Koncernkontoret
Området för krisberedskap, säkerhet och miljö

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

RAPPORT

Datum: 2020-02-10
Dnr: 1900672

Rapport till Regionstyrelsen om informationssäkerhetsarbetet

Denna rapport utgör den information som enligt Socialstyrelsens föreskrifter[1] och enligt Region Skånes riktlinjer för informationssäkerhet en gång om året ska lämnas till Regionstyrelsen. Rapporten utgör underlag till ledningen med information om status på informationssäkerhetsarbetet och om effektiviteten i ledningssystemet för informationssäkerhet[2].

Regionstyrelsen beslutar om handlingsplan som följer med denna rapport.

Johan Reuterhäll
Informationssäkerhetschef

[1] 1 kap. 6§ Socialstyrelsens föreskrifter (HSLFS-FS 2016:40) om informationshantering och journalföring i hälso- och sjukvård
[2] Enligt kapitel 5.3 punkt b, ISO 27001:2017

Innehåll

Sammanfattning

Informationssäkerhetsarbetet har utvecklats i positiv riktning under 2019. Tidigare fattade beslut av Regionstyrelsen och Regiondirektören implementeras i den takt som är möjlig för att nå de mål som Regionfullmäktige och Regionstyrelsen beslutat om.

Informationsägarnas och systemägarnas ansvar har implementerats i flera processer. Arbetet fortgår och en uthållighet bör finnas då organisationens storlek och komplexiteten i processerna innebär att förändringsarbete tar lång tid.

Ett systemstöd för genomförande, dokumentation och uppföljning av informationsklassificering och riskanalys har under året upphandlats och är för närvarande under införande under ledning av Området för krisberedskap, säkerhet och miljöledning (KSM). Vid fullt införande kommer systemstödet innebära att Region Skåne får ökad kontroll över sina informationstillgångar. Det skapar förutsättningar för att säkerställa att informationen får det skydd som verksamheten och lagstiftaren kräver.

Antalet medarbetare har under året utökats i det regionala informationssäkerhetsarbetet. Informationssäkerhetsarbetet gynnas av detta då de centrala resurserna kan bistå och stödja förvaltningarna i högre utsträckning vilket är positivt och uppskattat i förvaltningarna. Samtidigt fortsätter digitaliseringsarbetet på bred front med en stor mängd projekt varav ett flertal är relativt stora och komplexa. Regionala resurser bedöms fortsatt behöva förstärkas för att stödja verksamheten i den utsträckning som behövs.

Cyberbrottsligheten fortsätter att vara lönsam verksamhet där information är ett eftertraktat byte vid olika typer av intrång. Hälso- och sjukvårdssektorn är utsatt vilket har visat sig vid ett flertal tillfällen, exempelvis i England och USA. Cyberbrottslighet i form av ransomware kan orsaka stora ekonomiska skador på en verksamhet och på förmågan att bedriva verksamheten.

Granskningar och revisioner av större betydelse

Externa granskningar

MSB angående Region Skånes mognadsnivå inom informationssäkerhet

Under 2018 genomförde MSB en mognadsbedömning av landstingens/regionernas informationssäkerhetsarbete. Resultatet rapporterades under 2019. Region Skåne bedömdes befinna sig på mognadsnivå två på en fyrgradig skala. Bedömningen baserades på ett flertal fokusområden; riskhantering, informationsklassificering, lärande, upphandling, säkerhetskultur och uppföljning.

Endast ett fåtal regioner når upp till nivå tre. Regiondirektörens ambitionsnivå är att Region Skåne ska uppnå nivå tre.

Granskning av IT-kontroller, Deloitte
Syftet var att utvärdera de kontroller och rutiner som omger de delar av IT-miljön som är centrala för Region Skånes kritiska processer kopplade till finansiell rapportering. De system som identifierats som mest kritiska för den finansiella rapporteringen och som valdes ut för granskning var Region Skånes ekonomisystem Raindance samt den personalrelaterade applikationen Personec P (del av HR Fönster). Den sammanfattande bedömningen var att Region Skåne har fungerande processer och kontroller avseende Raindance och Personec P. Deloitte noterade dock förbättringsområden avseende verksamhetens IT-kontroller kopplat till både Raindance och Personec P.

