Yttrande över Landstingsrevisorernas Projektrapport 8/2018 – Grundläggande arbetet med informationssäkerhet – Karolinska Universitetssjukhuset, Stockholms läns sjukvårdsområde
(1 bilaga)

Ärendet

Revisorerna i revisionsgrupp II har överlämnat rapporten ”Grundläggande arbetet med informationssäkerhet” till styrelsen för Stockholms läns sjukvårdsområde för yttrande.

Revisorerna har genomfört en granskning om informationssäkerhetsarbetet på Karolinska Universitetssjukhuset och Stockholms läns sjukvårdsområde (SLSO) är implementerat i sådan grad att verksamheternas lägsta operativa nivå har ett grundläggande systematiskt informationssäkerhetsarbete på plats och avrapporterat detta i ”Projektrapport 8/2018: Grundläggande arbetet med informationssäkerhet”.

Revisorernas rapport omfattar följande områden:
• Roller, ansvar och informationsägande.
• Arbete med riskanalyser.
• Utbildning och kunskap om informationssäkerhet.
• Avvikelser och förbättringsarbete

Utifrån de granskade områdena ger Landstingsrevisorerna i rapporten **tre** rekommendationer till SLSO:s styrelse som bör säkerställa att:

• det grundläggande systematiska informationssäkerhetsarbetet omfattar samtliga verksamheter på alla nivåer.
• samtliga anställda genomgår regionens utbildning för informationssäkerhet.
• roller och ansvar för informationssäkerhetsarbetet tydliggörs och kommuniceras på samtliga nivåer i verksamheten.

Förvaltningens arbete

Under 2018 har informationssäkerhetssamordnaren tillsammans med VIR-projektet (Verksamhetsbaserad Informations Redovisning) arbetat med en kartläggning av vilka personuppgifter SLSO hanterar och även kravställt en systeminventering från Verksamhetstöd eHälsa och IT. Beslutsprocesser avseende innovation har tydliggjorts under 2018 och informationssäkerhetssamordnaren är nu representerad i innovationsslussen i syfte att säkerställa en mer effektiv och systematisk hantering av ärenden gällande exempelvis informationssäkerhet.

Anpassningen till dataskyddsförordningen (GDPR) har under året ägt rum parallellt med informationssäkerhetsarbetet där fokus varit systeminventering, egenkontroller av IT-system samt säkerställande att SLSO har de rutiner som krävs för att leva upp till registrerades rättigheter samt SLSO:s skyldigheter enligt dataskyddsförordningen.

Förvaltningens synpunkter

Landstingsrevisorernas rapport fokuserar på det grundläggande systematiska informationssäkerhetsarbetet på lägsta operativa nivå medan SLSO under 2018 arbetat framför allt på strategisk nivå, en diskrepans i landstingsrevisorernas rapport och SLSO:s kontinuerliga arbete under 2018 med informationssäkerhet finns. Målet för SLSO:s systematiska informationssäkerhetsarbete är att alla nivåer inom organisationen omfattas men i nuläget så riktas fokus mot övergripande/strategiska nivå.

Under 2019 sker en satsning att etablera en organisation med informationssäkerhetsombud i syfte att lyfta kunskapsnivån inom SLSO samt förbättra kommunikationen med både verksamhetsområden och verksamhetsstöd gällande informationssäkerhet. Det är även SLSO:s förhoppning att inrättandet av informationssäkerhetsombud ska klargöra roller och ansvar kopplat till informationssäkerhet samt aktualisera och medvetandegöra e-utbildningen i informationssäkerhet (DISA).

För att stödja och förbättra det systematiska arbetet med informationssäkerhet inom SLSO kommer en handlingsplan för sjukvårdsområdets informationssäkerhetsarbete för 2019-2020 att utarbetas och fastställas under andra kvartalet 2019. En fastställd handlingsplan möjliggör planläggning, styrning och uppföljning av arbetet med att egenkontrollera, utvärdera och förbättra informationssäkerheten på både strategisk och operativ nivå. Ett systematisk arbetet med Compliance portalen på strategisk-, verksamhets- och teknisk nivå är en förutsättning för att SLSO ska utveckla och förbättra det systematiska informationssäkerhetsarbetet, på alla nivåer.

Vidare så arbetar SLSO med att skapa en e-utbildning i syfte att tillgodose utbildningsbehovet kopplat till dataskyddsförordningen vilken är en viktig del i informationssäkerhetsarbetet, detta arbete beräknas vara klart andra kvartalet 2019. I samband med lansering av e-utbildningen för dataskyddsförordningen kommer SLSO även betona vikten av att alla anställda även genomför DISA.

Informationssäkerhetsavvikelser rapporteras från och med 2018 på ledningens genomgång samt till SLSO:s styrelse.

Revisorernas samlade bedömning i projektrapporten ger Stockholms läns sjukvårdsområde god vägledning i det fortsatta arbetet med att vidareutveckla det systematiska informationssäkerhetsarbetet i enlighet fullmäktiges policy och riktlinjer.

Förslag till beslut

Styrelsen för Stockholms läns sjukvårdsområde föreslås besluta

att avge yttrande till Landstingsrevisorernas Projektrapport 8/2018 i enlighet med ovanstående, samt

att förklara paragrafen omedelbart justerad.

Mikael Ohrling
Sjukvårdsdirektör

Bilaga 1: Projektrapport 8/2018 - Grundläggande arbetet med informationssäkerhet – Karolinska Universitetssjukhuset, Stockholms läns sjukvårdsområde

PROJEKTRAPPORT NR 8/2018

Grundläggande arbetet med informationssäkerhet

Karolinska Universitetssjukhuset och Stockholms läns sjukvårdsområde

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Kort om rapporten

Region Stockholm hanterar stora mängder känslig information och verksamheternas arbete med informationssäkerhet är därför avgörande för en säker hantering av personuppgifter och verksamhetskritisk information. Varje nämnd/styrelse har ansvar för informationssäkerheten inom sitt verksamhetsområde och ska årligen planlägga och löpande följa upp informationssäkerhetsarbetet. Granskningen visar att grundläggande systematiskt informationssäkerhetsarbete på Karolinska Universitetssjukhuset och SLSO har implementerats i olika grad och att kvaliteten därför varierar mellan sjukhusets olika verksamheter och på SLSO:s olika vårdcentraler. Avsaknaden av ett systematiskt informationssäkerhetsarbete för vissa enheter innebär även att det i stor utsträckning saknas en heltäckande process för både utbildning och förbättringsarbete avseende informationssäkerhet.

