Landstingsstyrelsen

Yttrande över landstingsrevisorernas projektrapport nr 02/2014, IT-säkerhet i nätverksansluten medicinteknisk utrustning

Föredragande landstingsråd: Daniel Forslund

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp I har lämnat projektrapport 02/2014, IT-säkerhet i nätverksansluten medicinteknisk utrustning för yttrande.

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att lämna yttrande över landstingsrevisorernas projektrapport 02/2014, IT-säkerhet i nätverksansluten medicinteknisk utrustning, enligt landstingsdirektörens tjänsteutlåtande.

Landstingsrådsberedningens motivering

Landstingsrevisorerna spelar en viktig roll i att granska verksamheterna, påtala brister och föreslå åtgärder. I rapporten om IT-säkerhet i nätverksansluten medicinskteknisk utrustning påtalar revisorerna ett antal brister. De rekommenderar att styrningen och kontroller stärks och samordnas på en landstingsövergripande nivå, dels för att uppnå en effektivare hantering inom landstinget, dels för att incidenter och brådskande ärenden som rör medicinskteknisk utrustning ska tas om hand på ett koordinerat och med hög prioritet.

Inom förvaltningen pågår ett arbeta med att skapa förutsättningar för tydlig styrning och struktur för IT inom landstinget. Arbete pågår även med att utveckla och breddinföra ett övergripande ledningssystem för informationssäkerhet. Arbetet med att inarbeta revisorernas rekommendationer i dessa uppdrag har påbörjats.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 10 november 2014
Landstingsrevisorernas projektrapport nr 02/2014, IT-säkerhet i nätverksansluten medicinskteknisk utrustning

Torbjörn Rosdahl

Daniel Forslund

Carl Rydingstam

Landstingsstyrelsens förvaltning
Biträdande förvaltningschef

TJÄNSTEUTLÅTANDE
2014-11-10

LS 1409-1050

Handläggare:
Vesna Lucassi

Landstingsstyrelsen

Ankom
Stockholms läns landsting
2014 -11- 18
Dnr LS 1409-1050
Rokel I

Yttrande över landstingsrevisorernas projektrapport nr 02/2014, IT-säkerhet i nätverksansluten medicinteknisk utrustning

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp I har lämnat projektrapport 02/2014, IT-säkerhet i nätverksansluten medicinteknisk utrustning för yttrande.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 10 november 2014
Landstingsrevisorernas projektrapport nr 02/2014, IT-säkerhet i nätverksansluten medicinskteknisk utrustning

Förslag till beslut

Landstingsstyrelsen föreslås besluta

att lämna yttrande över landstingsrevisorernas projektrapport 02/2014, IT-säkerhet i nätverksansluten medicinteknisk utrustning, enligt landstingsdirektörens tjänsteutlåtande.

Förvaltningens förslag och motivering

Sammanfattning
Landstingsrevisorerna konstaterar vid revisionstillfället år 2014 att styrning och kontroll av IT-säkerheten i nätverksansluten medicinteknisk utrustning behöver stärkas och samordnas på landstingsövergripande nivå. Landstingsstyrelsens förvaltning anser att landstingsrevisorernas rapport i huvudsak ger en rättvisande bild av situationen vid revisionstillfället. Inom förvaltningen pågår ett arbete med att skapa förutsättningar för tydlig styrning av och struktur för IT inom landstinget. Arbete pågår även med att utveckla och breddinföra ett övergripande ledningssystem för informationssäkerhet. Arbetet med att inarbeta revisorernas rekommendationer i dessa uppdrag har påbörjats.

Bakgrund
Revisionen har granskat landstingets styrning och kontroll av IT-säkerheten i närverksansluten medicinteknisk utrustning, MTU. Granskningen har genomförts under innevarande år genom intervjuer av ansvariga på olika nivåer samt genom dokumentstudier. Granskningen har genomförts vid landstingsstyrelsens förvaltning samt vid akutsjukhusen Karolinska universitetssjukhuset, Danderyds sjukhus AB och Södertälje sjukhus AB.

Den övergripande revisionsfrågan i granskningen var:

- Finns tillfredsställande styrning och kontroll av nätverksansluten medicinteknisk utrustning så att IT-säkerheten säkerställs?

Den övergripande revisionsfrågan bröts ner i delfrågor som motsvarar tre områden som pekas ut i standarden SS-EN80001:1 *Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplad till medicintekniska produkter*: utpekade resurser med tydlig ansvarsfördelning, styrande regelverk (policy) samt tydlig riskhanteringsprocess under hela livscykeln.

I projektrapporten konstaterar revisionen brister inom granskade områden. Landstingsrevisorernas samlade bedömning är att styrning och kontroll behöver stärkas och samordnas på landstingsövergripande nivå dels för att uppnå en effektivare hantering inom landstinget, dels för att incidenter och brådskande ärenden som rör medicinteknisk utrustning ska kunna tas om hand på ett koordinerat sätt och med hög prioritet.

Landstingsstyrelsen ges i rapporten följande rekommendationer:

- Landstingsstyrelsen bör komplettera regelverket för informations-säkerhet med specifika krav för nätverksansluten medicinteknisk utrustning så att stöd finns för praktisk tillämpning i verksamheten för exempelvis anslutningsprocesser, uppdateringar och styrning av fjärråtkomst
- Landstingsstyrelsen bör stärka och tydliggöra ansvaret för IT-säkerhet kopplat till MTU på landstingsövergripande nivå och tydliggöra hur den organisatoriska samverkan mellan SLL IT och akutsjukhusens MT-avdelningar ska ske vad gäller säkerhetskrav. Samverkan mellan SLL IT och akutsjukhusen bör även omfatta utveckling av supportprocesser anpassade för MTU.
- Landstingsstyrelsen bör ta fram ett samordnat underlag för gemensamma IT- och säkerhetsrelaterade krav i samband med

upphandling av MTU samt utreda möjligheten till ramavtal för området.

Utifrån dessa övergripande rekommendationer lämnar revisionen ett antal mer detaljerade rekommendationer, liksom rekommendationer riktade till de granskade akutsjukhusen.