Granskning av IT och informationssäkerhet, KPMG
Syftet var att bedöma om Region Skåne har ändamålsenliga och väl fungerande IT-system och rutiner som kan generera ändamålsenliga och korrekta underlag för redovisningen. Uppdraget var avgränsat till att granska kritiska IT system och gränssnitt som hanterar stora transaktionsvolymer för att säkerställa en korrekt redovisning. Rapport från granskningen har inte blivit slutförd men beräknas vara klar under början av 2020.

Informationssäkerhetsarbetet i förvaltningarna

Ett flertal förvaltningar har under året fått informationssäkerhetssamordnare och dataskyddssamordnare. Utbildning, informationsinsatser revisioner och övningar genomförs. Samordnarna har också vid flera tillfällen varit med och stöttat arbetet med riskanalyser avseende regionala IT-system.

Informationssäkerhetsarbetet i SDV

I samband med analys av risker vid implementering av möjliga lösningar avseende tillämpning av Patientdatalagen (PDL) i Millenium har en ny metodik provats. Vid bedömning av riskerna utvärderades åtgärder med utgångspunkt i vilken påverkan åtgärden hade på följsamhet mot lagstiftning, bedömd patientsäkerhetsrisk samt användarvänlighet. Beroende på påverkan lades förslag på åtgärd fram för beslut hos informationsägaren. Även om metoden kan synas vara enkel är den effektiv eftersom åtgärden kräver en dialog med såväl verksamheten som experter inom juridik vilket är något som bör eftersträvas. Resultatet bedöms skapa en god balans mellan att å ena sidan uppfylla flera lagkrav och å andra sidan att följa tänkt flöde i Millenium samt aspekterna effektivitet och patientsäkerhet.

Under hösten har projektet SDV genomfört en riskanalys. Resultatet visar på potentiella förbättringsområden inom informationssäkerhetsarbetet. SDV har utrett hur identifierade brister kan åtgärdas. Dialog har skett med dataskyddsombud och informationssäkerhetschef då vissa åtgärder ligger på

regional nivå eller då samverkan behövs med regional nivå. Några åtgärder som redan nu kan nämnas är att SDV har anlitat en informationssäkerhetssamordnare som ska jobba brett inom SDV för att förbättra processerna med målet att informationssäkerhetsaspekterna ska finnas med i lämpliga processer och aktiviteter. Ett av uppdragen är att sammanställa och koordinera informationsklassificeringar och riskanalyser inom SDV samt åtgärder.
SDV förstärker arbetet inom informationssäkerhet med en beredningsgrupp/expertgrupp, med representant från bland annat enheten för informationsstyrning, enheten för juridik, samt de regionala funktionerna för dataskydd och informationssäkerhet tillsammans med verksamhetens kliniska experter.

Regionstyrelsen beslutade i förra årets handlingsplan[3] för informationssäkerhet att ge Regiondirektören i uppdrag att inom ramen för SDV genomföra fördjupade riskanalyser avseende krav på tillgänglighet till system som stödjer samhällsviktig verksamhet med målet att identifiera åtgärder som behöver vidtas för att säkerställa tillgängligheten såväl under normala omständigheter, som under höjd beredskap och krig.
Arbetet inom detta område ska prioriteras av SDV. Nödvändiga åtgärder ingår bland de insatser som föranleds av den riskanalys som togs fram under hösten inom SDV.

Förändringar i externa eller interna frågor som är relevanta för ledningssystemet för informationssäkerhet

Omvärldsbedömning

Cyberbrottslighet

Data fortsätter vara ett viktigt mål och en handelsvara i cyberbrottslighet. Det gör att arbetet med att skydda data blir allt viktigare. GDPR som började gälla i maj 2018 har påverkat arbetet positivt. Bristande informationssäkerhet får större utrymme i tidningsrubriker och sanktionsavgifter har i flera fall dömts ut.

