer inom verksamheten.

Av stickprov framgår, som redogjorts ovan, att dataskydd inte inkluderats i riskanalyser, samt att den konsekvensbedömning vi mottagit för ett av tre verksamhetsöverskridande system som behandlar personuppgifter, är bristfällig. Den aktuella konsekvensbedömningen genomfördes 2020.

**Bedömning**

*Hålls riskanalyser och konsekvensbedömningar aktuella på ett ändamålsenligt sätt?*

Vi bedömer att riskanalyser och konsekvensbedömningar inte hålls aktuella på ett ändamålsenligt sätt vilket kan leda till att Karolinska inte vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt genomförande av grundläggande dataskyddsprinciper eller integrerar de nödvändiga skyddsåtgärderna i behandlingen när förutsättningar väsentligen förändras. Vi kan inte verifiera om

[84] Dokumentnr: K62392.

konsekvensbedömningar årligen revideras efter behov eller när omständigheter förändras. En brist är att det inte finns någon övergripande kontroll och enhetlig process för att hantera riskanalyser och konsekvensbedömningar relaterade till personuppgiftsbehandlingar och att vi därför inte kan verifiera att dessa görs eller hålls aktuella på ett ändamålsenligt sätt.

Bedömningen i den aktuella konsekvensbedömningen är att behandlingen innebär en risk för de registrerades integritet, och man bedömer även att fem av sju kriterier som ligger till grund för om konsekvensbedömning behövs, är uppfyllda. Vi bedömer det som bristfälligt att man inte gått vidare och färdigställt konsekvensbedömningen såsom planerat. Sannolikt har det också skett förändringar och uppdateringar som medfört behov av uppdaterad konsekvensbedömning, men det har vi inte kunnat se att det har genomförts.

## Revisionsfråga 12: Genomförs uppföljningen av dataskyddsarbetet på ett ändamålsenligt sätt?

**Utgångspunkter**

Systematisk uppföljning av dataskyddsarbete är ett sätt att säkerställa att Karolinska följer de lagar, regler och riktlinjer som gäller för hantering av personuppgifter. Genom uppföljning kan Karolinska identifiera och åtgärda eventuella brister, risker eller incidenter samt utvärdera och förbättra sina processer, rutiner och system löpande för att säkerställa ett ändamålsenligt dataskyddsarbete och regelefterlevnad. Omfattningen av uppföljningen behöver stå i proportion till risknivån. En verksamhet som Karolinska bedriver innebär generellt en hög risknivå avseende dataskydd, och därför behöver uppföljningen vara relativt omfattande.

För att leva upp till regeln i kommunallagen om att nämnden ska se till att verksamheten följer gällande regler och ha en tillräcklig intern kontroll, behöver nämnden följa upp hur regelefterlevnaden i praktiken fungerar. För att kunna leva upp till principen om ansvarsskyldighet som finns i GDPR (det vill säga att kunna visa både att dataskyddslagstiftning efterlevs och hur det görs) behöver också uppföljning ske. Det innebär i sin tur att även uppföljning av specifika personuppgiftbehandlingar behöver göras.

Att genomföra uppföljning av personuppgiftsbehandlingar och dataskydds arbetet innebär också att den personuppgiftsansvarige regelbundet utvärderar riskerna med olika behandlingar av personuppgifter, vilket i sin tur ger möjlighet till att systematiskt minska riskexponeringen på detta område.

Om dataskyddsarbetet inte följs upp, kan det både leda till brister avseende regelefterlevnad och förhöjda säkerhetsrisker, samt att arbetet inte sker effektivt och utifrån beslutade prioriteringar.

**lakttagelser**
Vi har inte kunnat identifiera att det genomförs någon uppföljning av dataskydd regelbundet inom organisationen, mer än den som ges av dataskyddsombudets årliga rapport.