Övervägande
Medicinteknisk utrustning omfattar en mängd produkter, från enkla förbrukningsartiklar till komplicerade högteknologiska utrustningar. Ett ökande antal medicintekniska produkter utformas idag för att utbyta information elektroniskt med annan IT-utrustning via nätverk. I den alltmer integrerade IT-infrastrukturen är det svårt för en enskild part, vårdgivare, tillverkare av MTU eller IT-leverantör, att ensam ansvara för IT-säkerheten och bedöma risker vid anslutning av MTU i nätverk.

Revisionen konstaterar att det, i enlighet med författningar och standarder inom området, är respektive vårdgivare som har ansvaret för att möjliggöra en säker användning och hantering av MTU. Revisionen pekar även på att det yttersta ansvaret för IT-säkerheten inom Stockholms läns landsting ligger på landstingsstyrelsen.

I de delar som rekommendationerna rör samspelet mellan landstingsstyrelsen och vårdgivarna menar förvaltningen att förbättringsåtgärderna i form av ett tydliggörande av hur den organisatoriska samverkan gällande säkerhetskrav ska ske är angelägna. Därutöver är tydliga riktlinjer och stöd för praktisk tillämpning liksom integreringen av krav i tjänsteavtal och upphandling viktiga för en framgångsrik samordning.

Landstingets styrande regelverk för informationssäkerhet beskriver krav för nätverksanslutna IT-system, men saknar konkretiseringar för nätverksansluten MTU specifikt. För närvarande pågår det ett arbete inom förvaltningen med att uppdatera de övergripande riktlinjerna för informationssäkerhet, liksom med att ta fram stödjande tillämpningsanvisningar för hälso- och sjukvården. Författningskrav avseende MTU, liksom i kraven i standarden SS-EN 80001:1 Riskhantering tillämpad på IT-nätverk, som innehåller eller är kopplat till medicintekniska produkter, behöver tydliggöras i landstingets styrande regelverk. Likaså behöver ledningssystemet för informationssäkerhet stärkas för att öka möjligheten att styra ansvars- och samverkansfrågor kopplade till MTU och IT specifikt.

Förvaltningen har identifierat behovet av styrande principer inom IT-säkerhetsområdet generellt. En plan för detta arbete kommer att tas fram och omfatta även IT-säkerhetsfrågor rörande nätverksansluten MTU.

Revisionen pekar vidare på att landstingsstyrelsen behöver ta fram tydliga krav på IT-säkerhet för MTU. Inom förvaltningen pågår ett arbete med att implementera ett landstingsgemensamt ledningssystem för informationssäkerhet. Arbete pågår även med att utveckla en metod- och processtödjande IT-stöd för systematiskt informationssäkerhetsarbete, i vilket stöd kommer finnas för processerna informationsklassificering och riskhantering liksom krav och kontrollpunkter för uppföljning av efterlevnaden. Detta arbete skapar bättre förutsättningar att möta revisionens rekommendationer gällande ökad styrning och uppföljning av säkerhetsarbetet kopplat till nätverksansluten MTU.

Ansvarfördelningen och samverkan mellan de granskade vårdgivarnas MT-avdelningar och SLL IT är enligt revisorernas granskning inte formaliserad. Förvaltingen delar revisionens bild av att tjänsteavtalen behöver ses över så att ansvarsförhållandet mellan vårdgivarnas MT-avdelningar och SLL IT tydliggörs.

Revisionen gör bedömningen att det saknas en effektiv samverkan inom upphandlingsområdet avseende säkerhetskrav kopplat till MTU. Av granskningen framkommer det även att intervjuade vårdgivare efterfrågar centralt stöd för kravställning av IT-säkerhet i samband med upphandling av MTU. Förvaltningen delar revisionens bild av att samverkan behöver stärkas inom upphandlingsområdet. Det arbete som sker inom ramen för Nya Karolinska Solna, NKS, och Framtidsplanen för hälso- och sjukvården, FHS, gällande kravsammanställningar vid upphandling torde utgöra en god utgångspunkt för ett sådant förbättringsarbete.

Av revisorernas rapport framgår att ärendehantering gällande nätverksansluten MTU sker i parallella system, hos respektive vårdgivare samt hos SLL IT, med risk för att ärenden dubbelregistreras, faller mellan stolarna eller inte prioriteras tillräckligt högt. En översyn av SLL IT:s rutiner och processer kommer att genomföras i syfte att åstadkomma en anpassning för nätverksansluten MTU.

Förvaltningen vill även uppmärksamma landstingsstyrelsens uppdrag åt landstingsdirektören att skapa ett nytt funktionsområde inom landstingsstyrelsens förvaltning samt att återkomma med förslag till uppdrag för funktionsområdet. Syftet med uppdraget är att skapa förutsättningar för tydlig styrning av och struktur för IT inom landstinget.

Det nya funktionsområdet är tänkt att utgöra den organisatoriska basen för strategiska IT-frågor, inklusive strategiska IT-säkerhetsfrågor, till vilken referens- och samordningsgrupper kan knytas. I uppdraget kommer styrningsfrågor kopplade till IT-säkerheten i nätverksansluten MTU att belysas närmare i samarbete med berörda förvaltningar och bolag.

Sammanfattningsvis delar förvaltningen revisionens samlade bedömning att styrning och kontroll av IT-säkerheten i nätverksansluten medicinteknisk utrustning behöver stärkas och samordnas på landstingsövergripande nivå. Underlaget i landstingsrevisorernas rapport nr 02/12 kommer att utgöra en viktig del i förvaltningens fortsatta arbete inom området.

Ekonomiska konsekvenser av beslutet

Det uppstår inga ekonomiska konsekvenser av beslutet. Kostnaderna för ovan beskrivna aktiviteter ryms inom ordinarie budget.

Miljökonsekvenser av beslutet

I enlighet med landstingets Miljöpolitiska program 2012-2016 har hänsyn till miljön beaktats och slutsatsen är att det inte är relevant med en miljökonsekvensbedömning i detta ärende.

Toivo Heinsoo
Landstingsdirektör

Anders Nyström
Biträdande förvaltningschef

PROJEKTRAPPORT NR 2/2014

Ankom
Stockholms läns landsting
2014 -09- 26
Dnr LS 1409- 1050

IT-säkerhet i nätverks-ansluten medicinteknisk utrustning

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Vad gör Landstingsrevisorerna?