Ransomware fortsätter vara det hot som ligger högst. Även om antalet attacker har gått ner något är de attacker som äger rum större, mer riktade och orsakar större ekonomisk skada. Så länge ransomware fortsätter vara en relativt enkel inkomstkälla och fortsätter orsaka stora skador och ekonomiska skador, är det sannolikt att detta hot kommer ligga högt på listan över cyberbrottlighet.

[3] Regionstyrelsens beslut (§ 278 punkt 1, dnr 160423, 2018-12-18)

Bedrägerier riktade mot VD:ar är inget nytt hot men har fortsatt att utvecklas. Målet med bedrägerier riktade mot VD:ar är att komma över pengar eller information. Den här typen av bedrägerier riktar sig inte enbart mot VD:ar utan alla personer som har en ställning där de har åtkomst till information eller möjlighet att initiera exempelvis beställningar eller betalningar. Bedragarna drar ofta nytta av att verksamheten de attackerar är uppdelad där olika delar i processerna har brister. Bedrägerierna kan ibland inbegripa social ingenjörskonst där medarbetare bearbetas under en tid innan attacken sker. Andra bedrägerier kan åstadkommas genom tekniska attacker genom skadlig kod eller intrång i nätverk. Vid dessa attacker är det information som är målet.

Överbelastningsattacker (DDoS-attacker) är ett annat reellt cyberbrott. Överbelastningsattacker genomförs ofta för att förhindra digitala besökare åtkomst till tjänster. Det kan vara biljettsystem eller e-tjänster inom sjukvården.

Fler företag och myndigheter outsourcar delar av sin verksamhet. Europol förväntar sig i det avseendet en ökning av antalet attacker mot olika försörjningskedjor. Attacker mot försörjningskedjor sker ofta mot de svagaste punkterna men påverkar hela kedjan negativt. Försörjningskedjor är många gånger beroende av information för att fungera. Ett avbrott i informationsförsörjningen påverkar direkt försörjningskedjan. Dessa typer av attacker kan också drabba flera kunder då försörjningskedjan används för leverans till flera kunder.

Ny lagstiftning

Lagstiftarna i EU och Sveriges riksdag har under året stiftat nya lagar som har betydelse för informationssäkerheten och krav på skydd av känslig information.

Säkerhetsskyddslagen

Den 1 april 2019 började den nya säkerhetsskyddslagen att gälla. Lagen påverkar alla som bedriver säkerhetskänslig verksamhet vilket Region Skåne gör i vissa delar. Säkerhetsskydd handlar om att genom förebyggande arbete skydda säkerhetskänslig verksamhet hos myndigheter och företag mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten. Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet eller som Sverige har förbundit sig att skydda genom internationella åtaganden.
I säkerhetsskydd ingår också att skydda uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, eller som skulle ha omfattats av den lagen om den varit tillämplig.
Den nya säkerhetsskyddslagen påverkar informationssäkerhetsarbetet eftersom det är en lag som ställer krav på ett riskbaserat och systematiskt informationssäkerhetsarbete.

NIS-direktivet
NIS-direktivet (Lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster) började gälla 2018. 2019 började ett flertal förordningar att gälla som påverkar Region Skåne. Bland annat en rapporteringsskyldighet av incidenter som får betydande inverkan på kontinuiteten i den samhällsviktiga verksamheten.

Införandet av Office 365

Införandet av Office 365 har pågått under en längre tid. Införandet har skett etappvis där olika produkter inom Office 365 införts.
Införandet och den framtida förvaltningen av Office 365-plattformen är av stor betydelse för Region Skåne. Dialog mellan projektet för Office 365 och de regionala funktionerna för dataskydd och informationssäkerhet behöver därför intensifieras.

