KAROLINSKA UNIVERSITETSSJUKHUSET

Handläggare Johnny Moraeus,
Informationssäkerhetssamordnare

Ärende/D-nr: K 2025-2603
Datum: 2025-03-24

Årsrapport för Informationssäkerhet vid Karolinska Universitetssjukhuset 2024

Syfte

Syftet med årsrapporten för informationssäkerhet är att beskriva Karolinska Universitetssjukhuset informationssäkerhetsarbete under 2024.

Sammanfattning verksamhetsår 2024

Omvärldssituation

Under senaste året ser vi en ökad hotbild och mer aktivitet kring cyberattacker i vår omvärld. Hälso- och sjukvård är inte längre förskonade från antagonistiska angrepp och incidenter som exempelvis ransomeware-attackerna mot Tietoevry (jan 2024), Sophiahemmet (feb 2024) liksom den felaktiga uppdateringen som lamslog stora delar av världen i Crowdstrike (juli 2024) visar konsekvenserna av en IT-relaterad säkerhetsincident.

Generellt skall och bör informationssäkerhetincidenter på Karolinska Universitetssjukhuset (Karolinska) alltid betraktas med allvarliga ögon. Hanteras inte data som innehåller journaltext, personuppgifter eller annan skyddsvärd information på ett advekvat sätt så kan det ge långgående konsekvenser för exempelvis våra patienter såväl som för vårdens förtroendekapital. Störningar som uppstår i våra IT-system pga driftsincidenter eller antagonistiska handlingar (via ransomeware-attacker eller liknande) är händelser som påverkar sjukhusets grundläggande uppdrag dvs vård, forskning och utbildning. Hot mot liv och hälsa finns med i konsekvensutfallet vid störningar i det robusta sjukhusets infrastruktur och kommunikationslösningar.

Ett adekvat informationssäkerhetsskydd innefattar regelbunden utbildning för personalen för att känna igen phishingförsök och andra hot, kontinuerliga säkerhetsuppdateringar av IT-system, robusta åtkomstkontroller för att minimera obehörig tillgång till känslig information och backup-lösningar för att snabbt återställa system och data vid incidenter. Ett starkt skydd bidrar både till att säkerställa vårdens kontinuitet och skydda patienternas förtroende för sjukhuset som en säker plats för vård. Samarbete på internationell, nationell och regional nivå kommer bli allt viktigare för Karolinska, särskilt i en tid av ökande globala hot och komplexa vårdbehov.

När det gäller uppdaterade regelverk som NIS2-direktivet, spelar dessa en central roll för att säkerställa cybersäkerhet inom vårdsektorn. NIS2 ställer högre krav på att implementera

robusta cybersäkerhetsåtgärder. Detta inkluderar riskhantering, incidentrapportering och skydd av känsliga patientdata. Direktivet betonar också vikten av att hantera leverantörskedjor och säkerställa kontinuitet i kritiska tjänster. För sjukhus som Karolinska innebär detta att vi bör och eller måste investera i modern teknik, utbilda personal och stärka våra säkerhetsprotokoll för att möta de nya kraven. Genom att kombinera samarbete på flera nivåer med efterlevnad av regelverk som NIS2 kan Karolinska inte bara förbättra sin beredskap och säkerhet utan också bygga förtroende hos patienter och i stort samhället.

Handlingsplan
Karolinska Universitetssjukhusets handlingsplan för informationssäkerhet (april till dec 2024) beskriver långsiktiga och kortsiktiga mål med informationssäkerhetsarbetet under 2024.
P.15 Karolinska sjukhusets handlingsplan för informationssäkerhet 2024 (K 2024-2391)

Extern revision Informationssäkerhet och dataskydd på Karolinska
En extern granskning, ledd av regionrevisorerna inom Region Stockholm, genomfördes mellan december 2023 och maj 2024 (K 2024-8525). Sammanfattat pekar revisonen på brister i prioritering av riskanalyser, en otydlighet i roller och ansvar, adekvat utbildning av samtliga anställda samt en medvetenhet kring informations och dataskyddsfrågor. Slutsatsen var att styrning och kontroll av informationssäkerhetsarbetet på Karolinska inte är tillräckligt robust.