Landstingsrevisorerna granskar den verksamhet som bedrivs av landstingets nämnder och bolagsstyrelser. Revisionsuppdraget är det största inom kommunal verksamhet. Landstingsrevisorerna omfattar både de förtroendevalda revisorerna och revisionskontoret.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, sakligt och integritet främja, granska och bedöma verksamheten. Den övergripande uppgiften för revisorerna är att granska hur nämnder och styrelser tar sitt ansvar. De förtroendevalda revisorerna är fullmäktiges och ytterst medborgarnas instrument för den demokratiska kontrollen. De har därmed en viktig funktion i den lokala självstyrelsen.

Ledamöter i nämnder och styrelser ansvarar inför fullmäktige för hur de själva, anställda och uppdragstagare genomför verksamheten. I ansvaret ingår att genomföra en ändamålsenlig verksamhet utifrån fullmäktiges mål, beslut och riktlinjer samt de föreskrifter som gäller för verksamheten, på ett ekonomiskt tillfredsställande sätt och med en tillräcklig intern kontroll samt att upprätta rättvisande räkenskaper.

I årsrapporter för nämnder och bolag sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna finns på Landstingsrevisorernas hemsida www.sll.se/rev. De kan också beställas från revisionskontoret. Det går även att prenumerera på Landstingsrevisorernas nyhetsbrev Nytt från landstingsrevisionen genom att anmäla intresse via e-postmeddelande till landstingsrevisorerna@rev.sll.se

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Revisorsgrupp I 2014-09-24 *Diarienummer:* RK 201403-0009

Landstingsstyrelsen

Projektrapport nr 2/2014
IT-säkerhet i nätverksansluten medicinteknisk utrustning

Revisorerna i revisorsgrupp I beslutade på möte 2014-09-24 att överlämna rapporten till landstingsstyrelsen för yttrande senast 2014-12-08.

Revisorernas samlade bedömning är att styrning och kontroll av IT-säkerheten i nätverksansluten medicinteknisk utrustning (MTU) behöver stärkas och samordnas på landstingsövergripande nivå.

Revisionen vill till landstingsstyrelsen särskilt framhålla behovet av att tydliggöra ansvarsfördelningen mellan SLL IT och akutsjukhusens MT-avdelningar när det gäller IT-säkerheten för MTU. Vidare bör regelverket för informationssäkerhet kompletteras med specifika krav för nätverksansluten MTU.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Kenneth Strömberg
ordförande

Anne Fahl
sekreterare

Landstingsrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08-737 25 00
Fax: 08-737 53 50
E-post: landstingsrevisorerna@rev.sll.se

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

Besök oss: Hantverkargatan 25 B. T-bana Rådhuset

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Revisorsgrupp II | 2014-09-24 | *Diarienummer:* RK 201403-0009

Styrelserna för
Danderyds sjukhus AB
Karolinska Universitetssjukhuset AB
Södertälje sjukhus AB

Projektrapport nr 2/2014
IT-säkerhet i nätverksansluten medicinteknisk utrustning

Revisorerna i revisorsgrupp II beslutade på möte 2014-09-24 överlämna rapporten till styrelsen för Danderyds sjukhus AB för yttrande och till styrelserna för Karolinska universitetssjukhuset och Södertälje sjukhus AB för kännedom och med möjlighet till yttrande senast 2014-12-08.

Revisorernas samlade bedömning är att ansvarsfördelningen mellan landstingets centrala IT-funktion och akutsjukhusen är otydlig avseende IT-säkerhet i nätverksansluten medicinteknisk utrustning (MTU). Danderyds sjukhus saknar en effektiv samverkan med SLL IT när det gäller MTU. Styrningen är idag till stor del beroende av informella processer och individuella insatser vilket leder till en ökad risk för IT-säkerheten i MTU.

Revisionen vill särskilt framhålla att Styrelsen på Danderyds sjukhus AB bör utveckla ett systematiskt IT-säkerhetsarbete som inkluderar nätverksansluten MTU.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Göran Hammarsjö
ordförande

Rikard Lindqvist
sekreterare

Landstingsrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08-737 25 00
Fax: 08-737 53 50
E-post: landstingsrevisorerna@rev.sll.se

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

Besök oss: Hantverkargatan 25 B. T-bana Rådhuset

INNEHÅLL

1 SLUTSATSER OCH REKOMMENDATIONER 4

2 UTGÅNGSPUNKTER FÖR GRANSKNINGEN 6

2.1 Motiv till granskningen 6
2.2 Revisionsfråga 6
2.3 Avgränsning 7
2.4 Bedömningsgrunder 7
2.5 Metod 7

3 ANSVARSFÖRDELNING OCH SAMVERKAN 8

3.1 Landstingsstyrelsens förvaltning 8
3.2 Samverkan Danderyds sjukhus AB och SLL IT 9
3.3 Samverkan Karolinska universitetssjukhuset och SLL IT 10
3.4 Södertälje sjukhus AB 10

4 POLICY OCH RIKTLINJER 11

4.1 Landstingsstyrelsens förvaltning 11
4.2 Danderyds sjukhus AB 11
4.3 Karolinska universitetssjukhuset 12
4.4 Södertälje sjukhus AB 13

5 SYSTEMATISKT SÄKERHETSARBETE 13

5.1 Landstingsstyrelsens förvaltning 13
5.2 Danderyds sjukhus AB 14
5.3 Karolinska universitetssjukhuset 14
5.4 Södertälje sjukhus AB 15

1 Slutsatser och rekommendationer

Revisionen har granskat landstingets styrning och kontroll av IT-säkerheten i nätverksansluten medicinteknisk utrustning (MTU). Den samlade bedömningen är att styrning och kontroll behöver stärkas och samordnas på landstingsövergripande nivå, dels för att uppnå en effektivare hantering i landstinget, dels för att incidenter och brådskande ärenden som rör MTU ska tas om hand på ett koordinerat sätt och med hög prioritet. Roller och ansvar behöver tydliggöras på både central och lokal nivå. Styrningen är idag till stor del beroende av informella processer och individuella insatser vilket leder till en ökad risk för IT-säkerheten i MTU.

Den otydliga ansvarsfördelningen mellan akutsjukhusen och landstingets centrala IT-funktion (SLL IT) har lett till suboptimering. Bland annat sker support- och ärendehanteringen i flera parallella system, utan tillräcklig koordinering och anpassning för MTU. Samverkan är sällan preciserad i tjänsteöverenskommelserna mellan SLL IT och de avtalsknutna sjukhusen. Detta påverkar handläggningstiderna, den tekniska säkerheten och i förlängningen riskerar även patientsäkerheten att påverkas. För Danderyds sjukhus vill revisionen framhålla att ett systematiskt IT-säkerhetsarbete som inkluderar nätverksansluten MTU behöver utvecklas.

