# Granskning av informations- och it-säkerhet med fokus patientdata

Rapport

Region Skåne

KPMG AB

2023-11-21

Antal sidor 24

Bilaga 1

**Region Skåne**
Granskning av informations- och it-säkerhet med fokus patientdata

2023-11-21

# Innehållsförteckning

# 1 Sammanfattning

KPMG har av Region Skånes revisorer fått i uppdrag att granska Region Skånes arbete med informations- och it- säkerhet med fokus på patientdata.

Syftet med granskningen har varit att bedöma om arbetet med it- och informationssäkerhet inom Region Skåne bedrivs på ett systematiskt och ändamålsenligt sätt.

**Vår samlade bedömning utifrån granskningens syfte är att arbetet med it- och informationssäkerhet inom Region Skåne inte är systematiskt och ändamålsenligt och att det finns risk att patientdata inte skyddas mot obehöriga.**

Region Skåne har inte säkerställt medborgarens integritet då patientinformation i journalsystem endast delvis är skyddade mot obehöriga. Det saknas ett systematiskt och riskbaserat informationssäkerhetsarbete och det arbete som genomförts är inte i nivå med de krav som ställs i lag och i interna styrdokument.

Det finns krav på obligatoriska utbildningar, men deltagandet är alltför lågt i förhållande till det stora antal användare som har tillgång till skyddsvärd information, så som känsliga patientuppgifter. Det saknas därtill kompletterande utbildning med obligatoriska moment som riktas särskilt till personal inom hälso- och sjukvård.

Region Skåne har delvis säkerställt ett tillräckligt skydd för sina databaser och system, inklusive molntjänster, mot externa hot. Säkerhetsåtgärder har etablerats och analyser genomförts för att identifiera behov av ytterligare införanden i förhållande till aktuella hot och risker. Däremot saknas en samlad bild avseende vilka skyddsbehov som finns för Region Skånes informationstillgångar då informationsklassning och riskbedömning inte genomförts i tillräcklig omfattning. Utifrån Region Skånes krav på efterlevnad av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster är det av vikt att informationssäkerhetsarbetet bedrivs med en högre grad av systematik och att det är riskbaserat.

Rutiner för incidenthantering finns men de saknar en tydlig beskrivning av ansvar, processer samt eskaleringsvägar i händelse av olika incidenttyper. Avvikelser och incidenter hanteras därför endast delvis i enlighet med gällande lagstiftning och regelverk.

På nästa sida redovisas våra bedömningar kopplat till revisionsfrågorna och de rekommendationer vi riktar till granskade styrelser och nämnder.

| **Revisionsfråga** | **Bedömning: Nej** |
|---|---|
| **Säkerställs medborgarens integritet och är patientinformation i journalsystem skyddade mot obehöriga (informationssäkerhet)?** | Vi bedömer att medborgarens integritet inte har säkerställts då patientinformation i journalsystem endast delvis är skyddade mot obehöriga. |
| **Revisionsfråga** | **Bedömning: Nej** |
| **Har Region Skåne säkerställt att det finns ändamålsenlig utbildning av berörd personal kring informationssäkerhet som exempelvis lagring och hantering av känsliga uppgifter om enskilda patienter?** | Vi bedömer att Region Skåne inte har säkerställt att det finns ändamålsenlig utbildning av berörd personal kring informationssäkerhet som exempelvis lagring och hantering av känsliga uppgifter om enskilda patienter. |
| **Revisionsfråga** | **Bedömning: Delvis** |
| **Har Region Skåne ett tillräckligt skydd för sina databaser och system inklusive molntjänster mot utomstående intressen som antingen vill komma åt information eller skada verksamheten (IT-säkerhet)?** | Vår bedömning är att Region Skåne delvis har ett tillräckligt skydd för sina databaser och system, inklusive molntjänster mot utomstående hot. |
| **Revisionsfråga** | **Bedömning: Delvis** |
| **Hanteras avvikelser och incidenter i form av exempelvis driftavbrott och säkerhetsintrång på IT-system i enlighet med gällande lagstiftning och regelverk?** | Vi bedömer att avvikelser och incidenter i form av exempelvis driftavbrott och säkerhetsintrång på it-system delvis hanteras i enlighet med gällande lagstiftning och regelverk. |

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Stärka den interna kontrollen av samtliga nämnder och styrelser avseende efterlevnad av de styrande dokument som utgör Region Skånes ledningssystem för informationssäkerhet.
- Utvärdera om nuvarande resurser för informationssäkerhetsarbetet motsvarar omfattning av Region Skånes krav på informationssäkerhet mot bakgrund av lagkrav och interna beslut.
- Genom regelbunden uppföljning tillse att pågående arbete med riskhantering av Region Skånes informationssystem fortgår och slutförs, samt att säkerhetsåtgärder vidtas som analyser visat behov av i syfte att skydda patientinformation och andra skyddsvärda uppgifter.
- Säkerställa att Region Skånes process för åtkomst- och behörighetshantering stärks vad gäller tilldelning, förändring och avslut av behörigheter så att endast behöriga har tillgång till information. Därutöver rekommenderas styrelsen att

säkerställa att tilldelning sker efter genomförd behovs- och riskanalys samt sker i enlighet med lagkrav.

- Utreda om det finns möjlighet att centralisera logghanteringen för att avlasta verksamheterna samt kvalitetssäkra och stärka Region Skånes förmåga att genomföra kontroller i tillräcklig omfattning.
- Säkerställa att Region Skånes medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att nuvarande rutiner för incidenthantering kompletteras med tydlig beskrivning avseende ansvar, processer och eskaleringsvägar i händelse av olika incidenttyper samt att rutinerna etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov på regionövergripande nivå.

Utifrån resultatet av vår granskning rekommenderar vi Sjukhusstyrelsen Ystad att:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som styrelsen ansvarar för.
- Följa upp att de tekniska säkerhetsåtgärder som identifierats utifrån skyddsvärde på informationstillgångar etableras.
- Säkerställa att behörigheter hanteras utifrån lagkrav samt att uppföljning och kontroll av tilldelade behörighet sker för att säkerställa dess aktualitet.
- Säkerställa att loggkontroller genomförs i enlighet med upprättade rutiner så att patientinformation skyddas mot obehöriga och att medborgares integritet därmed säkerställs i högre grad.
- Säkerställa att tvåfaktorautentisering införs på de system som hanterar känsliga uppgifter i enlighet med krav.
- Säkerställa att medarbetare genomför obligatorisk utbildning som finns tillgänglig samt följa upp deltagarantalet.
- Utvärdera behov av kompletterade utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att rutiner för incidenthantering etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov.

Utifrån resultatet av vår granskning rekommenderar vi primärvårdsnämnden att:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.
- Följa upp att de tekniska säkerhetsåtgärder som identifierats utifrån skyddsvärde på informationstillgångar etableras.
- Säkerställa att behörigheter hanteras utifrån lagkrav samt att uppföljning och kontroll av tilldelade behörighet sker för att säkerställa dess aktualitet.
- Säkerställa att loggkontroller genomförs i enlighet med upprättade rutiner så att patientinformation skyddas mot obehöriga och att medborgares integritet därmed säkerställs.
- Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att rutiner för incidenthantering etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov.