2019-01-29 RK 2018-0021

Stockholms läns sjukvårdsområde

Projektrapport 8/2018
Grundläggande arbetet med informationssäkerhet

Revisorerna i revisorsgrupp II beslutade vid sitt möte 2019-01-29 att uppdra till kontoret att överlämna rapporten till styrelsen för Stockholms läns sjukvårdsområde för yttrande senast 2019-04-30.

Revisorernas samlade bedömning är att det grundläggande systematiskt informationssäkerhetsarbete på Karolinska Universitetssjukhuset och Stockholms läns sjukvårdsområde, SLSO, har implementerats i olika grad och att kvaliteten därför varierar mellan sjukhusets olika verksamheter och på SLSO:s olika vårdcentraler. Avsaknaden av ett systematiskt informationssäkerhetsarbete för vissa enheter innebär även att det i stor utsträckning saknas en heltäckande process för både utbildning och förbättringsarbete avseende informationssäkerhet.

Revisorerna vill till styrelsen för Stockholms läns sjukvårdsområde lyfta vikten av att det grundläggande systematiska informationssäkerhetsarbetet omfattar samtliga verksamheter på alla nivåer och att samtlig personal genomgår regionens utbildning för informationssäkerhet. Det är även viktigt att roller och ansvar för informationssäkerhetsarbetet tydliggörs och kommuniceras på samtliga nivåer i verksamheten.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Hans-Erik Salomonsson
Ordförande

Christina Holmqvist
Sekreterare

Landstingsrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08-737 25 00
E-post: landstingsrevisorerna.rev@sll.se

Säte: Stockholm
Org.nr: 23 21 00 - 0016
www.sll.se/rev

Besöksadress: Hantverkargatan 25 B. T-bana Rådhuset

Innehåll

1 Slutsatser och rekommendationer 1

2 Utgångspunkter för granskningen 3
2.1 Motiv till granskningen 3
2.2 Revisionsfråga 4
2.3 Avgränsning 4
2.4 Bedömningsgrunder 4
2.5 Metod 5

3 Systematiskt informationssäkerhetsarbete på Karolinska Universitetssjukhuset och SLSO 6
3.1 Utgångspunkter för styrelsernas arbete 6
3.2 Roller, ansvar och informationsägande 7
3.3 Arbete med riskanalyser 9
3.4 Utbildning och kunskap om informationssäkerhet 11
3.5 Avvikelser och förbättringsarbete 13

1 Slutsatser och rekommendationer

Enligt policy och riktlinjer för informationssäkerhet beslutade av Stockholms läns landsting, nuvarande Region Stockholm, ska ett systematiskt säkerhetsarbete bedrivas i syfte att skydda regionens information. Varje nämnd/styrelse har ansvar för informationssäkerheten inom sitt verksamhetsområde och ska årligen planlägga och löpande följa upp informationssäkerhetsarbetet som ska säkerställa att viktiga informationstillgångar omfattas av väl avvägda skyddsåtgärder. Revisionen har granskat om informationssäkerhetsarbetet på Karolinska Universitetssjukhuset (Karolinska) och Stockholms läns sjukvårdsområde (SLSO) är implementerat i sådan grad att verksamheternas lägsta operativa nivå har ett grundläggande systematiskt informationssäkerhetsarbete på plats.

Revisionen bedömer att ett grundläggande systematiskt informationssäkerhetsarbete har påbörjats för de flesta av verksamheterna i Compliance-processen (Regionens process för styrning och arbete med systematiskt informationssäkerhetsarbete) på Karolinska men för SLSO saknas det på flera av de granskade vårdcentralerna. SLSO är i uppstartsfasen för arbete i enlighet med Compliance-processen och kommer inledningsvis arbeta med gap-analyser, vilket utgör en grundförutsättning för arbetet med riskanalyser. Det finns ett systematiskt arbete med riskanalyser, handlingsplaner och klassificering av information vid flera verksamheter på Karolinska. Vid SLSO:s verksamheter har inte några liknande ”goda exempel” identifierats. För både Karolinska och SLSO kvarstår i många fall att ta fram riskanalyser och handlingsplaner på enhetsnivå. Inom båda verksamheterna finns en mängd olika rutiner och system som enligt revisionen gör det extra angeläget att komma igång med riskanalysarbetet på enhetsnivå i samtliga verksamheter. När riskanalysarbetet är avklarat bör tillhörande handlingsplaner upprättas och klassificering av informationen ske genom att verksamheterna på enhetsnivå tillämpar regionens, fastställda av dåvarande landstinget, informationsklassificering.

Region Stockholm har en grundläggande e-utbildning (DISA) i informationssäkerhet som är obligatorisk för nyanställda. En generell iakttagelse är att det finns svårigheter att motivera anställda sedan längre tid att genomgå utbildningen. Det är viktigt att samtliga anställda har en grundläggande kunskap om informationssäkerhet och att den generella riskmedvetenheten hos medarbetarna kontinuerligt upprätthålls.