Rapporten som avser 2022/23[85] belyser att i slutet av 2022 beslutades om en omorganisation där sjukhuset framgent skulle ha ett dataskyddsombud och en dataskyddsjurist istället för två dataskyddsombud. Det bedöms att behandlingsregistret fortfarande är ofullständigt, att det finns behov av förenklat arbetssätt och mer utbildning avseende konsekvensbedömningar, att 19 personuppgiftsincidenter rapporterats till IMY under 2022 men att man uppskattar att det totala antalet är betydligt fler samt att hanteringen av personuppgifter i kvalitetsregister brister på ett flertal punkter. Dataskyddsombuden uppger vidare att arbetet för 2023 ska fokuseras på personuppgiftsincidenter samt konsekvensbedömningar.

Rapporten som avser 2023/24[86] lyfter samma brister som den föregående rapporten avseende behandlingsregister och konsekvensbedömningar. Av rapporten framgår att Karolinska rapporterade 10 personuppgiftsincidenter till IMY 2023 men att dataskyddsombudet befarar att antalet incidenter är betydligt högre. Dataskyddsombudet bedömer att sjukhuset har ett väl fungerande arbetssätt avseende rapportering av incidenter, men däremot bedöms att kunskapsnivån avseende vad som utgör en personuppgiftsincident är låg.

Dataskyddsombudet ger nämnden ett antal rekommendationer för att implementera ett riskbaserat arbete med dataskyddsfrågor (såsom GDPR stipulerar). Bland annat rekommenderas att identifiera vilka behandlingar som görs genom ett behandlingsregister, att varje behandling ska riskbedömas samt att arbeta med att minimera riskerna.

Vi har inte kunnat identifiera att den årliga rapporten har följts upp av exempelvis en dokumenterad åtgärds- eller handlingsplan, eller beslut om specifikt uppdrag, för att hantera bristerna.

Vid intervjuer uppges att Region Stockholms verktyg med självdeklarationer i Complianceportalen inte avser dataskydd utan endast informationssäkerhet och att dataskyddsombud inte har tillgång till informationen i Complianceportalen. Det uppges att antalet ärenden som inkommer till funktionsbrevlådan för dataskydd räknas, men att dataskyddsarbetet inte mäts eller följs upp på annat sätt.

I enkäten har svaren på frågan om och i så fall hur dataskyddsarbetet följts upp besvarats varierat. De flesta har svarat att dataskydd inte följs upp alls, alternativt att det följs upp på sjukhusnivå. Några svar hänvisar till avvikelserapportering, incidenthanteringsrutiner, loggkontroller eller diskussioner på arbetsplatsträffar.

[85] Dataskyddsombudens årsrapport till styrelse 2023-04-24, dnr K 2023-3784.
[86] Dataskyddsombudens årsrapport till Karolinska Universitetssjukhusets styrelse 2024-04-23, dnr K 2024-3369.

Avseende uppföljning till nämnden sker den genom återrapportering av dataskyddsombudets rapport. I övrigt har vi inte kunnat identifiera att någon uppföljning eller återrapportering sker.

**Bedömning**

*Genomförs uppföljningen av dataskyddsarbetet på ett ändamålsenligt sätt?*

Vi bedömer att uppföljning av dataskyddsarbetet inte sker på ett ändamålsenligt sätt.

Den årliga rapporten av dataskyddsombudet är ett bra verktyg för uppföljning, men vår bedömning är att den inte bygger på ett systematiskt inhämtat underlag, utan snarare på dataskyddsombudets iakttagelser. Det är viktiga iakttagelser som behöver lyftas till nämnden, men de behöver kompletteras av systematisk uppföljning för att nämnden ska kunna säkerställa att Karolinska efterlever lagstiftning och interna regler (exempelvis genom stickprov eller systematisk uppföljning på övergripande nivå). Vår bedömning av svaren i enkäterna är att ansvariga chefer antingen inte är medvetna om någon uppföljning, alternativt att man hänvisar till moment som inte utgör egentlig uppföljning (exempelvis incidenthantering).