Dokumenthantering

Med dokument avses inte endast allmänna handlingar utan alla typer av dokument som hanteras inom myndigheten och med externa parter. En trend är att dokument hanteras i allt fler informationssystem.
Informationssäkerhetsmässigt innebär en ökad komplexitet att det blir allt svårare att få kontroll över informationsbehandlingen. Ökat fokus kommer från informationssäkerhetsfunktionen att ägnas detta område.

Hanteringen av dokument som utgör beslutsunderlag till den politiska ledningen uppfattas som god. Det finns processer, rutiner och utpekade system som ska användas i beredningen. Detta gynnar informationssäkerheten positivt då myndigheten har kontroll över dokumenten i dessa system. I detta fall bedöms möjligheterna att uppnå ”en god offentlighetstruktur” vara bättre. I det begreppet ingår bland annat att säkerställa sekretesskyddet.

Sekretessbelagda uppgifter och externa leverantörer

Begränsningarna att behandla sekretessbelagd information i tjänster med utländska leverantörer är omfattande. Utredningar från eSam[4] och Kammarkollegiets inköpscentral[5] är exempel på utredningar som tar upp och beskriver de bakomliggande orsakerna. Det finns inget fall som prövats rättsligt vilket gör att Region Skåne, liksom andra myndigheter, tvingas att göra kvalificerade bedömningar om riskerna.

---

[4] eSam ”Rättsligt uttalande om röjande och molntjänster” (2018-10-23), eSam ”Kompletterande information om molntjänster” (2019-09-20) samt ”Outsourcing 2.0 – En vägledning om sekretess och dataskydd”, december 2019
[5] Kammarkollegiet ”Förstudierapport Webbaserat kontorsstöd”, dnr 23.2-6283-18, 2019-02-22

Regeringen har uppmärksammat problemen och på sikt kan exempelvis svenska nationella molntjänster skapas som möjligtvis löser en del av problemen.

Förbättringsåtgärder

Informationsägare och systemägare

Regionstyrelsen beslutade[6] 2015-11-05 att rollen informationsägare införs i Region Skåne. Informationsägarnas ansvar ligger i linje med de beslut och mål som Regionstyrelsen beslutat om.

Införandet av informationsägare har inneburit en ökad riskmedvetenhet hos beslutsfattare och bedöms medföra en kvalitetshöjning i de tjänster som upphandlas eller utvecklas. Riskmedvetenheten kommer av att dokumenterade informationsklassificeringar och riskanalyser, vilka fastställs av informationsägaren, med identifierade risker och konsekvenser tydliggörs och synliggörs. Detta ökar sannolikheten att rätt krav ställs vid upphandling av informationssystem eller andra varor och tjänster där verksamhetens information ska hanteras.

Införandet av informationsägare i processen tar tid och fordrar att processer och arbetssätt förändras. Bedömningen är att när processerna väl utformats kommer Region Skånes förmåga att upphandla och utveckla med hög kvalitet att öka. Det tar tid att få nödvändiga processer uppdaterade och implementerade varför uthållighet från ledningen krävs.

Belastningen kommer initialt att öka på de personer som har roll som informationsägare. Inledningsvis kommer de beslutsunderlag som tas fram till informationsägare vara av varierande kvalitet. I takt med att organisationen mognar och processerna kommer på plats kommer belastningen att minska.

Inom ramen för det regionala riskhanteringsverktyget pågår arbete med att ta fram en grundstomme med säkerhetskrav baserat på informationsklass som gör att endast avvikelser från beslutade krav behöver lyftas framgent för beslut till informationsägare.

Framtagningen av beslutsunderlag till informationsägarna innebär att olika analyser behöver sammanställas där kompletterande frågor behöver besvaras. Detta kan vara komplicerat och kräver kunskap och tid. Det har framkommit behov av resurser som kan stödja informationsägarna med detta. Behovet gäller kompetenser inom både informationssäkerhet och dataskydd.