Utifrån resultatet av vår granskning rekommenderar vi nämnden för operativ regiongemensam verksamhet att:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.
- Säkerställa att tekniska säkerhetsåtgärder vidtas utifrån identifierat skyddsvärde hos egna informationstillgångar men även övriga styrelser och nämnders identifierade behov i informationsklassning och riskbedömning.
- Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Säkerställa att rutiner för incidenthantering etableras i organisationen.
- Säkerställa att inträffade incidenter dokumenteras, analyseras och utgör underlag för att identifiera förbättringsbehov för att stärka it-säkerheten.

# 2 Bakgrund

Region Skåne är beroende av fungerande informationssystem med hög patientsäkerhet. Brister i informationssäkerhetsarbetet kan medföra:

- Att informationen röjs för obehöriga
- Att informationen inte är tillgänglig när den behövs
- Att informationen är oriktigt

Revisionen har genom tidigare granskningsinsatser identifierat ett antal brister i Region Skånes informations- och it-säkerhetsarbete och har därigenom i sin riskanalys bedömt att detta behöver granskas.

## 2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen är att bedöma om arbetet med it- och informationssäkerhet inom Region Skåne bedrivs på ett systematiskt och ändamålsenligt sätt.

För att uppnå ovanstående syfte kommer nedanstående revisionsfrågor att besvaras:

1. Säkerställs medborgarens integritet och är patientinformation i journalsystem skyddade mot obehöriga (informationssäkerhet)?
2. Har Region Skåne ett tillräckligt skydd för sina databaser och system inklusive molntjänster mot utomstående intressen som antingen vill komma åt information eller skada verksamheten (IT-säkerhet)?
3. Hanteras avvikelser och incidenter i form av exempelvis driftavbrott och säkerhetsintrång på IT-system i enlighet med gällande lagstiftning och regelverk?
4. Har Region Skåne säkerställt att det finns ändamålsenlig utbildning av berörd personal kring informationssäkerhet som exempelvis lagring och hantering av känsliga uppgifter om enskilda patienter?

Granskningen omfattar regionstyrelsen som har det övergripande ansvaret för informationssäkerhet och it-säkerheten och nämnden för operativ regiongemensam verksamhet samt sjukhusstyrelse Ystad och primärvårdsnämnden.

## 2.2 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

- Kommunallagen (2017:725) - kap 6:6
- Dataskyddsförordningen (The General Data Protection Regulation)
- MSB FS 2021:9 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (NIS-direktivet)
- HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Säkerhetsskyddslag (2018:585)
- Offentlighets- och sekretesslag (2009:400)
- Patientdatalag (2008:355)
- Säkerhetspolicy (RF 2017-06-20)
- Säkerhetsstrategi (regionstyrelsen 2017-12-07)
- Riktlinjer för informationssäkerhet (regionstyrelsen 2017-12-07)
- Instruktioner och anvisningar för informationssäkerhet

## 2.3 Metod

Granskningen har genomförts genom dokumentstudier, intervjuer och systemgranskning av tre utvalda system.

- Intervjuer har genomförts med verksamhetsföreträdare inom Primärvården, Ystad sjukhus, Förvaltningen koncernkontoret- koncernstab kansli område Informationsstyrning och informationsförvaltning samt Förvaltning Digitalisering IT och MT.
- Dokumentanalysen har bland annat omfattat övergripande styrdokument fastställda av regionfullmäktige, regionstyrelsen och regiondirektören i Region Skåne. Exempel på styrande dokument är reglemente för styrelser och nämnder i Region Skåne, Säkerhetspolicy, Säkerhetsstrategi, Riktlinjer för informationssäkerhet, Instruktioner och anvisningar för informationssäkerhet.
- Dokumentgranskning har även inkluderat riskanalyser och uppföljning inom ramen för intern kontroll, patientsäkerhetsberättelse samt uppföljning av det övergripande informationssäkerhetsarbetet inom respektive förvaltning.
- I systemgranskningen har vi analyserat dokument och underlag i form av systemdokumentation, riskanalyser och åtgärdsförslag.

Samtliga intervjuade har beretts möjlighet att sakgranska innehållet i rapporten.

# 3 Resultat av granskningen

## 3.1 Inledning

Enligt den svenska regleringen av EU:s NIS-direktiv är Hälso- och sjukvård en av de sektorer som identifieras som samhällsviktig tjänst och står under kraven i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Samtliga regioner i Sverige omfattas av lagkraven. Dessa verksamheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med grund i ett ledningssystem för informationssäkerhet som minst motsvarar kraven utifrån ISO 27001 samt vidta säkerhetsåtgärder i enlighet med kraven i ISO 27002.

Det finns ett flertal lagar och föreskrifter som reglerar hur patientuppgifter ska hanteras för att skyddas. Dataskyddsförordningen är överordnad övriga lagstiftningar och måste därför följas för information där personuppgifter ingår, även patientinformation.

Enligt 4 kap. 2 § patientdatalagen (2008:355) ska en vårdgivare bestämma villkor för tilldelning av behörigheter för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

I Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) preciseras kraven på ett strukturerat arbete med informationssäkerhet. Föreskrifterna tydliggör styrningen av behörigheter där vårdgivaren ansvarar för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter samt att beslut om behörighet ska föregås av en behovs- och riskanalys. Vårdgivaren ska därtill ha rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella.

## 3.2 Informationssäkerhetsarbetet i Region Skåne

### 3.2.1 Ledningssystem för informationssäkerhet

Region Skåne har ett ledningssystem för informationssäkerhet (hädanefter benämnt LIS). LIS syftar till att utgöra en gemensam struktur för informationssäkerhetsarbetet i Region Skånes verksamheter. Informationssäkerhetsarbetet ska enligt styrande dokument utgå från den etablerade standarden SS-ISO/IEC 27001 samt SS-ISO/IEC 27002.

I LIS finns ett stort antal instruktioner, anvisningar och mallar för att konkretisera hur informationssäkerhetsarbetet ska bedrivas. Bland annat ingår anvisningar i syfte att reglera hanteringen av patientuppgifter, journalföring, personuppgifter samt patientsäkerhet och sekretess. Som förtydligande av vilka lagar och regler som verksamheten har att förhålla sig till i sin personuppgiftsbehandling finns en instruktion, *Personuppgiftsbehandling i Region Skåne - Sammanställning av regler och krav*, reviderad senast 2018-05-07.

I intervjuer beskrivs informationssäkerhetsarbetet utifrån LIS som bristfälligt och inte i enlighet med den standard som finns beslutad. Den bild som förmedlas är att det på ett strategiskt plan finns styrdokument och beskrivningar av hur arbetet ska bedrivas, men att efterlevnaden är låg.

I den årliga uppföljningen av informationssäkerhetsarbetet som Region Skånes informationssäkerhetschef har i ansvar att sammanställa och rapportera till regionstyrelsen bekräftas ovan uppgifter. I uppföljningen framgår att Region Skånes nuvarande ledningssystem för informationssäkerhet inte fungerar tillfredsställande utifrån rådande interna och externa behov samt identifierade risker.

Av uppföljningen framgår därtill att utvecklingen av Region Skånes ledningssystem för informationssäkerhet och dataskydd är central för att öka mognadsgraden för Region Skånes informationssäkerhets- och dataskyddsarbete. En utveckling av ledningssystemet syftar bland annat till att förtydliga styrningen och ledningen av arbetet med informationssäkerhet och dataskydd och att tydligare definiera processer samt roller och ansvar. En del i förbättringsarbetet uppges vara att införa ett digitalt systemstöd för att förenkla det operativa arbetet samt att etablera tydligare processer och metoder.