Vi bedömer också att nämnden agerat passivt i och med att dataskyddsombudets rapport indikerat brister, men vi har inte kunnat se att detta har resulterat i någon form av agerande eller uppdrag från nämndens sida.

Eftersom vi i övrigt inte kunnat identifiera att det sker någon uppföljning, är vår bedömning att Karolinska inte har kontroll över om lagstiftning eller interna regler i realiteten följs.

På detta område vill vi också uppmärksamma den knapphändiga uppföljningen av det operativa arbetet (exempelvis mätning av volymer för ärenden, vissa typer av ärendetyper, nöjdhet hos verksamheten och så vidare). Att kvantitativt följa upp arbetet, och analysera den datan, hjälper till att kunna allokera resurser till rätt områden, att sätta in utbildningsinsatser där det mest behövs och att över tid kunna följa om organisationen utvecklas och förbättras inom området. För att arbeta resurseffektivt med dataskydd är detta en viktig åtgärd. Exempel på sådan uppföljning är att följa personuppgiftsincidenter och analysera dessa. Detta kan ge insikter om var risker och brister finns och hur dessa mest effektivt kan åtgärdas (exempelvis om det behövs uppdaterade tekniska skyddsåtgärder eller utbildningsinsatser). Ett annat exempel är att följa upp vilka konsekvensbedömningar som görs och för vilka system/personuppgiftsbehandlingar de saknas för. På så sätt kan arbetet prioriteras och resurser kan allokeras till de områden där riskerna är som störst.

# Uppföljning av tidigare granskningar

Uppföljningen av nedanstående rekommendationer har genomförts integrerat med den huvudsakliga granskningen. Däremot redovisas bedömningen av rekommendationernas genomförande särskilt i denna rapport för tydlighetens skull. Vissa av rekommendationerna sammanfaller med revisionsfrågor i den huvudsakliga granskningen, varför uppgifter och resonemang kan återkomma i detta avsnitt.

## Egenkontroller och riskanalyser avseende regelefterlevnad av GDPR (id 29845)

Utifrån iakttagelser och bedömningar under revisionsfrågorna 6, 8-10 samt 12 bedömer vi inte denna rekommendation som genomförd.

## Grundläggande systematiskt informationssäkerhetsarbete för samtliga verksamheter på alla nivåer (id 29851)

Utifrån iakttagelser och bedömningar under revisionsfrågorna 1-5 bedömer vi denna rekommendation som delvis genomförd.

## Utbildning för alla medarbetare i informationssäkerhet och systematisk uppföljning av att dessa genomförs (id 29852) och (id 97668)

Utifrån iakttagelser och bedömning under revisionsfråga 4 gör vi bedömningen att statusen avseende dessa rekommendationer inte har ändrats i någon väsentlig utsträckning. Incitamenten för att se till att medarbetare genomför DISA-utbildningen har minskat sedan rekommendationen gavs eftersom genomförandet inte längre är en förutsättning för att erhålla tjänstelegitimation. Antalet anställda som genomför DISA-utbildningen följs upp. Samtidigt uppges i intervjuer att uppföljningen innehåller stora felmarginaler. Felmarginalerna innebär därför sannolikt att fler anställda har genomgått utbildningen än registrerat.

## Åtgärdsplan och nyckelkontroller för att säkerställa efterlevnad av NIS-direktivet (id 97667)

**Iakttagelser**

Vid intervjuer uppges att arbete avseende områden som är kopplade till NIS-direktivet (främst IT-, informations-, och cybersäkerhet) pågår kontinuerligt. En åtgärd som lyfts fram är den gap-analys som genomförts, och som i sin tur resulterade i en handlingsplan för att åtgärda de identifierade bristerna. Det uppges att utfallet av gap-analysen resulterade i ett resurstillskott för arbete med IT-säkerhet eftersom bristerna var så pass allvarliga. Det uppges att gap-analysen rapporterats till sjukhusdirektören, dock inte till nämnd.