Landstingets styrande regelverk för informationssäkerhet omfattar inte specifika krav för att hantera nätverksansluten MTU och täcker inte behovet av stöd vid säkerhetsmässiga avvägningar vid systemintegration. Detta gör det svårt för både landstingsstyrelsens förvaltning och akutsjukhusen att säkerställa efterlevnad av krav i policyer och riktlinjer.

Avsaknaden av en central styrning och stöd inom området medför en skiftande hantering och tekniska variationer inom landstinget. Leverantörerna riskerar få ett alltför stort inflytande över de tekniska lösningarna om inte landstinget säkerställer att all nätverksansluten MTU uppfyller en gemensam nivå på generella krav. Exempelvis behövs landstingsgemensamma krav i form av IT-säkerhetskrav liksom dokumentation av nätverksskisser, gränssnittsbeskrivningar för exempelvis MTU-leverantörers fjärråtkomst etc. Det behöver även utvecklas ett samordnat centralt stöd för upphandling och livscykelhantering av nätverksansluten MTU.

Behov finns även av ett systematiskt säkerhetsarbete med samordnade riskbedömningar och säkerhetsanalyser av vårdprocesser inte minst i och med att MTU i allt högre grad ansluts till nätverk, och att den snabba utvecklingen inom området väntas leda till hantering som omfattar exempelvis även mobila enheter. MTU kommer dessutom att få en allt viktigare roll i nätverkssjukvården som en förutsättning exempelvis inom avancerad sjukvård i hemmet. Samordnade riskbedömningar både på central och på lokal nivå behöver därför genomföras i takt med de nya förutsättningarna.

Det systematiska säkerhetsarbetet av nätverksansluten MTU är idag beroende av insatser på lokal nivå. Sjukhus med interna ledningssystem för informat-

ionssäkerhet (LIS) har bättre förutsättningar för detta genom en tydlig ansvarsfördelning och metoder och mallar som stödjer ett systematiskt säkerhetsarbete.

Inom SLL IT på landstingsstyrelsens förvaltning pågår ett arbete med utveckling av ett ledningssystem för informationssäkerhet vilket på sikt bör ge bättre förutsättningar för ett säkerhetsarbete som även inkluderar nätverksansluten MTU.

Rekommendationer:

Landstingsstyrelsen bör komplettera regelverket för informationssäkerhet med specifika krav för nätverksansluten medicinteknisk utrustning (MTU) så att stöd finns för praktisk tillämpning i verksamheten för exempelvis anslutningsprocesser, uppdateringar och styrning av fjärråtkomst.

Landstingsstyrelsen bör stärka och tydliggöra ansvaret för IT-säkerhet kopplat till MTU på landstingsövergripande nivå och tydliggöra hur den organisatoriska samverkan mellan SLL IT och akutsjukhusens MT-avdelningar ska ske vad gäller säkerhetskrav. Samverkan mellan SLL IT och akutsjukhusen bör även omfatta utveckling av supportprocesser anpassade för MTU.

Landstingsstyrelsen bör ta fram ett samordnat underlag för gemensamma IT- och säkerhetsrelaterade krav i samband med upphandling av MTU samt utreda möjligheten till ramavtal för området.

Styrelsen på Danderyds sjukhus AB bör utveckla ett systematiskt IT-säkerhetsarbete som inkluderar nätverksansluten MTU.

2 Utgångspunkter för granskningen

2.1 Motiv till granskningen

Medicinteknisk utrustning (MTU) omfattar en mängd produkter, från enkla förbrukningsartiklar till komplicerade högteknologiska utrustningar som datortomografer. MTU omfattar också medicinska behandlingshjälpmedel[1]. Från och med mars 2010 omfattas även informationssystem och programvara som hanterar information kring patienten. Avancerad MTU finns främst på akutsjukhusen.

Enligt föreskrifter[2] har respektive vårdgivare ansvaret för att möjliggöra en säker användning och hantering av medicintekniska produkter. Det yttersta ansvaret för IT-säkerheten inom Stockholms läns landsting ligger på landstingsstyrelsen (LS).

Det finns flera betydande risker förknippade med medicinteknisk utrustning som ansluts till nätverk. En risk är att utrustningen kan vara svår att säkerhetsuppdatera. Leverantörer garanterar sällan utrustningens funktionalitet om skydd mot virus och intrång installeras eller uppdateras. Detta kan leda till att skyddet mot skadlig kod blir föråldrat och att risken för virus eller intrång i systemen ökar.

Behovet av samverkan kommer att öka i takt med att MTU ansluts till nätverk i allt större omfattning. Det krävs effektiva rutiner och en systematisk samverkan mellan MT-avdelningarna och nätverksleverantören för att riskerna ska hållas på en acceptabel nivå. Brister i systemintegrationen kan leda till funktionsstörningar på MTU och riskerar därmed att påverka patientsäkerheten.

Nätverksansluten MTU kommer att få en allt viktigare roll i den nya nätverkssjukvården. Det är därför viktigt att samarbetet mellan akutsjukhusens MT-avdelningar och den egna IT-beställaravdelningen fungerar väl, särskilt vad gäller utvecklingen av e-hälsa[3] vid avancerad vård i hemmet.

2.2 Revisionsfråga

Övergripande revisionsfråga:

Finns tillfredsställande styrning och kontroll av nätverksansluten medicinteknisk utrustning så att IT-säkerheten säkerställs?

Den övergripande revisionsfrågan har brutits ner i följande delfrågor:

A. Hur säkerställer landstingsstyrelsen tydlig ansvarsfördelning och effektiv samverkan vad gäller säkerhetskrav mellan SLL IT som nätverksleverantör och akutsjukhusens MT-avdelningar?
B. Hur säkerställer landstingsstyrelsen respektive akutsjukhusens MT-avdelningar att nätverksansluten medicinteknisk utrustning uppfyller krav i policyer och riktlinjer?

[1] För fullständig definition av MTU se EU:s medicintekniska direktiv och lagen om medicintekniska produkter.
[2] SOSFS 2008:1
[3] eHälsa handlar om hur framtidens vård och omsorg som helhet ska fungera och förbättras med hjälp av e-tjänster(http://www.nationellehalsa.se/nationell-ehalsa).

