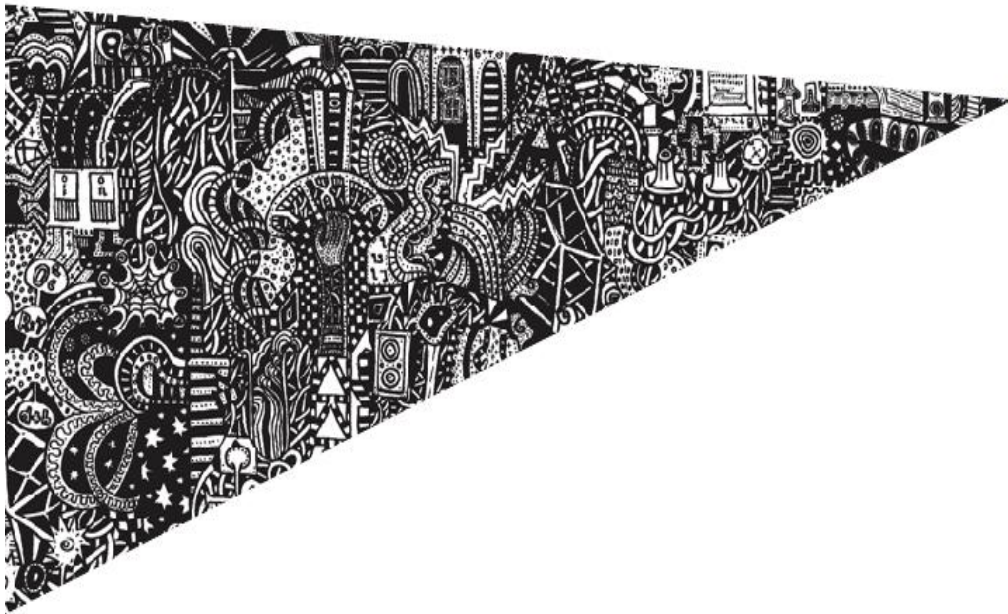


Västra Götalandsregionen

Revisionsrapport:

Kan IT-säkerheten påverka patientsäkerheten?

Göteborg, 2009-12-22



Innehållsförteckning

1. Sammanfattning och slutsatser	2
2. Inledning	5
2.1. Bakgrund	5
2.2. Syfte	5
2.3. Genomförande och avgränsningar.....	5
2.4. Revisionskriterier	6
2.5. Metod och frågeställningar.....	6
3. Iakttagelser från en förstudie.....	8
4. Iakttagelser från fördjupade granskningar	10
4.1. Huvudfrågor.....	10
4.2. Kartläggning av fem IT-relaterade avvikelser i vården.....	11
4.3. Styrning, ansvar och riskhantering "Före-Under-Efter"	15
4.4. Rutiner.....	17
4.5. Uppföljning och rapportering.....	22
4.6. Roller och ansvar.....	24
Bilaga 1 Dokumentförteckning.....	29
Bilaga 2 Redogörelse för fem avvikelser.....	30

1. Sammanfattning och slutsatser

Bakgrund och genomförande

Skador i hälso- och sjukvården är ett område som får allt mer uppmärksamhet. Socialstyrelsen redovisade under våren 2009 uppgifter om att en femtedel av ett stort antal Lex Maria-fall, som rapporterats under 2008, hade sin grund i datorer som inte fungerat som de skulle. Att brister i IT-miljön har stor påverkan på patientsäkerheten har tidigare också uppmärksammats genom bl.a. revisionsrapporter och i media.

Inom Västra Götalandsregionen har vården under en längre tid arbetat med systematiska förbättringar genom att bl.a. använda systemet MedControl för rapportering och uppföljning. Regionen har under senaste åren tagit fram nya regelverk för att styra och förbättra IT-säkerheten. Utöver detta gäller det också att säkerställa att det finns en förståelse för patientsäkerhet i alla led. Vidare förutsätter arbetet med att utveckla rutiner och förbättra systematiken att undvika vårdskador som är IT-relaterade att det råder en fungerande samverkan, uppföljning och gemensamma processer.

På uppdrag av de förtroendevalda revisorerna i Västra Götalandsregionen har Ernst & Young granskat hur IT-säkerheten påverkar patientsäkerheten. Syftet med granskningen har varit att ge en bild av hur IT-säkerhetsarbetet kan påverka patientsäkerheten och att granska hur IT-relaterade avvikelser hanteras när de inträffar inom regionen.

Granskningens inledande förstudie visade att avvikelser i vården, som orsakades av IT, inte dokumenterades på ett så systematiskt sätt att det gick att ge en underbyggd bild av dess omfattning. Förstudien gav också indikationer på att processen för avvikelshantering inte fungerade tillfredsställande. Den fortsatta granskningen fick därigenom en målsättning att beskriva hur arbetet kring IT-relaterade avvikelser bedrivs i regionen och vad detta arbete leder till. Den fortsatta granskningen inriktades på att följa upp fem avvikelser som inrapporterats under det senaste året. Vidare har granskningen omfattat styrning, rutiner och organisation kring regionens arbete kring IT-säkerhet och hur detta följs upp.

Granskningen har genomförts under hösten 2009 genom analys av relevant dokumentation samt intervjuer med 28 medarbetare.

Slutsatser

På den övergripande frågan om IT-säkerheten kan påverka patientsäkerheten är svaret, ja definitivt och det är aktörer i flera olika led som har ansvar för olika delar, vilket påverkar komplexiteten. Därför är det viktigt att understryka, att precis som det står i regionens säkerhetsstrategi, så krävs det en helhetssyn av flertalet aktörer eftersom säkerhetsfrågorna ofta skär igenom olika verksamhetsområden utan hänsyn till gränser.

Trots att granskningen visar på att det finns flera förbättringsområden, så är vår bedömning att Västra Götalandsregionen har goda utsikter och förutsättningar att styra IT-säkerheten på ett sådant sätt att införandet av IT i vården inte försämrar patientsäkerheten. Detta grundar vi främst på att Regionen har utarbetat ett ändamålsenligt regelverk som överlag stämmer väl överens med krav i relevanta lagar och föreskrifter. Vidare bör det regiongemensamma MedControl, som införs efter årsskiftet 2010, ge goda förutsättningar att frambringa en regiongemensam process och hantering av avvikelser. En regiongemensam databas kommer också ge större möjligheter till uppföljning och därigenom bättre beslutsunderlag vid prioriteringar för

investeringar i åtgärder, där de gör störst nytta. Detta är utgångspunkten för att nå de effekter som ett systematiskt förbättringsarbete innebär.

IT-säkerheten, utgör en högst väsentlig del av det som ofta benämns informationssäkerhet. Informationssäkerhet brukar definieras som säkerställande av information avseende tillgänglighet, riktighet, konfidentialitet och spårbarhet. Säkerhetsdirektören beskriver att säkerställande av tillgänglighet och riktighet är de dimensioner som främst påverkar patientsäkerheten, d.v.s. risken för vårdskador. Konfidentialitet och spårbarhet (ansvarighet och oavvislighet) utgör snarare ett skydd mot patientens integritet.

Ansvariga politiker har en viktig uppgift att besluta om och ge uttryck för att framtagna regelverk skall vara gällande samt att följa upp dem. Verksamhetscheferna ansvarar för att de implementeras i förvaltningarna. Det gäller säkerhetsåtgärder såväl i datorsystem, fysisk säkerhet, kontinuitetsplaner och avvikelshantering, vilket det återkommande ställs krav på.

Verksamhetscheferna har, enligt Socialstyrelsens föreskrifter, ett långtgående säkerhetsansvar. Dock har de sällan resurserna att tillse att åtgärder vidtas och säkra system används i samband med vård av patienter. Ett sätt att möjliggöra för verksamhetscheferna att ta sitt säkerhetsansvar är att stärka dialogen mellan vårdverksamheten och VGR IT. Kommunikation uppges av flera intervjuade vara en av de viktigaste förutsättningarna för att få en sömlös avvikelshantering mellan vård och IT. Ett annat område är samverkan mellan vård, Medicinteknik och IT. Här handlar det mycket om möte mellan olika kulturer och att övervinna prestige och revirtänkande.

Ett par initiativ har tagits på regional nivå att utveckla samverkan och formerna för att arbeta med IT och patientsäkerhetsfrågor på en regional nivå. Ett regionalt MedControl är det tydligaste exemplet på detta. De erfarenheter som hittills gjorts genom uppföljningen av avvikelser inom en enskild förvaltning, bör framöver kunna tillgodogöras hela regionen på ett betydligt bättre sätt. Ytterligare exempel på ökad samverkan inom regionen är riskhanteringsrådet, som har bildats under 2009.

Regionen har hittills inte bedrivit något strukturerat arbete kring uppföljning av avvikelser som är just relaterade till IT-systemen. I Socialstyrelsens föreskrifter Ledningssystem för kvalitet och patientsäkerhet (2005:12) framgår tydligt att IT inte är undantaget kravet på avvikelserapportering. Om det förhåller sig på det sätt som indikeras av Socialstyrelsen undersökning som redovisades i våras, att vart femte Lex Maria fall är relaterat till IT-systemen, så finns det uppenbara motiv att införa ett mer strukturerat sätt att samla och följa upp patientavvikelser där IT är en av orsakerna. Ett syfte bör vara att erfarenheterna skall användas i arbetet med att identifiera och prioritera områden där riskeliminering och förbättringsarbete ger största nytta. På regional nivå är därför viktigt att det sker en återkoppling av avvikelshandlingen till IT-strategiska avdelningen samt till FOA vård och infrastruktur.

IT-systemen utgör ett stort stöd för vårdverksamheten och flera av de utvecklingsprojekt som sker inom IT har som mål att bl.a. höja patientsäkerheten. T.ex. läkemedelslista, sammanhållen journal som ger bättre beslutsunderlag o.s.v. Det ökade IT-beroendet medför också att sårbarheten ökar eftersom påverkansgraden för verksamheten blir långt större när IT-säkerheten brister. Att övervaka och underhålla säkerheten i IT-infrastrukturen är VGR IT:s ansvar. För att utföra detta fordras att VGR IT har ett tydligt mandat från politik och ledning och gehör från brukarna att det är de som kontrollerar infrastruktur, nätverk och system. Det krävs att VGR IT avsätter resurser för lösningar och rutiner kring övervakning, för att snabbare detektera problem och fel. Det krävs också att de utvecklar rutiner för avvikelshantering.

Flera av regionens system är inte klassificerade med utgångspunkt ur den regionala modellen för informationsklassificering. Informationsklassningen utgör en av de grundläggande delarna för de säkerhetsnivåer som bör överenskommas genom servicenivåavtal mellan en förvaltning och VGR IT. En sådan klassning skulle ge Servicedesk ytterligare underlag i sina prioriteringar och eskalering vid olika ärenden. En fråga i sammanhanget som också bör besvaras är om Regionservice roll och åtaganden i avvikelshantering är självklar, eller är detta kanske en ytterligare en tjänst som bör definieras i servicenivåavtal?

Rekommendationer

Våra mest väsentliga rekommendationer med anledning av våra iakttagelser i denna granskning handlar om att:

- Regelverken kring IT-säkerhet utgör en bra grund men de kan förbättras genom förtydligande av hur arbetet kring avvikelshantering är kopplat till arbetet med informationssäkerhet. Det fordras dessutom ett fortsatt målmedvetet arbete med att medvetandegöra all personal om vikten av och sambandet mellan patientsäkerhet och informationssäkerhet. Det gäller också att arbetet med att utveckla rutiner fortsätter, inte minst kring ändringshantering.
- Det bör säkerställas att rutinerna kring ett regionalt MedControl omfattar IT-relaterade avvikelser och att alla berörda aktörer blir delaktiga. En framgångsfaktor är att arbetet följs upp och resultaten redovisas. Detta har politikerna ett särskilt ansvar att efterfråga.
- Regionservice och VGR IT i synnerhet bör utveckla rutiner och utse ansvariga för att hantera avvikelser i ett ärendes olika steg. Detta fordrar förmodligen också en särskild utbildning eller informationsinsats för Regionservice personal.
- I den beställar-/utförarmodell regionen har kan det vara lämpligt att Regionservice åtagande kring avvikelshantering skall betraktas som en tjänst, med en definierad servicenivå. Det ger en tydlighet där förväntningar omsätts i krav.
- Granskningen har visat på behovet av fler forum för dialog och samverkan samt bättre återkoppling för att åstadkomma en sömlös avvikelshantering över förvaltningsgränser och verksamhetsområden. Detta gäller tydligast mellan verksamhetschefer inom vården och VGR IT respektive VGR IT och Medicinteknik.

2. Inledning

2.1. Bakgrund

Skador i hälso- och sjukvården är ett område som får allt mer uppmärksamhet. En rapport¹ från Socialstyrelsen visar att risken att drabbas av skador i vården är relativt stor. Årligen drabbas ca 105 000 patienter av vårdskador som skulle kunnat undvikas. Socialstyrelsen har i sina mätningar kommit fram till att omkring 3 000 personer årligen avlider av vårdskador, sex gånger fler än i trafikolyckor.