I underlaget för Karolinskas verksamhetsplan ingår en riskkartläggning. Där finns flera risker inom detta område upptagna; robusthet i IT-system för att kunna motstå olika former av attacker och tydlighet avseende roller och ansvar kopplat till IT-säkerhet samt informationssäkerhet. Ett antal åtgärder är beskrivna i dokumentet och dessa ska vara genomförda under 2024.

**Bedömning**

Vår bedömning är att rekommendationen delvis är uppfylld.

Bedömningen är att medvetenheten avseende betydelsen av IT-, informations-, och cybersäkerhet är hög, och lyhördheten för de identifierade bristerna är tydlig. Vi uppfattar däremot inte att något strukturerat arbete specifikt riktat mot NIS-efterlevnad pågår, eller att kontroll finns att lagkraven efterlevs.

Eftersom ett nytt NIS-direktiv finns, och en ny lagstiftning förväntas träda i kraft 1 januari 2025 (cybersäkerhetslagen) bedömer vi det som viktigt att Karolinska fokuserar sitt arbete utifrån den nya lagstiftningen. Den förväntas innebära relativt stora förändringar och ökade krav, vilket innebär att det är viktigt att Karolinska gör en bedömning av dess status i relation till de nya kraven, och vilka åtgärder som behöver vidtas.

## Systematisk kontinuitetsplanering avseende informationssäkerhet (id 97669)

**Iakttagelser**

Vid intervjuer uppges att utifrån ett centralt säkerhetsperspektiv finns det endast resurser (0,5 heltidstjänster) som räcker till att arbeta övergripande med att styra och stödja arbetet med kontinuitet. Detta görs genom policy för kontinuitetsplanering[87] och ett metodstöd som är under framtagande. I intervjuer uppges också att vid de större kris- och katastrofövningarna inkluderas även informationssäkerhetsperspektivet. På det sättet uppges att kontinuitetsplaneringen avseende informationssäkerhet på övergripande nivå övas och utvecklas.

Policyn slår fast att Karolinskas chefer ansvarar för kontinuitetsplanering inom sina egna ansvarsområden, att lyfta identifierade risker och sårbarheter som inte går att åtgärda inom den egna verksamheten samt att analysera verksamheten och ta fram kontinuitetsplaner därefter.

I enkätsvaren beskrivs från central IT-förvaltning att man arbetar med informationssäkerhet utifrån ett IT-perspektiv genom tester, utveckling av rutiner samt säkerställande av att rutinerna följs. Verksamhetscheferna å sin sida uppger exempelvis att kontinuitetsplanering avseende informationssäkerhet hanteras “på sjukhusnivå” eller att man inte vet. Ingen av de svarande har uppgett att de själva hanterar frågan och testar sina planer utifrån ett informationssäkerhetsperspektiv.

Under granskningen har vi inte kunnat identifiera att kontinuitetsplanering avseende informationssäkerhet finns upptagen i underlaget för sjukhusets verksamhetsplan eller plan för internkontroll, varken för 2023 eller 2024.

**Bedömning**

Vår bedömning är att rekommendationen inte är genomförd.

Det är tydligt att Karolinska arbetar med kontinuitetsplanering på olika sätt, men vår bedömning är att perspektivet informationssäkerhet inte är inkluderat på ett systematiskt sätt. Vi bedömer inte heller att arbetet hålls samman eller följs upp, vilket i sin tur

[87] Policy Kontinuitetsplanering, dokumentnr. STAB7332.

innebär att varken förvaltningen eller nämnden kan bedömas ha kontroll på att informationssäkerhetsperspektivet i kontinuitetsarbetet är säkerställt.

# Samlad bedömning

## Systematiskt informationssäkerhetsarbete

Utifrån genomförd granskning är vår samlade bedömning att Karolinska universitetssjukhuset delvis bedriver ett ändamålsenligt arbete avseende systematisk informationssäkerhet.