---

[6] Beslut i Regionstyrelsen 2015-11-05, § 189, dnr 1502668,

Regionalt riskhanteringsverktyg

Regionstyrelsen beslutade 2015 om att ge Regiondirektören i uppdrag att besluta om vilket eller vilka verktyg (systemstöd) som ska användas för inventering, informationsklassificering, uppföljning och dokumentation av informationssystem och tillhörande skyddsåtgärder i Region Skåne.
Under 2019 genomfördes upphandling av ett verktyg som stödjer processerna för informationsklassificering, riskanalys och uppföljning av beslutade säkerhetsåtgärder. Systemet stödjer inte endast informationssäkerhetsfunktionens behov utan ska tillgodose hela säkerhetsområdets behov av riskanalyser och uppföljning. Samverkan kring behoven skedde via Region Skånes krisberedskaps- och säkerhetsråd. Systemstödet införs för närvarande och stort intresse finns från förvaltningarna i att delta. Systemstödet förväntas vara i drift under första kvartalet 2020.
En framgångsfaktor för att lyckas med införandet är att det initiala beslutet som togs av Regionstyrelsen ligger fast, d.v.s. att systemstödet ska utgöra hela Region Skånes systemstöd för riskhanteringsprocessen. Det innebär att systemstödet ska användas av systemägare, informationsägare och den personal som arbetar med riskhantering, oavsett organisationstillhörighet.

SDV har beslutat att systemstödet ska användas för informationsklassificering och riskanalys.
Förvaltningen Regionfastigheter kommer i början av 2020, att börja dokumentera informationsklassificering och riskanalyser i det nya systemstödet.

Under 2020 planeras riskanalyser kopplat till miljöarbetet att hanteras i systemstödet vilket ligger helt i linje med tidigare fattat beslut om att systemstödet ska kunna hantera alla typer av riskanalyser.

Utbildning i säker informationshantering

Projektet med att implementera GDPR i Region Skånes verksamheter visade på att kunskapsbristen vad gäller säker informationshantering är stor. Med anledning av detta har Informationsstyrningsrådet i Region Skåne beslutat att en gemensam grundläggande basutbildning ska tas fram inom informationssäkerhet, dataskydd och informationsstyrning. Arbetet bedrivs i projektform och målet är att alla medarbetare i Region Skåne ska ha samma grundläggande kunskaper om säker informationshantering. Projektet kommer bland annat att leverera ett digitalt lärandestöd, en grundläggande utbildning i powerpoint-format, översyn av informationen som finns på Region Skånes webbplatser och identifiering av vilka specialistroller som behöver fördjupningsutbildningar. De positiva effekterna som väntas är många; en ökad kompetens i hur man som anställd i offentlig verksamhet ska hantera information, bättre förutsättningar att förebygga felaktig hantering av information, tydlighet kring vilket ansvar varje medarbetare har när det gäller säker informationshantering, ökad medvetenhet kring incidentrapportering, att lära sig känna igen olika typer av incidenter och avvikelser, hur de ska rapporteras, och på sikt, färre inträffade incidenter

och avvikelser. Syftet är att säker informationshantering ska bli en mer naturlig och integrerad del i det dagliga arbetet.

Gemensamma samverkansmöten

Samverkan mellan den regionala informationssäkerhetsfunktionen och den regionala dataskyddsfunktonen fungerar bra. Mer samverkan efterlyses dock av förvaltningar. I de flesta fall finns gemensamma frågor som ofta utreds tillsammans. Av den anledningen har dataskyddsombudet och informationssäkerhetschefen beslutat att de regionala möten som tidigare genomförts var för sig framöver ska ske tillsammans. Bedömningen är att det gagnar samverkan mellan de olika funktionerna både regionalt och inom förvaltningarna. Information ges vid samma tillfällen och det finns utrymme för gemensamma diskussioner som många gånger rör båda funktionerna.