C. Finns ett systematiskt säkerhetsarbete inkl. riskanalyser gällande teknisk säkerhet och informationssäkerhet i nätverksansluten medicinteknisk utrustning såväl lokalt som centralt inom SLL?

Delfrågorna följer därmed de tre områden som pekas ut i standarden[4] som nödvändiga för en strukturerad riskhantering av nätverksansluten MTU:

- Utpekade resurser med tydlig ansvarsfördelning – delfråga A
- Styrande regelverk (policy) – delfråga B
- Tydlig riskhanteringsprocess under hela livscykeln – delfråga C

2.3 Avgränsning

Granskningen omfattar nätverksansluten medicinteknisk utrustning och bedömning av om tillfredsställande rutiner finns i samband med både upphandling, systemförvaltning samt IT-säkerhet när det gäller hantering av medicinteknisk utrustning inom SLL.

Granskningen har inriktats på landstingsstyrelsens förvaltning och akutsjukhusen som har merparten av nätverksansluten medicinteknisk utrustning i landstinget. Det yttersta ansvaret för IT-säkerheten inom SLL ligger på landstingsstyrelsen, men granskningen avser samtliga nivåer i styrkedjan till sjukhusens olika ansvarsnivåer.

Följande enheter ingår i granskningen; Södertälje sjukhus AB (Södertälje), Karolinska universitetssjukhuset (Karolinska), Danderyds sjukhus AB (DSAB) och landstingsstyrelsens förvaltning (LSF).

2.4 Bedömningsgrunder

Följande dokument har utgjort bedömningsgrund i granskningen:

- SLL:s riktlinjer för informationssäkerhet, främst de delar som handlar om krav på informationshantering och nätverksansluten utrustning (fullmäktige 2013-03-19, LS 1112-1733).
- SS-EN 80001:1 Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter, (fastställd 2011-09-07, SIS).
- SLL:s upphandlingspolicy, främst kraven på samordning (fullmäktige 2011-04-12, LS 1102-0181).
- Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården, SOSFS 2008:1 (inkl. SOSFS 2013:6 Ändring i föreskrifterna (SOSFS 2008:1)), främst 4-7 §§ om ansvar för vårdgivare och verksamhetschef.
- Ledningssystem för informationssäkerhet, kraven på utpekade resurser med tydlig ansvarsfördelning, styrande regelverk (policy) och tydlig riskhanteringsprocess under hela livscykeln (ISO/IEC 27001:2013 IDT).

2.5 Metod

Styrningen har granskats genom intervjuer av ansvariga på olika nivåer i de utvalda enheterna och genom dokumentstudier. Granskningen ute på sjukhusen har även omfattat verifiering av rutiner genom dokumentstudier.

[4] SS-EN 80001:1 Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter.

3 Ansvarsfördelning och samverkan

3.1 Landstingsstyrelsens förvaltning

Granskningen visar att landstingsstyrelsens förvaltning inte arbetar landstingsövergripande med IT-säkerhetsfrågor kopplat till MT-utrustning. Däremot arbetar SFI[5] vid LSF, på strategisk nivå med samordning av MT och IKT[6] inom Nya Karolinska Solna (NKS) och Framtidens Hälso- och Sjukvård (FHS). I det arbetet ingår att sammanställa erfarenheter och överföra kunskap till sjukhusen. En inventering ska genomföras av strategiska kompetenser inom MT- och IKT-området i syfte att underlätta samverkan. SLL IT deltar inte i dessa utvecklingsarbeten utan agerar som en renodlad leverantör IT-infrastruktur.

Det finns idag en medvetenhet inom SLL IT om att MTU numera i hög grad är ansluten till de stora nätverken vilket är en helt annan situation än för några år sedan då MTU fanns på separata, mindre nätverk.

Det pågår ett nationellt arbete med en gemensam MT-nomenklatur där SLL representeras framförallt av Karolinska och Danderyds sjukhus. IT-området generellt har samordnats genom SLL IT, däremot ingick inte MT-frågor då dessa i praktiken har hanterats på lokal nivå. Vid intervjuerna framkom att MT-avdelningarna och SLL IT nu börjat utveckla ett samarbete, t.ex. nämndes det nära samarbetet mellan SLL IT och Karolinskas MT-avdelning när det gäller krav i tjänsteöverenskommelsen.

Granskningen visar att det saknas en formaliserad ansvarsfördelning och samverkan mellan SLL IT och MT-avdelningarna, förutom den som finns i tjänsteöverenskommelserna[7] för hur nätverksansluten MTU ska hanteras. SLL IT beskriver att deras huvudsakliga uppdrag är att leverera nät till kunder och att informera om störningar i näten. SLL IT saknar överblick om vilken utrustning som ansluts till nätverken då det inte finns krav på verksamheterna om att informera SLL IT om detta.

I de nätverk som SLL IT ansvarar för utför de tjänster utifrån de krav som respektive MT-avdelning ställer på säkerhet. SLL IT uppger att de inte känner till hur ansvaret för riskhantering inom sjukhusens MT-avdelningar fungerar om det inte framgår av tjänsteöverenskommelsen och påpekar att ansvaret för riskanalyser och riskhantering ligger hos vårdgivarna.

I samband med införande av ledningssystem för informationssäkerhet (LIS) på SLL IT har möjligheten att skapa en särskild rutin för riskhantering och åtgärder kopplat till MTU diskuterats. Centralt på LSF finns även planer på att i det SLL-gemensamma ledningssystemet ta fram tillämpningsanvisningar för hur kraven i de övergripande riktlinjerna för informationssäkerhet kan tillämpas på MT.

Av intervjuer har framkommit att kunskapen om IT-säkerhetens koppling till patientsäkerhet hos IT-personalen på SLL IT är ojämn. Detta kan medföra att

[5] Strategisk fastighetsinvestering
[6] Informations- och kommunikationsteknik
[7] Är de interna avtal som tecknas mellan sjukhusen och SLL-IT

ärenden som handlar om säkerheten i MTU får olika behandling utan att det har motiverats av ärendenas karaktär eller risknivå.