Ytterligare en annan observation är att det saknas ett koncept för systematisk vidareutbildning inom informationssäkerhetsområdet. För att stärka detta arbete bör Region Stockholm överväga ta fram ett sådant i syfte att dess verksamheter kontinuerligt ska kunna möta och vara uppdaterad om nya lagar och informationssäkerhetshändelser. Eftersom ett systematiskt informationssäkerhetsarbete saknas i majoriteten av de granskade verksamheterna vid SLSO saknas det även en process för förbättringsarbete avseende informationssäkerhet. Medarbetare ska rapportera avvikelser, i vissa fall också gällande informationssäkerhet, i rapporteringssystemet Händelsevis. Vilket är en viktig del av förbättringsarbetet. Revisionen anser att det är viktigt att alla verksamheter kommer igång med ett systematiskt informationssäkerhetsarbete där samtliga medarbetare involveras i förbättringsarbetet.

Revisionen bedömer att ansvar och roller för informationssäkerhetsarbetet kan tydliggöras, mer för SLSO än för Karolinska universitetssjukhuset. Verksamheter som vilar på informella riktlinjer för roller och ansvar bör fokusera på att ta fram formella arbetsbeskrivningar. Revisionen anser också att det är viktigt att förändringar i roller och ansvar för informationssäkerhetsarbetet kommuniceras till berörda medarbetare.

Riskanalysarbetet avseende informationssäkerhet på Karolinska Universitetssjukhuset uppvisar variationer. Vissa verksamheter har ett systematiskt riskanalysarbete på plats medan andra verksamheter inte har påbörjat riskarbetet, men har påbörjat sitt informationssäkerhetsarbete i Compliance-processen. Skillnaderna går i regel att koppla till vana att hantera känslig information i verksamheten. Karolinska Universitetssjukhuset har också påbörjat ett arbete med att leva upp till kraven i dataskyddsförordningen (GDPR), arbetet har bedrivits parallellt med informationssäkerhetsarbetet i Compliance-processen. Säkerhetsklassificering av information har främst skett utifrån GDPR och är inte alltid kopplad till informationssäkerhetens klassificeringsmodell.

Roller och ansvar för informationssäkerhetsarbetet inom SLSO behöver tydliggöras. Exempelvis genom att ta fram formella arbetsbeskrivningar som tydliggör vilket ansvar medarbetarna har för att hantera information på ett korrekt och säkert sätt. Det är även viktigt att förändringar i roller och ansvar för informationssäkerhetsarbetet kommuniceras till berörda medarbetare. Även instruktioner och rutiner gällande arbetet med informationssäkerhet inom SLSO bör tydliggöras och implementeras för samtliga verksamhetsnivåer, exempelvis när det gäller riskanalys, uppföljning och förbättringsarbete. Verksamheterna bör även involvera medarbetarna i informationssäkerhetsarbetet och utbilda dem så att det exempelvis blir tydligare vem som är informationsägare. När det gäller SLSO:s arbete med informationssäkerhet och anpassningen till dataskyddsförordningen så sker arbetet med anpassningen till dataskyddsförordningen i informationssäkerhetsarbetet. Revisionens samlade bedömning är att det saknas ett grundläggande systematiskt informationssäkerhetsarbete som omfattar medarbetarna på Karolinska och SLSO.

Rekommendationer:

- Styrelsen för Karolinska Universitetssjukhuset bör säkerställa att
    - det grundläggande systematiska informationssäkerhetsarbetet omfattar samtliga verksamheter på alla nivåer.
    - samtliga anställda genomgår regionens utbildning för informationssäkerhet.

- Styrelsen för SLSO bör säkerställa att
    - det grundläggande systematiska informationssäkerhetsarbetet omfattar samtliga verksamheter på alla nivåer.
    - samtliga anställda genomgår regionens utbildning för informationssäkerhet.
    - roller och ansvar för informationssäkerhetsarbetet tydliggörs och kommuniceras på samtliga nivåer i verksamheten.

2 Utgångspunkter för granskningen

2.1 Motiv till granskningen

Region Stockholm hanterar stora mängder känslig information och verksamheternas arbete med informationssäkerhet är därför avgörande för en säker hantering av personuppgifter och verksamhetskritisk information[1]. Brister i arbetet med informationssäkerhet kan bland annat öka riskerna för förlust av information, att information kommer i orätta händer, att verksamhetskritisk information inte finns tillgänglig för personal och patienter och att informationens korrekthet inte kan garanteras. Region Stockholm, dåvarande Landstingsfullmäktige och landstingsstyrelsen, har fastställt policy och riktlinjer samt tillämpningsanvisningar för informationssäkerhet. I fullmäktiges budget 2018[2] och i handlingsplan för informationssäkerhet[3] finns det ett antal mål för informationssäkerhetsarbetet, se vidare avsnitt 2.4 nedan. Grunden i informationssäkerhetsarbetet ska, enligt fullmäktige, vara ett ISO[4]-anpassat ledningssystem för informationssäkerhet hos varje nämnd och styrelse.

I regionstyrelsens, dåvarande landstingsstyrelsens, uppsiktsrapport för 2017[5] görs bedömningen att merparten av nämnderna och styrelserna har avvikelser i regelefterlevnaden i styrdokumenten för informationssäkerhet[6]. I några fall bedömer regionstyrelsen, dåvarande landstingsstyrelsen, att avvikelserna är väsentliga. Det konstateras vidare att nämnder och styrelser med väsentliga avvikelser behöver etablera en tydlig och genomtänkt styrning och ledning av informationssäkerhetsarbetet så att insatserna kan riktas utifrån en aktuell riskbild.

Vidare visar årsbokslutet[7] för dåvarande Stockholms läns landsting 2017 att målet säkra processer, dvs. andel nämnder och styrelser som har infört verktyg och metoder för att arbeta systematiskt med säkerhet och informationssäkerhet, inte uppnås. Andelen nämnder och styrelser som bedöms bedriva ett systematiskt informationssäkerhetsarbete uppgår till 10 procent, att jämföra med målet på 60 procent eller mer. Den låga graden av systematiskt informationssäkerhetsarbete i regionen kan leda till oönskade risker i det dagliga informationssäkerhetsarbetet. Det är därför viktigt för revisionen att granska detta arbete utifrån de lokala verksamheternas perspektiv. Detta inte minst med tanke på de ökade säkerhetskraven i samhället både vad gäller lagar och förordningar, t.ex. den nya dataskyddsförordningen (GDPR).