Information och utbildning av ledningsgrupper

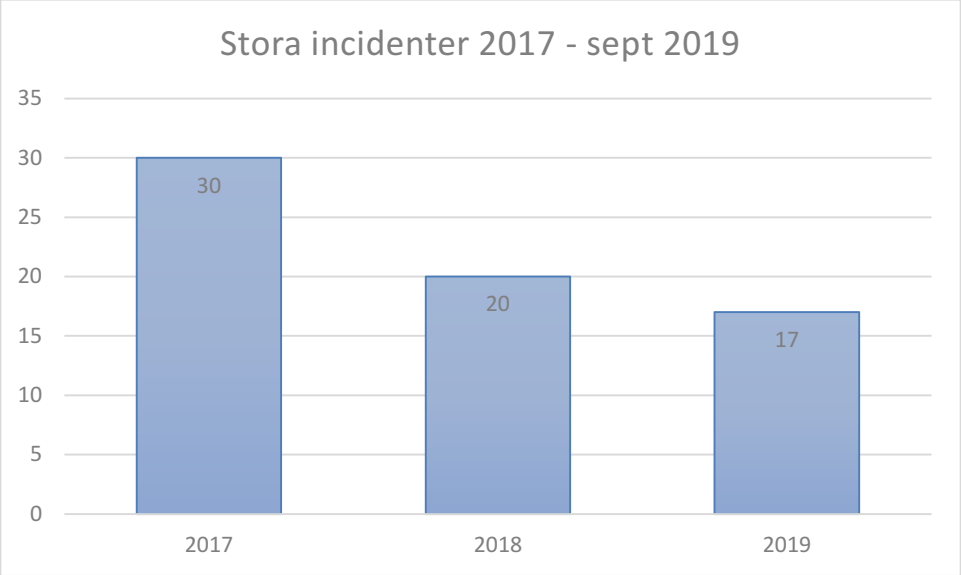
Informationssäkerhetschefen och dataskyddsombudet har under 2019 besökt förvaltningarnas ledningsgrupper. Besöken syftar till att informera ledningsgrupperna om hur Region Skåne arbetar med informationssäkerhet inklusive dataskydd samt informera om gällande interna regelverk, lagstiftning och informationsägarnas roll. Besöken har varit uppskattade och insatsen bedöms ha stor betydelse för hur förvaltningarna väljer att organisera sina resurser inom området. Det ökar också kunskapen om vilka risker felaktig behandling av information kan få och vilka processer och aktiviteter som finns som förebygger detta.
Besöken kommer att förtsätta framöver och som komplement har informationssäkerhets- och dataskyddssamordnarna i uppdrag att genomföra utbildning och informationsinsatser i ledningsgrupper inom respektive förvaltning.

Incidenter

Rutinerna för hantering av personuppgiftsincidenter har etablerats och fungerar väl. Många incidenter beror på den mänskliga faktorn eller bristande rutiner. Rapportering av incidenter och en funktion som tar hand om dem gör att åtgärder kan vidtas för att förhindra upprepning. Det kan vara att uppdatera rutiner, utbilda och informera på arbetsplatsträffar.

Ett flertal incidenter rör hanteringen av patienter med skyddad identitet där Region Skånes interna riktlinjer inte följts. Rutinerna kring hanteringen av skyddade personuppgifter har setts över och kommer under 2020 att utvärderas.

Antalet incidenter redovisas i år genom totala antalet s.k. ”stora incidenter”. Även om hela 2019 kan redovisas förefaller trenden vara att antalet stora incidenter minskar.



Uppföljning av tidigare beslut

Underlag till besluten återfinns i föregående års rapporter. Nedan återges besluten i korthet med tillhörande uppföljning.

Beslut om logganalysverktyg

Regionstyrelsens beslut (§ 189, dnr 1502668, 2015-11-05):
Regionstyrelsen ger regiondirektören i uppdrag att ge förvaltningen Medicinsk service ett förnyat uppdrag *[ursprungligt uppdrag från Beredningen för integritetsfrågor]* att ge verksamhetsansvariga, som har skyldighet att genomföra kontroll av loggar i journalsystem, tillgång till ett automatiserat logganalysverktyg i enlighet med regionstyrelsens tidigare beslut.