Granskningen visar att landstingsstyrelsens förvaltning inte heller arbetar landstingsövergripande med IT-säkerhetsfrågor kopplat till upphandling av MT-utrustning specifikt. Karolinska har därför i arbetet med upphandlingar till NKS, tagit fram generella IT-säkerhetskrav som även berör MT. SLL Upphandling har emellertid ett särskilt uppdrag att stötta NKS upphandlingar av MTU och IKT[8].

Revisionens bedömning
Att MT-utrustning idag i högre utsträckning är ansluten till de stora nätverken ställer större krav på säkerheten, men även på samverkan mellan MT- och IT-avdelningarna och leverantörerna. MT-utrustning ska idag kunna kommunicera direkt med andra vårdgivare både inom landet (så kallad nätverkssjukvård) och utom landet vid konsultationer. Det innebär ett ökat behov av styrning och samverkan från central nivå.

Revisionen bedömer att det inom SLL IT finns en medvetenhet om de alltmer komplexa säkerhetsfrågorna vad gäller nätverksansluten MT. Men, det saknas en tydlig ansvarsfördelning och effektiv samverkan vad gäller säkerhetskrav mellan SLL IT som nätverksleverantör och akutsjukhusens MT-avdelningar. Det finns inte någon formaliserad samverkan mellan SLL IT och de avtalsknutna sjukhusens MT-avdelningar förutom de tecknade tjänsteöverenskommelser som normalt sett inte berör MT. Undantaget är de specifika MT-frågor som finns inom ramen för arbetet med NKS och FHS. Även inom upphandlingsområdet, saknas idag en tillräcklig samordning kring säkerhetskrav på central nivå inom SLL.

3.2 Samverkan Danderyds sjukhus AB och SLL IT

Danderyds sjukhus (DSAB) har inte utsett någon specifik riskhanterare för MTU. Ansvaret för riskhantering ingår i uppdraget till respektive MT-ingenjör med huvudkompetens för utrustningen. Av intervjuer framgår att det saknas ett tydligt avtalsförhållande och samverkansformer mellan DSAB och SLL IT för MTU vilket skapar problem vid exempelvis avbrott. Samverkan i stort präglas, enligt intervjusvaren av ett informellt arbetssätt på lokal nivå och ett stort beroende av kunskap och upparbetade informella kontaktvägar. DSAB anger att ärendehanteringen inte fungerar optimalt, bland annat med långa svarstider. Detta upplevs som besvärande då MTU ofta spelar en väsentlig roll ur ett patientsäkerhetsperspektiv.

Revisionens bedömning
Av revisionen framgår att Danderyds samverkan lokalt präglas av ett informellt arbetssätt. Sjukhuset har inte heller en effektiv samverkan med SLL IT när det gäller MTU. Ett exempel på detta är att det inte finns något tydligt avtal som specificerar ansvarsförhållandet mellan SLL IT och MT-avdelningen. Detta leder till att sjukhuset är beroende av individuella kontaktvägar och att dokumenterade riskbedömningar som även omfattar nätverken inte kan göras.

[8] Informations- och kommunikationsteknik

3.3 Samverkan Karolinska universitetssjukhuset och SLL IT

Karolinska universitetssjukhuset (Karolinska) beskriver att de inte har utsett en riskhanterare enligt standarden, men de intervjuade anser att efterlevnaden i övrigt är god. Inom Karolinska sker samverkan effektivt inom ramen för ledningssystemet. Ledningssystemet för informationssäkerhet (LIS) innehåller mallar för samverkan kring exempelvis informationssäkerhetsklassningar. Karolinska uppger att det sker tät samverkan mellan MT och IT på sjukhuset och att ledningssystemet preciserar ansvar på olika nivåer. Det finns avtal mellan SLL IT och Karolinska och återkommande operativa samverkansmöten sker.

Vid sjukhuset finns kravsammanställningar som kan användas vid upphandlingar av MTU, där krav på nätverksanslutning och IT-säkerhet framgår. All nätverksansluten MTU uppges vara förtecknad i IT-stöd. Ett problem som lyfts är att Karolinska önskar bättre skisser över nätverken från SLL IT för att underlätta bland annat arbete med segmentering[9]. Kännedomen om policy och regelverk för informationssäkerhet bland personalen beskrivs som god, men att det finns utbildningsbehov för tillämpningen av MTU.

Revisionens bedömning

Genom sitt ledningssystem för informationssäkerhet bedöms Karolinska universitetssjukhuset ha möjlighet att styra ansvarsfrågor och samverkan mellan IT och MT. Det finns ett avtal med SLL IT som ger förutsättningar för en effektiv samverkan. Bedömningen är att det finns ett behov av bättre och mer detaljerad information om den tekniska IT-miljön för att underlätta samverkan och ett systematiskt IT-säkerhetsarbete. Sammantaget finns goda förutsättningar för effektiv samverkan och tydliga ansvarsförhållanden vid Karolinska.

3.4 Södertälje sjukhus AB

Södertälje sjukhus AB (Södertälje) redovisar att sjukhuset har en informationssäkerhetssamordnare, men inte en utsedd riskhanterare enligt standard[10]. Chefsläkarna är ytterst ansvariga för patientsäkerheten och de samverkar med lokal MT- och IT-personal och informationssäkerhetssamordnaren i ett gemensamt ledningsforum. Södertälje köper även vissa tjänster av Karolinska i Huddinge. I höstas genomfördes en dokumenterad säkerhets- och sårbarhetsanalys av hela verksamheten, vilket inkluderade även MT. Det finns förteckningar över nätverksansluten MTU i IT-stöd.

Samverkan mellan sjukhuset och SLL IT fungerar inte tillfredställande enligt Södertälje. Sjukhuset beskriver ineffektiva beställningsvägar med långa handläggningstider och behov av att utnyttja personliga kontakter för att få åtgärder utförda. När det gäller säkerhetskrav i policy och regelverk nämner Södertälje att MT-frågor inte täcks in av nuvarande regelverk. De anställda på sjukhuset uppges ha god kännedom om säkerhetskraven och var de finns tillgängliga.

Revisionens bedömning

På lokal nivå inom Södertälje sjukhus bedöms ansvarsfördelning och samverkan mellan IT och MT fungera bra. Sjukhuset har god kontroll på nätverksansluten MTU och tydliga processer för installation av nya system. Lokal sam-

[9] Innebär att dela upp ett eget nätverk i underavdelningar
[10] SS-EN 80001:1 Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter

verkan underlättas av att sjukhuset är en liten enhet med egen IT-avdelning. Samverkan på central nivå med SLL IT bör dock utvecklas och formaliseras för att förbättra styrning och uppföljning och minska beroendet av personliga kontakter för problemlösning.