Det är uppenbart att ett ambitiöst och gediget arbete har lagts ner avseende styrande och stödjande dokumentation. Genom intervjuer ges också en bild av att mognadsgraden inom organisationen har höjts senaste åren. Det är också positivt att flera områden relaterat till informationssäkerhet finns med i nämndens riskanalyser och internkontrollplaner. Vi uppfattar också att en medvetenhet om brister inom främst IT-säkerhet finns (utifrån den GAP-analys som genomförts) och det är positivt att det pågår ett förbättringsarbete inom det området.

Samtidigt bedömer vi att arbetet kan utvecklas på flera områden. Styrningen kan utvecklas framförallt genom en korrekt beslutshantering och en mer effektiv uppföljning avseende efterlevnad av både interna regelverk och lagstiftning. Granskningen visar också att även om roller och ansvar är relativt tydligt beskrivna i olika styrande dokument, är rollerna i praktiken inte tydliga och till viss del inte möjliga att utöva.

Det framgår också av främst enkätsvaren att det finns en del missförstånd kring olika funktioners ansvar och roller.

Vår bedömning av arbetet med riskanalyser avseende informationssäkerhet är att det genom styrande dokument är tydligt att de ska göras. I praktiken är det sedan inte lika tydligt när och hur de ska genomföras och hur identifierade risker ska hanteras. Utifrån stickproven tagna i denna granskning framstår det också som att system med större icke hanterade risker ändå används, vilket innebär en risk för hela sjukhuset.

Det genomförs utbildning avseende informationssäkerhet för samtliga medarbetare inom Karolinska. Medvetenheten om utbildningarna och deras syfte är hög tillika genomförandegraden. Dock saknas en systematik för att upprepning/uppdatering av utbildningen och fördjupade utbildningar inom området, vilket kan leda till att kunskapsnivån inte är stadigvarande eller i linje med förändringar i arbetssätt och regelverk.

## Dataskyddsarbete

Utifrån genomförd granskning är vår samlade bedömning att Karolinska universitetssjukhuset inte bedriver ett ändamålsenligt dataskyddsarbete.

Sjukhusets riktlinje för behandling av personuppgifter är en bra utgångspunkt för dataskyddsarbetet, men utifrån riktlinjen behöver arbetet utvecklas inom flera olika områden. Styrningen kan utvecklas framförallt genom en korrekt beslutshantering och en mer effektiv uppföljning avseende efterlevnad av både interna regelverk och lagstiftning. Utifrån främst enkätsvar och intervjuer bedömer vi att det finns avsevärda oklarheter kring roll- och ansvarsfördelning avseende dataskyddsarbetet.

Granskningen visar också att det saknas en tydlig och känd fördelning av operativt ansvar, vilket återspeglas i bristande genomförande av exempelvis behandlingsregister och konsekvensbedömningar. Eftersom Karolinska saknar ett fullständigt register över de personuppgifter som behandlas och vilka risker som är förknippade med dem, saknas systematisk dokumentation av vilka personuppgifter som samlas in, hur de används och vilka åtgärder som vidtas för att skydda dessa. Det innebär att det finns risk för att GDPR inte kan efterlevas.

Avseende riskanalyser och konsekvensbedömningar enligt GDPR bedömer vi att detta arbete till vissa delar är delvis ändamålsenligt och till vissa delar inte är ändamålsenligt. Det finns instruktioner och mallar, men vi bedömer att genomförandet brister på olika sätt. Granskningen visar att varken riskanalyser eller konsekvensbedömningar följs upp i någon större eller systematisk utsträckning.

Granskningen har inte kunnat identifiera mer uppföljning avseende dataskyddsarbetet, än dataskyddsombudets årliga rapport. Enbart den uppföljningen (utifrån hur den är utformad), bedömer vi inte som ändamålsenligt utan en mer systematisk och övergripande uppföljning behövs. Avseende uppföljning bör även nämnden se till att de brister och utvecklingsområden som redan har identifierats, blir åtgärdade.

21 augusti 2024

*Charlotte Arnell* *Kristian Damlin*

---