### 3.2.2 Ansvarsfördelning informationssäkerhet

I reglemente för styrelser och nämnder[1] saknas reglering och fördelning av ansvar avseende Region Skånes säkerhetsarbete, inklusive informationssäkerhet. Ansvar för Region Skånes it- och informationssystem framgår inte heller av beslutat reglemente.

Ansvarsfördelningen beskrivs däremot i ett flertal styrande dokument, se bilaga A för detaljer. I det följande beskrivs ansvaret på en mer övergripande nivå.

Regionstyrelsen har det övergripande ansvaret för informationssäkerheten och regiondirektören ska tillse att arbetet kan genomföras ändamålsenligt. Regiondirektören beslutar om informationsägare för informationstillgångar som är gemensamma för Region Skåne.

Enligt regiondirektörens beslut[2] är hälso- och sjukvårdsdirektör informationsägare för ”*Information inom hälso- och sjukvård som rör patienter (personuppgifter inom hälso- och sjukvård) samt regionala och nationella kvalitetsregister där Region Skåne är centralt personuppgiftsansvarig*”.

Digitaliserings- och IT-direktör är informationsägare men även systemägare för ”*Informationstillgångar avseende IT-system, exklusive information i dessa som omfattas av annans informationsägarskap*”.

Region Skåne har en informationssäkerhetschef. Informationssäkerhetschefen tillhör koncernkontorets förvaltning koncernstab kansli, område Informationsstyrning och informationsförvaltning. I enlighet med beskrivning i styrande dokument uppger intervjuade att det finns utsedda informationssäkerhets- och dataskyddssamordnare i förvaltningarna. Däremot framgår av våra intervjuer en bild av att dessa funktioner

[1] Fastställt 2022-12-13, 2020-POL000492, § 11
[2] Beslutat 2018-05-22, Dnr 1800025

saknar tillräckliga förutsättningar att bedriva ett systematiskt informations-säkerhetsarbete inom den verksamhet som de tillhör. Som exempel lyfts att det endast finns en heltidstjänst som informationssäkerhets- och dataskyddssamordnare, samt en deltidstjänst som även omfattar uppdrag som verksamhetsspecialist för avvikelsehanteringssystemet som resurser i informationssäkerhetsarbetet för samtliga verksamheter som lyder under Primärvårdsnämnden. Detsamma gäller för sjukhusstyrelsen Ystad som har två motsvarande roller, dessa har utöver Ystad även ansvar att samordna arbetet inom tre ytterligare sjukhusstyrelser, i Lund, Landskrona och Trelleborg. Uppgifter som tillfaller verksamhetsansvaret i informations-säkerhetsarbetet genomförs därför endast i vissa delar och arbetet uppges vara till största delen reaktivt utifrån frågeställningar och behov och inte planerat i förhållande till aktiviteter som styrande dokument ställer krav på.

Detta bekräftas av dokumentation som vi tagit del av i form av den årliga uppföljningen av Region Skånes informationssäkerhetsarbete som rapporteras till regionstyrelsen. Uppföljningen visar att analysen av de regionala funktionerna för informationssäkerhet mot bakgrund av det som inkommit från förvaltningarnas årsrapporter utgör en tydlig utmaning inom organisationen kopplat till befintliga arbetsprocesser och resurssättning.

Intervjuade beskriver detta som att det saknas en organisation och struktur så att ansvar kan fördelas på en operativ nivå för att ledningssystemet ska få effekt i samtliga verksamheter.

### 3.2.3 Ansvarsfördelning mellan verksamhet och driftsorganisation för informationssystem

Styrande dokument för informationssäkerhet anger att arbetet med informationssystem ska genomföras i enlighet med Region Skånes fastställda förvaltningsmodell, Verksamhetsstyrd styr- och förvaltningsmodell för IT- och MT-system. Modellen beskriver samarbetsformerna för styrning och förvaltning av it- och medicintekniska system där ansvarsfördelning och uppgifter för roller tydliggörs genom ett antal instruktioner och bilagor.

I beskrivningen av modellen framgår att styrningen sker på tre nivåer – strategisk, taktisk och operativ nivå. Den strategiska nivån utgörs av koncernledningen. I modellen framgår att ärenden gällande vårdsystem som eskaleras från styrgruppen på taktisk nivå först ska hanteras i en grupp med förvaltningschefer från hälso- och sjukvården som beredning inför eventuell hantering av koncernledningen. På en övergripande nivå anges följande ansvarsfördelning i arbetet med Region Skånes informationssystem. Verksamheterna ansvarar för att de system som används förvaltas enligt styr- och förvaltningsmodellen. Driftsorganisationen har ansvar för att tillhandahålla system efter verksamhetens behov och säkra dess tillgänglighet och information enligt gällande policys och lagar.

I enlighet med modellen finns förvaltningsgrupper med utsedda representanter. Dels från verksamheterna som nyttjar systemen, dels systemansvariga som tillhör Förvaltning Digitalisering IT och MT. I modellen finns ytterligare roller från verksamheter samt från Digitalisering IT och MT på olika nivåer, vilka bemannas utifrån behov kopplat till omfattningen på systemens användning och dess komplexitet.

### 3.2.4 Riskhantering för informationstillgångar som hanteras i informationssystem

Av *instruktion för tillämpning av riktlinje för informationssäkerhet* framgår att det ska finnas ett systematiskt arbete med riskbedömningar, med hänvisning till flera lagrum. Varje verksamhet ska enligt instruktionerna genomföra och dokumentera analyser avseende vilka risker som kan påverka informationssäkerheten, och utifrån dessa analyser vidta lämpliga skyddsåtgärder. För varje risk som identifieras under riskbedömningen ska ett riskhanteringsbeslut fattas. Informationsägaren har ansvar för informationstillgångar och beslutar om informationshantering inom ramen för befintlig lagstiftning och interna regelverk.

Av både styrande dokument, beskrivningar av aktiviteter som ska genomföras i Region Skånes systemförvaltningsarbete samt i det beslut vi nämnt ovan, fattat av regiondirektören, framgår krav på genomförande av riskanalyser och etablering av lämpliga skyddsåtgärder. I analyserna ska ingå kontroll av att systemen följer interna och juridiska krav. Av regiondirektörens beslut framgår det som ett ansvar för informationsägaren att tillse att arbetet genomförs, dokumenteras samt följs upp för att säkerställa att skyddsåtgärder vidtagits som analyser visat behov av för att skydda informationen.

#### *3.2.4.1 Systemgranskning*

Som en del i metoden för granskningen har ingått att genomföra en systemgranskning av tre system som hanterar patientdata inom hälso- och sjukvården (slutenvården och primärvården).

De system som har ingått i granskningen har varit i drift länge inom Region Skåne, ett av dem i närmare 40 år. I genomförda intervjuer har vi erhållit motstridiga uppgifter om huruvida informationsklassning och riskbedömning har gjorts över tid i enlighet med krav som ställs både i lag och interna styrdokument. Vi har efterfrågat dokumentation från tidigare genomfört arbete men inte erhållit detta. Vi konstaterar att dokumentationen enligt ansvariga är spridd både internt och hos externa leverantörer och det saknas en samlad bild av vilka underlag som finns och var system-dokumentationen har lagrats i syfte att vara tillgänglig över tid.

