Informationssäkerhet 2025

HSLF-FS 2016:40, 7 kap. 1§

Syftet med informationssäkerhetsarbetet är att säkerställa informationens konfidentialitet, riktighet och tillgänglighet. Det systematiska informationssäkerhetsarbetet är ett riskbaserat förebyggande arbete för att kontinuerligt värdera och anpassa informationsskyddet utifrån organisationens behov och de identifierade risker som finns. Informationssäkerhet är en del av patientsäkerheten, information behöver finnas tillgänglig och vara riktig för att säkerställa patientsäkerheten och den behöver hanteras konfidentiellt för att säkerställa patientintegriteten.

Ledningssystemet för informationssäkerhet utvecklas i enlighet med ISO 27000 serien i vårt gemensamma kvalitetsledningssystem. Systematiken är uppbyggt på att riskidentifiering och analys genomförs, åtgärdsplan beslutas om, säkerhetsåtgärder vidtas och därefter följs de upp.

Nedan presenteras information enligt HSLF-FS 2016:40, 7 kap. 1 §. Detta är den information som patientsäkerhetsberättelsen ska innehålla utöver det som anges i patientsäkerhetslagen (2010:659), 3 kap. 10 §.

Varje år genomförs en övergripande riskanalys med utgångspunkt i regionens roll som leverantör av samhällsviktig tjänst enligt 12 § i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Riskanalysen syftar till att identifiera och bedöma risker som kan påverka regionens förmåga att upprätthålla dessa tjänster. Utifrån den genomförda riskanalysen tas en åtgärdsplan fram som redovisades för Centrala ledningsgruppen i september 2025. De identifierade åtgärderna ligger därefter till grund för de säkerhetsåtgärder som planeras och genomförs under kommande år. Inför framtagande av en ny riskanalys och åtgärdsplan genomförs alltid en uppföljning av föregående års arbete. Som en del av detta används Cybersäkerhetskollen, som är Myndigheten för samhällsskydd och beredskaps nationella uppföljning. Cybersäkerhetskollen fungerar samtidigt som ett viktigt stöd i regionens egenkontroll och används som underlag för att identifiera förbättringsområden och ta fram relevanta säkerhetsåtgärder.

Riskanalyser ur ett informationssäkerhetsperspektiv genomförs både övergripande och som en del av riskanalyser inom andra verksamhetsområden. Informationssäkerhet är därmed på väg att bli en integrerad del av organisationens samlade riskhantering. Vid införande av nya informationssystem, samt vid förändringar eller vidareutveckling av befintliga system, ska arbetet planeras och föregås av riskanalyser av berörda informationstillgångar. Utifrån dessa analyser vidtas nödvändiga åtgärder för att säkerställa att informationen skyddas på rätt nivå, så att kraven på konfidentialitet, riktighet och tillgänglighet uppfylls. Sammankoppling av nätverk får endast ske efter att en riskanalys har genomförts och efter att erforderliga skyddsåtgärder har införts.

Riskanalyser utgör en central grund för prioriteringar och beslut vid införande av nya system och tjänster. Ett exempel på ett mer omfattande och systematiskt riskanalysarbete är införandet av journalsystemet Cosmic. Inför planerad driftsättning den 23 april 2025 genomfördes i november 2023 en övergripande riskanalys som underlag för beslut om införande.

Som en del av införandeprocessen genomfördes även en fördjupad granskning av systemleverantören Cambio under perioden april–maj 2025. Syftet med granskningen var att säkerställa att Cambio, i rollen som personuppgiftsbiträde, tillhandahåller en tillräcklig och ändamålsenlig säkerhetsnivå för skydd av personuppgifter i Cosmic. Granskningen visade att Cambio har gjort framsteg sedan den tidigare säkerhetsrevision som genomfördes av XLENT Cyber Security i februari 2024. Granskningen fokuserade primärt på de 36 kritiska brister som identifierades i föregående revision, samt på 28 särskilt framtagna granskningsfrågor (F001–F028) som användes för att skapa en fördjupad förståelse för Cambios implementering av sitt ledningssystem för informationssäkerhet enligt ISO/IEC 27001:2022. Granskningen omfattade organisatoriska, tekniska, fysiska och personrelaterade säkerhetskontroller.

Under året har ett omfattande arbete bedrivits med informationsspridning och intern kommunikation i syfte att tydliggöra objektens ansvar för informationssäkerheten. Ett centralt mål har varit att stärka förståelsen för att informationssäkerhet är ett gemensamt ansvar och att varje objekt behöver ta ett mer aktivt och strukturerat ansvar för sina informationsmängder och system.

Informationsinsatserna har särskilt fokuserat på vikten av att genomföra informationsklassningar, ta fram och följa upp handlingsplaner samt genomföra riskanalyser som en naturlig del av förvaltning och vidareutveckling. Genom att tydliggöra roller, ansvar och förväntningar har arbetet bidragit till ökad medvetenhet om hur bristande informationssäkerhet kan påverka verksamheten, patientsäkerheten och skyddet av personuppgifter.

Även ett antal tekniska åtgärder har vidtagits, till exempel införande av Harmony SASE och Threatlocker, för att minska riskerna vid arbete utanför regionens nätverk och att skadlig kod körs på regionens IT-utrustning. Andra tekniska åtgärder och tillhörande tjänster som etablerats under året bidrar till att regionens system och nätverk blivit robustare. Även detta år har stort fokus för informationssäkerhetsarbetet legat på införandet av Cosmic i syfte att nå en säker hantering av vår patientinformation. Både regionala åtgärder och gemensamma i SUSSA samverkan har genomförts, såsom till exempel uppföljning av leverantörens säkerhetsarbete.

Bytet av journalsystem till Cosmic i april 2025 har inneburit begränsade möjligheter att genomföra stickprovskontroller, då nödvändiga loggrapporter inte varit tillgängliga. Logguppföljning via LogPoint färdigställdes under december 2025 och planeras att införas för alla verksamheter under januari–februari 2026, vilket bedöms möjliggöra full efterlevnad av rutinen framöver. Rutin för systematisk stickprovskontroll av loggar i journalsystemen finns i ledningssystemet och uppdaterades i december 2025. Rutinen innebär att ett urval av användare med läsbehörighet granskas varje månad, med målsättning att samtliga användare ska omfattas under ett år.