Vårdens system är komplexa och information återfinns ofta i olika system som på ett eller annat sätt är beroende av varandra vilket innebär att medarbetarna behöver

[1] Med informationstillgångar menas informationen i sig och de resurser som används för att hantera den, t.ex. programvaror, tjänster och fysiska tillgångar. Se (LS 1112–1733) Riktlinjer för informationssäkerhet inom Stockholms läns landsting, nuvarande Region Stockholm.
[2] LS 2017–0452 sid 77.
[3] LS 2016–0646.
[4] Internationella standardiseringsorganisationen representerat av nationella standardiseringsinstitutioner.
[5] Beslutades av landstingsfullmäktige, nuvarande regionfullmäktige 2018-05-08.
[6] Policy och riktlinjer för informationssäkerhet (LS 1112–1733).
[7] LS 2017–0126.

hantera samma information i flera olika system. Detta ökar bl.a. risken för diskrepans mellan systemen. En viktig grundförutsättning för informationssäkerhetsarbetet är att det är tydligt vem som är informationsägare och därmed har ansvaret enligt policy och riktlinjer

2.2 Revisionsfråga

Hur säkerställer Stockholms läns sjukvårdsområde och Karolinska Universitetssjukhuset att det finns ett grundläggande systematiskt informationssäkerhetsarbete som omfattar verksamheternas lägsta operativa nivå i enlighet med regionens, dåvarande landstingets, mål, policy och riktlinjer för informationssäkerhet?

Delfrågor:

- Är roller och ansvar för informationssäkerheten kända och blir medarbetarna informerade om förändringar i ansvar och roller?
- Genomförs riskanalyser avseende informationssäkerhet lokalt?
- Är det tydligt vem som äger informationen?
- Sker det utbildning och kontinuerlig fortbildning i informationssäkerhet?
- Deltar medarbetare i förbättringsarbetet kring informationssäkerhet genom att rapportera avvikelser och förbättringsförslag?

2.3 Avgränsning

Revisionen har vid flera tillfällen granskat regionens, dåvarande landstingets, centrala arbete med informationssäkerhet och ledningssystemet för informationssäkerhet. Det är viktigt att även vårdens medarbetare ute i verksamheterna är involverade i arbetet med ett systematiskt informationssäkerhetsarbete. Därför granskas två av vårdens största verksamheter; Stockholms läns sjukvårdsområde (SLSO) och Karolinska Universitetssjukhuset (Karolinska), för att fånga upp eventuella brister.

2.4 Bedömningsgrunder

Bedömningsgrunderna för granskningen utgörs av regionens, dåvarande landstingets, policy och riktlinjer för informationssäkerhet samt Handlingsprogram för informationssäkerhet 2016–2020[3] inkl. elva inriktningsmål för informationssäkerhet.

Målområde 5 rörande medarbetare i handlingsprogrammet för informationssäkerhet är en särskild utgångspunkt: Region Stockholms medarbetare är säkerhetsmedvetna och ansvarstagande, och bidrar till förbättringar i ett öppet klimat. Målområdet har följande effektmål 2020:

- Region Stockholms verksamheter har förmåga att hantera informationssäkerhetsfrågor i enlighet med identifierat behov.

- Region Stockholms verksamhetschefer tar återkommande upp informationssäkerhet med medarbetare i syfte att skapa insikt om informationens värde och behov av skydd.
- Region Stockholms medarbetare är utbildade i informationssäkerhet i den omfattning som är relevant för befattningen.
- Medarbetare deltar aktivt i förbättringsarbetet genom att bland annat rapportera avvikelser och förbättringsförslag.

Handlingsprogrammets[3] elva inriktningsmål för informationssäkerhet särskilt målen om ansvarstagande organisation, god säkerhetskultur.

Kapitel 4 i SLL:s riktlinjer för informationssäkerhet, personalresurser och informationssäkerhet, och där särskilt avsnitt 4.4 utbildning och fortbildning i informationssäkerhet.

2.5 Metod

Intervjuer har genomförts i enlighet med avgränsningar ovan och dokumentstudier[8] där främst regionens, dåvarande landstingets, informationssäkerhetspolicy har legat till grund för granskningen. Ett urval av intervjupersoner (10–15 personer per verksamhet) har gjorts i samråd med verksamheterna. Den primära målgruppen utgörs av 1: a linjens chefer/motsvarande (dvs. den nivå som inte i sin tur har chefer under sig) och några medarbetare. När det gäller SLSO innebär det oftast chef för vårdcentral och för Karolinska universitetssjukhuset informationssäkerhetskoordinatorer ute på teman och staber.

Granskningen har genomförts av projektledare Max Eliasson och projektmedarbetare Jakob Hallén på regionens revisionskontor samt informationssäkerhetskonsulter från Secure State Cyber.

[8]Främst regionens, dåvarande landstingets, policy och riktlinjer för informationssäkerhet samt Handlingsprogram för informationssäkerhet 2016–2020 inkl. elva inriktningsmål för informationssäkerhet.

3 Systematiskt informationssäkerhetsarbete på Karolinska Universitetssjukhuset och SLSO

3.1 Utgångspunkter för styrelsernas arbete

Myndigheten för samhällsskydd och beredskap (MSB) har skapat ett metodstöd[9] för hur organisationer på ett systematiskt sätt bör arbeta med informationssäkerhet. Metoden innehåller fyra olika arbetsprocesser där fokus ligger på att klargöra hur olika organisationer kan utforma sitt arbete så att de uppfyller kraven som ställs i standarderna. Detta metodstöd bygger på internationella standarder och ligger i linje med hur regionen, dåvarande landstinget, formulerat sin informationssäkerhetspolicy och metodstöd. Den internationella standarden inom informationssäkerhet ISO/IEC 27000 ligger som stöd för regionens, dåvarande landstingets, ledningssystem för informationssäkerhet (LIS) tillsammans med MSB:s föreskrift om informationssäkerhet.