Intervjuade beskriver att det vid tiden för granskningen pågår ett omfattande arbete med riskhantering av informationssystem. Det arbete som pågår hänvisas till *projektdirektiv U537* där samtliga Region Skånes system ska riskbedömas och beslut därefter ska fattas av informationsägare avseende fortsatt drift. Enligt uppgift är detta ett uppdrag från tidigare regiondirektör men vi har inte erhållit beslut eller underlag som styrker detta.

I intervjuer beskrivs att arbetet är omfattande och väntas ta ytterligare något år innan alla system har arbetats igenom då samtliga, ca 600–700 system, som är i drift ska riskbedömas. Enligt uppgift har en prioritering gjorts utifrån de system som är mest verksamhetskritiska. Samtliga tre system som omfattas av denna granskning tillhör denna kategori.

Arbetet genomförs i projektform och drivs från IT-säkerhetsenheten som är en del av Förvaltning Digitalisering IT och MT. Det finns en utsedd projektledare som har det övergripande ansvaret för projektet och en styrgrupp som resultatet löpande återrapporteras till. I projektgruppen ingår en riskanalysledare, informationssäkerhets-samordnare med kunskap om informationsklassning tillika dataskyddssamordnare samt IT-säkerhetsansvarig. Övrig kompetens i form av IT-säkerhetsansvarig/-specialist eller domänarkitekter inom säkerhet eller medicinsk teknik, allokeras från linjeorganisationen. Vid genomförandet av momenten ställs krav på deltagande från verksamheterna, för att informationshantering och nyttjande av respektive system ska kunna bedömas så tillförlitligt som möjligt.

Vid genomförandet används av Region Skåne fastställd metod och mall för riskhantering av informationssystem. Enligt dokumentet består riskhanteringsprocessen av de tre aktiviteterna informationsklassificiering, riskbedömning och åtgärdsanalys.

Då arbetet med riskhantering nyligen har genomförts för de tre systemen som ingår i granskningen har ingen uppföljning hunnit genomföras avseende om säkerhets-åtgärder har etablerats och åtgärder har inte heller utvärderats. Vi kan se av dokumentationen att ansvar har tilldelats och att det finns en tidsplan för när åtgärder ska vara på plats. För flertalet åtgärder finns däremot även en notering om att det är osäkert om åtgärder kommer att genomföras eller när detta i sådana fall kommer att ske. Detta har i förekommande fall resulterat i att riskvärdet som sattes innan införande av åtgärder kvarstår.

Enligt det underlag vi tagit del av framgår att beslut om driftgodkännande från informationsägaren sker efter att identifierade risker har hanterats och verifierats utifrån, av informationsägaren, beslutade åtgärdsbehov. Beslut om driftsgodkännande utgör en verifiering av att de risker som inte åtgärdats därmed är acceptabla och att systemet uppfyller lagkrav och verksamhetskrav. Vi har fått uppgifter om att processen efter att risker identifierats är i behov av utredning och har eskalerats till styrgruppen. Det har dock inte fattats något beslut som leder denna process framåt.

Vi uppfattar genom dokumentation samt från intervjuer att resultatet av riskhanteringen innebär att informationsägaren inte kan besluta om riskacceptans eller drifts-godkännande då alltför betydande risker kvarstår för att systemet ska bedömas som tillräckligt informationssäkert. Beslut om fortsatt drift skulle därmed strida mot gällande interna krav. Detta trots att systemen har varit samt fortfarande är i drift sedan många år.

Intervjuade beskriver att det även tidigare har funnits en problematik med processen för driftsgodkännande. Detta då samtliga underlag presenteras för informationsägaren samtidigt. Det innebär att beslut om driftsgodkännande fattas utan att informations-ägaren i tidigare skede fått information om de risker som föreligger. Informations-ägaren har därigenom inte beretts möjlighet att kontrollera och säkerställa att säkerhetsåtgärder vidtagits för att minska tidigare identifierade risker. Detta bekräftas av dokumentation vi tagit del av för dessa beslut, där samtliga underlag är daterade med samma datum.

Översiktliga iakttagelser från genomförd systemgranskning

Mot bakgrund av att alltför detaljerad information om risker och sårbarheter kan utgöra risk för Region Skåne, återges i rapporten endast en övergripande bild av resultatet i riskhanteringen. Nedan redovisas de generella iakttagelserna för de system som granskats:

- Två av tre system har bedömts stödja samhällsviktig verksamhet och samtliga tre system stödjer verksamhetskritiska processer.
- Samtliga tre system har erhållit klassificering tillgänglighet 4, riktighet 4 och konfidentialitet 4 (där 4 utgör det högst bedömda skyddsvärdet).
- Inget av systemet är molntjänst utan finns på lokal server eller på server hos extern driftsleverantör.
- Det finns en osäkerhet för flertalet risker kopplat till drift av systemen hos extern leverantör. Protokollen anger att detta ska bedömas i separat riskanalys.
- Systemdokumentation saknas i vissa delar internt hos Region Skåne och finns i alltför hög grad hos externa leverantörer vilket leder till bristande kännedom om integrationer och uppsättning i systemen.

Vi har även gjort vissa specifika iakttagelser för de tre systemen vilka återges översiktligt nedan.

- Systemet inom slutenvård som granskats har ett stort antal identifierade risker som kvarstår med mycket höga värden även efter föreslagna åtgärder. I riskhanteringsprotokollet finns det särskild notering om att lagkrav inte efterlevs vilket innebär att merparten av Region Skånes användare har tilldelats en alltför vid behörighet, på grund av en otillräcklig behovs- och riskanalys. Incidenter i form av dataintrång, av egen personal, sker regelbundet och vid ett fåtal tillfällen har driftsavbrott skett där kontinuitetsplaneringen inte fungerat fullt ut.
- Systemet inom primärvård som granskats har ett antal risker som är identifierade som mycket höga. Åtgärder har föreslagits som för flera av riskerna uppges leda till acceptabel risknivå. Vi konstaterar dock att flertalet åtgärder endast är identifierade men ännu inte etablerade och det framgår av dokumentationen att det inte är beslutat att åtgärder ska genomföras. Ytterligare iakttagelser är att systemet har låga risker kopplade till frågor om åtkomst och behörigheter.
- Det administrativa system som valts ut för granskning är inte ett journalsystem men hanterar personuppgifter som delas till ca 50 andra system i Region Skåne och är därigenom bedömt som prioriterat. Det finns ett antal risker som är identifierade som mycket höga där åtgärder har genomförts eller är identifierade så att risker når en acceptabel nivå. Riskerna handlar bland annat om att det inte i tillräcklig grad är begränsat vilken information som kan registreras i systemet vilket kan föranleda att uppgifter finns om patienter eller anhöriga som inte bör registreras. Det finns även risk för att uppgifter röjs i samband med kommunikation via sms med patienter avseende tidsbokning.

## 3.2.5 Behörighetshantering och loggkontroll

### *3.2.5.1 Behörighetshantering*

Baserat på både dokumentgranskning och muntliga uppgifter framkommer att Region Skåne har behov av att stärka sitt arbete på övergripande nivå inom åtkomsthantering. I nuläget uppges förmågan påverkad av att informationssäkerhetsarbetet är fragmenterat och inte sker sammanhållet vilket innebär att det finns ett gap mellan det organisatoriska arbetet och det tekniska arbetet.