4 Policy och riktlinjer

4.1 Landstingsstyrelsens förvaltning

Intervjuerna visar att det saknas centralt stöd för kravställning av IT-säkerhet i samband med upphandling av MTU. SLL IT kommer ofta in sent i processen, först när MTU inte fungerar. SLL upphandling har hittills inte deltagit i sjukhusens MT upphandlingar, men har nu byggt upp en kompetens kring den typen av upphandlingar i och med arbetet med NKS. Det saknas krav i de övergripande riktlinjerna för informationssäkerhet[11] liksom uppföljning på central nivå av IT-säkerheten i nätverksansluten MTU.

För att SLL IT ska kunna anpassa säkerheten specifikt för MTU bör kunderna, i egenskap av informationsägare, göra informationssäkerhetsklassningar enligt landstingets övergripande riktlinjer för informationssäkerhet, samt delge SLL IT resultatet av klassningen. Detta sker inte i dagsläget. Enligt SLL IT är det SLL upphandling och sjukhusens respektive informationssäkerhetssamordnare som bör se till att leverantörer av MT-utrustning uppfyller landstingets IT-säkerhetskrav. SLL IT har ingen kontakt med MTU-leverantörer. Det sker inget erfarenhetsutbyte mellan MT-personal, MTU-leverantörer och IT-personal.

Revisionens bedömning

Det saknas tydliga krav i de övergripande riktlinjerna för informationssäkerhet vad gäller IT-säkerhet i MT-utrustning specifikt. Därmed finns inte heller någon uppföljning av hur kraven efterlevs. Behovet av tydliga säkerhetskrav ökar i takt med att MT i allt större utsträckning ansluts till nätverk, och att den snabba utvecklingen inom området väntas leda till hantering som omfattar exempelvis även mobila enheter.

Den informationssäkerhetsklassning som genomförs av MTU på lokal nivå bör komma SLL IT till del så att arbete med anpassade och ändamålsenliga skyddsåtgärder kan underlättas. Det pågående arbetet på LSF med att införa ett landstingsgemensamt ledningssystem för informationssäkerhet bör säkerställa att LSF får information som ger en överblick över risker och IT-säkerhet i MT-utrustningen inom SLL, i syfte att öka förutsättningarna för styrning och samordning av säkerhetsarbetet.

LSF bör ta fram tydliga krav på IT-säkerhet för MT-utrustning som stöd vid upphandlingar inom landstinget.

4.2 Danderyds sjukhus AB

DSAB beskriver att det ställs standardiserade krav på själva medicintekniska utrustningen men att det inte finns motsvarande när det gäller kommunikationslösningar när utrustningen ansluts till nätverk. Det finns behov om en mer detaljerad beskrivning av nätverk. uttrycks f. DSAB beskriver en informell dialog

[11] LS 1112-1733

med SLL IT för att efterleva krav i policy och riktlinjer, men efterfrågar ytterligare stöd från SLL IT för att säkerställa efterlevnad av nätverksrelaterade krav och tydligare beskrivningar av gränssnitt för anslutning. Av intervjuerna framgår att sjukhuset upplever att de riktlinjer som finns inte är anpassade för MTU. I avsaknad av central styrning för att formulera krav på leverantörerna vid upphandling blir konsekvensen att MT-leverantörerna istället ställer krav på anpassningar på sjukhuset. Detta kan innebära risker för IT-säkerheten i stort för hela landstinget enligt de intervjuade.

Revisionens bedömning
Det finns inte någon strukturerad hantering för att säkerställa efterlevnad av riktlinjer inom DSAB och dialog sker på ett informellt sätt. Det innebär att risken för olika tolkningar och tillämpningar ökar, särskilt då dagens styrande regelverk inte omfattar IT-säkerhetskrav gällande MTU. Styrningen vid DSAB skulle bli mer enhetlig med ett generellt stöd för att hantera säkerhetskrav vid upphandlingar. Ett sådant stöd skulle minska både personberoendet och omfattningen av kravarbetet samt öka kvaliteten i upphandlingsunderlagen.

4.3 Karolinska universitetssjukhuset

Karolinska uppger i intervjuerna att sjukhuset har ett väl etablerat ledningssystem för informationssäkerhet som ska underlätta kravefterlevnad. Sjukhuset har också arbetat för att införa SS-EN 80001-1[12]. Karolinska efterlyser mer information kring MTU i det styrande regelverket[13].

Vid sjukhuset finns en grupp med IT-säkerhetskunniga som är involverade i de flesta upphandlingsprojekt för att driva IT-säkerhetsfrågor. Sjukhuset har tagit fram en mall för IT-säkerhetskrav i samband med upphandling av MTU tillsammans med den egna upphandlingsenheten. Dokumenten används som underlag vid upphandling, men det är enligt Karolinska osäkert om verifiering av IT-säkerhetskrav genomförs efter tilldelningsbeslut. Karolinska anser att de inte får tillräckligt stöd från SLL IT när det gäller IT-säkerhetskrav och skulle vilja se ett initiativ till utvecklade beskrivningar av den tekniska IT-miljön för att underlätta kravställning vid upphandling. När det gäller kravefterlevnad över tid uppger Karolinska att det är problematiskt att leverantörers uppdateringar av utrustning och vilka konsekvenser de kan få. Karolinska är restriktiva med leverantörers uppdateringar eftersom de vill ha möjligheter att testa uppdateringarna i den egna IT-miljön innan de genomförs. Fjärråtkomst från leverantörer tas upp som ett exempel där det saknas ett tydligt regelverk för styrning.

Revisionens bedömning
Genom att ha egna IT-säkerhetsresurser i upphandlingsprojekten och generella IT-krav har Karolinska skapat goda förutsättningar för att säkerställa att krav i policy och riktlinjer efterlevs, även om det framkommer vissa svårigheter att styra leverantörernas uppdateringar och fjärråtkomst. Bedömningen är att styrningen av leverantörerna skulle underlättas om det i landstingets nuvarande regelverk för informationssäkerhet görs specifika förtydliganden gällande nätverksansluten MTU.