Regelverket för informationssäkerhet är uppbyggt enligt följande struktur:



Bild: Hierarki för dokument med tillhörande ansvarsfördelning som ledningssystemet för informationssäkerhet baseras på.

Enligt policyn styrs informationssäkerhetsarbetet med hjälp av regionens, dåvarande landstingets, ledningssystem för informationssäkerhet. Policyn och riktlinjerna anger att respektive nämnd/styrelse är ytterst ansvarig för informationssäkerheten inom sitt verksamhetsområde och svarar för att det, inom ramen för det övergripande ledningssystemet, finns ett lokalt ledningssystem för informationssäkerhet. Respektive nämnd/styrelse ansvarar även för att årligen planlägga och löpande följa upp informationssäkerhetsarbetet.

[9] https://www.informationssakerhet.se/metodstod-for-lis/att-anvanda-metodstodet/

Inom regionens, dåvarande landstingets, nämnder och styrelser ska ett systematiskt och långsiktigt informationssäkerhetsarbete bedrivas. Utöver nämndernas/styrelsernas ansvar fastslår styrdokumenten roll- och ansvarsfördelningen mellan VD, informationssäkerhetssamordnare, informationssägare, IT-chef och den enskilda medarbetaren.

Informationssäkerhetspolicyn inom regionen är baserad på säkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Att dessa fyra säkerhetsaspekter tillsammans med det systematiska informationssäkerhetsarbetet fungerar väl i praktiken är väsentligt för att informationssäkerheten ska kunna garanteras.

Både Karolinska universitetssjukhuset och SLSO har lokala riktlinjer och anvisningar för informationssäkerheten som bygger på centrala styrdokument beslutade av Stockholms läns landsting, nuvarande Region Stockholm. För båda är den stora utmaningen att säkerställa kännedom, efterlevnad och uppföljning av dessa för samtliga verksamhetsnivåer.

3.2 Roller, ansvar och informationsägande

I riktlinjer för informationssäkerhet beskrivs informationssäkerhetsansvar för vissa generella roller. Här tas ansvar upp för t.ex. styrelser och nämnder, förvaltningschef/VD, informationssäkerhetssamordnare, informationsägare och systemägare. Eftersom vårdens verksamheter ofta har flera olika organisatoriska nivåer och enheter finns det risk för otydligheter i struktur, roller och ansvar vad gäller informationssäkerhetsarbetet. Vidare kan det stora antalet medarbetare, personalomsättning och inhyrd personal leda till att medvetenhet och kunskap om informationssäkerhet bland medarbetarna är låg.

I riktlinjerna för informationssäkerhet framgår även att det för varje viktig informationstillgång ska utses en informationsägare, med uppdrag att hantera alla delar av informationssäkerheten.

3.2.1 Karolinska universitetssjukhuset

Karolinskas organisation för informationssäkerhet är relativt ny. Informationssäkerhetskoordinatorrollen är under utveckling och mandatet är därför ännu inte helt klart för varje koordinator. Roller och ansvar är i allmänhet inte skriftligt dokumenterade.

Intervjuerna visar att roller och ansvar för informationssäkerheten i verksamheterna i huvudsak är kända och tydliga. Ansvaret för informationssäkerhet uppges av merparten av de intervjuade följa verksamhetsansvaret, i enlighet med riktlinjerna för informationssäkerhet. Det egna personliga ansvaret för hantering och rapportering lyfts också. I något fall, rörande medarbetare i nya roller, finns en upplevd osäkerhet kring roller och ansvar för informationssäkerhet. Några uppger att det finns tydlig information om hur sekretessbelagd information ska hanteras på intranätet Inuti.

Förändringar i roller och ansvar avseende informationssäkerhetsarbetet delges medarbetare. Arbetsplatsträffar uppges vara den huvudsakliga vägen för information om

förändringar men även mail och intranät används. Medarbetarna ska hålla sig uppdaterade om information på intranätet men det gör inte alla och kontroll av att det sker görs i regel inte.

Ackrediterade verksamheter, t.ex. laboratorier, har kvalitetsledningssystem, flera certifieringar och genomför flertalet interna och externa revisioner årligen. De har även definierade roller för varje IT-system med nyttjare, systemägare och systemförvaltare. Ackrediterade verksamheter har genomfört informationsklassificering. Det är systemägaren och informationsägarna (verksamhetsägarna) som har ansvaret för klassificeringen.

Informationsägarskapet på Karolinska universitetssjukhuset är i viss utsträckning känt i verksamheterna. Enligt delegationsordningen är det patientområdeschefer/funktionsområdeschefer/stabschefer som är informationsägare. Informationsägarskapet eller informationssäkerhetsklassificering framgår dock inte alltid.

Den enskilda medarbetarens ansvar för information finns, med något undantag, inte dokumenterat och upplevs inte heller tydligt av alla informationssäkerhetskoordinatorer. Tystnadsplikt skrivs genomgående på vid anställning. På intranätet finns det dokumenterat vad den anställde får och inte får göra gällande hantering av information och IT-utrustning, t.ex. datorer. Det upplevs inte som tydligt vem som är informationsägare för patientdata. Otydligheter i informationsägarskapet finns även när data från flera olika system/källor hanteras/bearbetas i t.ex. en gemensam databas där det inte framgår vilka de olika informationsägarna är.

3.2.2 SLSO

För ungefär hälften av vårdcentralerna finns dokumenterat vilka roller och ansvarsfördelningar för informationssäkerhetsarbetet som gäller i verksamheten. Den andra hälften har en mer informell struktur. I några fall saknas rutiner för att informera de anställda på vårdcentralerna om förändringar när det gäller ansvar och roller för informationssäkerheten. Intervjuade har i de flesta fall tydliggjort att medarbetarna på vårdcentralerna har kännedom om grundläggande förhållningssätt till hantering av IT-utrustning. Vilket är en del av informationssäkerheten. Många upplever problem med att ett flertal olika IT-system som inte är integrerade används vid informationshantering.