Enligt uppgift skulle det behöva etableras en organisation och mer automatiserad och regelbaserad behörighets- och åtkomsthantering, så kallad Identity and access management (IAM). Detta innebär att det skulle finnas möjlighet att ansluta system till IAM, där behörigheter definieras för respektive system, vilka kan baseras på specifika roller eller en standardanvändare. Detta ställer dock krav på att Region Skåne i samband med detta även tydliggör krav på behovs- och riskanalyser inför tilldelning av behörigheter, så att inte de roller eller regler som den mer automatiserade processen utgår från är alltför generösa.

I intervjuer beskrivs att processer och ansvar för åtkomst och behörighet på region-övergripande nivå är tydliga då det finns styrande och stödjande dokument som reglerar detta. Koncernkontoret har tagit fram *instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter* [3]. Instruktionen anger att behörighet ska baseras på den behovs- och riskanalys som genomförts utifrån verksamhetens uppdrag. Behörigheten ska motsvara det faktiska behovet och ska därmed varken vara för snäv, vilket kan medföra patientsäkerhetsrisker eller för vid, vilket kan innebära att patientens integritet påverkas negativt. I behörighetshanteringen ingår även borttagning av behörigheter. Borttagning ska ske så snart behörigheten inte längre är nödvändig och syftar till att behörigheten ska motsvara medarbetarens faktiska behov.

Ansvaret vilar i hög grad på verksamhetschefer som behöriga beställare av behörigheter vilket även inkluderar förändringar och avslut. Av intervjuer framgår att det saknas tydlighet i vilka behörigheter som ska tilldelas och hur uppföljning av behörigheter sker. Det upplevs generellt saknas en systematisk uppföljning och kontroll av behörigheter, till exempel när en person byter tjänst eller arbetsplats inom Region Skåne. En generell uppfattning bland intervjuade är att det finns brister i genomförande av behovs- och riskanalyser inför tilldelning samt otillräckliga kontroller att behörigheter är aktuella och korrekta.

Det har framförts att behörighetskontrollen skiljer sig åt mellan olika system. Respektive systemansvarig ansvarar för att det finns rutiner för hur tilldelning, förändring och borttagning av behörigheter ska gå till utifrån de förutsättningar som systemstödet har. Vi har i granskningen efterfrågat om ansvarsfördelning avseende behörighetshanteringen för de tre system som ingår i granskningen och de svar vi fått bekräftar att ansvar för beställning samt även tilldelning, förändring och avslut åligger

[3] Beslutat av hälso- och sjukvårdsdirektör 2019-03-08 dnr: 1800025

respektive verksamhet. Vi uppfattar att beställningsförfarandet sker på olika sätt och att det inte finns någon fastställd gemensam rutin eller riktlinje över hur detta ska gå till.

Som vi beskrivit i avsnitt 3.2.4.1 så framgår av riskhanteringsprotokollet att nuvarande behörighetshantering för användare inom slutenvården är i strid med 4 kap. 2 § och 6 kap. 7 § patientdatalagen och 4 kap. 2 2 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Detta beror på att Region Skåne inte har begränsat behörigheterna till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Detta innebär att merparten av Region Skånes användare har tilldelats en alltför vid behörighet i journalsystemet inom slutenvården, på grund av en otillräcklig behovs- och riskanalys. I nuläget saknas därtill krav på tvåfaktorautentisering (med SITHS-kort alternativt annan identifieringslösning som andra faktor utöver användarnamn och lösenord) vid inloggning till journalsystemet inom slutenvården.

#### *3.2.5.2 Loggkontroll*

I *instruktion för åtgärder vid misstanke om dataintrång avseende patientuppgifter*[4] beskrivs att det är verksamhetschefens ansvar att anställdas åtkomst till patientuppgifter följs upp, vilket även omfattar kontroll av åtkomst till andra vårdgivares patientuppgifter. Uppföljningen sker via loggkontroller enligt särskilda instruktioner.

Utöver riktade loggkontroller vid misstanke ska det även regelbundet genomföras systematiska stickprovskontroller. Enligt *instruktioner om loggkontroll för granskning av åtkomst till patientuppgifter*[5] ska stickprovskontrollerna ske månadsvis på cirka 10 % av personalen under en total tid av minst 24 timmar. Samtliga kontroller som genomförs ska dokumenteras övergripande i avsett formulär som finns tillgängligt på Region Skånes intranät.

I intervjuer beskrivs att det i en del verksamheter inte sker systematiska loggkontroller enligt rutin. Uppdraget beskrivs vara krävande både tids- och systemkompetens-mässigt och uppdraget upplevs inte alltid motsvara de resurser som finns till förfogande för att göra regelbundna loggkontroller.

Av den årliga uppföljningen av Region Skånes informationssäkerhetsarbete framgår att antal incidenter har minskat jämfört med tidigare år. Uppföljningen visar dock att det skett ett stort antal personuppgiftsincidenter och att majoriteten av dessa är konfidentialitetsbrott, exempelvis genom att en medarbetare begått dataintrång eller att information inte skyddats på rätt sätt vid överföring eller lagring.

### 3.2.6 Utbildning för att etablera riskmedvetenhet om informationssäkerhet

Region Skåne erbjuder vid nyanställning en utbildning i informationssäkerhet som heter ”Säker informationshantering”. Utbildningen är obligatorisk och det är anställande chef som ska tillse att nyanställda genomför utbildningen. Chefen erhåller uppföljning på vilka som har genomfört utbildningen. I intervjuer beskrivs att deltagandet i utbildningen är bristfällig och endast en mindre del av Region Skånes medarbetare har genomfört

[4] Beslutad av informationssäkerhetschef 2021-10-25 dnr 2021-O002308
[5] Beslutad av hälso- och sjukvårdsdirektör 2019-11-12 dnr: 1800025

den, trots att den är obligatorisk. Muntliga uppgifter vid intervju, då intervjupersonen kontrollerade genomförandegrad, var att inte ens hälften av Region Skånes anställda genomfört utbildningen vid den tidpunkten. Att höja kompetensen kring informations-säkerhet för medarbetare beskrivs ha varit underprioriterat i verksamheterna och det görs därför kommunikationsinsatser från koncernkontoret för att öka genomförandegraden.

It-säkerhetsenheten inom Förvaltning Digitalisering IT och MT har på eget initiativ tagit fram en it-säkerhetsutbildning som ska göras tillgänglig för samtliga medarbetare. Utbildningen är för närvarande under granskning för godkännande på HR på koncernkontoret. Utbildningen kommer inte vara obligatorisk, men detta vore enligt intervjuade önskvärt då behovet av ytterligare kunskap bedöms finnas.

### 3.2.7 Bedömning

**Vi bedömer att medborgarens integritet inte har säkerställts då patientinformation i journalsystem endast delvis är skyddade mot obehöriga.**

Vi bedömer att regionfullmäktige och regionstyrelsen genom beslut har fastställt styrande dokument som reglerar ansvar för informationssäkerhet och krav på hur arbetet ska bedrivas. Trots detta kan vi konstatera att det saknas ett systematiskt och riskbaserat informationssäkerhetsarbete inom samtliga revisionsobjekt då arbetet inte genomförs i nivå med de krav som ställs i lag och interna styrdokument. Vi noterar att reglemente för styrelser och nämnder saknar reglering av hur ansvaret för informationssäkerhet och informationssystem är fördelat inom Region Skåne. Ansvar är dock dokumenterat i ett flertal styrande dokument som reglerar Region Skånes arbete med säkerhet och informationssäkerhet samt i förvaltningsmodell för informationssystem och medicinsktekniska system.