Uppföljning:
I samband med upphandlingen av Skånes Digitala Vårdsystem (SDV) har krav ställts på automatiserad logganalys vilket innebär att beslutet i så fall genomförs för de större journalsystemen, inklusive andra system där patientuppgifter behandlas och där logguppföljning krävs enligt Socialstyrelsens föreskrifter.

Riskbedömningar med informationsklassning

Regionstyrelsens beslut (§ 189, dnr 1502668, 2015-11-05):
Regionstyrelsen uppdrar åt regiondirektören att definiera processerna för riskbedömningar och informationsklassning och besluta om vilket eller vilka verktyg som ska användas inom hela Region Skåne för inventering, informationsklassificering, uppföljning och dokumentation av informationssystem och tillhörande skyddsåtgärder.

Uppföljning:
Upphandling har genomförts och ett projekt för införande pågår.

Fördjupade riskanalyser inom SDV
Regionstyrelsens beslut (§ 278, dnr 1604263, 2018-12-18)
Med anledning av det ökande beroendet till externa leverantörer ges Regiondirektören i uppdrag att inom ramen för SDV genomföra fördjupade riskanalyser avseende krav på tillgänglighet till system som stödjer samhällsviktig verksamhet med målet att identifiera åtgärder som behöver vidtas för att säkerställa tillgängligheten såväl under normala omständigheter, som under höjd beredskap och krig.

Uppföljning:
Fördjupande riskanalyser håller på att genomföras.

Övning vid otillgänglig IT-infrastruktur
Regionstyrelsens beslut (§ 278, dnr 1604263, 2018-12-18)
Regionstyrelsen ger Regiondirektören i uppdrag att under 2018/2019 genomföra minst en övning där Region Skånes IT-infrastruktur är otillgänglig för hälso- och sjukvården.

Uppföljning:
Övningen har genomförts.

Åtgärder kopplat till utlämnande av patientuppgifter
Regionstyrelsens beslut (§ 278, dnr 160423, 2018-12-18)
Regionstyrelsen ger Regiondirektören i uppdrag att snarast möjligt, dock senaste 30:e juni 2019:

- genomföra översyn av samtliga pågående utlämningar till kvalitetsregister och forskning för att kontrollera att utlämnandet sker på laglig grund och att beslut om utlämnande har fattats av behörig
- vidta åtgärder för att förhindra att patientuppgifter lämnas ut innan beslut fattats av Samrådsgrupp - Kvalitetsregister, vårdinformationssystem och beredning (S-KVB)
- lämna förslag till Regionstyrelsen med underlag till beslut om vem eller vilka som ska besluta om tillfälligt utlämnande av hälsodata.

Uppföljning:
Regionstyrelsens beslut är inte genomfört. Frågan kommer aktualiseras i S-KVB där beslut om utlämnande för forskning och kvalitetsregister idag ligger.

Handlingsplan (förslag till beslut i Regionstyrelsen)

I samband med ledningens genomgång ska förslag till handlingsplan lämnas.

1. Regionstyrelsens inriktning är att informationsägarskapet ska utvecklas vidare i enlighet med tidigare av Regionstyrelsen fattade beslut. Informationsägarna är en viktig komponent för att kunna fatta informerade beslut om vilka risker Region Skåne kan acceptera samt skapa spårbarhet i beslutsfattandet. Informationsägarnas nuvarande position innebär också en stark verksamhetsanknytning som bedöms gagna arbetet.

2. Regionstyrelsens inriktning avseende regionalt systemstöd för riskhanteringsprocessen är att arbetet är prioriterat och trycker särskilt på vikten att det är ett regiongemensamt verktyg. Detta för att full effekt ska uppnås i genomförande, dokumentation och uppföljning av identifierade risker och för sammanställning av risker på regional nivå.