Det råder tveksamhet bland intervjuade i fråga om vem som är informationsägare och om informationsägarskapet finns dokumenterat. Tre av fem vårdcentraler har uppgett att de vet vem som är informationsägare.

När det gäller informationssäkerhetsklassificeringen enligt regionen modell så sker det främst på central nivå. Vårdcentraler gör t.ex. inte en informationssäkerhetsklassificering av IT-system (där mycket av informationen finns) utan en sådan informationssäkerhetsklassificering sker centralt, ofta i samband med gap-analyser i Compliance-portalen[11].

3.2.3 Bedömning

Revisionen bedömer att ansvar och roller för informationssäkerhetsarbetet kan tydliggöras, mer för SLSO än för Karolinska universitetssjukhuset. Verksamheter som vilar på informella riktlinjer för roller och ansvar bör fokusera på att ta fram formella arbetsbeskrivningar. Arbetsbeskrivningarna ska tydliggöra vilket ansvar medarbetarna har för att hantera information på ett korrekt och säkert sätt i enlighet med handlingsprogram för informationssäkerhet[10]. Revisionen anser också att det är viktigt att förändringar i roller och ansvar för informationssäkerhetsarbetet kommuniceras till berörda medarbetare.

Revisionen bedömer att informationsägarskapet på Karolinska i viss utsträckning är känt. Medarbetare på sjukhuset har mestadels god kännedom om vem som är informationsägare men revisionen menar att det finns oklarheter vad gäller informationsansvaret för patientdata och annan data som kommer från flera olika system/källor. Revisionen bedömer att det är viktigt att sjukhuset tydliggör vad som gäller i dessa fall. Vidare bedömer revisionen att det även återstår ett arbete med att tydliggöra fastställd klassificeringsinformation för väsentliga informationstillgångar.

När det gäller SLSO är revisionens bedömning att verksamheterna på lokal nivå bör klassificera sin information enligt informationsklassificeringen som är framtagen av SLL. Den klassificering som genomförs centralt på SLSO bör spridas ut till enheterna. Verksamheterna bör även utbilda medarbetarna så att det blir tydligare vem som är informationsägare.

Karolinska universitetssjukhuset har en lokal organisation med informationssäkerhetskoordinatorer som är under uppbyggnad. Revisionen bedömer att det är viktigt att dessa får den utbildning och det stöd som rollen kräver eftersom rollen är relativt ny och flera av de intervjuade är dessutom nya i rollen.

3.3 Arbete med riskanalyser

Enligt regionens, dåvarande landstingets, riktlinjer ska varje verksamhet, för sin verksamhet, IT-system, processer och motsvarande, genomföra och dokumentera analyser avseende vilka hot, risker och sårbarheter som kan påverka verksamheten. Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. Riskbedömningar ska revideras när förutsättningar väsentligen förändras. Det är viktigt att arbetet med riskanalyser även omfattar samtliga verksamhetsnivåer och att riskerna omhändertas i handlingsprogram

3.3.1 Karolinska universitetssjukhuset

Arbetet med riskanalyser uppvisar variation i Karolinskas verksamheter. Vissa verksamheter har inte gjort, och har heller inte planerat att göra, någon riskanalys. Andra verksamheter ska genomföra riskanalys i närtid medan somliga har genomfört riskanalyser. Kännedomen om riskanalysarbetet är också mycket varierande mellan olika verksamheter. För att stödja processarbetet ska regionens verksamheter använda sig

[10] Målområde 5, där det bl.a. framgår att regionens medarbetare ska vara utbildade i informationssäkerhet i den omfattning som är relevant för befattningen.

av Compliance-portalen[11] för att genomföra risk- och åtgärdsbedömningar. De flesta verksamheterna har påbörjat ett arbete i Compliance-processen[11] och därmed lagt grunden för framtida riskanalysarbete. Några av Karolinskas verksamheter gör detta, i synnerhet ackrediterade verksamheter (labb) som genomför systematiska och dokumenterade riskanalyser löpande.

Arbetet med att utforma handlingsplaner med nedbrutna och konkretiserade delmål och åtgärder för att förverkliga handlingsplanernas intentioner uppvisar naturligt samma variation som arbetet med riskanalyser eftersom de är beroende av varandra. Av samma anledning finns också stora skillnader i arbetet med informationssäkerhetsklassificering av information. Vissa verksamheter har informationssäkerhetsklassificerat sin information medan andra verksamheter endast har säkerhetsklassificerat sin information utifrån personnummer och skyddad identitet. I det senare fallet är det främst speciallagstiftningar t.ex. dataskyddsförordningen (GDPR) och patientdatalagen som styrt och informationen har då inte klassificerats enligt landstingets modell för informationssäkerhetsklassificering som bygger på standarder och praxis.

3.3.2 SLSO

Vid de flesta av vårdcentralerna genomförs det inte några riskanalyser på lokal nivå och det finns inte heller kännedom, rutiner eller några direktiv om att det ska genomföras. I vissa fall uppges att informationssäkerhetsrisker inom verksamheten är så pass kända och väl inarbetade att en riskanalys skulle tillföra mycket lite. En vårdcentral har genomfört ett arbete med riskanalys inom området informationssäkerhet, både på egen hand och tillsammans med SLL informationssäkerhet vid ett gemensamt tillfälle i Compliance-portalen. SLL Informationssäkerhet och en vårdcentral har tillsammans genomfört en riskanalys i Compliance-portalen vilket medarbetarna har uttryckt uppskattning för. Informationsklassificering har inte gjorts i något fall men medarbetarna uppges veta vad som är patientsekretess och inte. För SLSO sker informationssäkerhetsklassificeringen enligt regionen modell främst på central nivå. Vårdcentraler gör t.ex. inte en informationssäkerhetsklassificering av IT-system utan en sådan informationssäkerhetsklassificering sker centralt, ofta i samband med inledande analysarbete i enlighet med Compliance-processen (sker i Compliance-portalen). Arbetet med riskanalyser startar med att genomföra gap-analyser och SLSO är i uppstartsfasen av användandet av Compliance-portalen. SLSO kommer inledningsvis att rikta in sig på att genomföra gap-analyser för att på sikt även genomföra riskanalyser.