Vi bedömer att nuvarande organisation och resurser inte är anpassade så att det på regionövergripande nivå eller i respektive verksamhet finns förutsättningar att genomföra arbetet i enlighet med de krav på informationssäkerhet som Region Skåne ställer genom sitt ledningssystem. Vi ser därtill att det finns behov av att stärka strukturer och processer för arbetet så att ledningssystemet ska bli mer effektivt och det operativa arbetet genomföras systematiskt och riskbaserat.

Vi baserar vår bedömning bland annat på att det finns betydande informations-säkerhetsrisker i de system som i huvudsak hanterar patientuppgifter inom hälso- och sjukvården där skydd av patientinformationen inte i tillräcklig grad har säkerställts vare sig organisatorisk eller tekniskt. Vi kan därigenom inte utesluta att det finns risk för att sjukhusstyrelsen Ystad idag inte uppfyller patientdatalagens krav om att behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Detta är en bedömning som avser samtliga vårdgivare inom slutenvård som nyttjar journalsystemet. Vår bedömning är att system som nyttjas inom verksamheter under primärvårdsnämnden, mot bakgrund av den dokumentation vi tagit del av, i högre grad uppfyller lagkrav och kravnivåer för informationssäkerhet även om det finns ett antal säkerhetsåtgärder som behöver etableras i syfte att säkerställa att patientuppgifter är skyddade mot obehöriga.

Vi konstaterar att informationsägare inte har fullföljt sitt ansvar i enlighet med styrande dokument då informationssystemen varit i drift under lång tid utan att de aktiviteter som det ställs krav på för att säkerställa en tillräcklig säkerhet har genomförts. Det är bland annat känt att det finns alltför generösa behörigheter samt att krav om tvåfaktorinloggning till system med känsliga uppgifter inte efterlevs.

Vi konstaterar även att systemägare och systemansvariga inte har fullföljt sitt ansvar i enlighet med styrande dokument då informationssystemen varit i drift under lång tid utan att de aktiviteter som det ställs krav på för att säkerställa en tillräcklig säkerhet har genomförts. Systemägare och systemansvariga svarar organisatoriskt under nämnden för operativ regiongemensam verksamhet, vilket leder till vår bedömning att nämnden brustit i sitt ansvar att säkerställa att arbetet genomförs i enlighet med de krav som ställs i interna styrdokument och det ansvar som regleras av Region Skånes Verksamhetsstyrda styr- och förvaltningsmodell.

Det finns därtill en bristande uppföljning och kontroll av tilldelade behörigheter så att dessa är aktuella över tid, exempelvis vid byte av arbetsställe eller avslut av tjänst. De loggkontroller som genomförs är enligt vår mening inte tillräckliga för att säkerställa att medborgares integritet är säkerställd genom att patientinformation är skyddad mot obehöriga då kontrollmoment som det ställs krav om inte är tillräckligt omfattande för att identifiera avvikelser och därtill inte genomförs enligt fastställd rutin.

**Vi bedömer att Region Skåne inte har säkerställt att det finns ändamålsenlig utbildning av berörd personal kring informationssäkerhet som exempelvis lagring och hantering av känsliga uppgifter om enskilda patienter.**

Vår bedömning gäller samtliga revisionsobjekt. Det finns krav på obligatoriska utbildningar men deltagandet är alltför lågt i förhållande till det stora antal användare som har tillgång till känsliga patientuppgifter eller annan skyddsvärd information. Region Skåne har inte heller kompletterande utbildning med obligatoriska moment särskilt riktade till personal inom hälso- och sjukvård avseende hantering av patientdata utifrån gällande lagar och regelverk.

## 3.3 IT-säkerhet

Inom Förvaltningen Digitalisering IT och MT finns en IT-säkerhetsenhet. På enheten finns exempelvis rollerna it-säkerhetschef, it-säkerhetsansvarig och it-säkerhetsspecialist.

Region Skånes styrande dokument för informationssäkerhet ställer krav på att it-säkerhetsåtgärder ska utgå från ISO-standarden 27002. Intervjuade uppger dock att kännedom om de styrande dokumenten är bristande och att informations-säkerhetsarbetet i verksamheterna därigenom inte genomförs i enlighet krav i styrande dokument. Det innebär att det i nuläget saknas underlag för vilka it-säkerhetsåtgärder som det finns behov av för att skydda Region Skånes informationstillgångar. Detta då informationsägaren eller representant för denna inte kommunicerat dessa behov så att systemägaren fått kännedom om behov och inom sitt ansvar etablerat de åtgärder som är nödvändiga. Det pågående arbetet med riskhantering för Region Skånes system som beskrivits tidigare i rapporten lyfts som exempel på att verksamheterna inte upprätthåller sitt ansvar inom informationssäkerhet där Förvaltning Digitalisering IT och MT tagit ansvar för att genomföra dessa aktiviteter, vilket går utöver deras ordinarie ansvar. Ytterligare exempel som lyfts är vid nya systeminföranden, då it-säkerhetsenheten får inleda arbetet med att göra informationsklassningar då detta inte har genomförts inom respektive verksamhet. Detta så att det ska finnas dokumenterade underlag där risker och sårbarheter identifierats och därefter kan åtgärdas genom korrekta tekniska säkerhetsåtgärder.

It-säkerhetsansvarig har deltagit i vissa av dessa moment och tagit del av risker och behov. Som vi beskrivit tidigare har dock arbetet nyligen avslutats och vi uppfattar av intervjuade att åtgärder i praktiken inte har etablerats vid tid för granskningen mot bakgrund av att beslut måste fattas av informationsägare och förmedlas till systemägaren. Sådana åtgärder som systemansvariga själva har mandat att besluta om inom budget för system samt sådana åtgärder där lösningar är tillgängliga internt eller via externa leverantörer uppfattar vi delvis har vidtagits.

Förvaltning Digitalisering IT och MT ansvarar för informationstillgångar i form av system och andra it-komponenter. Region Skånes Instruktion för informationsklassning reglerar att informationstillgångar i form av programvara, system, datorer och utrustning som krävs för hantering av informationen ska klassificeras och riskbedömas. Vi uppfattar dock av intervjuade att detta inte har genomförts.

Däremot framgår från intervjuer att it-säkerhetsenheten regelbundet genomför ett risk- och sårbarhetsanalyser i syfte att identifiera behov av åtgärder för att stärka it-säkerheten samt att externa leverantörer inkluderas i riskanalysarbetet för rådgivning om säkerhetsnivåer. Resultatet av arbetet presenteras i en ”säkerhets-roadmap” för prioriterade åtgärder. Vi har tagit del av denna och noterar att ett flertal åtgärder är införda och en stor del är planerade att genomföras under 2023 och 2024. Intervjuade beskriver att planering och prioritering av åtgärder följer den ordinarie budgetprocessen och vissa åtgärder har identifierats och kommer att ingå i budget och planering för 2025.

Inom IT-säkerhetsenheten uppges det strategiska och operativa it-säkerhetsarbetet baseras på enskilda funktioners kompetens, råd och stöd från externa leverantörer, omvärldsbevakning samt ”best practice”. Den samlade bilden av genomförda intervjuer är att Digitalisering IT och MT har arbetat systematiskt för att etablera it-säkerhet för it-komponenter som de ansvarar för, exempelvis nätverk, serverhallar, plattform mm i syfte att skydda Region Skånes informationstillgångar.