För att åtgärda de brister som identifierats påbörjades ett förbättringsarbete, under hösten -24 och som fortgår 2025, som syftar till att:

- Tydliggöra roller och ansvar
- Etablera en årlig handlingsplan som är mer funktionell i relation till strategiskt informationssäkerhetsarbete
- Utföra en analys, mappning av vilka sektorer Karolinska kommer träffas i relation till det nya NIS2-direktivet och den lagstiftning som träder i kraft under 2025, för att säkerställa efterlevnad.
- Grundlig genomgång av metodstöd och processer i syfte att förbättra riskhantering i stort samt prioritera områden för förbättring, exempelvis inköp eller driftsättning av IT-system.
- Identifiera målgrupper och utbilda personal inom olika grupper

Med utgångspunkt från revisionsrapporten och 2024 års handlingsplan har följande utförts under 2024, varav mycket av arbetet fortgår även under 2025:

Operativt stöd
Att ge råd och stöd direkt till verksamhet och informationskoordinatorer i olika frågor, exempelvis upphandlingar, informationsklassningar, internkontroll/compliance-deklarationer, riskanalyser och åtgärdsplaner, är viktiga och tidskrävande delar av arbetet. Vi har bl.a bidragit i kravställning, analys och granskning inom exempelvis Karolinska@Home, Precisionsmedicin, nytt regionalt avvikelsehanteringssystem, regionens nya AI-bottar och AI-operationsplaneringsverktyg. Avdelningen har även deltagit i kravställningen i upphandling av nytt regionalt IT-stöd för bl.a informationssäkerhet, dataskydd och riskhantering, vilket implementeras under Q3-Q4 2025.

Arbete för stärkt IT-säkerhet
Under året har IT-säkerhetsarbetet fokuserat på att stärka vår digitala motståndskraft och skydd av skyddsvärda informationstillgångar mot ett ständigt ökande och föränderligt hot. Genom ett systematiskt informationssäkerhetsarbete, riskhantering och tydligare kravställningar vid upphandling och utveckling har vi ökat vår resiliens. Även i det integrerade linjearbetet pågår löpande säkerhetsarbete som syftar till en robustare IT-infrastruktur. Gjorda analyser har skapat en tydligare nulägesbild vilket ger bättre möjligheter till prioriteringar framåt. Arbetet med att ta fram en tydlig IT-säkerhetsarkitektur, som täcker hela nämndens uppdrag, är påbörjad och är essentiell för en trygg och stabil digital miljö för framtidens vård och innovationer.

Avdelningen Informations- och IT-säkerhet är etablerad
I maj 2024 etablerades avdelningen IT-och Informationssäkerhet under Stab Teknik och Verksamhetsområde IT. Där samlas kompetens inom både informationssäkerhet och IT-säkerhet för att få synergieffekt och ge en starkare koppling till IT som berörs extra mycket av informationssäkerhetskrav. Avdelningen har dock hela Karolinska som ansvarsområde. Området har genom åren haft stor personalomsättning, arbetsmiljöproblem och högt konsultberoende. Även 2024 hade utmaningar i arbetsmiljön vilket bl.a hanterades genom byte av chef och arbete för stärkt stabilitet inom avdelningen genom konsultväxling.

Enkelt att göra rätt
En sida har skapats för avdelningen på Inuti för att samla relevant information om Karolinskas informationssäkerhetsarbete, samt länkar till regionens styrande och stödjande dokument. Sidan kommer att vidareutvecklas under 2025. Under verksamhetsåret har avdelningen även publicerat information om vad man behöver tänka på vid användning av publika AI-baserade chatbots samt tips om användning av lösenordshanterare.