Enligt SLSO:s centrala riktlinjer är ansvaret för den övergripande uppföljningen av efterlevnad av policy och riktlinjer förlagd på respektive verksamhets- och resultatenhetschef. Någon handlingsplan för informationssäkerhetsarbetet med omhändertagande av risker finns inte framtagen för vårdcentralerna (med ett undantag). Det saknas ett systematiskt arbete kring hur styrelsen säkerställer att styrdokumentens krav

[11] IT-stöd för uppföljning av kravefterlevnad/regelefterlevnad (i det här fallet efterlevnad av regionens riktlinjer för informationssäkerhet) i enlighet med Compliance-process i regionen som används för att styra det kontinuerliga arbetet med att egenkontroll, utvärdera och förbättra informationssäkerheten samt upprätthålla tillräcklig intern kontroll

på riskanalysarbete implementeras och kommuniceras ut i verksamheten. När det gäller SLSO:s arbete med informationssäkerhet och anpassningen till dataskyddsförordningen så sker arbetet med anpassningen till dataskyddsförordningen i informationssäkerhetsarbetet. Vid t.ex. genomgångar av informationssäkerhet med hjälp av Compliance-portalen så bedöms även regelefterlevnaden gällande dataskyddsförordningen.

3.3.3 Bedömning

Granskningen visar att det i några fall finns ett systematiskt arbete med riskanalyser och handlingsplaner lokalt vid Karolinska och SLSO medan det i andra fall inte har genomförts någon riskanalys alls. Revisionen menar att det är allvarligt att det inte genomförts någon riskanalys med tillhörande handlingsplan och klassificering eftersom det kan finnas risker som inte identifieras som bland annat kan påverka patientsäkerheten. Mot bakgrund av detta är det viktigt att alla verksamheter på Karolinska universitetssjukhuset och SLSO genomför riskanalyser med tillhörande handlingsplan och klassificering. Resultatet av riskanalyserna ska dokumenteras och delges medarbetarna. Det är bra att Karolinskas verksamheter har påbörjat ett arbete i Compliance-processen och därigenom lagt grunden för kommande arbete med riskanalyser. SLSO är i uppstarten av ett arbete i Compliance-processen som ska lägga grunden för ett riskanalysarbete. Revisionen anser att det är viktigt att det påbörjade arbetet drivs skyndsamt så att riskanalysarbetet kan påbörjas.

3.4 Utbildning och kunskap om informationssäkerhet

I regionens, dåvarande landstingets, handlingsprogram för informationssäkerhet, målområde 5, framgår bl.a. att regionens medarbetare ska vara utbildade i informationssäkerhet i den omfattning som är relevant för befattningen. Vidare framgår av handlingsprogrammet även att verksamhetschefer återkommande ska ta upp informationssäkerhet med medarbetare i syfte att skapa insikt om informationens värde och behov av skydd. Revisionen ser en risk med att det stora antalet medarbetare, personalomsättning och inhyrd personal kan leda till att medvetenheten och kunskapen om informationssäkerhet bland medarbetarna är låg.

3.4.1 Karolinska universitetssjukhuset

Antalet medarbetare som genomgått DISA-utbildning[12] (datorstödd informationssäkerhetsutbildning för användare) är mycket varierande i Karolinskas verksamheter. Det gäller även uppföljning av att medarbetare genomgått utbildningen. I de verksamheter som följt upp antalet medarbetare som genomgått DISA-utbildningen uppvisas en stor variation, från samtliga medarbetare i vissa verksamheter till knappt hälften i andra. Detta beror till stor del på verksamhetens storlek där stora verksamheter i allmänhet uppvisar en lägre andel genomgångna utbildningar. DISA-utbildningen är obligatorisk vid nyanställning i samtliga verksamheter. Befintliga anställda

[12] DISA utbildningen byttes ut av Landstinget i november 2017 och alla tidigare utbildade nollställdes. Fram till 2017 hade endast 3800 (~24%) av medarbetarna på Karolinska under de tre år utbildningen funnits genomgått utbildningen. Sedan november 2017 och fram till 2018-12-12 har 3 661 (~22%) av sjukhusets medarbetare (både nya och gamla) gått utbildningen. Målet för 2019 är >50%.

uppges dock vara svåra att motivera att genomföra DISA-utbildningen. Flera intervjuade lyfter fram att det vore bra om DISA-utbildningen görs obligatorisk för att få ut e-tjänstekort i likhet med t.ex. brandutbildningen.

Utöver DISA-utbildningen uppges det vara upp till respektive informationssäkerhetskoordinator att söka fördjupad kunskap i informationssäkerhetsfrågor. Det sker oftast ingen kontinuerlig vidareutbildning av verksamhetens medarbetare i informationssäkerhet.

Av genomförda intervjuer framgår att medarbetare, och ibland även informationssäkerhetskoordinatorer, har svårt att skilja på arbetet med informationssäkerhet och sådant som är hänförligt till arbetet med dataskyddsförordningen (GDPR). Till följd av det intensiva arbete som i flera verksamheter genomförts under året kopplat till dataskyddsförordningen nämns på flera håll dataskyddsförordningen vid besvarandet av frågor som rör informationssäkerhet.