Som en del i uppföljning av implementerade säkerhetslösningar har it-säkerhetsenheten genomfört penetrationstester för att utvärdera nuvarande säkerhet i syfte att hitta sårbarheter och bedöma hur effektiva nuvarande skydd är mot externa hot. Risker och åtgärder delges löpande övriga enheter inom Digitalisering IT och MT men enligt uppgift kan arbetet struktureras ytterligare i syfte att sprida kunskap och medvetenhet om nuvarande säkerhetsnivåer i förhållande till aktuella hot och risker.

### 3.3.1 Bedömning

**Vår bedömning är att Region Skåne delvis har ett tillräckligt skydd för sina databaser och system, inklusive molntjänster mot utomstående hot.**

Vi konstaterar att driftsorganisationen inom Nämnden för operativ regiongemensam verksamhet har etablerat ett antal säkerhetsåtgärder i syfte att skydda Region Skånes it-miljö, system och informationstillgångar. Analyser har gjorts i syfte att prioritera ytterligare införanden.

Vi bedömer däremot att det saknas en samlad bild avseende vilka skyddsbehov som finns för Region Skånes informationstillgångar. Informationsklassning och riskbedömning har inte genomförts i tillräcklig omfattning, vare sig för informationssystem eller för it-komponenter i it-infrastrukturen, vilket medför att tekniska säkerhetsåtgärder inte i nuläget har etablerats i förhållande till det skyddsvärde som informationsklassning med tillhörande risk- och konsekvensanalyser visat behov av. Detta är en grundläggande aktivitet i ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med de beslutade standarder som Region Skåne fastställt att arbetet ska utgå från.

Utifrån Region Skånes krav på efterlevnad av lag om informationssäkerhet för samhällsviktiga och digitala tjänster är det av vikt att informationssäkerhetsarbetet bedrivs med en högre grad av systematik och att det är riskbaserat. I nuläget ser vi en risk med att arbetet med informationssystem och it inte är en integrerad del i ett systematiskt informationssäkerhetsarbete.

## 3.4 Avvikelser och incidenthantering

*I Instruktion för tillämpning av riktlinjer för informationssäkerhet* framgår att informationssäkerhetshändelser ska hanteras enligt fastställda processer. Region Skåne har utöver detta upprättat instruktioner för hantering av informationssäkerhetshändelser- och incidenter. Instruktionerna har upprättats mot bakgrund av att det i etablerade processer saknas metoder för klassificering av incidenter för att dessa ska kunna prioriteras korrekt.

Instruktionerna omfattar vilka myndigheter som utgör tillsynsmyndigheter vid rapportering av en incident, samt hur anmälan till Polismyndigheten ska göras vid misstanke om dataintrång. Intervjuade anger att anmälan till tillsynsmyndighet i enlighet med NIS-direktivet utförs av tjänstepersoner inom Förvaltning Digitalisering IT och MT.

Vid genomförande av förebyggande underhåll, så som exempelvis uppgradering av informationssystem eller plattform, är det systemansvarig som innehar det övergripande ansvaret för att detta sker med så liten påverkan som möjligt på verksamheten. I arbetet ska verksamhetsansvarig konsulteras och systemspecialisten ansvarar för genomförandet. Vid intervjuer uppges att det finns ett väl fungerande samarbete där systemansvarig kopplar på systemförvaltningsgruppen i det arbete som ska genomföras. Under granskningstillfället genomfördes ett planerat driftstopp på ett av de system som omfattas av granskningen där övergång till reservrutiner var en del. Enligt uppgift fungerade etablerade reservrutiner och uppgraderingen kunde genomföras utan påverkan på verksamhet eller informationstillgångar.

Intervjuade uppger att Region Skåne har utsedda roller för incidenthantering, vilka följer etablerad standard för it-processer. I den SOC-tjänst (Security Operations Center) som Region Skåne upphandlat, som har i uppdrag att övervaka och agera på it-säkerhetshändelser dygnet runt, finns en utsedd incident manager. It-chef i beredskap ingår i den eskaleringskedja som beslutats i händelse av allvarlig störning eller incidenter.

Av den årliga rapporteringen av Region Skånes samlade informationssäkerhetsarbete framgår att hantering av informationssäkerhetsincidenter är i behov av utveckling. En samlad uppfattning från genomförda intervjuer är att upprättade instruktioner inte är etablerade i organisationen och att det saknas ett regionövergripande och enhetligt sätt att anmäla och hantera inträffade incidenter. Därtill framkommer att nyckelpersoner i form av säkerhetsansvariga, informationssäkerhetschef inte alltid får kännedom om inträffade incidenter.

Detta bekräftas även av de riskhanteringsprotokoll som vi tagit del av. Där framgår att incidenter tappats bort och att rapportering till tillsynsmyndigheter inom fastställd tidsram inte alltid genomförs. Bland annat anges att incidenter rapporteras på många olika sätt. Bland de sätt som beskrivs nämns bland annat ärendehanteringssystem för it-relaterade frågor samt Region Skånes avvikelsehanteringssystem, funktionsbrevlåda samt genom direktkontakt med olika funktioner. Därtill framgår att flödet när en incident har anmälts behöver utvärderas och förbättras.

Uppföljning av informationssäkerhetsincidenter ska ske enligt respektive organisations rutin och omfatta kartläggning av orsak och förlopp av enskilda incidenter. En regelbunden uppföljning av samtliga incidenter ska göras i syfte att urskilja eventuella mönster och systematiska felkällor som ett sätt att identifiera eventuella förbättringsåtgärder. De intervjuer vi genomfört ger bilden att det till viss del genomförs ett uppföljningsarbete av inträffade incidenter i samband med informationssäkerhetsrådets[6] möten. Inträffade incidenter utgör även en del av det strategiska it-säkerhetsarbete som bedrivs inom säkerhetsenheten. Dock saknas dokumenterade underlag som styrker dessa iakttagelser.

### 3.4.1 Bedömning

**Vi bedömer att avvikelser och incidenter i form av exempelvis driftavbrott och säkerhetsintrång på it-system delvis hanteras i enlighet med gällande lagstiftning och regelverk.**

Rutiner för incidenthantering finns men vi bedömer att dessa saknar en tydlig beskrivning av ansvar, processer samt eskaleringsvägar i händelse av olika incidenttyper.

Därtill konstaterar vi att rutinerna inte är tillräckligt etablerade vilket leder till att incidenter i nuläget hanteras på flera olika sätt. Det får i sin tur konsekvensen att rapporteringsskyldigheten inte alltid efterlevs. Därtill försvåras möjligheten att ha översikt över inträffade incidenter så att dessa kan analyseras och vara en viktig informationskälla för att identifiera förbättringsbehov. Bristen av detta stärks ytterligare då övergripande ansvariga, exempelvis informationssäkerhetschef eller säkerhetsansvariga inom respektive verksamhet, inte alltid får information och kännedom om inträffade incidenter.

[6] Informationssäkerhetsrådet har till uppgift att stödja, samordna och följa upp Region Skånes informationssäkerhetsarbete på en övergripande nivå. Utöver informationssäkerhetschefen ska rådet bestå av informationssäkerhetssamordnare från respektive förvaltning.

# 4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om arbetet med it- och informationssäkerhet inom Region Skåne bedrivs på ett systematiskt och ändamålsenligt sätt.

**Vår samlade bedömning utifrån granskningens syfte är att arbetet inte är systematiskt och ändamålsenligt och att det finns risk att patientdata inte skyddas mot obehöriga.**

Region Skåne har inte säkerställt medborgarens integritet då patientinformation i journalsystem endast delvis är skyddade mot obehöriga. Det informationssäkerhets-arbete som genomförts är inte i nivå med de krav som ställs i lag och i interna styrdokument.

Region Skåne har delvis ett tillräckligt skydd för sina databaser och system, inklusive molntjänster, mot externa hot där säkerhetsåtgärder etablerats och där analyser genomförts för ytterligare införanden. Däremot saknas en samlad bild avseende vilka skyddsbehov som finns för Region Skånes informationstillgångar då informationsklassning och riskbedömning inte genomförts i tillräcklig omfattning.

Rutiner för incidenthantering finns men de saknar en tydlig beskrivning av ansvar, processer samt eskaleringsvägar i händelse av olika incidenttyper. Avvikelser och incidenter hanteras därför endast delvis i enlighet med gällande lagstiftning och regelverk.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Stärka den interna kontrollen av samtliga nämnder och styrelser avseende efterlevnad av de styrande dokument som utgör Region Skånes ledningssystem för informationssäkerhet.
- Utvärdera om nuvarande resurser för informationssäkerhetsarbetet motsvarar omfattning av Region Skånes krav på informationssäkerhet mot bakgrund av lagkrav och interna beslut.
- Genom regelbunden uppföljning tillse att pågående arbete med riskhantering av Region Skånes informationssystem fortgår och slutförs, samt att säkerhetsåtgärder vidtas som analyser visat behov av i syfte att skydda patientinformation och andra skyddsvärda uppgifter.
- Säkerställa att Region Skånes process för åtkomst- och behörighetshantering stärks vad gäller tilldelning, förändring och avslut av behörigheter så att endast behöriga har tillgång till information. Därutöver rekommenderas styrelsen att säkerställa att tilldelning sker efter genomförd behovs- och riskanalys samt sker i enlighet med lagkrav.
- Utreda om det finns möjlighet att centralisera logghanteringen för att avlasta verksamheterna samt kvalitetssäkra och stärka Region Skånes förmåga att genomföra kontroller i tillräcklig omfattning.

- Säkerställa att Region Skånes medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att nuvarande rutiner för incidenthantering kompletteras med tydlig beskrivning avseende ansvar, processer och eskaleringsvägar i händelse av olika incidenttyper samt att rutinerna etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov på regionövergripande nivå.

Utifrån resultatet av vår granskning rekommenderar vi Sjukhusstyrelsen Ystad:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som styrelsen ansvarar för.
- Följa upp att de tekniska säkerhetsåtgärder som identifierats utifrån skyddsvärde på informationstillgångar etableras.
- Säkerställa att behörigheter hanteras utifrån lagkrav samt att uppföljning och kontroll av tilldelade behörighet sker för att säkerställa dess aktualitet.
- Säkerställa att loggkontroller genomförs i enlighet med upprättade rutiner så att patientinformation skyddas mot obehöriga och att medborgares integritet därmed säkerställs i högre grad.
- Säkerställa att tvåfaktorautentisering införs på de system som hanterar känsliga uppgifter i enlighet med krav.
- Säkerställa att medarbetare genomför obligatorisk utbildning som finns tillgänglig samt följa upp deltagarantalet.
- Utvärdera behov av kompletterade utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att rutiner för incidenthantering etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov.

Utifrån resultatet av vår granskning rekommenderar vi primärvårdsnämnden:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.
- Följa upp att de tekniska säkerhetsåtgärder som identifierats utifrån skyddsvärde på informationstillgångar etableras.
- Säkerställa att behörigheter hanteras utifrån lagkrav samt att uppföljning och kontroll av tilldelade behörighet sker för att säkerställa dess aktualitet.
- Säkerställa att loggkontroller genomförs i enlighet med upprättade rutiner så att patientinformation skyddas mot obehöriga och att medborgares integritet därmed säkerställs.
- Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
- Säkerställa att rutiner för incidenthantering etableras i organisationen.
- Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov.

Utifrån resultatet av vår granskning rekommenderar vi nämnden för operativ regiongemensam verksamhet:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.
- Säkerställa att tekniska säkerhetsåtgärder vidtas utifrån identifierat skyddsvärde hos egna informationstillgångar men även övriga styrelser och nämnders identifierade behov i informationsklassning och riskbedömning.
- Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
- Säkerställa att rutiner för incidenthantering etableras i organisationen.
- Säkerställa att inträffade incidenter dokumenteras, analyseras och utgör underlag för att identifiera förbättringsbehov för att stärka it-säkerheten.

**Region Skåne**
Granskning av informations- och it-säkerhet med fokus patientdata

2023-11-21

Datum som ovan

KPMG AB

Jenny Thörn
*Verksamhetsrevisor*

Ida Larsson
*Verksamhetsrevisor*

Simon Homander
*Verksamhetsrevisor*

Veronica Hedlund Lundgren
*Certifierad kommunal revisor*

# 5 Bilaga 1 – Sammanställning av dokumenterad ansvarsfördelning

| Styrande dokument | Beskrivning |
|---|---|
| Säkerhetspolicy | Beskriver säkerhets- och verksamhetsansvaret på alla nivåer och inom alla verksamhetsprocesser. Det ska finnas styrande dokument som reglerar hur säkerhetsarbetet ska bedrivas och hur ansvar fördelas. |
| Säkerhetsstrategi | Beskriver att ansvaret för att avsätta tillräckliga resurser samt att löpande stämma av tillämpningen följer linjeansvaret. Stödjande i arbetet är region- och förvaltningsövergripande säkerhetsfunktioner. Regionövergripande säkerhetsfunktion är samordnande och utvecklande. |
| Riktlinjer för informationssäkerhet | Regionstyrelsen har det övergripande ansvaret för informationssäkerhet i Region Skåne och ska minst årligen informeras om status för informationssäkerhetsarbetet och besluta om övergripande handlingsplan och kortsiktiga mål för arbetet.<br>Regiondirektören ansvarar för att informationssäkerhetsarbetet bedrivs effektivt så att informationssäkerhetsmålen kan uppnås. |
| Riktlinjer för informationssäkerhet | Informationssäkerhetschef ansvarar för att leda, utveckla, samordna och övergripande följa upp informationssäkerhetsarbetet inom Region Skåne.<br>I ansvaret ingår att förvalta riktlinjen för informationssäkerhet, regionövergripande instruktioner och anvisningar samt den övergripande handlingsplanen och målen för informationssäkerhet. |

| | |
|---|---|
| Instruktion för tillämpning av riktlinjer för informationssäkerhet | Inom respektive förvaltning ska finnas en organisation som hanterar frågor om informationssäkerhet inklusive dataskydd.<br><br>Förvaltningen ska avsätta tillräckligt med resurser för att arbetet ska kunna bedrivas effektivt. Storleken på organisationen avgörs utifrån förvaltningens storlek samt mängden och känsligheten i den information som hanteras.<br><br>Vidare framgår att det är av vikt att organisationen för informationssäkerhet har koppling till ledningen i förvaltningen för effektiv rapportering och eventuella beslut om åtgärder. |
| Verksamhetsstyrd styr- och förvaltningsmodell för informationssystem och medicinsktekniska system | Koncernledning utgör strategisk nivå.<br><br>Ärende gällande vårdsystem som eskaleras från styrgruppen på taktisk nivå ska först hanteras i gruppen med förvaltningschefer Hälso- och sjukvård inför Koncernledningen. |