Vården inom Västra Götalandsregionen har under en längre tid arbetat med att rapportera avvikelser och systematiska förbättringar. Förvaltningarna använder systemet MedControl för rapportering och uppföljning.

I ytterligare uppgifter² som redovisades Socialstyrelsen under våren 2009 att en femtedel av ett stort antal Lex Maria-fall som rapporterats under 2008 hade sin grund i datorer som inte fungerat som de skulle. Socialstyrelsen uppger också att det finns en underrapportering och problemen kan vara ännu större. Redan tidigare har det uppmärksammats, bl.a. genom revisionsrapporter i Västra Götalandsregionen och i media, att brister i IT-miljön har stor påverkan på patientsäkerheten.

Med ovanstående som bakgrund och med tillägg att datoriseringen i sjukvården ökar och IT blir alltmer verksamhetskritiskt är det väsentligt att också IT-verksamheten, systemleverantörer m.fl. inblandade aktörer omfattas av sjukvårdens arbete för att systematiskt minimera risker och öka säkerheten. En del av detta är att regionen har tagit fram nya regelverk för att styra och förbättra IT-säkerheten. Det gäller också att säkerställa att det finns en förståelse för patientsäkerhet i alla led samt att det råder en fungerande samverkan, uppföljning och gemensamma processer i arbetet med att utveckla rutiner och förbättra systematiken att undvika vårdskador som är IT-relaterade.

2.2. Syfte

Syftet med granskningen ”Kan IT-säkerheten påverka patientsäkerheten?” är att ge en bild av hur IT-säkerhetsarbetet kan påverka patientsäkerheten och att granska hur IT-relaterade avvikelser hanteras när de inträffar i Västra Götalandsregionen.

2.3. Genomförande och avgränsningar

Granskningen har genomförts i följande delar:

1. En förstudie med målsättning att ge en övergripande beskrivning av hur avvikelser i vårdverksamheten, relaterade till IT-systemen, rapporteras samt bilda oss en uppfattning om hur väl processen fungerar.
2. En fördjupad kartläggning och analys av hanteringen av fem IT-relaterade avvikelser som rapporterats i MedControl eller i VGR IT:s Servicedesk.

¹ Vårdskador inom somatisk slutenvård, 2008, Socialstyrelsen

² <http://www.vardfacket.se/Vanstermeny/Webbnyheter/Datorproblem-bakom-var-femte-lex-Maria-anmalan/>

3. En granskning av förutsättningar i IT-miljön som har påverkan på patientsäkerheten, bl.a.: styrning, riskhantering, rutiner, roller och ansvar, från tjänstemän till politiker.

Den fördjupade kartläggningen har omfattat fem av de avvikelser som identifierades under förstudien.

Avvikelser/ärenden i MedControl:

Kategori:

- | | |
|--|------------------------|
| 1. 08-3351 SÄS: Stopp i Melior. | Journalssystem, Melior |
| 2. 08-5007 SÄS: Stopp i Melior. | - ” - |
| 3. SU09-05460 Bilder kan ej ses. | Radiologi, WebAdapt |
| 4. SU09-05469 Kan ej komma åt röntgenbilder | - ” - |
| 5. 2009-06-11 SÄS Ambulansen Borås -
telefonlinjer är felkopplade | Telefoni |

Granskningen har omfattat följande utförarstyrelser och nämnders verksamhetsområden:

Nämnd:	Verksamhet:
Styrelsen för Sahlgrenska Universitets-sjukhuset	• Område 3, 5 och 6
Styrelsen för Södra Älvsborgs Sjukhus	• Hjärt- Lungkliniken, Borås • Medicinkliniken Skene • Ambulanssjukvården
Servicenämnden	• VGR IT
Regionstyrelsen	• Säkerhetsstrategiska avdelningen • Riskhanteringsrådet

2.4. Revisionskriterier

Granskningen tar sin utgångspunkt ur regionens interna regelverk och beslut samt tillämpliga föreskrifter bl.a. SOSFS 2005:12, Socialstyrelsens föreskrifter om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården samt SOSFS 2005:28 Socialstyrelsens föreskrifter och allmänna råd om anmälningsskyldighet enligt Lex Maria.

2.5. Metod och frågeställningar

Granskningen har genomförts genom dokumentstudier (se förteckning i bilaga 1) och 28 intervjuer med relevanta intressenter, för både regional ledning, företrädare för verksamhetsområden inom sjukvården, VGR IT m.fl.

Granskningen inleddes under maj-juni med en inledande kartläggning i syfte att få en övergripande förståelse för vilka rutiner och vilka delar av organisationen som involveras. Den andra, fördjupade delen genomfördes genom ett större antal intervjuer under september-oktober.

2.5.1. Intervjuer

Urvalet av intervjupersoner har gjorts av Ernst & Young tillsammans med Västra Götalands-regionens revisorer. Personer med följande roller har intervjuats:

Granskningens förstudie/kartläggning:

- Viceordförande Sjukhusläkarföreningen
- Säkerhetsdirektör, Regionkansliet, Säkerhetsstrategiska avdelningen
- MedControlansvarig SU område 5
- MedControlansvarig SÄS Akutvård
- Sektionschefer vid helpdesk på SU och SÄS

Företrädare för Riskhanteringsrådet samt ledning inom sjukvård och medicinteknik:

- Säkerhetsdirektör, Regionkansliet, Säkerhetsstrategiska avdelningen
- IT-direktör, Regionkansliet, IT-strategiska avdelningen
- Medicinteknisk chef, SÄS

Företrädare för projektet "Regiongemensamt MedControl" samt förvaltningarnas MedControlansvariga:

- Projektledare
- MedControlansvariga SU område 3, 5 och 6
- MedControlansvarig SÄS

Regionsservice:

- Enhetschef telefoniservice, Regionsservice
- Chef för VGR IT
- Sektionschefer för ServiceCenter, Göteborg respektive Sjuhärad, VGR IT
- IT-säkerhetsansvarig, VGR IT
- Incident Manager, VGR IT

Företrädare från verksamheter för utvalda avvikelser (se avsnitt 2.3):

- Systemägare och ansvariga för Melior på SÄS
- Systemansvariga för Bild och funktionsregister/WebAdapt på SU
- Ansvariga verksamhetschefer vid de avdelningar som rapporterat utvalda avvikelser
- Säkerhets-/informationssäkerhetsansvariga vid de avdelningar som rapporterat utvalda avvikelser
- Ansvariga för ambulanstransporter SÄS
- Ansvariga för telefoni SÄS

3. Iakttagelser från en förstudie

I syfte att öka förståelsen och ge underlag för en fördjupad granskning, genomfördes under maj-juni en begränsad kartläggning av hanteringen av IT-relaterade avvikelser i sjukvården och på vilket sätt VGR IT är involverade.

Kartläggningen avgränsades till SU område 5 och SÄS Akutvård. Intervjuer gjordes med MedControlansvariga och sektionschefer för Servicedesk på VGR IT. I syfte att få ett övergripande perspektiv genomfördes också intervjuer med Säkerhetsdirektören och 2:e viceordförande för läkarföreningen. Kartläggningen baserades på åtta huvudfrågor och väsentliga iakttagelser som redovisas nedan.

Förstudien revisionsfrågor	Iakttagelser/bedömning
1. Hur fungerar rutinen för rapportering av avvikelser?	• Det finns olikheter i rutiner för användningen av systemet MedControl mellan SU område 5 och SÄS akutverksamhet. • SU registrerar endast patientanknutna avvikelse rapporter medan det på SÄS registreras ärenden i MedControl i följande kategorier: Personalärenden, Patientärenden och Andra ärenden (IT, fastighet, miljö).
2. Hur väl fungerar rutinerna? Finns det ett mörkertal av händelser som inte rapporteras?	• Rutinerna fungerar bäst när det gäller personal- och patientärenden. • Mörkertalet upplevs vara stort. Det visas också i Läkarförbundets kampanjer. • Inrapportering av IT-relaterade ärenden fungerar sämre, uppskattningsvis till ~50% rapporteras.
3. Sker det någon klassificering eller prioritering av avvikelser?	• I MedControl görs klassificering av ärenden avseende allvarlighetsgrad (mindre-katastrofal) och sannolikhet för upprepande (mycket liten-mycket stor). • En patientavvikelse klassificeras dessutom på SU i 5 olika grupper: Vård och behandling, organisation, Regler och resurser, Bemötande, Medicinsk teknisk utrustning och Säkerhet. Prioritering av avvikelser görs enligt Socialstyrelsens modell enligt "Handbok för patientsäkerhetsarbete". • Ärenden som anmäls till VGR IT registreras av Servicecenter i ärendehanteringssystemet USD (Unicenter Service Desk). USD har ingen koppling till MedControl, vilket försvårar spårning av ärenden mellan systemen. • Servicecenter prioriterar ärenden med hänsyn till omfattning, antal berörda personer och system samt om incidenten kan hota patientsäkerheten.
4. Hur identifieras orsaken till avvikelser?	• Vårdverksamheterna analyserar orsakerna på ett liknande sätt. • Vid allvarliga avvikelser utför SU en händelseanalys m.h.a. ett speciellt granskningsprogram.
5. Vem beslutar om åtgärder och på vilka grunder? Vem följer upp resultatet?	• Beslut om åtgärder fattas på liknande sätt i verksamheterna. Utifrån orsaksutredarens slutsatser kan ärendeansvarig fatta beslut om åtgärder. • Allvarligare ärenden skall eskaleras till incidentchefen inom VGR IT. • Större avvikelser skall alltid rapporteras till säkerhetsdirektören och en uppföljning ske. Detta sker idag inte systematiskt.
6. Går det att urskilja vilka avvikelser som är förknippade med IT-användning?	• Det går inte att göra en urskiljning via kategorier av händelsetyper i MedControl. Vanligtvis har IT-relaterade avvikelser registrerats under kategorierna "Andra avvikelser eller Annat". • Den urskiljning som är möjlig, är om den som registrerat ärendet angett VGR IT som orsaksutredare. Då kommer emellertid inte de ärenden som skickats till IS-IT enhet eller Medicinteknik att komma med.
7. Hur sker sammanställning och uppföljning av inrapporterade avvikelser?	• Uppföljning och analys av inrapporterade avvikelser görs regelbundet och på olika nivåer i verksamheten. • Ansvar för uppföljning och analys är tydligt. • Återrapporteringen av avvikelser till nämnderna sker mindre frekvent.

Förstudien revisionsfrågor	Iakttagelser/bedömning
8. Vilken rapportering av incidenter/avvikelser sker till VGR IT?	- MedControl-ansvarig upplever att många kontakter VGR IT direkt utan att senare registrera ärendet i MedControl (detta är det vanliga förfarandet på SÄS). - De ärenden där VGR IT är angiven som mottagare i MedControl rapporteras automatiskt vidare till ansvarig person på VGR IT.
Övriga iakttagelser	- Uppdelningen på SU av IT-organisationen mellan SU IS/IT och VGR IT medför oklarheter för användare om vem som ska kontaktas när IT-problem uppstår. - VGR IT:s adjungerade representant i den lokala styrgruppen på SU för MedControl är sällan med på gruppens möten. - En av de intervjuade poängterar att det är en brist att VGR IT inte visar en tillräcklig förståelse för patientsäkerhet och inte har en helhetssyn över vilka olika IT-projekt som pågår och deras inbördes koppling. - Det finns en uppgivenhet och frustration i vårdverksamheten över brister i stödet från VGR IT, vilket uppges bidra till att färre avvikelser rapporteras. - Det är skillnader beträffande placering av ansvar i Hälso- och sjukvårdslagen i förhållande till kommunallagen. Enligt HSL är det verksamhetscheferna som har ansvaret för patientsäkerheten, men till mångt och mycket äger de inte lösningen på sina problem. - En uppfattning är att en lösning på regional nivå kan vara bildandet av ett riskhanteringsråd: Syftet är att behandla frågor som kommer upp i verksamheten på en högre nivå. Försök att skapa lokala riskhanteringsråd har tidigare gjorts. - Kommunikationen med systemleverantörerna bör förbättras för att öka patientsäkerheten. Vårdpersonalen måste vara mer delaktig i utformningen av systemet. - Ofta saknas manuella rutiner att använda vid systemavbrott.

Kartläggningen resulterade också i beslut av fördjupad granskning av fem av de IT-relaterade avvikelser som identifierats.

Kommentarer:

Förstudien pekar på:

- att det troligtvis finns ett stort antal avvikelser som inte registreras i MedControl, där IT-stödet är den bakomliggande orsaken.
- att det är svårt att säga exakt hur många avvikelser i MedControl som berör VGR IT.
- att klassificeringen av avvikelser beträffande allvarlighetsgrad sker på ett liknande sätt inom SU och SÄS.
- att det inte finns någon spårbarhet eller koppling mellan MedControl och det ärendehanteringssystem som VGR IT använder sig av.
- att det råder en viss begreppsförvirring gällande incident och avvikelse. Vården använder sig av begreppet avvikelse medan VGR IT använder sig av incident.
- att beslut om åtgärder vid en avvikelse fattas på ett liknande sätt inom SU och SÄS.
- att återrapportering till ansvarig nämnd sker i mindre utsträckning.