3.4.2 SLSO

Endast en av de fem vårdcentraler som ingått i granskningen känner till regionens, dåvarande landstingets, policy och riktlinjer för informationssäkerhet. Uppfattningen är att merparten av personalen har inte genomgått DISA-utbildning eller någon vidareutbildning med fokus på informationssäkerhet. SLSO centralt har haft svårigheter att sammanställa en uppföljning av andelen medarbetare som har genomfört utbildningen. Systematisk vidareutbildning efter introduktionen för nyanställda när det gäller informationssäkerhet saknas för samtliga vårdcentraler.

3.4.3 Bedömning

Revisionen anser att det är viktigt att alla medarbetare är utbildade i informationssäkerhet i den omfattning som är relevant för befattningen. Revisionens bedömning är därför att samtliga medarbetare ska genomföra en grundläggande informationssäkerhetsutbildning (t.ex. DISA) och inte bara nyanställda, i enlighet med landstingets riktlinjer för informationssäkerhet, avsnitt 2.4. För att kontinuerligt möta och vara uppdaterad om nya lagar och informationssäkerhetshändelser menar revisionen att det är viktigt att både Karolinska universitetssjukhuset och SLSO genomför systematisk vidareutbildning inom området.

Karolinska universitetssjukhuset har påbörjat ett arbete med att leva upp till GDPR-kraven vilket skett parallellt med informationssäkerhetsarbetet. Det är viktigt att arbetet med det grundläggande systematiska informationssäkerhetsarbetet kopplar på GDPR-arbetet så att alla teman, funktioner och staber får igång ett systematiskt informationssäkerhetsarbete.

Händelsevis är en huvudsaklig väg för avvikelserapportering men i vissa fall även för incidenter rörande informationssäkerhet. Rapportering till närmsta chef och informationssäkerhetssamordnare sker vid incidenter. Kännedomen om vad som är brott mot informationssäkerhetsreglerna varierar i verksamheterna och uppges inte ha kommunicerats ut till medarbetarna.

3.5 Avvikelser och förbättringsarbete

I landstingets handlingsprogram för informationssäkerhet kapitel 5 framgår bl.a. att medarbetare ska delta aktivt i förbättringsarbetet genom att bland annat rapportera avvikelser och förbättringsförslag.

3.5.1 Karolinska universitetssjukhuset

Mot bakgrund av att utvecklingsarbetet kopplat till informationssäkerhet i Karolinskas verksamheter har hunnit olika långt uppvisar även förekomsten av ett aktivt förbättringsarbete där medarbetarna involveras skillnader. I verksamheter där ett systematiskt informationssäkerhetsarbete ännu inte kommit igång finns av naturliga skäl heller inget systematiskt förbättringsarbete. Förekomst av en process för förbättringsarbete avseende informationssäkerhet finns i flera verksamheter. I de flesta fallen sker förbättringsarbete genom Compliance-portalen och i något fall finns informationssäkerhetsarbete med som en del i verksamhetsplan.

I samtliga verksamheter uppger intervjuade att medarbetare ska rapportera avvikelser i avvikelserapporteringssystemet Händelsevis, att så faktiskt sker har inte kontrollerats inom ramen för denna granskning. Ackrediterade verksamheter uppger att de dessutom har kompletterande system för rapportering av avvikelser. Avvikelserapporteringen är en del i förbättringsarbetet. Rapportering av rena förbättringsförslag sker i mindre utsträckning.

3.5.2 SLSO

Mot bakgrund av att utvecklingsarbetet kopplat till informationssäkerhet i SLSO:s verksamheter har hunnit olika långt uppvisar även förekomsten av ett aktivt förbättringsarbete där medarbetarna involveras skillnader. I verksamheter där ett systematiskt informationssäkerhetsarbete ännu inte kommit igång finns av naturliga skäl heller inget systematiskt förbättringsarbete. Förekomst av en process för förbättringsarbete avseende informationssäkerhet finns endast i ett fåtal verksamheter.

Förbättringsarbete inom informationssäkerhetsområdet uppges vara något medarbetare sällan deltar i. I vissa fall finns processer för generellt förbättringsarbete och hur förbättringsförslag ska framföras. Det förbättringsarbete som genomförs utförs enligt uppgift oftast vid arbetsplatsträffar och då i samband med ett redan upplevt problem.

Intervjuade uppger att rapportering av avvikelser görs av medarbetare från alla vårdcentraler. Rapporteringssystemet Händelsevis uppges vara väl utbrett och känt bland medarbetare. Att så är fallet har inte kontrollerats inom ramen för denna granskning.

3.5.3 Bedömning

Förekomsten av en process för förbättringsarbete avseende informationssäkerhet på Karolinska Universitetssjukhuset är beroende av om verksamheten kommit igång med sitt systematiska informationssäkerhetsarbete. Revisionen bedömer att det är viktigt att sjukhuset ser till att alla verksamheter påbörjar ett systematiskt informationssäkerhetsarbete där samtliga medarbetare involveras i förbättringsarbetet.

På vårdcentralerna sker förbättringsarbete inom informationssäkerhet sporadiskt på arbetsplatsträffar och delaktigheten är förhållandevis låg. Förbättringsarbetet kräver därför tydligare rutiner för genomförande och uppföljning. Revisionen bedömer att det är viktigt att SLSO ser till att alla verksamheter påbörjar ett systematiskt informationssäkerhetsarbete där samtliga medarbetare involveras i förbättringsarbetet.

Vad gör Landstingsrevisorerna?

Landstingsrevisorerna granskar den verksamhet som bedrivs av regionens, dåvarande landstingets, 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 Landstingsrevisorernas hemsida www.sll.se/rev. De kan också beställas från revisionskontoret. Det går även att prenumerera på Landstingsrevisorernas nyhetsbrev Nytt från landstingsrevisionen genom att anmäla intresse via e-postmeddelande till landstingsrevisorerna.rev@sll.se.

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Postadress: Box 22230, 104 22 Stockholm
Besöksadress: Hantverkargatan 25 b (T-bana Rådhuset)
Telefon: 08-737 25 00
E-post: landstingsrevisorerna.rev@sll.se
Hemsida: www.sll.se/rev
Org.nr: 232100-0016