Informationssäkerhetstillgångar
Listan över Karolinskas prioriterade system vid större IT-relaterade incidenter, s.k. prio-listan, uppdaterades under hösten 2024 och fastställdes 2025-03-17 (K2025-2236). Arbetet med att inventera Karolinskas informationstillgångar har påbörjats och kommer fortlöpande stärkas och ges en bättre struktur.
Det nätverk för Informationssäkerhetskoordinatorer som finns på sjukhuset har fått en omstart och i den grupperingen har införande av en sk. kontrollplan påbörjats. Kontrollplanen syftar till att visa aktuell status samt 3års plan för compliance-aktiviteter inom verksamheterna. Processen kring anskaffning av nya applikationer och system behöver intensifieras ytterligare då kunskap och/eller förståelse för processen brister inom områdena hantering, ägandeskap samt kunskap om vad en informationstillgång faktiskt är. Detta ingår i utbildningsplanen tillika handlingsplanen för 2025.

Ökad säkerhetsmedvetenhet
För att öka en bred säkerhetsmedvetenhet så har beslut tagits att införa 5-årsintervall för den regiongemensamma informationssäkerhetsutbildningen DISA inom Karolinska. Det har initialt informerats via Karolinskas nyhetsbrev för chefer, och kommer följas upp med ytterligare kommunikation och uppföljning under Q2-2025.
En utbildningsplan med fördjupande utbildningar för viktiga målgrupper har påbörjats och

kommer slutföras under 2025. En föreläsning med Anne-Marie Eklund Löwinder, en av Sveriges ledande experter inom cybersäkerhet, anordnades för ledande roller inom bl.a Stab Teknik och Säkerhetsenheten. Därutöver har avdelningen börjat att träffa T/F/S-ledningar för att informera om vikten av systematiskt informationssäkerhetsarbete, deras roll och ansvar, en mötesserie som planeras att fortsätta under 2025.

Ledningssystem för informationssäkerhet (LIS)
Under verksamhetsåret har det skett en översyn av sjukhusets LIS som i vissa delar har anpassats för att förbättra följsamheten av bl.a Region Stockholms informationssäkerhetsriktlinjer samt av regulatoriska krav som ställs på verksamheten. Informationen på Inuti har till viss del förenklats, nya tillämpningsanvisningar samt vägledningar har skapats på området.
Kartläggning av hur regional och lokal LIS förhåller sig till varandra kommer resultera i ett mer överskådligt LIS. Arbetet med detta kommer slutföras under Q2 2025. Fokusområden i det här arbetet är regelbundna riskbedömningar samt kompetensökning av personal för att säkerställa att både informationssäkerhet och dataskydd hanteras effektivt.

Informationssäkerhet vid upphandling, inköp och utkontraktering
För att säkerställa korrekt informationshantering enligt Region Stockholms och sjukhusets krav ska avtalsbilagan för informationssäkerhets användas. Vägledning och mallar är till viss mån framtagna men efterlevnaden har identifierats som delvis bristfällig. En djupare genomlysning av inköpsprocessen påbörjades 2024 och ska slutföras 2025 där förslag på hur informationssäkerhetsfrågorna kan implementeras på ett naturligt sätt i ett tidigare skede i processen kommer läggas fram. Verksamhetsutveckling i den här processen är tänkt att lyfta och säkerställa kvalité vid upphandling och utveckling av nya system, applikationer och tjänster likväl internt som externt.

Incidenter
En välfungerande och välkänd incidentprocess i organisationen är en viktig del i en robust IT-leverans samt minskar risken för större och långvariga vårdpåverkande störningar. Alla som arbetar på Karolinska har ett ansvar för att ha kännedom om sin roll i processen och agera enligt plan. Även risker och identifierade sårbarheter behöver rapporteras så de kan hanteras på en aggregerad nivå och prioriteras för åtgärd. Ett samarbetsforum för avstämning av incidenter har etablerats under året. Uppdatering av incidentprocessen så den möter kraven i NIS2 är framtaget och kommer synkas med regionen när den nya lagstiftningen finns på plats under 2025. Kompetensökning kommer ligga som prioriterat område i den här processen.

Region Stockholms måluppföljning
Egenkontroll för Strategisk informationssäkerhet samt regionens årsuppföljning Informationssäkerhet 2024 genomfördes och återfinns i Årsrapport Karolinska 2024.
Årlig rapportering av uppfyllelse av informationssäkerhetsmål för Region Stockholm skall genomföras under 2025.