[12] SS-EN 80001:1 Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter.
[13] Fullmäktiges policy och riktlinjer för informationssäkerhet

4.4 Södertälje sjukhus AB

Södertälje uppger att tillämpliga standarder och landstingets regelverk används som underlag när MTU upphandlas och att sjukhuset medverkar i upphandlingsgrupper med IT- och MT-resurser. Policy och regelverk bifogas upphandlingsunderlagen och IT-säkerhetsaspekter analyseras inför upphandlingarna tillsammans med IT-resurser. Ofta är dock kravställningen ganska öppen för leverantörerna att besvara utifrån hur deras produkter fungerar. Sjukhuset upplever att regelverket för informationssäkerhet är delvis föråldrat och inte anpassat för nätverksansluten MTU, vilket exempelvis kan medföra osäkerhet kring hur extern fjärråtkomst av leverantörer ska hanteras. Det finns också otydligheter i gränssnittsbeskrivningar som är anpassade för specifik utrustning. I stort säkerställs efterlevnad av säkerhetskrav lokalt genom ett nära samarbete på informell nivå mellan IT- och MT-resurser.

På samma sätt som för de övriga akutsjukhusen ingår policy och styrande regelverk i förfrågningsunderlaget vid upphandlingar som Södertälje sjukhus genomför i syfte att säkerställa efterlevnad av krav. Då det av granskningen framgår att det inte finns något samlat centralt stöd för att formulera krav på detaljerad nivå finns det risk att kvaliteten varierar på upphandlingsunderlagen och att kraven blir otydliga.

Revisionens bedömning
Eftersom sjukhuset är litet sker ett nära erfarenhetsutbyte och daglig återkoppling mellan IT och MT lokalt vilket gynnar förutsättningarna för efterlevnad av policy och regelverk på lokal nivå.

Det finns viss risk att kravställningen mot leverantörer sker mer på leverantörernas villkor för sina produkter än utifrån verksamhetens behov då sjukhuset har begränsade resurser för kravställning och det saknas ett stöd från landstinget centralt.

5 Systematiskt säkerhetsarbete

5.1 Landstingsstyrelsens förvaltning

Det sker en del IT-säkerhetsrelaterat arbete inom ramen för arbetet med NKS och FHS och då främst tekniska krav i samband med upphandling av MTU. Ansvaret för att göra riskanalyser och bedömningar vid uppdateringar av MTU ligger enligt SLL IT på sjukhusen, såvida inget annat anges i avtalet. SLL IT gör riskanalyser inför förändringar av nätverken eller vid konstaterade störningar, men inget specifikt görs för MTU.

Alla ärenden kring MTU, även akuta, hanteras via servicedesk på SLL IT. När det gäller ansvarsfördelningen för den dagliga övervakningen är det SLL IT infrastruktur som fångar upp felen och rapporterar enligt avtal. SLL IT har behov av att få förbättrad information om nätverksansluten MTU. Oftast finns inget specifikt uttalat i tjänsteöverenskommelsen som rör MTU utom i något fall där det ställts särskilda villkor på nätverket till någon speciell MTU.

Incidenthanteringen sker enligt avtal med respektive kund. Incidenterna gäller avvikelser generellt och inte MT specifikt. Det kan finnas vissa klausuler om att MT är viktigt. SLL IT uppger att krav i avtal kan vara otillräckligt, men

SLL IT påtalar att kunden har möjligheter att ställa specifika krav kring det systematiska säkerhetsarbetet. Högre krav innebär emellertid högre kostnader för kunden.

Revisionens bedömning
En förbättrad central samordning för att styra riskhanteringen och samverkan mellan sjukhusen och SLL IT skulle öka IT-säkerheten i MT-utrustning och därmed även bidra till högre patientsäkerhet. Det behöver även finnas överblick på SLL IT över nätverksansluten MTU som förutsättning för säkerhetsarbetet.

5.2 Danderyds sjukhus AB

DSAB beskriver att det inte bedrivs ett systematiskt lokalt informationssäkerhetsarbete samlat för all nätverksansluten MTU. De riskbedömningar som görs gäller antingen ett övergripande verksamhetsperspektiv eller för enskilda MT-utrustningar. MT-leverantören ansvarar oftast för riskanalyser av enskild utrustning i samband med uppdateringar. Intervjuade uppger att det inte finns något generellt metod- eller verktygsstöd för att göra riskbedömningar och att det skulle underlätta om detta togs fram centralt.

När det gäller ärendehantering görs denna i två olika system beroende på om det är MT-personal eller IT-personal som registrerar ärendet. Det finns inget sätt utöver informella kontakter att prioritera akuta MT-ärenden. Uppföljningen kring patientsäkerhetsrisker sker i HändelseVis[14]. Det finns inga strukturerade rutiner lokalt för att hantera IT-säkerhetsrisker, enligt sjukhuset.

Revisionens bedömning
Revisionens bedömning är att det systematiska säkerhetsarbetet kan utvecklas vid Danderyds sjukhus. Det finns exempelvis inga mallar eller metodstöd för riskbedömningar och det saknas en enhetlig process vid införande av ny medicinteknisk utrustning. Dessa förhållanden påverkar förutsättningarna för ett systematiskt säkerhetsarbete negativt och behöver utvecklas.

När det gäller ärendehanteringen sker detta i parallella system med risk att ärenden dubbelregistreras eller faller mellan stolarna. Det finns också risk att akuta ärenden inte prioriteras då ingen rutin/process för snabb hantering av denna ärendetyp finns. Följden av detta blir att sjukhuset blir beroende av personliga kontaktvägar för att lösa problem. Det kan också medföra säkerhetsrisker, både i ett patient- och IT-säkerhetsperspektiv, om incidenter inte rapporteras eller följs upp.

5.3 Karolinska universitetssjukhuset

Karolinska beskriver att ett systematiskt säkerhetsarbete finns som utgår från leverantörernas riskanalyser för utrustningen, exempelvis vid uppdateringar. Stöd för riskanalyser, både vad gäller IT-säkerhet och patientsäkerhet ges enligt Karolinska som en integrerad del av sjukhusets egna ledningssystem. Det finns mallar och metodstöd för riskbedömningar. Vid anslutning av ny MTU beskriver sjukhuset att de tar formella driftsättningsbeslut efter validering av installationen.

[14] Gemensamt rapporteringssystem inom SLL för rapportering av risker och avvikelser.