4. Iakttagelser från fördjupade granskningar

Andra delen av uppdraget har genomförts på två sätt; dels en fördjupad analys av hanteringen av fem IT-relaterade avvikelser som rapporterats i MedControl eller i VGR IT:s Servicedesk, dels en granskning av ett antal förhållanden i IT-miljön som har påverkan på patientsäkerheten såsom styrning, ansvar, riskhantering och uppföljning.

4.1. Huvudfrågor

Intervjuerna har för båda delarna baserats på följande huvudfrågor:

Kartläggning av fem IT-relaterade avvikelser i vården

1. Har regionens regelverk kring informationssäkerhet och angreppssätt kring riskhantering "före, under och efter" haft påverkan på de avvikelser som valts ut för granskningen?
2. Hur har styrningen tillämpats i samband de aktuella avvikelserna?
3. Vad hade gjorts preventivt i de enskilda fallen för att förhindra eller minska risken för det som inträffade? Vilka åtgärder vidtogs i samband med att avvikelserna inträffade?
4. Har VGR IT:s riktlinjer och rutiner fungerat och har kommunikationen fungerat inom VGR IT och i förhållande till andra aktörer
5. Är ärendena i MedControl utredda, besvarade och avslutade på ett ändamålsenligt sätt? Inom vilken tidsram har detta gjorts? Vilken uppföljning har skett?

Styrning, ansvar och riskhantering "Före-Under-Efter"

6. Är styrningen tydlig för hantering av IT-relaterade avvikelser?
7. Finns det en centralt framtagna rutin för hantering av IT-relaterade avvikelser samt hur skall samordningen mellan olika intressenter ske?
8. I vilken omfattning finns i den lokala verksamheten rutiner och planer (beredskap, reservrutiner, övningar, incidentutredningar) och hur tillämpades dessa i samband med de avvikelser som granskningen omfattar?
9. Hur fungerar hantering av IT-relaterade avvikelser i vården i relation till VGR IT:s rutiner för IT-incidenter? Finns det forum för att diskutera frågan?
10. Har utredningar eller uppföljningar lett till åtgärder, som en del av det systematiska förbättringsarbetet?
11. Hur kommuniceras resultaten ut till respektive verksamhet?
12. Hur sker rapportering till politiker? Har ansvariga politiker efterfrågat någon uppföljning?
13. Vilken uppföljning sker av åtgärdsplaner och de effekter som åtgärderna skall leda till?
14. Är ansvarsfördelningen, från tjänstemän till politiker, ändamålsenlig och kommunicerad? Hur har kommunikeringen gått till?
15. Förekommer otydligheter beträffande vilket ansvar berörda aktörer har, VGR IT m.fl.? Är ansvar, roller och arbetsfördelning klargjorda?
16. Vilken kunskap finns om patientsäkerhet hos berörda aktörer, VGR IT m.fl.? Vad görs för att skapa/bibehålla en medvetenhet?

4.2. Kartläggning av fem IT-relaterade avvikelser i vården

I syfte att ge en bild över hur rutinerna kring avvikelshantering fungerar i praktiken för IT-relaterade avvikelser som inträffat i vården, har granskningen följt fem utvalda ärenden från registrering, orsaksutredning, åtgärd, uppföljning och fram till de avslutats i MedControl. Urvalet av avvikelser har gjorts i samråd med företrädare för regionens revisorer.

I följande avsnitt ges kortfattad beskrivning över var och en av avvikelserna som underlag för att besvara huvudfrågorna (i avsnitt 4.2.4). En mer detaljerad redogörelse för var och en av händelserna redovisas i bilaga 2.

4.2.1. Två Meliorärenden

Två liknande avvikelser rapporterades i MedControl på SÄS under hösten 2008. Den första på medicinvårdsavdelningen i Skene i september 2008 och den andra drygt tre månader senare på lungvårdsavdelningen i Borås i december. Båda rapporterna avsåg stopp i journalsystemet Melior. Avbrotten förhindrade vårdpersonalens åtkomst till journalerna och möjligheter att dokumentera. Avbrotten varade under ett par timmar under nattetid och reservrutiner fick tas i bruk. Reservrutinerna innebar att journalen fick läsas i en speglad läskopia (s.k. titt-databasen) och journalanteckningar fick föras manuellt. Ingen patient kom till skada. Avvikelse rapporter upprättades och skickades i båda fallen till VGR IT.

Vid det ena tillfället försökte VGR IT flytta över databasen till en annan server och sedan fungerade systemet igen. Vid det andra tillfället vidtogs ingen direkt åtgärd.

Av intervjuerna framkom att problemen återkom vid flera tillfällen under hösten. Det var den lokala IS-IT-enheten som upptäckte orsaken. Ett script för att läsa ut data till ett register hade installerats under september. Detta script som kördes schemalagt en gång i veckan tog så mycket kapacitet att det uppstod låsningar i databasen. Åtgärder som vidtogs bestod både av att tidpunkten för scriptet ändrades och att leverantören Siemens engagerades för att ändra scriptet.

Ett hinder som bidrog till att det tog tid innan problemens omfattning uppdagades var bristen på dialog och återkoppling mellan den lokala IS-IT-enheten och VGR IT. VGR IT tog emot de flesta avvikelse rapporterna och supportärenden, men hittade inte problemet. De fel som identifierats och åtgärder som vidtagits sammanställdes i en särskild information till vårdavdelningarna senare under våren 2009.

4.2.2. Två WebAdapt-ärenden

Två avvikelser rapporterades på SU den 25 maj 2009. Båda avsåg störningar i åtkomsten till röntgen i programmet WebAdapt. Den ena av avvikelserna rapporterades på Hjärt- och kärlavdelningen på område 6. Det framgår av avvikelserapporten att störningen påverkade möjligheterna att ta beslut om en operation. Ärendet skickades till verksamhetschefen för röntgen för orsaksutredning, vilken besvarades tre månader senare. Orsaken visade sig vara en förändrad rutin som VGR IT vidtagit kring åtkomsten till VGRnet för externa leverantörer. Indirekt påverkade rutinen driftleverantören av bildarkivet så att de inte kunde växla IP-adresser till servrarna för bildarkivet utan att kontakta en person på VGR IT. Det andra avvikelseärendet inträffade när en patient var på remissbesök på Ortopedmottagningen i Mölndal. Avvikelse rapporten som skickades till VGR IT, blev aldrig besvarad och ärendet i MedControl var vid granskningen följaktligen ännu inte avslutad.

Av intervjuerna framgick att avvikelserna som rapporterades hade föregåtts av en rad liknande störningar under våren 2009. Det framstod tydligt att samverkan mellan VGR IT, medicinteknik och systemansvariga inte fungerar på ett effektivt sätt, vilket troligen bidrog till att det tog tid innan åtgärder vidtogs så att problemen kunde lösas. En av de åtgärder som bl.a. vidtogs var att stänga ned barnporrfiltret Netclean. En åtgärd som med facit i hand kanske inte hade någon effekt på problemet. Ett ytterligare problem som framkom vid intervjuerna är att vårdpersonalen känner sig osäker på till vem de skall skicka denna typ av avvikelser för orsaksutredningar.

4.2.3. Ett telefoniärende

Den 12 juni 2009 uppstod ett fel i telefonin till ambulansstationen i Borås. Patienter som avsåg att ringa en psykiatrisk öppenvårdsmottagning hamnade istället på ambulansstationen.

Felet som visade sig höra ihop med IP-telefonin rapporterades så snart det uppstod till VGR IT Servicedesk där det registrerades i deras ärendehanteringssystem VGRUSD, tillsammans med flera abonnenter som ringde om samma problem.

Vid de kontakterna vi hade inledningsvis per telefon med inblandad personal fick vi uppgift om att händelsen också föranlett en avvikelserapport i MedControl. Det visade sig senare att så inte varit fallet utan störningarna hade endast anmälts till Servicedesk.

4.2.4. Fem frågor i samband med kartläggningen

Fråga 1: Har regionens regelverk kring informationssäkerhet och angreppssätt kring riskhantering "före, under och efter" haft påverkan på de avvikelser som valts ut för granskningen?

Slutsats: Regionens policy och ramverk för säkerhetsarbete anger i korthet att avvikelser, som en del av säkerhetsarbetet, skall rapporteras, orsaken skall utredas, åtgärder vidtas och en återföring skall ske till fler än bara de som varit direkt inblandade, i syfte att öka kunskapen och därigenom minska risken att händelsen återupprepas igen. Ramverket beskriver att regionens säkerhetsprocess skall vara gemensam för att garantera att säkerhetsarbetet genomförs på likartat sätt. Säkerhetsprocessen består av tre delar, Före-Under-Efter, där avvikelserapportering är ett centralt moment i "Efter". Av både handledningen "Före-Under-Efter" och riktlinjerna för informationssäkerhet framgår att MedControl skall användas för att dokumentera alla avvikelser inklusive fel och störningar som kan uppstå i IT-miljön.

I sak innebär regionens regelverk att socialstyrelsens föreskrifter för avvikelshantering skall följas och att alla verksamhetsdelar skall använda ett gemensamt arbetssätt. Detta innebär att en avvikelse skall kunna hanteras över förvaltningsgränser och mellan olika yrkesgrupper.

Alla som intervjuats i samband med de fem avvikelser som kartlagts har uppgivit att de är medvetna om regionens regelverk, såväl som lagstiftning, men det finns behov av ytterligare utbildning/information. I praktiken fungerar inte alla delar i avvikelshantering på det sätt som främst lagstiftningen anger. Det gäller bl.a. MedControl-installationerna som hittills är förvaltningsspecifika och därigenom inte stödjer ärendeflöde mellan förvaltningar. Det gäller också inaktuella register över mottagare, i MedControl, som inte speglar aktuella förhållanden och ärendehantering övergår därför att hanteras i utskriven form. Det gäller även samverkan, inte

minst mellan VGR IT och medicinteknik/systemansvariga i samband med orsaksutredningar. Olika funktioner (telefoni och IT) inom Regionsservice har ännu inte infört ändamålsenliga rutiner för att hantera ärenden i MedControl och VGR IT registrerar fortfarande alla sina egna incidenter i VGRUSD, som är deras eget ärendehanteringssystem för att registrera alla inkommande felanmälningar, beställningar och förfrågningar från användare.

Fråga 2: Hur har styrningen tillämpats i de aktuella avvikelserna?

Slutsats: Av de fem aktuella avvikelserna har fyra rapporterats i MedControl. Bedömningen är att tre av dessa avvikelser i det stora hela hanterats enligt regionens regelverk. Även om det finns förbättringar att göra, främst avseende dialogen mellan olika instanser vid orsaksutredningarna, så följdes avvikelserna upp, åtgärder vidtogs och återrapporterades till de avdelningar som registrerat händelserna. De två Melior-ärendena på SÅS ledde dessutom, tillsammans med ytterligare liknande händelser, till en mer utförlig information och återkoppling om vidtagna åtgärder till flera avdelningar som använder Melior. Återkopplingen från orsaksutredningen beträffande WebAdapt gav inte vårdavdelningen som anmält händelsen någon bra förklaring till problemet eller hur det lösts.

För en av WebAdapt-händelserna på SU, som inträffade i maj 2009, har ingen orsaksutredning registrerats, utan avvikelserna stod fortfarande kvar som oavslutad i MedControl. Den femte händelsen (telefonin) ledde till en anmälan som ett supportärendet till Servicedesk och registrerades i deras ärendehanteringssystem VGRUSD. Avvikelsen rapporterades alltså inte i MedControl, vilket kanske hade varit rimligt med tanke på att det var en så tidskritisk funktion som en ambulansstation som var drabbad.

Fråga 3: Vad hade gjorts preventivt i de enskilda fallen, för att förhindra eller minska risken för det som inträffade? Vilka åtgärder vidtogs i samband med att avvikelserna inträffade?

Slutsats: Den viktigaste reservrutinen på SÅS vid störningar på Melior, är en spegling av databasen som uppdateras var 5:e minut, den s.k. tittdatabasen, som alla avdelningar som använder Melior har åtkomst till. Ytterligare en reservrutin vid avbrott i Melior är att alla anteckningar förs på papper på avdelningarna, så att de kan registreras i efterhand. Vid tillfällena när problem uppstod vidtog VGR IT inga åtgärder som egentligen löste problemen. P.g.a. att VGR IT och IS-IT enheten inte hade någon dialog om problemen i ett tidigare skede, tog det troligen onödigt lång tid innan de m.h.a. systemleverantören hade tagit fram en lösning.

När det gäller händelserna på SU och i WebAdapt användes inga reservrutiner, utan konsekvensen var risk för försenade operationer till följd av att beslutsunderlag saknades. Vi konstaterade att det trots allt finns reservrutiner på SU för avbrott i WebAdapt, som ger avdelningarna möjlighet att hämta ut bilder från röntgen, om WebAdapt inte fungerar. Rutinen anses dock inte vara funktionell, i synnerhet inte när det är mer bråttom att få fram bilder. Vad rutinen i praktiken innebär är heller inte känt av flera av dem som intervjuats. Även i samband med avvikelserna kring WebAdapt framstår att bristen på kommunikation, mellan VGR IT och i det här fallet RIT (Radiologisk Informations Teknik), bidragit till att det tog onödigt lång tid innan omfattningen av problemen framkom och lösningen med en ny rutin för ompekning av DNS togs fram.

Vad beträffar fel som drabbar IP-telefonin, har VGR IT numer tagit fram en förteckning över abonnemang som de skall kunna testringa om det skulle uppstå störningar i framtiden.

Fråga 4: Har VGR IT:s riktlinjer och rutiner fungerat och har kommunikationen fungerat inom VGR IT och i förhållande till andra aktörer?

Slutsats: VGR IT har inga dokumenterade riktlinjer eller rutiner för hur avvikelser skall hanteras som kommer till dem via MedControl. Både på SU och SÄS har VGR IT utsett en person som är mottagare av MedControl-ärenden. På SU är det den som är s.k. Incident Manager medan det på SÄS är enhetschefen för Servicedesk.

Däremot har VGR IT standardiserade processer med rutiner hur de skall ta emot, dokumentera, klassificera och hantera ärenden som anmäls via Servicedesk. VGR IT tar emot ett mycket stort antal sådana anmälningar och för dessa är det inte aktuellt att utföra orsaksutredningar, återkoppling och kunskapsåterföring om det inte handlar om ett frekvent kommande ärende. Ärenden som anmäls till Servicedesk behandlas som anmälningar av fel, som skall avhjälpas så snart som möjligt utifrån allvarlighetsgrad. VGR IT har också olika åtagande för olika system. När det gäller WebAdapt, som är ett gränssnitt mot användaren för olika system (röntgenjournal och bild), så tar VGR IT som regel emot ärenden, gör feldiagnos och vidarebefordrar sedan till systemansvarig eller support för respektive system, t.ex. leverantören GE som har hand om bildarkivet.

Fråga 5: Är ärendena i MedControl utredda, besvarade och avslutade på ett ändamålsenligt sätt? Inom vilken tidsram har detta gjorts? Vilken uppföljning har skett?

Slutsats: Varje förvaltning har angivit en målsättning hur lång tid ärendehanteringens får ta för de olika stegen i MedControl. Det tycks vara gemensam målsättning att ett ärende får ta ca 90 dagar, från det händelsen registreras till den följs upp av ärendansvarig och avslutas. Orsaksanalys och åtgärd bör ske inom 5 veckor.

För Melior-ärendena på SÄS tog det två respektive fem veckor innan VGR IT registrerade orsak, åtgärder och beskrev vilken uppföljning de ämnade göra. I det ena fallet angavs att "ständig uppföljning skall ske kontinuerligt" medan det i andra fallet inte ansågs vara aktuellt med en uppföljning. Ärendena avslutades ytterligare en respektive två månader senare. Enligt intervjuer har händelserna och åtgärderna diskuterats vid APT-möten på vårdavdelningarna.

Det tog tre månader för det ärende i WebAdapt på SU som uppdaterades i MedControl innan orsaksutredning avslutades. Det framgår inte om det gjordes en uppföljning och ärendet var inte avslutat när vår revision utfördes. Även på SU har händelserna och åtgärderna diskuterats vid APT-möten på avdelningarna. Ett problem man upplever där är att läkarna som registrerar händelserna inte tillhör avdelningarna, utan uppföljningen skickas från avdelningscheferna till verksamhetschefen som skall vidarebefordra informationen till läkarna.

Risker och rekommendationer:

- Det är en stor utmaning att få en rutin för avvikelshantering att fungera med så många inblandade aktörer som det är frågan om. En gemensam process och ett gemensamt system som stödjer processen förbättrar förutsättningarna. Vi har dock identifierat ett antal brister i hanteringen av de fem avvikelser som kartläggningen omfattat.

Rekommendationer: De största behoven av förbättring avser VGR IT som inte har inrättat riktiga rutiner eller definierat roller för att hantera ärenden i MedControl. Det gäller också i hög grad att förbättra formerna för samverkan vid orsaksutredningar mellan VGR IT, IS-IT enhet samt Medicinteknik.

För att få en större utväxling av de erfarenheter som görs i samband med avvikelshanteringen så borde också fler initiativ tas inom vården med målsättning att sprida erfarenheterna till fler än de vårdavdelningar som drabbats.

- En viktig iakttagelse är att både avvikelserna som drabbade Melior och WebAdapt var föranledda av förändringar i IT-miljön. I det ena fallet var det ett script som installerats som skulle förbättra underlag för statistik i vården. Scriptet orsakade oväntade och oönskade problem. I det andra fallet var det ändrade rutiner med syfte att öka säkerheten och kontrollen av extern åtkomst till regionens nät. Tyvärr förutsågs inte konsekvensen att ändringen skulle påverka de rutiner som användes för att öka driftsäkerheten av bildarkivet hos den externa leverantören.

Rekommendationer: Båda exemplen belyser vikten och behovet av strukturerade rutiner för ändringshantering, inklusive risk- och konsekvensutredningar.

4.3. Styrning, ansvar och riskhantering "Före-Under-Efter"

Fråga 6: Är styrningen tydlig för hantering av IT-relaterade avvikelser?

Slutsats: De regionala styrande dokument som beslutats av regionstyrelsen och som införts under de senaste två åren har en tydlig målsättning att avvikelshantering skall hanteras på ett likartat sätt i hela regionen. Alla slags avvikelser skall rapporteras i MedControl, d.v.s. inklusive de som är IT-relaterade. Enligt riktlinjen för informationssäkerhet är chefen för VGR IT ansvarig för att IT-relaterade incidenter avrapporteras i MedControl.

Iakttagelser:

De styrande dokument som utgör regionens ramverk för säkerhet har omarbetats under de senaste två åren. Regionens Säkerhetspolicy samt Ramverk och riktlinjer för säkerhetsarbetet beslutades av regionstyrelsen 2008 och så sent som 2009-06-23 togs beslut om den aktuella versionen av "Riktlinjer för informationssäkerhet i Västra Götalandsregionens verksamheter". De styrande dokumenten tar sin utgångspunkt ur lagkrav och Socialstyrelsen föreskrifter, främst Patientdatalagen (SFS 2008:355) och SOSFS 2005:12 Ledningssystem för kvalitet och patientsäkerhet m.fl. Riktlinjen för informationssäkerhet, som utgår från ISO/IEC 27002³,

³ ISO/IEC 27002, Ledningssystem för informationssäkerhet

handlar till stor del om behandlingen av information med stöd av IT och är därigenom mest relevant för denna granskning. Ytterligare väsentliga dokument i ramverket är den regionala strategin för säkerhetsarbetet i regionen (2008) samt en uppsättning broschyrer med utvalda väsentliga delar av ramverket, framtagna som stöd för intern information.

Dokumentet beskriver hur säkerhetsarbetet i regionen skall bedrivas med delprocesser, ”före, under och efter”. *Före* innebär förebyggande arbete, t.ex. riskanalyser, *Under* är processen för att hantera oönskade händelser när de inträffar och *Efter* omfattar det reaktiva arbetet, att följa upp i efterhand, dra erfarenheter som leder till förbättringar.

Både säkerhetsstrategin och broschyren ”Före-Under-Efter” (handledning för chefer hur säkerhetsarbete ska bedrivas i VGR) understryker att det är angeläget att regionen arbetar med ett likartat avvikelshanteringssystem och att regionen för detta ändamål har valt MedControl. Detta är något som emellertid inte framgår alls lika tydligt i riktlinjerna för informationssäkerhet.

Flera av de intervjuade delar uppfattningen att innehållet i de styrande dokumenten är bra, men i flera avseenden ännu inte har omsatts i praktiken och det återstår mycket förändringsarbete innan man kan se resultat. Den nya policyn och riktlinjerna är kommunicerade till samtliga nämnder som sedan har ansvaret för att dessa kommuniceras ut i organisationen och åtgärder vidtas. Av de intervjuade så uppger majoriteten att de känner till att dokumenten finns och vad de i stort innebär, men inte vad de i detalj innehåller.

De underliggande stödjande anvisningar och rutiner som tagits fram av VGR IT har däremot hittills inte blivit kommunicerade eller gjorts kända. Trots det förväntas de gälla alla, eftersom VGR IT har till uppgift att tillse att en stor del av kraven på IT-säkerhet uppfylls. Ett problem är att styrande dokument på olika nivåer är så utspridda, de borde samlas i en IT-säkerhetshandbok. Det krävs också mer utbildning och personal för att hantera detta och det är resurser som VGR IT inte har idag.

Risker och rekommendationer:

- Riktlinjerna för informationssäkerhet saknar en konkret anvisning om att IT-relaterade avvikelser och incidenter skall registreras i MedControl. Det är framför allt otydligt i avsnittet 10 Incident och händelserapportering, där begreppet avvikelse inte förekommer alls. Istället anges att incidenter inom IT skall rapporteras till närmaste chef, PUO eller säkerhetsdirektören. Risken är att de samlade regelverken kan uppfattas otydliga eller motsägelsefulla.

Rekommendationer: Riktlinjerna för informationssäkerhet bör revideras med avseende på att de på ett bättre sätt skall beakta regler för avvikelshantering. Det gäller främst avsnitt 10 Incident- och händelserapportering. Det vore även lämpligt att det i riktlinjen klargjordes om begreppet *incident* skall betraktas vara synonymt med *avvikelse* och eventuellt gavs en definition i avsnittet för begrepp och terminologi.

- Det är en risk att de regler och anvisningar som skall stödja övergripande dokument, och upprättas av främst VGR IT, inte är samlade eller kommuniceras på ett sådant sätt att de är tillgängliga och når dem som de är avsedda för på ett lämpligt vis. En ytterligare del av denna problematik och risk är att VGR IT har för lite resurser att ägna åt information och att genomföra utbildningar kring IT-säkerhet.

Rekommendationer: Med en samlad plats och regiongemensam IT-säkerhetshandbok på intranätet, kan VGR IT på ett bättre sätt tillse att all verksamhet följer de riktlinjer för IT-

säkerhet som regionen har beslutat om. Detta tillsammans med ökade resurser för VGR IT att bedriva utbildning kring rutiner och riktlinjer tillsammans med en förstärkning av personalstyrkan kan ge Regionservice en bättre möjlighet att utföra sitt uppdrag på ett ändamålsenligt sätt.

4.4. Rutiner

Fråga 7: Finns det en centralt framtagna rutin för hantering av IT-relaterade avvikelser, samt hur skall samordningen mellan olika intressenter ske?

Slutsats: Det finns ännu inte någon regional rutin för hantering av avvikelser och detta inkluderar då förstås även IT-relaterade avvikelser. Alla rutinbeskrivningar som finns är såldes lokala och hanteringen skiljer sig följaktligen åt, bl.a. är störningar inom IT inte alltid självklara att de alla skall rapporteras.

De avvikelser som registreras i MedControl hanteras och åtgärdas lokalt på verksamhetsnivå, inklusive de som orsakas av IT-stödet. Inte heller VGR IT:s Service desk som är lokalt placerade har några specifika rutiner för MedControl-ärenden, men de bekräftar att det finns ett behov av att detta upprättas. VGR IT håller på att ta fram en instruktion som skall användas för eskalering vid större IT-incident/driftstörning d.v.s. i säkerhetsprocessen "Under".

Fr.o.m. januari 2010 är målet att det skall finnas ett regiongemensamt MedControl. Målet är också att förbättra avvikelshanteringen genom bättre processer. Sökord och begrepp, t.ex. händelser, kommer omfatta IT, men arbetet med rutiner kring IT-relaterade avvikelser har inte kommit igång i projektet. Ett hinder för detta är att IT-organisationen inte tidigare använt MedControl.

Bristen på samordningen mellan olika intressenter är ett problem när en avvikelse skall analyseras och åtgärder tas fram. Detta har visat sig både genom intervjuer och genom de avvikelser som granskats mer ingående. Det finns ingen plan för hur detta skall utvecklas.

Iakttagelser:

Det finns inga regiongemensamma rutiner som beskriver specifikt hur IT-relaterade patientavvikelser skall hanteras. Vården involverar de personer inom VGR IT som är placerade på respektive sjukhus ungefär som man gjorde innan Regionservice bildades. När det gäller avvikelshanteringen så arbetar personalen inom VGR IT på olika sätt och de har inget regionalt utbyte eller erfarenhetsåterföring med varandra. Detta har sin förklaring i att MedControl, som infördes i början av 2000-talet, har använts på olika sätt av förvaltningarna och till viss del för rapportering av olika slags avvikelser.

Det som främst styr och håller samman hanteringen så att den är någorlunda enhetlig, är arbetsgången som finns i MedControl. Men skillnader finns, av utskrifter att döma skiljer det sig bl.a. åt vilka uppgifter som registreras i ett ärende beroende på vilken version av MedControl sjukhuset använder. Olika versioner ger också utrymme för olika tolkningar och vägval.

Under 2009 har IT-direktören och regionens chefsläkare för HSA initierat ett projekt med målsättning att införa en gemensam installation av MedControl för regionen, med en gemen-

sam databas och gemensamma rutiner. En projektledare från SkaS leder det operativa arbetet i projektet. Avsikten är att fr.o.m. januari 2010 skall alla slags avvikelser registreras i samma system, med gemensam nomenklatur för alla förvaltningar, vilket inkluderar Regionsservice med VGR IT. Projektet innebär också att rutiner och roller definieras och ensas och en regiongemensam systemförvaltning tillträder. Intervjuerna visar att det finns ett stort stöd för att enas om en regional process och användning av MedControl kring all avvikelshantering. Hittills har rutiner för IT emellertid inte haft något större utrymme i det regionala projektet.

Det finns en medvetenhet hos företrädarna för VGR IT om att det finns brister i deras egen hantering. De har inte några bra rutiner eller klara roller för att omhänderta ärenden i MedControl på ett enhetligt och bra sätt. En orsak är att personalen inom VGR IT inte fått utbildning kring MedControl och avvikelshantering. Dessutom har VGR IT själva hittills inte använt sig av MedControl för att rapportera "egna" IT-relaterade avvikelser, utan all dokumentation förs i VGRUSD.

VGR IT:s Incident Manager har under hösten 2009 lämnat ett förslag till ledningen för VGR IT, hur VGR IT skall bemanna roller för de olika arbetsstegen i MedControl. Hittills har inga beslut tagits, utan VGR IT följer det regionala projektet kring MedControl genom Regionsservice, där fokus så här långt har varit rutiner för avvikelser kring personal och säkerhet.

Risker och rekommendationer:

- En förutsättning när en rutin för hantering av IT-relaterade avvikelser skall utformas är att VGR IT är en självkostnadsfinansierad intern leverantör. I praktiken innebär detta att nya eller större ändringar i VGR IT:s åtagande bör definieras i ett servicenivåavtal och eventuellt prissättas. Därigenom blir det tydligt vilka förväntningar vårderna har på handläggningstider o.dyl. och vilka resurser VGR IT ges utrymme att avsätta för att tillgodose dessa.
- En ytterligare förutsättning att få en samordnad och fungerande process som också omfattar IT-organisationen är att VGR IT inför samma hantering som vårderna med analyser, riskhantering och metoder för utredningar samt ger den egna personalen relevant utbildning.

Fråga 8: I vilken omfattning finns i den lokala verksamheten rutiner och planer (beredskap, reservrutiner, övningar, incidentutredningar)?

Slutsats: Omfattningen av rutiner och planer för att hantera olika störningar/avbrott skiljer sig åt beroende på vilket IT-system som drabbats. På en central regional nivå tycks det saknas en fungerande organisation som kan hantera störningar av större dignitet.

Iakttagelser:

Omfattning av reservrutiner i vårderna, för att bedriva verksamheten vid bortfall av eller vid störningar i IT-systemen, varierar i hög grad. I vissa delar av verksamheten finns det, i andra delar inte alls, menar de personer som uttalar sig om ett regionalt perspektiv.

Här redovisas förhållandet för de förvaltningar och avdelningar som intervjuerna omfattat.

Reservrutiner för Melior på SÄS

Som tidigare redovisats i fråga 3 (avsnitt 4.2.4) har man inom SÄS en speglad version av Meliordatabasen, den s.k. tittdatabasen. Varje klinik har dessutom i uppdrag att ta fram en rutin där personalen skall övergå till att dokumentera för hand, om det blir avbrott i Melior. Vidare har verksamhetscheferna på SÄS tillsammans med VGR IT tagit fram prioriteringslistor för återstart efter oplanerade och planerade avbrott i systemen. På detta sätt vet VGR IT vilka system som är viktigast att få igång ur ett patientsäkerhetsperspektiv. Behoven av tillgänglighet till support och serviceavtal med systemleverantörer anses vara tillgodosedda. Någon rutin om åtkomsten till tittdatabasen inte skulle fungera finns enligt uppgift inte. Något som också saknas är rutiner för att göra regelbundna teståterläsningar från säkerhetskopior.

Reservrutiner för WebAdapt på SU

På intranätet för SU finns dokumentet "Reservplaner vid driftstörningar digitalasystem Adapt/RIS". Av planerna framgår att vårdavdelningar kan få hjälp av radiologin att få ut utskrivna bilder. Ett ytterligare alternativ är att bilder också kan finnas tillgängliga på respektive s.k. IMAC-station. Intervjuerna visar att ingen av de intervjuade verksamhetscheferna, vid de två klinikerna inom SU som rapporterat avvikelserna rörande WebAdapt, känner till någon dokumenterad rutin för hur avbrott skall hanteras. I samband med att WebAdapt infördes för ett par år sedan skall dock information ha getts till berörd personal, om möjligheterna att få tillgång till utskrivna bilder hos radiologin.

Reservrutiner för telefonin för ambulanssjukvården på SÄS

Inom ambulanssjukvården vid SÄS finns det enligt uppgift tydliga och välfungerande rutiner vid händelse av ett eventuellt avbrott i kommunikationen med SOS Alarm och akutmottagningen vid sjukhuset i Borås. När det gäller rutiner vid störningar för regionens telefonister handlar det ofta om att hitta alternativa kommunikationsvägar. Rutinerna ger olika möjligheter att koppla om linjer och styra om trafik beroende på kapacitet. Rutiner finns även för att nå ut med information om telefonin helt skulle gå ned.

En åtgärd efter den händelse som granskningen omfattat, var att en lista över samtliga abonnemang och användare av ip-telefoni inom SÄS-området upprättades, för att VGR IT snabbt skall kunna komma i kontakt med dem i fall felet skulle uppstå igen. Rekommendationen från Regionervice telefonienhet är att det bör finnas externa abonnemang på varje avdelning, i händelse av problem med växeln. Detta finns dock inte i någon större utsträckning.

Beredskap hos VGR IT

Inom IT-drift och kommunikation har VGR IT ett flertal reservrutiner. Vi har inte gjort någon kartläggning eller bedömning av ändamålsenlighet av dessa inom ramen för denna granskning.

VGR IT har en intern rutin och en organisation för att hantera incidenter som klassificeras som mer omfattande och allvarliga, s.k. "major incident". En del av incidentrutinen innebär att så snart gruppen aktiverats och de gjort en första analys informeras chefen för VGR IT, Chefen för Regionervice, säkerhetsdirektören samt IT-direktören. Det finns dock behov av att förbättra kompetensen i incidentgruppen och rutinerna för incidentutredningar behöver förbättras.

Regional beredskap

Det har tidigare funnits en regional IT-incidentorganisation som aktiverades när större och allvarliga oönskade händelser inträffade. Denna uppges dock inte ha fungerat tillfredsställan-

de, sedan Regionservice bildades och nyckelpersoner bytte roller och organisationstillhörighet. Uppfattningen är att denna organisation skulle behöva övas och hållas mer uppdaterad.

Risker och rekommendationer:

- Det finns en hel del reservrutiner som används och fungerar, men det finns också ett stort behov av att informera om och testa dem samt också se över vilka rutiner som behövs för att kunna hantera avbrott som kan innebära risk för patientsäkerheten.

Fråga 9: Hur fungerar hanteringen av IT-relaterade avvikelser i vården i relation till VGR IT:s rutiner för IT-incidenter och finns det forum för att diskutera frågan?

Slutsats: Medan vården rapporterar avvikelser i MedControl, med tillhörande rutiner för orsaksutredning och uppföljning, så registrerar VGR IT:s Servicedesk både supportärenden och incidenter i sitt ärendehanteringssystem VGRUSD. I praktiken finns det stora likheter men också olikheter i hur en avvikelse i rapporteras i dessa båda system.

Bristen på rutiner inom VGR IT, hur avvikelserapporter i MedControl skall behandlas och följas upp kännetecknas av att ärenden kommer till olika mottagare inom VGR IT och det är upp till enskilda handläggare att besvara eller skicka dem vidare. Därmed är det också otydligt var ansvaret för hanteringen är placerad inom VGR IT. VGR IT har hittills bara agerat som orsaksutredare och registrerar aldrig själva några nya avvikelser.

Iakttagelser:

VGR IT använder ett eget ärendehanteringssystem, VGRUSD för att registrera flertalet IT-relaterade kundärenden. Vanliga supportärenden registreras därför tillsammans med ärenden som kan höra ihop med patientavvikelser och IT-säkerhetsärenden. VGR IT har hittills aldrig själva registrerat någon incident som en avvikelse i MedControl och det är bara ett fåtal medarbetare inom VGR IT som är användare av MedControl.

I flera avseenden påminner hanteringen av ärenden i VGRUSD om hanteringen i MedControl. Ärenden registreras, klassificeras, åtgärdas, följs upp och skall kunna användas som erfarenhetsdatabas och källa till förbättringar. De primära syftena är dock olika. Medan MedControl i första hand används i säkerhetsprocessen "Efter" så används VGRUSD i första hand "Under", d.v.s. när en händelse, t.ex. ett fel, behöver åtgärdas.

När ett ärende tas emot och registreras i VGRUSD görs en prioritering av *påverkan* och hur *brådskande* det är enligt en 3-gradig skala. En 3:a innebär att det också skall genomföras en utredning i efterhand. Om händelsen bedöms påverka patientsäkerheten sätts en 4:a för *påverkan*.

VGR IT har sedan två år tillbaka hållit på att utforma och införa processer för sin interna verksamhet. Processerna baseras på ITIL⁴, som är ett etablerat ramverk som beskriver hur IT-

⁴ Information Technology Infrastructure Library

organisationer skall bedriva sin verksamhet genom standardiserade processer. Bland de första processerna som införts handlar det om att alla ärenden skall registreras och klassificeras och eskaleras för åtgärd, *Incident Management*. Enligt uppgift återstår fortfarande arbete att få processen att fungera som det är avsett. Alla ärenden registreras inte och de blir inte alltid avslutade.

Företrädarna för VGR IT bekräftar att de hittills inte hunnit anpassa sin organisation eller införskaffa kunskap och ta fram rutiner för att hantera s.k. MedControl-ärenden på ett lämpligt sätt. Även om VGR IT är en regionalt sammanhållen organisation så använder man, för att anpassa sig efter kunden, olika arbetssätt i uppdragen åt olika förvaltningar. Hittills har flertalet MedControl-ärenden från SU (och även Kungälvssjukhus) kanaliserats till VGR IT:s Incidentmanager medan de skickas till sektionschefen för Servicedesk på SÄS.

När ett ärende kommer till VGR IT i MedControl så saknar deras mottagare ofta kontaktvägar för att föra ärendet vidare. De saknar t.ex. uppgift om systemförvaltare för en del system och ibland är det Medicinteknik eller andra leverantörer som är svåra att identifiera.

VGR IT upplever att deras organisation är så "slimmad" att de inte hinner med att utföra orsaksutredningar i tid, eftersom de är efterfrågade att vara med på många ställen. Det blir mycket "brandsläckning" som upptar tiden.

Företrädare för vården menar att VGR IT ofta är bra på att avhjälpa tillfälliga problem. De är däremot sämre på att återkoppla till förvaltningarna under tiden de arbetar med problemlösning eller när lösningar tagits fram. De borde också kommunicera till andra som kan beröras på motsvarande sätt. VGR IT menar att de har en rutin när något händer, att hålla kontakt med IT-ansvarig för drabbad förvaltning samt använda sig av "IT-nytt" på intranätet för att nå ut med information till en bredare målgrupp.

Majoriteten av företrädarna för vården som intervjuats anser också att VGR IT ofta tar för lång tid på sig i samband med orsaksutredningar och vårdverksamheten efterfrågar också en betydligt bättre återkoppling på MedControl-ärenden som gått för utredning till VGR IT. Av intervjuerna framgår också att det många gånger är otydligt vem vårdavdelningarna skall ange som mottagare för en orsaksutredning när händelsen berör IT-systemen. De kan välja mellan VGR IT, systemansvariga på lokala IS-IT enheter eller Medicinteknik inklusive röntgen. Alla dessa får ärenden via MedControl, men VGR IT får troligen flest.

Forum för att diskutera hur rutiner kring avvikelshantering enligt MedControl fungerar i förhållande till VGR IT:s egna system sker inte på verksamhetsnivå enligt de intervjuer som genomförts i samband med granskningen av de fem utvalda avvikelserna. På central nivå finns vissa mötesplatser så som riskhanteringsrådet. Enskilda personer har enligt uppgift fört fram åsikter kring brister i rutinerna fungerar i förhållande till varandra till bl.a. IT-direktören och säkerhetsansvarig inom SÄS.

4.5. Uppföljning och rapportering

Fråga 10: Har utredningar eller uppföljningar lett till åtgärder, som en del av det systematiska förbättringsarbetet?

Slutsats: Ja, exempel har givits i samband med några av de fem avvikelser som kartlagts i denna granskning. Generellt kan man säga att förbättringar till följd av avvikelser oftast sker efter utredningar av flera sammanhängande händelser.

Iakttagelser:

Enligt svaren i intervjuerna är det sällan som enstaka avvikelser leder till några åtgärder, utan oftast så är det ett antal händelser som utgör underlag för utredningar som resulterar i att åtgärder vidtas.

Ett exempel är störningarna i Melior som pågick under en längre tid, men som resulterade i ett antal förbättringsåtgärder, främst:

- Utbyte till Meliorsservrar med bättre prestanda.
- En lösning av problemen med scriptet för överföring av statistik till Cognos.

Fråga 11: Hur kommuniceras resultaten ut till respektive verksamhet?

Slutsats: Återrapportering av avvikelser sker inom verksamheten främst via arbetsplatsträffar (APT).

Iakttagelser:

När ett ärende har avslutats i MedControl återrapporterar ärendansvarig, ofta tillika avdelingschef/enhetschef till berörd personalgrupp om behov föreligger. Den person som har upprättat avvikelser i MedControl får en återkoppling om vad som har hänt i ärendet när det har avslutats. Verksamheten upplever att VGR IT ofta tar lång tid på sig att återkoppla till verksamheten. VGR IT upplever att de inte alltid vet till vem de ska vända sig till i verksamheten.

Inom SÄS tog Melior-förvaltningen tillsammans med VGR IT och leverantören av journalsystemet, Siemens ett gemensamt grepp om den stora mängd inrapporterade händelser. Tillsammans har de utrett och vidtagit åtgärder för de vanligast förekommande ärendena. IS-IT enheten har därefter informerat verksamheterna om vilka åtgärder som vidtagits samt vilka områden som man fortfarande arbetar med. Detta har uppskattats av verksamheterna då de känner att de får återkoppling på sina problem.

Fråga 12: Hur sker rapportering till politiker? Har ansvariga politiker efterfrågat någon uppföljning?

Slutsats: Återrapportering av samtliga avvikelserapporter till ansvariga politiker skall ske en gång per år. Så tycks dock inte vara fallet i samtliga förvaltningar. Säkerhetsstrategiska avdelningen gör en sammanställning av samtliga nämnders redovisningar och rapporterar till regionstyrelsen årligen. IT-relaterade avvikelser särskiljs inte i denna rapportering.

Ansvariga politiker har inte efterfrågat någon uppföljning av patientsäkerhetsavvikelser.

Iakttagelser:

Verksamhetens bild är att Regionstyrelsen inte uttalar något större intresse för uppföljning av patientsäkerhetsavvikelser och i vilken utsträckning dessa är relaterade till IT.

Den praktiska avvikelshanteringen skall följas upp av respektive nämnd. Det är verksamhetschefernas ansvar och sker genom att MedControl-ansvariga tar fram en årlig sammanställning. Denna redovisning har, enligt uppgift inte skett i alla nämnder.

Ett sätt att uppmärksamma ansvariga politiker på hur brister i IT-system påverkar patientsäkerheten är, enligt en av chefsläkarna på SU, att anmäla avvikelser enligt Lex Maria eftersom dessa skall redovisas för ansvarig nämnd.

På en övergripande nivå rapporteras årligen förvaltningarnas säkerhetsarbete enligt en särskild mall framtagen av Säkerhetsstrategiska avdelningen. Även om den årliga redovisningen uppfattas som "trubbig" så har den för år 2008 redovisats av ca 80% av alla förvaltningarna. Säkerhetsstrategiska avdelningen har sedan uppgift att sammanställa nämndernas redovisning till regionstyrelsen. Denna redovisning innehåller ingen särredovisning över antalet avvikelser som är relaterade till IT. Det har heller inte uttryckts något intresse eller behov av att detta.

Fråga 13: Vilken uppföljning sker av åtgärdsplaner och de effekter som åtgärderna skall leda till?

Slutsats: Det finns inga bra rutiner, i några led i organisationen, för uppföljning av åtgärder och de effekter dessa leder till.

Iakttagelser:

För den enskilda avvikelserna är det ärendansvarig som har ansvaret att ärendet följs upp och avslutas efter orsaksutredning och åtgärd.

Varje ledningsnivå skall regelbundet följa upp rapporterade avvikelser och återföra erfarenheter i organisationen. SÄS analyserar halvårsvis inrapporterade avvikelser på klinik-, områdes- och förvaltningsnivå.

Möjligheterna att följa upp händelserna i MedControl får en hel del kritik. Det upplevs som ett väldigt tungt system, det är svårt att utläsa vem som äger enskilda ärenden och se en struktur. När ärenden inte fullföljs hela vägen så blir de kvar öppna hos ärendansvarig eller någon annan i kedjan.

Det är verksamhetschefernas ansvar att det sker en uppföljning av åtgärder och rapportering till nämnden, något som enligt uppgift inte sker i alla förvaltningar.

Uppföljning av effekter till följd av åtgärder är något som i stort sett inte sker alls.

4.6. Roller och ansvar

Fråga 14: Är ansvarsfördelningen, från tjänstemän till politiker, ändamålsenlig och kommunicerad? Hur har kommunikeringen gått till?

Slutsats: Fördelningen av ansvaret för säkerheten överensstämmer väl med krav som ställs i lagar och föreskrifter. I regionens policy, ramverk för säkerhetsarbete och riktlinjer för informationssäkerhet är ansvaret beskrivet på olika nivåer. Vår bedömning är att Regionstyrelsens och i nämndernas ansvar är tydligt framställt och de styrande dokumenten är formellt beslutade. Nämnderna har ansvaret för att de kommuniceras i förvaltningarna.

Hälso- och sjukvårdsutskottet har det delegerade ansvaret som vårdgivare medan Säkerhetsstrategiska avdelningen utför flera av uppgifterna som är beskrivna i Socialstyrelsens föreskrifter. Ansvarsfördelningen för tjänstemännen är också tydligt formulerad i riktlinjerna för informationssäkerhet. Dock har de ej funnit sin roll avseende avvikelsehantering fullt ut.

Iakttagelser:

Det finns ett antal lagar och föreskrifter som fastställer var ansvaret är placerat för patientsäkerhet och för informationshantering för god och säker vård.

SOSFS 2005:12 Socialstyrelsens föreskrifter om Ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården ställer krav på att vårdverksamheten skall ha rutiner för avvikelshantering och föreskriften anger att det är vårdgivaren som har det yttersta ansvaret för att ge direktiv och säkerställa att det i varje verksamhet finns ett ändamålsenligt ledningssystem med mål, organisation, rutiner, metoder och vårdprocesser som säkerställer kvaliteten. Definitionen för *vårdgivare* är en "fysisk eller juridisk person som yrkesmässigt bedriver hälso- och sjukvård".

Enligt SOSFS 2005:12 har verksamhetscheferna ansvar för att, inom ramen för vårdgivarens ledningssystem, ta fram, fastställa och dokumentera rutiner för kvalitetsarbetet samt formulera mål för verksamheten och se till att de uppnås. Ansvaret inkluderar också uppföljning och analys av verksamheten, så att åtgärder kan vidtas för att förbättra vården.

SOSFS 2008:14 Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården anger att det är vårdgivaren som har ansvar för att det finns en informationssäkerhetspolicy i verksamhetens ledningssystem. Vårdgivaren har också ansvar för att det finns rutiner för hur patientuppgifter hanteras och dokumenteras samt att journalanteckningar signeras. Vårdgivaren skall utse personer som ansvarar för informationssäkerhetsarbetet, vilket bl.a. innebär att riskanalyser och granskningar genomförs och förbättringsåtgärder vidtas. Arbetet skall utföras med följsamhet till svensk standard för informationssäkerhet och omfatta styrning av öppna nät, behörigheter, åtkomst till patientuppgifter, kontroll av åtkomst och säkerhetskopiering. Föreskriften fastställer också ansvaret för verksamhetschefen som omfattar kontroll av utdelade behörigheter samt uppföljning och information till personalen.

2008:1 1 Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården utgår från vårdgivarens ansvar för ledningssystem men ger också utrymme att ansvaret kan delegeras åt en verksamhetschef, för samtliga eller vissa områden som föreskriften omfattar, förutsatt att uppgifterna dokumenteras. Föreskriften anger att verksamhetschefen har ansvar för att de informationssystem som används för medicintekniska produkter är säkra. Utöver ordinarie avvikelshantering skall anmälan göras till Läkemedelsverket vid allvarliga händelser.

2006:544 Lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap är ytterligare en lagstiftning som har haft stor betydelse för definitionerna av ansvar som ges i regionens regelverk.

Fördelningen av ansvar i regionen:

Våra intervjuer och dokumentgranskning indikerar att kraven i lagar och föreskrifter i det stora hela har applicerats genom de regionala regelverk som beslutats under de senaste två åren.

I Västra Götalandsregionen har Regionstyrelsen delegerat det ansvar som en vårdgivare har enligt Socialstyrelsens föreskrifter till Hälso- och sjukvårdsutskottet. Flera av uppgifterna har delegerats till Säkerhetsstrategiska avdelningen och Säkerhetsdirektören inom Regionkansliet.

I regionens *Ramverk och riktlinjer för säkerhetsarbetet* är tyngdpunkten krishantering och ansvaret är beskrivet på en sådan nivå att det är Regionstyrelsen som ansvarar för att en god säkerhet upprätthålls i regionen. Nämnd, styrelse och bolag har det yttersta ansvaret inom respektive verksamhetsområde och förvaltningschefen eller VD:n ansvarar för att upprätta en organisation för ett systematiskt säkerhetsarbete. Ett regionalt Riskhanteringsråd skall samordna arbetet med riskhantering och säkerhet. I ramverket beskrivs sedan i ett längre avsnitt hur säkerhetsarbetet skall genomföras och inom vilka områden säkerhetsåtgärder skall vidtas.

Av *Riktlinjer för informationssäkerhet i Västra Götalandsregionen* framgår att Regionstyrelsen har ansvar för att samordna, leda och utveckla säkerhetsarbetet. Regionstyrelsen har också ett ansvar att följa upp hela regionens säkerhetsarbete och detta sker årligen genom rapporter från nämnderna. Det är Regionstyrelsen som beslutat om regionens nya riktlinjer för informationssäkerhet, i vilka olika roller och dess ansvar är beskrivet. Regionala beslutade regler och riktlinjer kommuniceras normalt från regionledning via nämnderna, som sedan har ansvaret för att dessa delges ända ut i förvaltningarna. På detta sätt har bl.a. de olika dokument som ingår i säkerhetsramverket kommunicerats.

Under 2009 har ett *Riskhanteringsråd* bildats med syfte att samordna arbetet med risker av övergripande och gemensam karaktär. Riskhanteringsrådet har hittills haft två möten och de har ännu inte satt någon agenda. Det kan enligt Säkerhetsdirektören, som är sammankallande, bli ett forum för att diskutera hur avvikelshantering skall utföras, följas upp och utvecklas. Riskhanteringsrådet har ingen beslutanderätt, men med nuvarande bemanning har deltagarna, i egenskap av sina roller, var för sig ett relativt långtgående mandat.

Det är i första hand Säkerhetsstrategiska avdelningen inom Regionkansliet som har huvuduppgift att driva utvecklingen. När det gäller utveckling av IT-säkerheten så sker detta vanligtvis i dialog med IT-strategiska avdelningen.

I *Riktlinjer för informationssäkerhet i Västra Götalandsregionen* står det mycket lite om avvikelshantering och hur ansvaret är placerat för detta. I avsnittet kring incident- och händelserapportering (avsnitt 10) anges att incidenter omgående skall rapporteras till närmaste chef och om det är olämpligt till ansvarig för intern kontroll eller säkerhetsdirektören. Den enda

rollen som i riktlinjerna som har ett uttalat ansvar för att IT-relaterade incidenter avrapporteras i MedControl är Chef för VGR IT samt systemägaren som ansvarar för analys och uppföljning av informationssäkerhetsincidenter i sitt system.

Risker och rekommendationer:

- Det finns behov att revidera riktlinjer för informationssäkerhet och förtydliga förutsättningarna för hur arbetet kring avvikelshantering är kopplat till arbetet med informationssäkerhet.

Fråga 15: Förekommer otydligheter beträffande vilket ansvar berörda aktörer har, VGR IT m.fl.? Är ansvar, roller och arbetsfördelning klargjorda?

Slutsats: Riktlinjerna för informationssäkerhet ger tydliga instruktioner om hur ansvaret skall fördelas. Ansvar och roller behöver kommuniceras och tydliggöras bättre. Vidare behöver formerna för samverkan mellan dels VGR IT och vårdverksamheten och dels VGR IT och Medicinteknik utvecklas ytterligare.

Iakttagelser:

En av de brister som de flesta som intervjuas framhåller är den otillräckliga dialogen och samverkan mellan VGR IT och vårdverksamheten. Framför allt är det företrädare för vårdverksamheten som saknar forum kring systemfrågor, de har ett funktionsansvar men saknar inflytande på tekniken. Enligt riktlinjerna för informationssäkerhet skall verksamheten klassificera informationen i syfte att ge informationen i sig ett lämpligt skydd. Det är något som enligt uppgift ännu inte genomförs i tillräcklig omfattning.

Dock tycks det vara få inom vårdverksamheten som vet att VGR IT inte äger alla frågor, eller har möjlighet att rätta till alla problem inom IT-miljön. Exempelvis är det MFT⁵ inom SU som ansvarar för driften av WebAdapt och inte VGR IT. För Bild- och funktionsregistret (BFR) är det GE (General Electric) med Volvo IT som underleverantör som svarar för drift och support.

MedControl stöder i dagsläget inte alla roller och mottagare som är erforderligt för att kunna vidarebefordra och delegera ärenden inom avvikelshanteringsprocessen. För en användare kan det innebära svårigheter att välja en mottagare av ett ärende i avvikelseprocessen. Det finns också mottagare som inte alls är upplagda och de får då ärendena i form av utskrifter, t.ex. handläggare inom VGR IT och telefoniansvariga på Regionservice m.fl.

Riktlinjerna har också ett särskilt avsnitt (6.5 Samarbete med medicinteknik) som beskriver vikten av samarbete mellan ansvariga för medicinteknik och ansvariga för tekniska lösningar inom IT-området. Det är IT-levererande part, d.v.s. VGR IT tillsammans med verksamhetsansvariga för medicinteknik som har ansvar att detta samarbete utvecklas. Det är dock mellan

⁵ Medicinsk Fysik och Teknik

flera aktörer det saknas en bra dialog. I synnerhet finns det en stor potential att överbrygga gapet mellan Medicinteknik och IT. Det är mycket inom Medicintekniken som är systemrelaterat och i praktiken har stora likheter och överlappar det som hanteras av VGR IT. Det gäller applikation- och serverdrift, kommunikation o.s.v. Det är uppenbart att det rör sig om två olika kulturer där de som arbetar med Medicinteknik har en betydligt större kunskap om och närmare relation till vårdverksamheten. Av det skälet tillåter t.ex. heller inte Radiologin att VGR IT sköter driften av deras system. Gränsskiktet eller snarare gråzonen mellan Medicinteknik och IT utgör ett hinder. De har i mångt och mycket en gemensam infrastruktur men olika rutiner, men organisatoriskt finns inte den samverkan som troligen bör eftersträvas. Initiativ till att skapa en bättre dialog mellan de två aktörerna har tagits både inom SÄS och SU.

Även på regional nivå finns önskemål om att bättre samarbetsformer infrias. På regional nivå har IT-strategiska avdelningen ansvaret för att det sker en utveckling av tekniken av regionens IT-säkerhet medan VGR IT ansvarar för att den löpande upprätthålls. Samarbetet mellan IT-strategiska och VGR IT uppges dock inte löpa av sig själv, utan det fordras som regel att andra intressenter driver på.

Risker och rekommendationer:

- Vikten av att kommunicera och tydliggöra ansvaret för olika rollinnehavare är stor. Det finns också ett behov av att på ett strukturerat sätt definiera de olika IT-systemens påverkan på patientsäkerheten och hur dessa skall hanteras. Genom att föra en diskussion så väl på regionnivå som på verksamhetsnivå kring frågan och göra de klassificeringar av information som beskrivs i riktlinjerna för informationssäkerhet, så ges underlag för att skapa rutiner för hur IT-avvikelser skall prioriteras och hanteras av både verksamheten och av VGR IT.
- Det finns brister i samarbetet mellan ansvariga för VGR IT och för Medicinteknik. Det är nödvändigt att detta utvecklas. Detta är något som tydligt framgår av de nya riktlinjerna för informationssäkerhet. Det finns behov av att klargöra ansvarsområden och hur samverkan skall bedrivas både på ledningsnivå och på mer operativ nivå. Det behöver t.ex. avgränsas hur Medicintekniken skall omfattas av samma krav som övriga IT-system, med bl.a. godkännande av VGR IT. Samtidigt behöver det klargöras vilka IT-systemen som kommer att omfattas av Läkemedelsverkets förslag till klassificering som kom våren 2009.

Fråga 16: Vilken kunskap finns om patientsäkerhet hos berörda aktörer, VGR IT m.fl. ? Vad görs för att skapa/bibehålla en medvetenhet?

Slutsats: Kunskapen hos hälso- och sjukvårdspersonalen uppges vara hög. Detta stöds av ett lagkrav. VGR IT har kunskap om patientsäkerhet men saknar till viss del förståelsen för hur förändringar i IT-miljön påverkar vården.

För hälso- och sjukvårdspersonalen görs kontinuerliga insatser för att upprätthålla kunskapen om patientsäkerhet.

Iakttagelser:

Kunskapen om patientsäkerhet uppges vara generellt hög hos hälso- och sjukvårdspersonalen. Detta är också ett lagkrav och det är verksamhetschefens ansvar att tillse att personalen är utbildad och hålls informerad. Under senare år har ny lagstiftning kommit som reglerar hur vården skall styra och hantera elektroniskt bearbetad information. Det gäller t.ex. information om patientdatalagen (SFS 2008:355) och Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) som ställer nya krav på vårdgivarnas arbete med att bygga upp säkra rutiner för hantering av patientuppgifter, tilldelning av behörigheter, kontroll av loggar o.s.v. För att öka antalet inrapporterade avvikelser påminner ansvariga chefer och MedControl-ansvariga löpande personalen om vikten av att skriva avvikelserapporter. Inom SU har särskilda kampanjer genomförts som visat att informationen resulterat i fler avvikelserapporter under en tid.

När det gäller kunskapen om och förståelsen för patientsäkerhet inom VGR IT så ger intervjuerna en mycket mer blandad bild. Avdelningschefer, verksamhetschefer och chefsöverläkare inom SU och SÄS har inte en gemensam uppfattning. Generellt kan man säga att ju närmare den praktiska vårdverksamheten man kommer så är uppfattningen att VGR IT:s kunskap om patientsäkerhet är alldeles för låg, medan ledningen oftare uppfattar att innebörden av patientsäkerhet är väl förankrad hos personalen inom VGR IT. Däremot är det en allmän uppfattning att VGR IT ofta visar brist på helhetssyn och de ser inte hur förändringar i IT-miljön kan påverka vården. Det har exempelvis hänt mer än en gång att patientsäkerhetsfrågor förbisetts i samband med VGR IT:s regionala IT-projekt. Ett exempel på ett sådant tillfälle är den ändrade rutin för ompekning av DNS som orsakade störningar på Webadapt. Andra exempel är DHCP-projekt, utbyte av datorer och förändrade bastjänster. ”De borde göra bättre konsekvensanalyser före” är en av kommentarerna från vårdverksamheten.

I stort sett är alla, inklusive VGR IT:s egna företrädare, också överens om att VGR IT har låg kunskap om regionens rutiner för avvikelshantering och MedControl samt vad som förväntas av dem i dessa ärenden.

Risk och rekommendationer:

- Företrädare för vårdverksamheten är särskilt kritiska, men samtidigt noterar vi att det inte tycks ske många initiativ till dialog utan diskussioner kring patientsäkerhet förs i hög grad inom och mellan företrädare för vården och personer inom säkerhetsorganisationen. Genom att etablera forum för dialog mellan vårdverksamheten och VGR IT kan förståelsen hos VGR IT öka och därmed också trovärdigheten i vårdverksamhetens ögon.

Göteborg den 8 december 2009

Johan Elmgren

Sofi Larsson

Bilaga 1 Dokumentförteckning

Vi har tagit del av följande dokument vid vår granskning:

Regiongemensamma

- Policy för säkerhetsarbetet, 2008-02-11
- Före-Under-Efter – Sammanfattning av policy, ramverk och strategi för säkerhetsarbetet i Västra Götalandsregionen, 2008-06-01
- Ramverk och riktlinjer för säkerhetsarbetet, 2008-03-11
- Riktlinjer för informationssäkerhet i Västra Götalandsregionens verksamheter, 2009-07-08
- Regional strategi för Säkerhetsarbetet i Västra Götalandsregionen 2008-2011, 2008-06-30
- Presentation om avvikelserapportering
- Regiongemensamt MedControl – projektdirektiv för att skapa ett regiongemensamt avvikelshanteringssystem, 2004-0-06
- Odlä säkerhetskultur – Information från säkerhetsstrategiska avdelningen VGR
- Förteckning över systemägare för regiongemensamma informationssystem samt funktionsägare – Regionservice
- Minnesanteckningar från möte med Riskhanteringsrådet
- Avvikelsehantering – att lära av misstagen – revisionsrapport från 2008
- Diverse artiklar om patientsäkerhet ur Läkartidningen, GöteborgsPosten och Dagens Medicin

VGR IT

- Utdrag ur handbok VGR IT IT-incidentorganisation
- Förslag till hantering av avvikelseärenden i MedControl samt incidentrapportering internt inom VGR IT – Regionservice

SU och SÄS

- Utdrag ur MedControl
- Rutiner för felsökning och felanmälan inom Radiologin SU
- Avvikelsehantering – riktlinje för Södra Älvsborgs Sjukhus och Primärvården Södra Älvsborg
- Rutin för utredningsgrupp för tillbud och negativa händelser med Medicintekniska produkter – SÄS
- Säker vård på SÄS – analys av avvikelser inom Hjärt-Lungkliniken första halvåret 2009

Bilaga 2 Redogörelse för fem avvikelser

4.6.1. Två Melior-ärenden

Två Melior-ärenden registrerade i MedControl		
Var? När? Status?	Medicinvårdsavdelningen., Skene, SÄS. 2008-09-08. Ärendet avslutat.	Lungvårdsavdelning, Borås, SÄS. 2008-12-19. Ärendet avslutat.
Händelse- beskrivning	Mellan 04.00 och 06.00 på natten går det ej att komma åt Melior. Detta hade enligt avvikelserapporten även hänt vid ett tidigare tillfälle men då ej rapporterats in i MedControl. Patient är inte direkt inblandad. Ärendet vidarebefordras till VGR IT:s avdelningschef för orsaksutredning.	Efter kl 03.00 går inte journalprogrammet Melior att öppna, programmet hänger sig direkt även efter omstart. Detta gäller samtliga datorer på avdelningen. Tittdatabasen går att nå från två av avdelningens datorer. Patient är inte direkt inblandad. Utan ett fungerande Melior tar det mer tid att ta fram underlag för ordination av mediciner, anteckningar får göras för hand och det går inte att göra signeringar. Ärendet vidarebefordras till VGR IT:s avdelningschef för orsaksutredning.
Orsaks- utredning	2008-09-19 Sektionschefen för VGR IT Servicecenter registrerar att det varit stopp i databasen.	2009-01-26 Vad som orsakat problemet är fortfarande okänt när sektionschefen för VGR IT Servicecenter registrerar att det varit ett felmeddelande i databasen och att leverantören av systemet kommer att kontakts om problemet uppstår igen. Frågan skall tas upp med förvaltaren av Melior.
Åtgärder	2008-09-19 Sektionschefen för VGR IT anger att databasen flyttades till en annan server och sedan fungerade systemet igen.	2009-01-26 Sektionschefen för VGR IT Servicecenter registrerar att åtgärd är utförd. <i>Någon åtgärd till följd av just detta ärende blev inte aktuell.</i>
Uppföljning	2008-09-19 Sektionschefen för VGR IT anger att en ständig uppföljning skall ske tillsammans med leverantören och förvaltaren (IS-enheten).	2009-01-26 Sektionschefen för VGR IT Servicecenter registrerar att någon uppföljning inte är aktuell.

Två Melior-ärenden registrerade i MedControl		
	Avdelningen har inte vidtagit några åtgärder till följd av avvikelsen.	
Avslut	2008-10-03 <i>Ingen information</i>	2009-03-19 <i>Ingen information</i>
Beredskap "Före och under"	Inom SÄS finns det en rutin för hur verksamheten skall agera vid avbrott i Melior. Om systemet inte fungerar skall personalen alltid ha tillgång till en s.k. tittdatabas som uppdateras var 5:e minut, där bl.a. all medicin som är ordinerad framgår. Eventuell ordination som sker medan systemet ligger nere skall dokumenteras för hand och föras in i Melior vid ett senare tillfälle. Så gjordes även i aktuella ärenden. Tittdatabasen fungerar som deras säkerhetsventil. Rutinen upplevs som välkänd inom verksamheten. Någon rutin för om tittdatabasen inte skulle finnas tillgänglig finns inte enligt intervjuade. I ett sådant läge får personalen använda sin yrkeskunskap och göra bedömningar i varje enskilt patientärende. Någon övning i ett sådant läge har inte genomförts.	
VGR IT Rutiner Kommunikation internt/med andra	Upplevelsen från avdelningscheferna är att VGR IT normalt avhjälper problem snabbt, men att återkopplingen till avdelningen via MedControl sedan kan dröja längre tid. <i>För de aktuella avvikelserna tog det drygt en vecka respektive en dryg månad. Målet på SÄS är att orsaksutredningen sker inom 3 veckor från att en avvikelse registreras och 6 veckor från att den är skriven ska åtgärd vara gjord eller planerad. Tre månader från att avvikelsen registrerades ska uppföljning göras.</i> Svaren som VGR IT lämnar i MedControl är ofta inte speciellt informativ, utan mer ett konstaterade att de har gjort något. Verksamheten har svårt att värdera om det är en tillräcklig åtgärd för att en liknande händelse inte ska inträffa igen. Senare inrapporterade avvikelser gällande samma problem har dock innehållit tydligare återkoppling	
Kommentarer	Avbrott av Melior nattetid var relativt vanligt förekommande i slutet av 2008 och i början av 2009. Ett flertal avvikelser rapporterades in och personalen vid avdelningarna uppmuntrades också till att rapportera in alla händelser för att visa på problemets dignitet. En av verksamhetscheferna hade minst sju liknande avvikelser under samma period. Troligtvis inträffade betydligt fler händelser som inte rapporterades i MedControl. Anledningen till detta är att personalen i vården tröttnar på att registrera samma slags ärenden flera gånger när de inte ser några resultat. Skulle en patient vara direkt inblandad, så skulle det däremot bli en rapport, menar de. Det var sjukhusets lokala IS-IT enhet (Informationssystem IT) på SÄS som kom fram till orsaken och senare en lösning till problemen. Intervjuerna visar dock att ansvariga systemförvaltare inte kände till de aktuella avvikelserna, utan problemen uppdagades för dem genom andra avvikelserapporter som kom till dem först runt årsskiftet. De kom till slut på att problemen berodde på en överföring till SAI (Sjukhusets antibiotika- och infektionsregister). Överföringen, som startades september 2008, kördes en gång per vecka tog mycket kapacitet och orsakade låsningar i några tabeller. Siemens kopplades in och som första åtgärd flyttades tidpunkten för indexeringen och scriptet för utsökning fick sedan skrivas om. Flertalet Melior-ärenden hamnar hos VGR IT för orsaksutredning och en mindre andel hamnar hos IS-IT enheten. En iakttagelse är att för en användare kan vara oklart vad som är applikations- respektive teknikproblem och därmed är det osäkert vem som skall vara orsaksutredare för ett ärende i MedControl.	

Två Melior-ärenden registrerade i MedControl	
	En slutsats av detta är att VGR IT initialt hanterade problemen själva, genom tillfälliga lösningar. Och de uppdaterade inte systemförvaltaren på felen som uppstod. Det tog troligtvis därför onödigt lång tid innan VGR IT och IS-IT enheten tillsammans med systemleverantören gemensamt analyserade problemen, som ledde fram till en lösning. Återkoppling till vårdpersonalen har framför allt vid skett via APT-möten. På klinikledningsnivå har även diskussioner kring systembekymmer förts. Deras möjlighet att påverka systembrister upplevs vara att påpeka problemen för VGR IT. En av verksamhetscheferna har också framfört sina åsikter till säkerhetschefen inom SÄS, som i sin tur fört det vidare upp i organisationen.

4.6.2. Två WebAdapt-ärenden

Två WebAdapt-ärenden registrerade i MedControl		
Var? När? Status?	Hjärt- och kärlavdelning SU, Område 6. 2009-05-25. Ärendet avslutat.	Ortopedmottagningen Mölndal, SU, Område 3 2009-05-25. Ärendet ej avslutat (2009-09-24).
Händelse- beskrivning	Åtkomsten till röntgenbilder via WebAdapt är ej tillgängligt ifrån någon av de datorer som finns tillgängliga på avdelningen. Patienten var inte direkt involverad, men effekten blev att beslut om eventuell operation dagen därpå inte kunde fattas vid det tillfället och patienten riskerade att inte få adekvat information vid inskrivning samt att operationen riskerade att bli uppskjuten. Ärendansvarig på mottagningen skickar ärendet till Verksamhetschef för Röntgen på Sahlgrenska för orsaksutredning.	Röntgensystemet WebAdapt är ej tillgängligt på mottagningen. Den som rapporterar i MedControl har utfört de instruktioner som man ska göra om systemet inte fungerar, enligt anvisningar på VGR IT:s hemsida, det fungerar fortfarande inte. Patienten är direkt involverad, är på remissbesök på avdelningen. Användare har haft samma problem 5 dagar tidigare och även dagen innan. Läkaren har haft långa väntetider alt. inte kunnat titta på röntgenbilderna före operation. Avdelningschefen, som är ärendansvarig på mottagningen skickar ärendet till Verksamhetschef VGR IT för orsaksutredning.
Orsaksutredning	2009-06-29 Kvalitetskoordinator 2009-08-27 Verksamhetschef Röntgen Återrapporteringen från radiologin har gjorts i två steg av två personer, dels gavs en återkoppling drygt en månad efter att avvikelserna skickades och sedan kom ytterligare återkoppling två månader senare. I MedControl framgår inte vilken information som rap-	<i>Information saknas,</i> <i>VGR IT har inte registrerat någon information i MedControl.</i>

Två WebAdapt-ärenden registrerade i MedControl		
	porterades in vid vilket tillfälle. De beskriver att orsaken till problemen är hinder med att växla IP-adresser till BFR⁶ till bildarkivet. Beskedet som ges är att radiologin inte kan åtgärda problemet, utan att ansvaret vilar på VGR IT samt BFR:s förvaltning.	
Åtgärder	2009-08-28 <i>Information saknas.</i> Enligt orsaksutredningen har VGR IT nu bemanning för att kunna byta ip-adresser dygnet runt. Det pågår ett arbete med att komma tillrätta med problemet. Vem som håller i detta arbete framgår ej.	<i>Information saknas.</i>
Uppföljning	<i>Datum saknas</i> Konsekvensen av den inträffade händelsen blev enligt MedControl längre väntetid för patienten. Inga åtgärder vidtogs på avdelningen. Enligt intervju med avdelningschefen är återkopplingen från radiologin inte tillfredsställande. Verksamheten förstår inte vilka insatser som skett för att åtgärda det uppkomna problemet och de vet inte hur de ska hantera återkopplingen.	<i>Information saknas.</i> <i>Vid intervjuerna påtalar avdelningschefen och MedControl-ansvarig inom område 3 att de upplever att återkopplingen från VGR IT har stora brister.</i>
Avslut	2009-08-28 Ärendet avslutas.	<i>Ärendet är inte avslutat</i> <i>Ärendet är ännu inte avslutat utan ligger som ett öppet ärende.</i> <i>Det innebär att ärendeansvarig automatiskt får påminnelser om att det finns ett öppet ärende. Ärendeansvarig har skickat påminnelserna vidare till verksamhetschefen och till VGR IT.</i>
Beredskap "Före och under"	Någon bra rutin för hur avbrott i WebAdapt skall hanteras finns enligt avdelningarna inte. Enligt verksamhetschefen uppmuntras läkarna att gå till röntgen för att via deras system kunna titta på röntgenbilderna, eller få en utskrift, men representanter för avdelningen menar att det inte utgör ett reellt alternativ, då röntgen inte har resurser för detta. Enligt verksamhetschefen på område 6 skall inte en operation genomföras om läkaren inte har tillgång till röntgenbilderna. Dock finns ingen	

⁶ BFR-förvaltningen står för bild- och funktionsregistret.

Två WebAdapt-ärenden registrerade i MedControl	
	tydlig instruktion för hur läkarna ska hantera en situation där de inte har tillgång till röntgenbilderna.
VGR IT Rutiner Kommunikation internt/ med andra	Ärenden har mottagits av VGR IT. Ansvarig har dock inte uppgift om hur just dessa två ärenden behandlades. De kan ha blivit liggande eller så har de förmodligen lämnats vidare till Medicinteknik (MT). I MedControl finns en roll Ärendansvarig WebAdapt, men inget namn, på område 4 MT, som brukar få WebAdapt ärendena genom att Incident Manager vidarebefordrar dem i MedControl. Enligt Incident Manager kan man inte sortera fram endast aktuella ärenden i MedControl, utan alla ärenden ligger blandade outredda och avklarade om vartannat i en lång lista. Detta gör det är svårt att bevaka enskilda ärenden. Incident Manager har inga etablerade kontakter med Röntgen eller Medicinteknik och VGR IT saknar f.ö. många gånger namn på systemansvariga eller kontakter till leverantörer för flera av systemen. Detta är en omständighet som försvårar möjligheterna till dialog kring orsaksutredningar och om problemlösning.
Kommentarer	I båda fallen framgår att det råder en otydlighet kring ansvarsfrågan om WebAdapt. Avdelningarna har vänt sig till VGR IT, medan MedControl-ansvarig och verksamhetschefen haft uppfattningen att ansvaret vilar på radiologen, eftersom det är från dem som bilderna kommer och de då borde ha ansvaret för att systemet fungerar. Numer är man överens om att WebAdapt-ärenden skall sändas till VGR IT, som har funktionsansvaret. VGR IT får sedan ta ärendet vidare om problemet visar sig ligga hos den externa leverantören som hanterar driften av Bildarkivet. I ett av ärendena har återkopplingen från VGR IT inte fungerat och ärendet har inte kunnat avslutas då VGR IT inte har utrett ärendet eller genomfört några åtgärder i MedControl. Detta är tyvärr inte ovanligt enligt intervjuerna. En annan teori som framkom är att en av de tidiga motåtgärderna under våren med att stänga ned barnporrfiltret Netclean för att lösa problemen med WebAdapt, kanske inte hade någon egentlig påverkan på störningarna. Rutinen med MedControl har en brist, där läkare som inte tillhör en avdelning gör en anmälan som sedan avdelningschefen får hantera, eftersom händelsen skall registreras där den inträffade. Tillvägagångssättet leder både till onödig administration för avdelningschefen som är ärendansvarig och det finns även risk för glapp i informationsöverföringen. En relevant kommentar från MedControl-ansvarig är att det är svårigheter med att urskilja avvikelser i efterhand som är relaterade till ett system, då de ofta inte registreras som en systemavvikelse utan som en annan typ av avvikelse trots att systemet har spelat en stor roll.

4.6.3. Ett telefoniärende

IP-telefoni-ärende registrerat i VGRUSD

IP-telefoni-ärende registrerat i VGRUSD	
Var? När? Status?	Ambulansstationen Borås, SÄS. 2009-06-12. Ärendet avslutat.
Händelse- beskrivning	En av de fasta telefonerna till ambulansstationen i Borås är felkopplade. Problemet uppmärksammas då patienter som tror sig ringa till en psykiatrisk öppenvårdsmottagning kommer till ambulansstationen. Efter att ha säkrat att stationens kommunikation med SOS Alarm samt akutmottagningen vid Borås lasarett fungerade, kontaktades VGR IT för att uppmärksamma dem på händelsen. Det fanns aldrig någon risk för att patientsäkerheten för ambulansstationens uppdrag var hotat. Ingen avvikelserapport registrerades i MedControl.
Orsaks- utredning	I VGR IT:s incidenthanteringssystem framgår att det specifika ärendet har hanterats tillsammans med andra inrapporterade incidenter rörande samma problem under samma dag. VGR IT har försökt att lösa problemet genom att bl.a. företrädare för leverantör kontaktats för att göra felsök.
Åtgärder	Några direkta åtgärder har inte vidtagits vid ambulansstationen då deras patientsäkerhet aldrig var hotat. VGR IT har som åtgärd upprättat en lista på alla enheter inom SÄS som har ip-telefoni för att snabbt kunna komma i kontakt med samtliga om problemet skulle uppstå igen.
Avslut	Någon återkoppling från VGR IT har inget skett.
Beredskap "Före och under"	Ambulansstationen har goda rutiner för att tillse att kommunikationen till och från ambulansstationen fungerar. Då denna avvikelse rörde en fast telefon som inte används för patientrelaterad kommunikation behövs det inte heller några specifika rutiner för att säkra funktionen.
VGR IT Rutiner Kommunikation internt/ med andra	Chefen för Telefonservice på Regionsservice hade vid intervjun, trots efterforskning, inte fått fram någon information om den aktuella händelsen inom ambulansen i Borås. Det är normalt Telefonservice som är mottagare av MedControl-ärenden, för de förvaltningar som anlitar Regionsservice för telefonitjänster. Orsaksutredningar hanteras av Chef för Telefonservice. Ett problem för dem idag är att MedControl inte är regionövergripande och Regionsservice är inte uppsatta som mottagare i de olika MedControl installationerna. Det innebär att de får alla ärenden utskrivna och besvarar dem följaktligen också på papper. Ärenden kommer från olika håll, ibland från chefen för VGR IT, ibland Incident Manager eller direkt från en ärendansvarig. Telefonservice har heller inte åtkomst till VGRUSD, vilket upplevs som en brist. Telefonservice får relativt få MedControl-ärenden, ca ett i månaden. Med bakgrund av att Telefonservice hanterar flera 100 medicinska akuta larm anser de att de bör involveras mer i avvikelshanteringen och etablera bättre rutiner och fastställa kontaktvägar med bl.a. VGR IT.

IP-telefoni-ärende registrerat i VGRUSD	
Kommentarer	Vid de första kontakterna med inblandade på ambulansstationen i Borås och även i samband med en av intervjuerna fick vi uppgift om att händelsen även registrerats som en avvikelse i MedControl. Först efter en tid konstaterades att detta inte hade gjorts, eftersom händelsen inte bedömdes utgöra någon risk för någon patient och därför inte vara så allvarlig. Om det är rätt eller fel beslut är svårt att bedöma. Ett tekniskt fel som leder till störningar på telefonin för en ambulansstation borde i teorin kunna leda till mer allvarliga konsekvenser och VGR IT har trots allt vidtagit en åtgärd genom att ta fram en lista över IP-telefonabonnemang, som de kan kontroll ringa om en störning skulle uppstå igen. Genom att även ha registrerat en avvikelse i MedControl hade hanteringen av händelsen hanterats på ett korrekt sätt. VGR IT valde att slå ihop alla ärenden som kommit in till deras incidenthanteringssystem vilket ger dem en överblick över hur många som drabbats. Dock skall samtliga avvikelser som inkommit via MedControl besvaras var och en för sig. I detta fall har någon återkoppling inte skett till verksamheten enligt uppgift.