Region Skånes revisorer

Fredrik Ljunggren
Certifierad kommunal revisor
fredrik.ljunggren@skane.se

MISSIV
Datum 2023-12-14
Dnr 2023-RG000032

Regionstyrelsen
Sjukhusstyrelse Ystad
Primärvårdsnämnden
Nämnden för operativ
regiongemensam verksamhet

Granskning av Informations- och IT-säkerhet – fokus patientdata - Rapport nr 7 – 2023

Den samlade bedömningen 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 patient-information i journalsystem endast delvis är skyddade mot obehöriga. Det informationssäkerhetsarbete 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. Däremot saknas en samlad bild avseende vilka skyddsbehov som finns för Region Skånes informations-tillgångar 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.

I bilaga till detta missiv lämnar vi rekommendationer till regionstyrelsen, sjukhusstyrelse Ystad, primärvårdsnämnden och nämnden för regiongemensam operativ verksamhet. I bilaga anges också instruktioner för yttrande samt svarsformulär.

Revisorskollegiet behandlade rapporten vid sammanträdet 2023-12-14 och beslutade att översända missiv och rapport för yttrande till ovan berörda nämnder/styrelser. Yttranden med uppgifter om verkställda och planerade åtgärder ska lämnas senast 2024-03-28.

För revisorskollegiet

Peter J Olsson
Ordförande

George Smidlund
Revisionsdirektör

Revisorernas rekommendationer

Rekommendationer till regionstyrelsen:

- 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.

Rekommendation till sjukhusstyrelse 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.

Rekommendationer till 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.

Rekommendationer till nämnden för operativ regiongemensam verksamhet:

- Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informations-tillgångar 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.

Anvisningar för yttrande

- Svaret ska innehålla uppgifter om vilka åtgärder som vidtagits eller planeras vidtas utifrån revisorernas rekommendationer.
- Det ska finnas en tydlig koppling mellan de rekommendationer som revisorerna lämnat och de åtgärder som beskrivs i svaret.
- Svaret bör så långt det är möjligt innehålla tidsangivelser för när åtgärderna genomförs.
- Svaret bör så långt det är möjligt innehålla beskrivning hur åtgärderna genomförs.
- Svaret bör så långt det är möjligt beskriva vilken eller vilka funktioner inom förvaltningen eller sjukhuset som fått i uppdrag att arbeta med åtgärderna.
- Om styrelsen/nämnden inte planerar att vida några åtgärder, motivera varför.
- Om styrelsen/nämnden inte kan svara på utsatt tid, kontakta revisionskontoret.

Nedan bifogas formulär som kan användas för svar på revisorernas rekommendationer. Syftet med formuläret är att underlätta kommunikationen och därmed tydliggöra vilka åtgärder styrelsen och nämnden vidtagit eller planerar att vidta.

Svarsformulär för regionstyrelsen

Stärka den interna kontrollen av samtliga nämnder och styrelser avseende efterlevnad av de styrande dokument som utgör Region Skånes ledningssystem för informationssäkerhet.
Regionstyrelsens svar:
Utvärdera om nuvarande resurser för informationssäkerhetsarbetet motsvarar omfattning av Region Skånes krav på informationssäkerhet mot bakgrund av lagkrav och interna beslut.
Regionstyrelsens svar:
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.
Regionstyrelsens svar:
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.
Regionstyrelsens svar:
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.
Regionstyrelsens svar:

Säkerställa att Region Skånes medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
Regionstyrelsens svar:
Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
Regionstyrelsens svar:
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.
Regionstyrelsens svar:
Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov på regionövergripande nivå.
Regionstyrelsens svar:
Övriga kommentarer:
Regionstyrelsens svar:

Svarsformulär för sjukhusstyrelse Ystad:

Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som styrelsen ansvarar för.
Sjukhusstyrelse Ystads svar:
Följa upp att de tekniska säkerhetsåtgärder som identifierats utifrån skyddsvärde på informationstillgångar etableras.
Sjukhusstyrelse Ystads svar:
Säkerställa att behörigheter hanteras utifrån lagkrav samt att uppföljning och kontroll av tilldelade behörighet sker för att säkerställa dess aktualitet.
Sjukhusstyrelse Ystads svar:
Säkerställa att loggkontroller genomförs i enlighet med upprättade rutiner så att patientinformation skyddas mot obehöriga och att medborgares integritet därmed säkerställs i högre grad.
Sjukhusstyrelse Ystads svar:
Säkerställa att tvåfaktorautentisering införs på de system som hanterar känsliga uppgifter i enlighet med krav.
Sjukhusstyrelse Ystads svar:

Säkerställa att medarbetare genomför obligatorisk utbildning som finns tillgänglig samt följa upp deltagarantalet.
Sjukhusstyrelse Ystads svar:
Utvärdera behov av kompletterade utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
Sjukhusstyrelse Ystads svar:
Säkerställa att rutiner för incidenthantering etableras i organisationen.
Sjukhusstyrelse Ystads svar:
Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov.
Sjukhusstyrelse Ystads svar:
Övriga kommentarer:
Sjukhusstyrelse Ystads svar:

Svarsformulär för primärvårdsnämnden:

Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.
Primärvårdsnämndens svar:
Följa upp att de tekniska säkerhetsåtgärder som identifierats utifrån skyddsvärde på informationstillgångar etableras.
Primärvårdsnämndens svar:
Säkerställa att behörigheter hanteras utifrån lagkrav samt att uppföljning och kontroll av tilldelade behörighet sker för att säkerställa dess aktualitet.
Primärvårdsnämndens svar:
Säkerställa att loggkontroller genomförs i enlighet med upprättade rutiner så att patientinformation skyddas mot obehöriga och att medborgares integritet därmed säkerställs.
Primärvårdsnämndens svar:
Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
Primärvårdsnämndens svar:

Utvärdera behov av kompletterande utbildning för personal som hanterar känsliga uppgifter inom hälso- och sjukvården.
Primärvårdsnämndens svar:
Säkerställa att rutiner för incidenthantering etableras i organisationen.
Primärvårdsnämndens svar:
Säkerställa att inträffade incidenter analyseras och utgör underlag för att identifiera förbättringsbehov.
Primärvårdsnämndens svar:
Övriga kommentarer:
Primärvårdsnämndens svar:

Svarsformulär för NORV:

Säkerställa att informationsklassning och riskbedömning sker i enlighet med interna styrdokument samt lagkrav för de informationstillgångar som nämnden ansvarar för.
NORVs svar:
Säkerställa att tekniska säkerhetsåtgärder vidtas utifrån identifierat skyddsvärde hos egna informationstillgångar men även övriga styrelser och nämnders identifierade behov i informationsklassning och riskbedömning.
NORVs svar:
Säkerställa att medarbetare genomför de obligatoriska utbildningarna som finns tillgängliga samt följa upp deltagarantalet.
NORVs svar:
Säkerställa att rutiner för incidenthantering etableras i organisationen.
NORVs svar:

Säkerställa att inträffade incidenter dokumenteras, analyseras och utgör underlag för att identifiera förbättringsbehov för att stärka IT-säkerheten.
NORVs svar:
Övriga kommentarer:
NORVs svar: