Case Studies in the Failure of Healthcare Information Systems

C.W. Johnson,

Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland.
http://www.dcs.gla.ac.uk/~johnson, johnson@dcs.gla.ac.uk

Abstract: Public and private organizations are investing increasing amounts into the development of healthcare information technology. These applications are perceived to offer numerous benefits. Software systems can improve the exchange of information between healthcare facilities. They support standardised procedures that can help to increase consistency between different service providers. Electronic patient records ensure minimum standards across the trajectory of care when patients move between different specializations. Healthcare information systems also offer economic benefits through efficiency savings; for example by providing the data that helps to identify potential bottlenecks in the provision and administration of care. However, a number of high-profile failures reveal the problems that arise when staff must cope with the loss of these applications. In particular, teams have to retrieve paper based records that often lack the detail on electronic systems. Individuals who have only used electronic information systems face particular problems in learning how to apply paper-based fallbacks. The following pages compare two different failures of Healthcare Information Systems in the UK and North America. The intention is to ensure that future initiatives to extend the integration of electronic patient records will build on the 'lessons learned' from previous systems.

Keywords: Healthcare Information Systems, Safety-Critical Computing, Software Standards.

1. Introduction

There has been considerable political support for electronic patient record systems and related information applications (Hoffman & Podgurski, 2008). For instance, healthcare informatics was a key element in the campaigns of both Senators McCain and Obama. These commitments have been carried into office with the passage of the American Recovery and Reinvestment Act of 2009, otherwise known as the 'Stimulus Bill'. This provides for an investment of some $148 billion in healthcare of which $19 billion is specifically ear-marked for healthcare information technology. Part of this investment is intended to support the development of a US national system for the electronic storage and exchange of patient records. There is an expectation that all clinicians will become 'meaningful users' of this infrastructure if they work within Federal healthcare programmes. The Stimulus Bill also established the post of National Coordinator for Health Information Technology. They will be responsible for defining and managing the standards that govern the operation of electronic health records. This post is also intended to help improve the security of the healthcare information infrastructures by creating common standards that avoid ad hoc local solutions for privacy and encryption.

The Stimulus Bill created a Federal Coordinating Council for Comparative Effectiveness Research. This body will ensure that any future software innovations yield tangible benefits in terms of patient outcomes and service delivery. The creation of the council is significant because political support is, in part, based on the assumption that any investments will increase the efficiency of long term healthcare provision. For instance, the development of e-prescribing should ensure the use of generic substitutes wherever possible. It should also help to minimise the waste that can occur through over-prescribing or through the continued use of drugs whose efficacy has been questioned. The delivery of electronic healthcare information systems should also drive improvements in accounting. The proponents of these initiatives argue that the Stimulus Bill will reduce iatrogenic errors by ensuring that clinical decision making is informed by the contents of patients' electronic records (Johnson, 2009).

At the same time, the U.K. National Health Service's Connecting for Health Directive has been working to implement the National Programme for IT (NPfIT). This initiative has already delivered a 'secure' email system to support the exchange of electronic healthcare information between some 170,000 registered users. It has also installed more than 15,000 connections across the NHS New National Network (N3); each of which conforms to a range of security and access control requirements. Further progress has been made in the procurement of Electronic Prescribing Services as well as a diagnostic imaging system capable of storing and exchanging high-quality X-ray images. Other projects within the UK NPfIT have focused on the use of software to support the scheduling and booking of consultations and of clinical procedures. As in the United States, these initiatives have carried a considerable price tag. The most recent estimates suggest that the programme will cost £12.4 billion, not allowing for inflation over the ten year life of the main contracts up to 2014. The central storage for the image system, known as PACS, has cost some £245 million. However, the collective bargaining power derived from centralised procurement through Connecting for Health has derived significant savings that are presently estimated at more than £860 million.

It is hard to underestimate the importance of healthcare information technologies once they become embedded within the everyday working practices of clinical staff. White (2008) summarises what he calls a paradigm shift; "the current paradigm of medical care depends heavily on the autonomous and highly trained doctor to collect and process information necessary to care for each patient. This paradigm is challenged by the increasing requirements for knowledge by both patients and doctors; by the need to evaluate populations of patients inside and outside one's practice; by consistently unmet quality of care expectations; by the costliness of redundant, fragmented, and suboptimal care; and by a seemingly insurmountable demand for chronic disease care. Medical care refinements within the old paradigm may not solve these challenges, suggesting a shift to a new paradigm is needed. A new paradigm could be considerably more reliant on health information technology because that offers the best option for addressing our challenges and creating a foundation for future medical progress, although this process will be disruptive".

Borriello, Stanford, Narayanaswami and Menning (2007) build on this vision when they describe the increasing deployment of healthcare information technology "By collecting patient data in settings more varied than doctors' offices, healthcare providers hope to better understand the many facets of patients' daily lives and then modify therapies to the individual. Another important context is emergency care to accelerate access to medical records at the emergency site or to bring experts to the scene virtually. By giving medical professionals appropriate, complete information, we expect to deliver better care that's tuned not only to the situation but also to the patient's history. The surgical field also receives much attention, as surgeons and nurses must monitor and control various vital functions under intensely stressful conditions. Technologists are developing systems to collect and process an ever-increasing range of telemetry from instruments used in an operating room and to augment human ability to detect patterns of concern that could require immediate action". However, the increasing deployment of healthcare information technology also raises a broad set of concerns. This paper focuses on a paradox that lies at the heart of innovation. The more that a team uses an application, the more vulnerable they become to the loss of those systems. The following pages illustrate these arguments using recent failures in the software infrastructures being developed to support both the UK National Health Service and the US Veteran's Affairs Administration.

2. UK National Health Service Connecting for Health CSC Data Centre Incident (July 2006)

As mentioned, the UK National Programme for IT (NPfIT) is intended to provide a 'step change' in the information infrastructure across the National Health Service (NHS) in England. The Department of Health set up the programme in October 2002 under the NHS Information Authority. A series of critical reports, in particular from the House of Commons Public Accounts Committee, eventually led to the Authority being replaced by the Connecting for Health Directive on 1st April 2005. The intention behind these initiatives is to improve the quality of patient care and to reduce the costs of providing services through the use of information technology. National Application Service Providers were identified where technical and cost concerns could justify the appointment of sole providers for

infrastructure facilities. For these reasons, contracts were awarded to BT for the NHS Care Records Service. This helps to ensure that patient records are available wherever they are required at different points of care. The same company was also responsible for the implementation of a standardized NHS National Network (N3) using an IP-based Virtual Private Network infrastructure. N3 is intended to provide resilient communications links, including voice over the Internet Protocol (IP), to acute hospitals and General Practitioners (GP) surgeries in England. Another company, Atos Origin, was awarded the contract to implement a 'Choose and Book' system. The main aim of this application was to enable patient choice. After being referred by their physician, the patient should be able to choose the hospital, date and time for an outpatient appointment. A third company, EDS, was awarded a contract to develop internal communications through the delivery of an NHSMail application. In 2004, this was terminated and Cable and Wireless assumed responsibility for these requirements.

Introduction to the UK NHS National Programme for IT: There was a concern to avoid single suppliers for services that did not automatically need to be provided by a natural monopoly. Wherever possible, healthcare infrastructures should be resilient to the failure of any single supplier. The NHS, therefore, also created five 'clusters' of Strategic Health Authorities (SHAs): Southern; London; East & East Midlands; North West & West Midlands; and North East. It was intended that each cluster would be serviced by a different Local Service Provider (LSP). These were to introduce an element of competition between the LSPs. BT Health London acted as LSP for the London area. Accenture was responsible for the North East and for the East & East Midlands cluster while the Fujitsu Alliance looked after the Southern LSP responsibilities. The Computer Sciences Corporation (CSC) held responsibility for the North West and West Midlands cluster through an alliance of companies.

The costs of the support can be illustrated by the contract with the CSC Alliance worth approximately £973 million over ten years. This consortium brought together a number of organisations, such as Hedra; the public sector change management specialist. The CSC Alliance also included iSOFT. Their software formed the core of the Lorenzo system that was chosen by the NHS to provide an integrated patient management and clinical record system (iSOFT, 2009). The scale of the Lorenzo Patient Administration System (PAS) can be illustrated by statistics for a single trust that consists of three hospitals. This organisation serves more than 1,000 square miles. The Lorenzo implementation now encapsulates data for more than 500,000 patients within this individual trust.

The CSC Alliance also included SCC, who provided infrastructure and desktop management services. These relationships were strained by both the complexity of the engineering challenges created by the CfH programme and also by the costs of meeting the NHS requirements. iSoft's debts grew to more than £93 million during 2006 and there was considerable doubt over the company's future as CSC and the Australian company IBA Health competed to acquire a stake in the software developer (Bolger and Costello, 2007). As the main user of iSoft code, CSC had the right to object to changes in management and was considering a cash offer for iSoft equity when IBA was first associated with the acquisition. By late June 2007, CSC removed their objections. However, this incident illustrates the organizational complexity that exists even within the successful consortia of CfH. The consequent uncertainty for the software supplier exacerbated communications problems with NHS procurement staff. IBA completed their acquisition of iSoft in August 2007 and subsequently changed their name to the iSOFT group.

This uncertainty also affected the development of regional Healthcare Information Systems within the CfH programme. Initial sector allocations were complicated by internal disruptions within the LSPs. In 2006, ComMedica's contract for supply of Picture Archiving and Communication System in the North-West/West-Midlands cluster was terminated, and they were replaced by GE Healthcare. The IDX Systems Corporation was replaced by the Cerner Corporation in the Fujitsu Alliance following contractual disputes during August 2005. The Alliance's contract for the Southern sector was later terminated in May 2008. Accenture handed over most of their work to CSC in January 2007, leaving BT Health as the only other remaining LSP. This has resulted in a situation where sectors can be

broadly divided into those that are associated with the Millennium system from Cerner/BT, and those that are engaged to the Lorenzo product from CSC and IBA Health. Every time that a sector contract was renegotiated, healthcare organizations not only faced changes in suppliers but also in the software components being offered by those contracting organizations. These amalgamations have also undermined the diversity and competition that were intended to lend resilience to the NHS healthcare information infrastructures.

Even though the initial contracts were based around Local Service Providers, they were deliberately drafted to ensure a unified approach across the NHS. This created considerable tensions when many decisions had to be taken at a local level within the constraints created by the need for national consistency. For instance, BT had been awarded a £1 billion contract to link up and standardize NpfIT systems across the London sector. However, the initial planning for this project did not reveal the rich and diverse requirements across many local healthcare providers. This created a series of demands for changes to support NHS functionality during relatively late stages of the project. BT felt obliged to meet these requests and consequent losses began to grow with some estimates identifying contingency provision of more than £1 billion to tailor the systems to these local demands. The tensions between national provision and local needs shaped the decision to remove the clusters in favour of the National Programme, Local Ownership programme (NLOP). Responsibility for the delivery of key elements in the NpfIT was devolved to ten English Strategic Health Authorities (SHAs). Under this reorganization, staff who had worked for the Connecting for Health programme in the local clusters was transferred to the SHAs. The CfH programme retained responsibility for managing the remaining contracts with the LSPs and with them the interactions with the SHAs.

Background to the Lorenzo Application: It is against this background that the NHS Connecting for Health programme suffered one of its most serious system failures around 10am on Sunday 30th July 2006 (NHS Connecting for Health, 2007). This resulted in a serious interruption to the computational infrastructure provided by CSC. The failure occurred in the organisation's Maidstone data centre and was compounded by problems with their recovery data centre in Royal Tunbridge Wells. Knock-on effects extended to information services in the North and West Midlands. The outage affected 80 trusts that were moving to CSC's implementation of iSoft's Lorenzo application.

As mentioned above, Lorenzo provides an integrated patient management system. It supports 'an at-a-glance view of a patient, their history and other critical medical information' (iSOFT, 2009). The present implementation collates information from more than a dozen other systems. GPs and community care workers can use these tools to access information throughout a trust. The aim is also to improve information exchange across the patient's trajectory of care. In particular, the Lorenzo tools can improve the accuracy and timeliness of patient data across a region when previously data was often isolated within individual healthcare institutions or departments. Lorenzo was developed to use workflow models and time management software as well as clinical data to meet the combined aims of improved information access and productivity.

Many trusts decided to support a gradual introduction of Lorenzo; this was intended to reduce the risks created by teething problems and by the need to tailor system support to local requirements. The aim was to gradually encourage the integration of healthcare information systems with existing processes and to maximise the reuse of applications which already supported local staff. For instance, several trusts chose to first focus on the introduction of the Lorenzo Patient Admission System. They then expanded the initial trials to include the use of the healthcare information system as a means of supporting the Trusts' administrative functions and correspondence systems. Further integration was required to implement Lorenzo's support for clinical resource scheduling, for networked pharmacy services and also for the support of particular Departments' records management functions, such as those within Accident and Emergency and maternity care.

Lorenzo can provide staff with real-time access to electronic patient records; 'in some specialties, as much as 95% of the results, notes, and correspondence can be called up from the EPR on-screen, so

some consultations are entirely paper free'(iSOFT, 2009). Additional support was provided for the generation of discharge summaries and the integration of prescriptions for drugs that patients would require after leaving the care of individual hospitals. GP's and community care staff could access this information to support patients once they returned to their homes. An NHS Consultant Physician and Medical Director for Clinical Effectiveness recently enthused about the benefits provided by Lorenzo; "(Staff) response has been amazing. Most now say that there's no way they could go back to working without this information" (iSOFT, 2009). As we shall see, these remarks turned out to be remarkably prescient.

Overview of the Incident: The immediate effects of the first failure in this paper focussed on part of the Lorenzo Storage Area Network (SAN) equipment based at the CSC Maidstone Data Centre in Kent. The SAN architecture is used to attach remote computer storage devices, including disk arrays and optical jukeboxes, in such a way that they appear to be locally attached to an operating system. In the NHS, this has significant benefits over Network Attached Storage (NAS) architectures where support staff are constantly aware of the remote location of these shared devices. There are further benefits of the SAN architecture in terms of resilience because a failed server can be replaced by another machine that itself boots from the shared file store of its predecessor. In the immediate aftermath of the failure, Connecting for Health described how "the affected trusts - all those which have had new administrative computer systems installed by CSC - are continuing to provide normal service by operating manual contingency systems. Some 80 trusts (72 primary care and 8 acute trusts) are affected. NHS CFH and CSC regret the inconvenience this incident is causing and are committed to resolving the issues as soon as possible" (NHS Connecting for Health, 2006). These end users suffered particular problems with the Lorenzo patient administration application, described in previous sections. However, one trust IT manager described how: "The data centre in Kent had major problems at the weekend. Every application provided is off at every hospital and Primary Care Trust. This will really hit places like the University of Birmingham, as Monday morning is always the busiest time" (eHealthMedia, 2006).

The CfH announcement went on to provide a high-level description of the causes behind the failure. These included 'technical issues' following a power system interruption that prevented local healthcare providers from accessing SAN data accessed via the servers (NHS Connecting for Health, 2006, 2007). CSC was also responsible for developing back-up systems, however, these coul not be brought on line immediately. CfH developed a schedule for recovery. Contingency plans had been developed for the loss of a data centre. Service level agreements specified the restoration of access within two hours for strategic services, including the provision of patient care records to acute hospitals. Most of the remaining data services should be restored within 12 hours of a failure involving a major data centre. Less critical services could then be restored over a 72 hour period. However, in this incident it was not possible to provide individual healthcare organizations with a precise estimate of the delay before services could be resumed. Many of these service level agreements had to be revised following the loss of service to the North and West Midlands. CfH contracts, typically, specified that a range of reliability engineering techniques should be used to protect critical applications:

1. System components should be subject to reliability assessments that identify mean time between failure and identify appropriate maintenance intervals;
2. System components should be replicated within a data centre to ensure that service provision can continue following any individual failure;
3. The data centre should be replicated in a different location so that services can be transferred following the loss of a primary facility.

The NHS investigation stressed that a pathological combination of events had overcome the defences that were designed into the infrastructure of the SAN and associated applications (NHS Connecting for Health, 2006). They traced the 'root cause' back to the failure of an Uninterruptible Power Supply (UPS). This was triggered by a high temperature alarm, in the CSC Maidstone Data Centre.

It is ironic that the UPS is, itself, one of the secondary protection mechanisms intended to increase resilience by providing an emergency supply during power failures. However, these units have triggered many similar failures in other industries (Johnson, Amar, Licu and Lawrence, 2008). The UPS manufacturer had conducted a number of diagnostic and other maintenance activities at the centre between the 22nd July and the failure on the 30th. The UPS was off-line while engineering teams worked on the systems. The maintenance activities were interrupted by fluctuating power supplies with a spike that led the circuit breakers to trip open. This caused a short circuit that interrupted the power supply to half of the data centre for three quarters of an hour. The SAN was shut down as a preventative measure. This failure affected both the primary supply and also the UPS that was being worked upon. It removed both the first and second levels of protection identified in the previous enumeration. The power interruption affected all clients, including the CfH sectors, which relied upon CSC data services from the Maidstone Data Centre.

Once power was restored, auxiliary services quickly came back on-line including the air conditioning systems. All of the SAN devices were restored. The only exceptions were two HDS 9980 data storage arrays that failed to boot. An HDS technician was on site and immediately began to diagnose the problem (NHS Connecting for Health, 2007). However, these two devices provided CfH services to the North and West Midlands sectors. The subsequent inquiry argued that the loss of both SAN disks was a failure of 'level two' resilience. Both devices failed at the same time rather than providing mutual support in the case of any single failure.

The two SAN devices could not be immediately restored because the disks were running different versions of the microcode. These differences had been introduced after an earlier software upgrade. Following this change, the power on the SAN devices should have been cycled. This would have triggered checks to ensure that their microcode was compatible. However, these tests had not been performed. The loss of power in this incident itself triggered the compatibility tests. These microcode checks failed because of the mutual incompatibility mentioned above and the servers could, therefore, not be brought back on-line.

The difficult in diagnosing and correcting the SAN microcode failure mode was exacerbated because the manufacturer had never seen a similar problem in the past. 'It is understood that around 350 such systems are installed globally and, until this incident, no systems had ever been unavailable for more than four hours' (NHS Connecting for Health, 2006). The supplier's staff and CSC technicians tried to conduct a 'force load' of the microcode on the two 9980 data storage arrays during the night and early hours between the 30th and 31st June. The incompatibility could not be resolved until some 72 hours after the failure began. "HDS immediately responded with technical engineers from the UK, Europe, Middle East & Africa and the Hitachi factory. The systems have now been restored to the users. No patient data was lost. However, during the period of time when the systems were affected, users had to use a manual backup system... We would like to stress the situation at CSC is highly unusual. Our storage systems are designed to protect critical customer data in the event of any planned or unplanned downtime and the Hitachi storage systems at CSC were restored with all data intact. ... The exact cause of the storage devices becoming temporarily unavailable is part of an in-depth investigation" (Mellor, 2006).

The Restoration of Services at Fall-back Sites: The third level of resilience within the CfH model calls for contracting organisations to provide fallback support at a second site. However, a common observation in previous incidents involving healthcare failures is that many organisations are very reluctant to use this alternative option to resume service provision (Johnson, 2009). For example, there are often concerns about transferring operations to a fallback resource before there is any clear diagnosis for the primary failure. There is a fear that any fault in the primary system will also be propagated into the back-up secondary system as well. In this incident, CSC staff, therefore, worked with CfH teams to assess the risks associated with migrating data resources to additional sites.

However, the decision to move support from the primary facility in Maidstone to the fallback centre in Tunbridge Wells was complicated by the different levels of criticality associated with the systems that were affected. The decision was also complicated by the different service level agreements that governed the restoration of primary systems at the back-up site. The subsequent Parliamentary brief describes how the decision to fall back to the Tonbridge Wells facility was delayed by over optimistic advice from HDS engineers (NHS Connecting for Health, 2007). CSC told the inquiry that HDS continually told them that they were close to fixing the problem. CSC, therefore, provided CfH with 'strong reassurance' that the problem would be fixed soon and that there was no need to incur the risks associated with falling back to the secondary system. By 15:00 on day of the failure, it was argued that the engineers should have recognised the problems in bringing the SAN devices on-line.

Most programmers will be familiar at some point in their career with the predicament faced by the HDS engineers. In such circumstances, it can be hard for the teams most closely involved in debugging to provide realistic estimates of the time taken to resolve complex failures. The optimism of the HDS engineers is also understandable given the pressure to restore services to the trusts as soon as possible in order to meet service level agreements for contingency provision. Strategic applications were to be restored within two hours while emergency bundles were to be implemented within 72 hours. Any decision to fallback to Tunbridge Wells on the Sunday night would have met the strategic requirements, covered in the contingency plans, but would have done little to meet the tactical and emergency commitments that formed the bulk of the systems affected by this incident. It was, therefore, decided to focus on restoring the original SAN devices during the 30th July and to inform the North West and West Midlands of the on-going problems. However, further delays occurred in the restoration of the SANs as work progressed into the morning of 31st July. This forced CfH and CSC staff to launch 'full disaster recovery procedures' by taking the decision to move to the secondary site.

This decision to use the secondary facility was taken around 11.00hrs on the 31st June. However, the operations to start the transfer of control did not begin until the evening – around 36 hours after the failure was triggered (NHS Connecting for Health, 2007). The rest of the time was used to establish that the fallback system shared the same configuration as the two primary SAN devices in the Maidstone data centre. It took a further seven hours to complete the transfer process. Although no data was lost as a result of the failure, it took more time than anticipated – especially to restore the tactical and emergency services. This was due to the problems in configuring complex applications to mirror changes that had been implemented in the primary systems. The existing recovery plans described individual procedures for particular application areas: Wintel, Unix, the SQL Server etc. However, they did not sufficiently consider the interdependencies between these applications nor did they consider the detailed sequence of actions necessary to transfer the systems and bring them up with the critical relationships preserved on the secondary server in the Tonbridge Wells centre.

Further problems stemmed from communications issues between HDS, CSC and CfH. Previous sections have described the optimism of the HDS engineers as they tried to diagnose the causes of the failure before the decision was taken to roll-back to the Tonbridge Wells secondary server. The subsequent investigation also argued that CSC were over optimistic when they informed CfH staff that the situation was 'under control' in the immediate aftermath of the power surge; 'they did not adequately invite or involve the available technical expertise from NHS Connecting for Health in diagnosis, problem solving and contingency planning' (NHS Connecting for Health, 2007).

The technical and organisational problems in diagnosing and correcting inconsistencies in the microcode between the two NHS SAN devices combined with a reluctance to use the fallback facility in Tonbridge Wells. Other private clients who shared the Maidstone data center had their services restored. However, the critical NHS applications were still not on-line for up to four days. This recovery process partly stemmed from the delay in initiating the move to secondary devices. It was exacerbated by the critical nature of many of the systems that were affected – the CSC Alliance members and contract staff had to carefully test each of the SAN drives before functionality could be

restored. Lorenzo and the associated applications, described in previous sections, were unavailable for 50 out of the 80 affected sites for two and a half day. The remaining trusts had access restored by the 3rd August, four days after the initial failure. During this time, clinical staff and hospital administrators had to resort to paper based systems. In most cases, the electronic information systems had not been in place long enough for staff to forget how to use the manual procedures. However, this incident shows that there an increasing reliance on healthcare information technology may erode the skills that are necessary for staff to operate these 'ultimate fallback procedures'.

Numerous lessons were learned from this failure. In particular, the differences between the primary configuration of the Maidstone SAN devices and the fallback provision at Tunbridge Wells revealed the need to ensure that the secondary resources mirrored the primary system more closely. There had been a test of recovery procedures during September 2005. The subsequent Parliamentary report argued that this had been less than adequate. It did not bring up the secondary site to confirm their 'configuration, data currency, performance, and connectivity were adequate to meet the business needs' (NHS Connecting for Health, 2007). A number of further lessons were learned from this incident:

- 'All processes have to be reviewed and revised to take account of all of the problems encountered during the incident;
- In the event of an Uninterrupted Power Supply being disconnected in future, the NHS will be offered the option of a planned power down rather than risk running live services without a UPS;
- The SAN solution has been upgraded to ensure that it is powered by both UPS's;
- Additional configuration management processes have been implemented to ensure solution compliance between production and back-up environments;
- Additional data centers have been built, commissioned and are operational;
- The HDS9980s involved in the incident at Maidstone and those providing the remote copy for Disaster Recovery are no longer using the combination of microcode known to cause the system to close down;
- HDS has re-created the conditions in CSC's UK laboratory and have demonstrated to CSC that new processes have removed the risk of future exposure.
- CSC have confirmed that HDS and Hitachi have reviewed the microcode quality assurance and release procedures to remove the possibility of other microcode combinations leading to a similar incident;
- Business continuity processes have been reviewed and updated and a senior and experience CSC Business Continuity manager has been appointed;
- A programme was put in place to implement tools and processes to:
    - Ensure that the recovery environments remain aligned with the production environment and instances;
    - Software versions at each site are fully aligned.
- Regular audits have been scheduled to verify Disaster Recovery site status;
- Disaster Recovery tests are carried out to provide proof of the business continuity arrangements with witness testing involving NHS staff;
- Compensation of £1.2 million in total was paid to the two Strategic Health Authorities involved to cover the NHS costs incurred as a result of the lack of systems availability whilst NHS business continuity processes were invoked' (NHS Connecting for Health, 2007).

The incident did not end with the restoration of services via the Tonbridge Wells secondary facility. Concerns over the original transfer justified extreme caution in the transfer back from the fallback site to the primary data centre in Maidstone. A senior CSC Vice President took four weeks to coordinate the return to normal operations. A walk-through exercise was conducted to validate the plan. This included the development of a communication plan that identified key decision makers within the alliance and across the NHS. Contingency plans were also developed in case there were problems in

the recovery from contingency. Partly as a result of these precautions, the eventual transfer went ahead as planned.

3. The United States' Veterans' Affairs VistA Server Failure (August 2007)

This paper identifies parallels between the engineering and management response to the failure of healthcare information technology in two very different national systems. In particular, it is possible to find similarities between the CfH SAN disk failure and a series of high-profile failures involving the Veterans' Affair (VA) Administration (Associated Press, 2009). These occurred during 31st August 2007and involved the VA's Sacramento facility. This was one of four data centres that had been created as the result of a centralisation process that is comparable to the changes that led to the creation of the CfH data centre in Maidstone.

Background to the VistA Failure: Prior to centralization in 2005, the VA's 150 medical centres had their own IT services, budgets and staff. After the reorganization, the VA moved local responsibility for IT infrastructure to four regional data processing centers, two in the east and two in the west. This centralization also had an impact on development practices. Before 2005, changes could be made to applications on a local or regional basis. This included updates to the Veterans' Health Information Systems and Technology Architecture (VistA) which is comparable to the NHS Lorenzo application, described in previous sections. The decentralised development practices within the VA prior to 2005, created a situation in which there might be several parallel versions of an application running in different centres. Local IT officers liaised with the centre directors in a manner that was perceived by many to be highly responsive to local needs and priorities. However, it also undermined the standardization that is critical for closer integration. These distributed development practices also created concerns over a range of non-functional requirements including security, infrastructure administration and disaster recovery that all have their parallels within the UK NHS IT modernisation programmes.

The VA reorganization created reporting and control structures that fundamentally changed this distributed model of software development. The original plan was that by 2008, the VA would create major departments in functional areas that included enterprise development, quality and performance as well as IT oversight and compliance. The scope of the project included the reassignment of 6,000 posts within a more centralized management framework. There were also changes in the associated development and acquisition models with the introduction of 36 management processes in an Information Technology Infrastructure Library (ITIL). A further example is provided by the coding compliance tool was introduced across all of the 33 medical centres within Region 1 of the four divisions mentioned above. This ensured that all of the VA facilities in that area were running the same version of an application.

The August incident was the most severe in a succession of more than fourteen failures that occurred since April of 2007 after the VA's Sacramento facility started hosting the VistA/ Computerized Patient Record System (CPRS) suite of clinical applications. Most incidents only lasted for a matter of minutes. However, in this case it took more than nine hours to restore services to the seventeen centres that were directly affected. Knock-on effects propagated to VA hospitals and clinics from Alaska to northern California, Los Angeles, Hawaii, Guam, Idaho, Nevada, Oregon, west Texas, American Samoa, the Philippines and Washington State. The VA's Guam centre was affected because they drew data from the Honolulu facility that was, in turn, connected to the Sacramento server. Knock-on effects extended beyond hospitals and medical centres; they also affected local pharmacies. Many of these used VistA applications to automatically produce orders and labelling. It is difficult to underestimate the scale of the disruption. For example, the Northern California Healthcare System supports more than 370,000 veterans with 2-3,000 visits per day. The director of clinical informatics for the San Francisco VA Medical Center described this incident as "the most significant technological threat to patient safety the VA has ever had" (Schaffhauser, 2007).

VA Contingency Plans: Around 07.30 on the morning of the incident, the end-users of the VistA system found that they could not log on to access the Computerized Patient Record System (CPRS) in

medical centres around Northern California. This prevented access to the on-line records for the veterans under their care. There were obvious concerns for patient safety in the medical facilities that were affected by the failure. Staff, therefore, resorted to a three tier contingency plan, which mirrors many aspects of the NHS Connecting for Health defences mentioned in the previous case study. As mentioned, this incident took place against the background of organizational centralization of IT operations from around 150 medical facilities to two regional data processing centers in the eastern United States and two in the west. These Western sites cover what are known as Regions 1 and 2 from Sacramento, California and from Denver. The first contingency plan was for the services that were previously provided by Sacramento to be handled by the Denver data centre in Region 2. The second level of defence used the same approach but assumed that it would not be possible for local sites to making any updates on the central copy of their patient data. In other words, they were to operate a 'read only' mode. Any changes in patient care would have to be logged locally and then updated on the central patient records system when access was restored. The final 'fallback' position was for healthcare facilities to use the local files that were stored on their own computers. These only provided brief summaries about each patient who was either on-site or who were scheduled to have appointments in the next two days. In this ultimate contingency, clinicians would not have access to any data for patients who appeared with conditions that required immediate, unscheduled care.

The first level contingency plan failed; support did not seamlessly transfer for the affected sites from the Region 1 facilities in Sacramento to the Region 2 centre in Denver (Schaffhauser, 2007). This is comparable to the problems that delayed the transfer from the UK NHS Maidstone servers to the backup systems in Tonbridge Wells. In the case of the VA failure, the intention had been that the Sacramento and Denver centres would provide mutual support in the event of a failure. Hence, data that was updated in once site was automatically mirrored by changes in the other centre. It should, therefore, have been a straightforward task to transfer operations from one site to the other. However, The VA Chief Information Officer (CIO) had a difficult decision to make. They had already witnessed six servers crash in the Sacramento data centre. An initial estimate judged that it would take up to two days to restore services from the longer term backups stored for the Region 1 facility. There was a concern that by running the software necessary to support the Sacramento users from the Denver facility that any problems with the Region 1 code would begin to affect the Region 2 infrastructure. Again this mirrors the complex risk assessment that had to be made by CSC and CfH staff following the SAN disk failure. In this case as in the NHS example, VA IT senior management were unwilling to risk the 11 remaining sites serviced from Denver without clearly understanding the reasons why the Sacramento system had failed. The decision was, therefore, taken not to transfer services from the Sacramento centre using the level 1 contingency plan.

The remaining local IT teams at 16 of the 17 VA facilities affected by the loss of Region 1 services followed the second stage in their contingency plans when they discovered that Sacramento would not be transferring support to the Denver centre. This involved configuring local applications to rely on 'read only' access using available patient data. One of the 17 facilities could not use this option. Earlier in the week, staff from the regional data centre had disabled the second level fallback support for this facility in order to create a number of new test accounts that were used to store the backup data. Although this process was repeated several times a year, there had not been any attempt to engineer the same level of contingency provision during these operations and so local staff had to rely on the summary records that were cached on the local hard drives. The limited information available to clinicians created significant concerns about patient safety. Not only were these records restricted to a subset of the patients visiting the facilities but they were also limited in terms of the information available. They provided rudimentary lab results, medication lists and known allergies as well as annotated problem descriptions. However, the pharmacy information was far from complete. Clinical staff could not review the previous day's results nor could they easily access longer term information about the patients in their care. The problems created by these test accounts are comparable to the problems created by UPS maintenance during the NHS SAN disk failure. In both cases, it was difficult to maintain contingency services during the routine maintenance of complex systems. Even minor changes in the configuration of primary applications, undermined the fall-back plans that had been developed for both healthcare information infrastructures.

The VA facility had to rely on third level of contingency plans. Patient care records were printed out on local personal computers. This created a delay during which the first round of consultations had to take place without access to any medical records. Staff quickly began to rely on hand-written notes for prescriptions, lab orders etc. The worst problems arose in those areas where the facility had made the most progress in the adoption of electronic information systems. In several instances, the parallel paper based forms were no longer available. Recent hires had little recollection of the procedures used before their electronic counterparts. Outpatient surgery was delayed because clinicians were uncertain about whether or not to proceed without completing the appropriate documentation. There was no way to order or update information on consultations. Patients discharged that day could not be scheduled for follow-up appointments electronically and were told that they would be contacted 'at a later date' which increased uncertainty and created the possibility that subsequent consultations might missed.

Recovery Actions: The lack of integrated communications between different departments created delays in obtaining discharge medications. This, in turn, meant that some patients remained on the wards longer than would otherwise have been required. These delays, in turn, had consequences for admissions and transfers creating a host of secondary logistic problems. Although nurses continued to administer medications using paper Medication Administration Records (MAR) there were further delays before the initial approvals or 'medication passes' could be printed and paper copies of the MAR were distributed. Pharmacies connected to the Sacramento data center were also affected as labeling and automatic dispensing equipment were directly controlled by VistA applications. The use of paper processes slowed the provision of healthcare services across the facilities and also created the potential for error as staff were forced to adopt a broad range of coping strategies – creating processes 'on the fly' rather than using agreed protocols. Particular problems arose during shift handovers where, for instance, nursing staff were used to the graphical overviews and detailed drill-down support provided by VistA applications. These consequences from the VistA failure were significantly worse than those in the NHS incident precisely because healthcare information technology was more widely adopted within the VA facilities. However, the problems in this facility provide a stark warning for all healthcare providers of the potential hazards from system failures as staff increasingly rely on the support provided by these innovative systems.

It is difficult to recreate the uncertainty that both technical and clinical teams faced in the hours following the initial failure. This was exacerbated by some of the consequences of centralization. In the past, local staff could call their local support officers for some estimate of the likely duration of a disruption. Some of this personal contact was lost when the VA increased the responsibilities of the regional data centres. Support officers in the Sacramento centre were urgently required to help diagnose the cause of the problem and so it was often difficult for the remaining support staff in local facilities to gain accurate technical information that they could pass to their co-workers. This created further confusion because without an accurate assessment of the duration of any disruption it became difficult for local management to make informed decisions about the activation and support for contingency operations - for instance in moving beyond the 'read only' access to paper-based processes. Communication between the data centre and the local facilities quickly increased once staff believed they had identified the cause of the problem, described in the following section. However, in some cases this created an alternate problem when the teams in Sacramento requested increasingly more detailed feedback on the apparent success or failure of changes they implemented in the underlying configuration of their servers. The software problems, therefore, exposed underlying communications weaknesses between local and centralized support teams across the VA. Again, there are strong parallels between both the US and the UK experience. The failure of the Maidstone data centre was exacerbated by the confusion that occurred when HDS engineers and CSC staff initially thought that they could restore services with minimal delays. CfH staff were told that the situation was 'under control' in the immediate aftermath of the power surge and this message was passed to the local trusts. They then had to revise their contingency plans when the estimates from the data centre engineering teams proved to be too optimistic.

At the time of the failure, members of the VA technical staff were working together with an external contractor reviewing the performance of a hardware platform running on a particular virtual memory

configuration. Hence there was a large number of people on-site to begin diagnosing the cause of the problem as they began to observe system performance degrading without any apparent cause. Although the availability of additional staff on-site helped to share workload in the response to the incident, it also increased the problems associated with maintaining shared situation awareness across large groups of co-workers. Again this has parallels in some of the communications issues between CSC, HDS and CfH staff following the Maidstone SAN disk failure.

After the local clinical teams had reverted to paper-based approaches or to the use of 'read only' access on the remaining servers, Region 1 support staff began to identify the cause of the technical failure. This stemmed from a change on the network port configuration for the servers that provided access to shared resources between the VA facilities. The executive director of VA's Office of Enterprise Infrastructure Engineering later reported that this led to a mismatch between the speed of the Region 1 servers with the speed of a telecommunications switch (Brewin, 2008). The configuration change had been implemented without following all of the documentation and approval practices that would have ensured different support teams were aware of the change. The change request was not properly documented or reviewed. Jeff Shyshka, deputy assistant secretary of enterprise operations and infrastructure at VA's CIO Office has described how the revised port configuration was 'rolled back' in order to rectify the problems in the Sacramento center (Mosquera, 2007). He went on to draw clear links between the technical causes of the failure and the wider political/organizational context; "As with any collocation undertaking of this magnitude, there will always be the potential for human error. Ensuring effective communications processes between the teams managing the collocated VistA systems and the IT staff at the local facilities is perhaps the greatest challenge." Again we can draw parallels between the root causes of these two incidents – the port configuration issues in VistA resemble the microcode configuration problems in the NHS SAN disks.

The decision was taken to shut down the seventeen VistA systems that were hosted by the Sacramento center so that they could be brought back one by one. A plan was drawn up to restore the sites in an order that was determined by their workload. Those centers that were closest to the end of their peak working hours would be brought back first. This was intended to minimize interference with any contingency or fallback plans that had been implemented in each of the local facilities. If the attempts to restore normal service exposed further problems then the impact would be reduced because the facility was no longer working at full capacity. Following this model, medical facilities in the Central time zone were brought up first, followed by the Pacific, Alaskan and Hawaiian centers. Throughout this time, support staff were in almost continual contact with the healthcare centers to determine whether or not the recovery plan was taking effect. Even as it became clear that the port reconfiguration had addressed the underlying problems, a huge effort began to restore data integrity. For all of the seventeen centers directly affected and the subsidiary sites caught up in the knock-on effects it was critical to update the electronic records with the new orders and procedures that were created while VistA was off-line. It took almost a week to bring the medication administration records up to date once the system was restored. It took administrative staff more than eight weeks to catch up with the paper backlog from consultations and tests that could not be logged directly onto VistA and the associated systems after the loss of the Region 1 data center. Concerns over patient safety lingered well beyond this recovery period. The Associate Chief of Staff, Clinical Informatics for the VA in Northern California presented written evidence to the Senate House of Representatives Committee on Veteran's Affairs (2007); "However, entering checkout data on all these patients many days after the fact is potentially inaccurate. Many providers have gone back into the Computerized Patient Record System (CPRS, within VistA) and tried to reconstruct notes that summarize the paper notes that they wrote in order to mitigate the risk of missing information. This work to recover the integrity of the medical record will continue for many months since so much information was recorded on paper that day. When you consider that hundreds of screening exams for PTSD, depression, alcohol use and smoking, and entry of educational interventions, records of outside results, discharge instructions and assessments are all now on paper and are not in a format that is easily found in the electronic record, the burden of this one failure will persist for a long time" (Conn, 2007).

Many commentators were quick to link the failure to the centralization of IT services (Mosquera, 2007, 2008). As we have seen, these arguments were partly based on technical concerns over the ability of remote IT departments to respond to the detailed clinical needs of diverse local facilities. However, they were also motivated by deep-seated political concerns within the VA. One of the medical directors who lost control of their local IT resources in the centralization from 2005-2007 argued that "Before regionalization of IT resources -- with actual systems that contained patient information in distributed systems -- it would have been impossible to have 17 medical centers [go] down… (centralization) in the name of standardization (has caused support to) wane to a lowest common denominator for all facilities" (Schaffhauser, 2007). Some of the response to the failure also provides insights into the Republican and Democrat perspectives on healthcare reform, especially when it focused on the role that external contractors had played. Before the reforms started in 2005, individual centers administered their IT budgets. They owned and operated most of their information infrastructure. In contrast, much of the infrastructure that supported the four regional centers was provided by commercial contractors. The VA leased proprietary IT services in stark contrast to the open source approach behind the VistA systems (Mosquera, 2007). The deputy CIO in VA's Office of Enterprise Development described how they were "We're hiring outside contractors to stand at the elbows and shoulders of our IT managers through the development organization to watch what they do on a day-by-day basis". When asked if the centralization of IT had played a role in the failure, he argued that "Had the IT reorganization never happened, this error might have happened on Aug. 31 anyway because somebody didn't follow a procedure" (Schaffhauser, 2007). These concerns over centralisation and control in the delivery of large scale IT services have also been raised across the NHS. Both incidents reveal tensions that are common when local healthcare providers must be integrated into national information system architectures.

Following the VA failure, some of the plans to migrate additional medical facilities to the regional centres were temporarily delayed. The Region 1 management organized an internal review that reported to the assistant secretary of the Office of Information and Technology. This was extended to consider a number of alternate architectures to provide different levels of resilience. One of the conclusions from the initial reports was that Region 1 management had been faced with a difficult choice – continue with inadequate levels of service across their centres or risk propagating an undiagnosed error to the neighbouring region. A key lesson learned from this incident and from the NHS SAN disk failure is that centralization does not by itself provide increased levels of resilience. In the immediate aftermath of the VA incident, changes were introduced into the VistA application to ensure that the level 2 contingency plan offering 'read only' access to electronic records would in the future be available following maintenance activities that forced one of the Region 1 centres to fall back on paper-based documentation.

A further side effect of the failure was that it highlighted the issue of compliance with the revised procedures introduced during the reorganization from 2005. Previous sections have described how several thousand staff were affected by the changes. It also described the introduction of 36 management processes in an Information Technology Infrastructure Library (ITIL) as well as the use of new systems, such as Region 1's coding compliance tool. As might be expected, it can be difficult to change the working practices of so many co-workers. However, the potential consequences of the failure for patient safety provided a valuable reminder of the importance of following the revised protocols. Change management procedures were more rigorously inspected and internal audit procedures were reviewed to ensure that modifications to the IT infrastructure could be traced back to appropriate levels of management. These changes are very similar to many of the configuration management recommendations that were intended to ensure consistency between future microcode updates on the NHS Lorenzo SAN disks.

In the aftermath of the August 2007 failure, the VA hired an external company to review their contingency plans. The 'read only access' to VistA was reorganized to ensure that the tier two fallback provision would continue even in situations where there had been account maintenance. Further studies were conducted into the risks of migration from a failed server to the tier one back-up systems in neighbouring regions. The executive director of VA's Office of Enterprise Infrastructure Engineering identified key lessons from the 2007 failure which included the need to tightly control

and supervise change and configuration management as well as diversify computer resources across the VA. The Region 1 data centre supported 17 hospitals and their outlying clinics. This created significant knock-on effects when the servers began to fail. The Executive Director, therefore, argued that future plans would be based around regional 'server farms' that would each support a smaller number of hospitals. Within the Sacramento area this might mean two or three farms each supporting six hospitals and providing an increased level of local redundancy. This approach would also make it easier to focus efforts on restarting services following any future failure (Brewin, 2008).

Concerns persist over the danger of bringing down a healthy server in the process of supporting a failed system. These revised contingency plans have been tested by a series of subsequent failures, although arguably none have had the same consequences as those described in the previous sections. For example, a hardware problem affected the support provided by the Region 2 centre in Denver during the afternoon of the 10th April 2008. This had a direct impact on VistA services provided to twelve medical centres from Colorado to California. As we have seen, however, the secondary impact of these interruptions propagated well beyond the primary user facilities. Different centres were affected for different periods of time between five and seven hours. In contrast to the previous incident, it took longer to diagnose the precise circumstances leading to the failure.

The recovery task was further compounded by a near simultaneous failure that affected the VA's commercial telecommunications carrier. This prevented some of the connectivity checks that might have helped support staff in diagnosing the VA's own hardware problems. The VA had previous changed their network service supplier in 2001 to a consortium of major providers headed by a 'government solutions' division of a major provider. This coincidence illustrates one of the key problems in contingency planning for patient safety. Even when 'market leading' solutions are chosen there is still the possibility that infrastructure failures will undermine service provision. The April 2008 failure also shows how significant investments following a previous incident are no guarantee of future reliability. In particular, the simultaneous loss of VA hardware and network service provision demonstrates the importance of extending the application of contingency planning techniques from other domains to support patient safety. This incident provides a case of what the power distribution and aviation industries term an 'n-2' failure; it is routine practice in these areas not simply to focus on mitigating the consequences of a single infrastructure component but also to develop contingency plans that address up to two simultaneous problems (Johnson et al, 2008). Hence the April 2008 incident illustrates that irrespective of the reasons for the failures there remain significant learning opportunities for organizations such as the VA to continue strengthening their IT infrastructures. Looking to the future, the executive director of the VA's Office of Enterprise Infrastructure Engineering said in 2008 repeated his commitment that in modernising VistA "we will not break it" but he was forced to recognise that some of the core databases developed in the previous 'open source' era will continue to be used a decade from now (Brewin, 2008).

3. Lessons Learned for the Development of Healthcare Information Systems

Previous sections have identified a host of lessons that emerge from a comparison of incidents affecting the NHS CfH and VA's VistA. There are superficial similarities in the proximate causes of the two incidents; both stemmed from configuration management problems. There were further similarities in terms of the response; in both cases the difficulty of diagnosing the causes of the failure prevented the organisations involved from using the secondary redundant facilities that had been designed to provide fallback protection. However, these two incidents also reveal deeper causes that lie in the political problems that stem from the centralisation of healthcare information technology. The difficulties that local clinicians experienced in obtaining accurate assessments about the extent of the failure from centralised software and maintenance teams helped to undermine confidence in the system. The two incidents in the UK and the US both exacerbated the tensions that were created as national initiatives sought to impose standardised processes of software procurement and development over infrastructures that had previously experienced considerable local autonomy. To this extent, there are as many political and organisational insights from these failures as there are technical lessons to be learned for the future development of healthcare information systems.

A number of further lessons can be identified from the problems experienced during the interruption to service provision in the Maidstone and Sacramento data centres:

1. **No exchange of lessons learned between US and UK/Europe.** The meta-level insights from these two failures include the need to create a forum for the exchange of best practices across national healthcare information systems. In writing this paper, the author has had considerable support and encouragement from individuals involved in these incidents. Their willingness to discuss the causes of the problems provides a valuable foundation for future development both in the UK NHS and in the VA. However, neither agency was aware that the other had faced almost identical problems with their information infrastructures. There is no easy way for technical teams and for systems management to exchange best practices in the same way that, for example, the aviation industry disseminated lessons learned between many different ICAO nations.

2. **The Importance of Configuration Management.** One of the most important technical insights from these two incidents is the role that configuration management plays in the delivery of complex, healthcare infrastructures (Johnson et al, 2009). In the VA and the NHS case studies, considerable skill and expertise was devoted to ensure the provision of redundant architectures for the provision of reliable information systems. However, these architectures were undermined by subsequent changes in configuration. In the Maidstone failure, staff did not recognise that one of the SAN disk arrays was configured with different microcode to their peer. In the Sacramento incident, the system was reconfigured to disable fallback provision while test accounts were created and to store backup data. The meta-level lesson is that the development of centralised IT support for healthcare information technology increases the need to follow consistent and rigorous configuration management processes because the consequences of any failure can extend across regional and local boundaries.

3. **Failure of Redundancy in Complex National Infrastructures.** Redundancy remains one of the more influential techniques for increasing the resilience of safety-critical systems. As we have seen, however, there is a danger that we are placing undue confidence in the use of this approach within complex software systems. In particular, the difficulty of diagnosing the causes of particular bugs will often dissuade senior management from rolling over a failed system onto available secondary hardware because of the risks that this might replicate the initial fault. One of the lessons from these two failures is that senior management must drill and rehearse the decision making processes that are required to coordinate the deployment of redundant architectures. The aim of these exercises is to reduce the uncertainty and the fear that can arise when organisations have to respond to major system failures. Unless management are prepared to make these difficult decisions then there is a risk that we are wasting enormous sums of money on the procurement of redundant, fallback systems that are then not used in the aftermath of an initial failure.

4. **Complexity of Maintaining Communications with Subcontractors.** In both incidents, it proved to be difficult to obtain accurate estimates about the extent of the problems from the sub-contractors who were responsible for maintaining the infrastructures that were affected by the failures. In the NHS case study, CfH staff had to deal both with teams from CSC and from the HDS hardware supplier. Similar communications issues affected VA staff as they coordinated their response with an external contractor who was simultaneously reviewing the performance of a hardware platform running on a particular virtual memory configuration.

5. **Complexity of Maintaining Communications with Local Clinicians.** The difficulty of obtaining accurate technical assessments of the extent and duration of these failures from their sub-contracting agencies had a number of knock-on effects in terms of managements' ability

to coordinate appropriate responses to the NHS and VA incidents. Arguably the most significant problems focused on communications with local clinicians. Senior IT management were seen to lack confidence in their initial predictions. This undermined clinical confidence in the response to the problem which was compounded by their focus on the provision of healthcare rather than on understanding the organisational and technical problems that prevented accurate estimates of the time to recover from any failure. Management uncertainty and the problems in communicating with local clinicians only served to exacerbate existing tensions over the centralisation of IT services in both the VA and the NHS. In previous years, clinicians knew who to contact to obtain accurate local assessments of potential failures. Delays from centralised IT services in providing information about the extent of the failures placed local IT managers in a difficult position. They could no longer give clinical staff the detailed predictions about the extent and duration of the failure that they required in order to schedule healthcare provision.

6. **Vulnerability of Paper Processes.** Both case studies demonstrated the vulnerability of healthcare providers to failures in their IT infrastructures. The impact was arguably greater in the case of the VistA problems because more progress had been made towards the integration of services through the IT architecture. Hence, the loss of facilities and the subsequent need to resort to manual alternatives following the loss of the Sacramento service provides numerous detailed insights for the future planning of IT resilience within the NHS. It also reiterates the importance of practicing the use of paper-based fallbacks as staff become more and more accustomed to the services provided by applications such as VistA and Lorenzo.

This list provides a partial summary of lessons that can be learned across national information systems. Further work remains to be done to identify further parallels between these and other failures that have affected UK and US healthcare architectures. For instance, recent security violations in both the VA and NHS have raised similar ethical concerns. It remains to be seen whether these failures share common root causes, just as the Maidstone and Sacramento failures stemmed from the difficulty of managing complex centralised software through a range of contracting organisations.

4. Conclusions and Further Work

Public and private organizations have invested increasing amounts into the development of healthcare information systems. These applications are perceived to offer numerous benefits. Standardization improves the exchange of information between healthcare facilities and helps to increase consistency between different regional service providers. Electronic patient records ensure minimum standards across the trajectory of care when patients move between different specializations. Healthcare information systems also offer economic benefits through efficiency savings; for example by helping to identify potential bottlenecks in the provision and administration of care. However, a number of high-profile failures have revealed the problems that arise when staff must cope with the loss of these applications. In particular, teams have to retrieve paper based records that often lack the detail they have become accustomed to with electronic systems. Individuals who have only ever used electronic information systems face particular problems in learning how to use paper based fallbacks. It is, therefore, important that we learn as much as possible from previous failures of healthcare information systems.

This paper has identified common lessons that can be learned from two different incidents in the UK NHS and the US Veteran's Affairs Administration. The UK case study focused on the loss of the Lorenzo system from incompatibilities in the microcode associated with two SAN disk servers. In contrast, the VA incident stemmed from a change to the network port configuration for the VistA servers. In both cases, the underlying causes related to problems in the provision of centralised services across complex local healthcare systems. The common features between these two incidents reveal an urgent need to improve the exchange of information about previous failures between Europe and North America. For example, both incidents illustrate the need for strong configuration management processes as local adaptations and updates are introduced into centralised architectures.

The two incidents studied in this paper also point to vulnerabilities in the use of redundancy as a means of increasing the resilience of national healthcare information systems. In both cases, senior management were reluctant to roll-back to secondary facilities in case they replicated the problems in primary facilities. Further lessons relate to the difficulty that information systems provider's face in obtaining accurate information about the scope and duration of a failure from different sub-contracting organisations. These problems, in turn, undermine clinical confidence in IT management when they cannot obtain accurate information about the impact of centralised failures on the local provision of healthcare services. Finally, it has been argued that the failure of the NHS and VA information systems reiterates the importance of training staff to use the paper fallbacks that are necessary when we cannot guarantee the availability of complex information systems. These observations reiterate the need to exchange lessons learned in previous failures across international borders as more and more countries extend the integration of electronic patient records into wider aspects of healthcare provision.

Acknowledgements

Thanks are due to the members of the US AHRQ project Reducing Risks by Engineering Resilience into Healthcare Information Technology for Emergency Departments (grant number R18 HS0 17902). Discussions within this group provided the initial idea for this paper and have helped to shape the arguments. Thanks are also due to both the Veterans' Affairs Administration and to the NHS Connecting for Health directorate. Unless UK and Federal agencies are willing to discuss the technical details of the small number of adverse events that affect their systems then there is little prospect that we will be resilient to future incidents. Any errors remain the sole responsibility of the author – the intention is to revise this draft in response to comments that should be sent to the address given at the start of this paper.

References

Associated Press, Software Hiccups Cause Drug, Treatment Errors at VA, January 14, 2009.

B. Brewin, Veterans Affairs Aims To Update and Centralize IT Systems, GovernmentExecutive.com, 21st February 2008.

J. Bolger and M. Costello, Sparks fly between ISoft and CSC: The troubled NHS contractor believes America's CSC may have unreasonably blocked its £233m deal with IBA. The Times Newspaper, 1st June 1, 2007.

G. Borriello, V. Stanford, C. Narayanaswami and W. Menning, Pervasive Computing in Healthcare, IEEE Pervasive Computing, (6)1:17 – 19, January-March 2007.

Committee on Veterans' Affairs in the US House of Representatives, The U.S. Department Of Veterans Affairs Information Technology Reorganization: How Far Has VA Come? 26th September 2007, Serial No. 110–47 (2007).

J. Conn, California System Faced Epic Vista Failures: Report. Modern Healthcare, 1st October 2007.

eHealthMedia, CSC failure leaves 80 trusts without IT systems, 31 Jul 2006. Available on: http://www.e-health-insider.com/News/2036/csc_failure_leaves_80_trusts_without_it_systems, last accessed October, 2009.

S. Hoffman and A. Podgurski, Finding A Cure: The Case For Regulation and Oversight Of Electronic Health Record Systems, Harvard Journal of Law & Technology, 22(1):104-165, 2008.

iSOFT, Case Study: Salford Royal Hospitals NHS Trust. Available on: http://www.isoftplc.com/text/customers/2495.asp, last accessed October, 2009.

C.W. Johnson, Politics and Patient Safety Don't Mix: Understanding the Failure of Large-Scale Software Procurement for Healthcare Systems. In P. Casely and C.W. Johnson (eds), Fourth IET Systems Safety Conference, IET Conference Publications, Savoy Place, London, 2009.

C.W. Johnson, G. Amar, T. Licu and R. Lawrence, High-Level Architectures for Contingency Planning in Air Traffic Management. In R.J. Simmons, D.J. Mohan and M. Mullane (eds.) Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008, International Systems Safety Society, Unionville, VA, USA, 0-9721385-8-7, 2008.

C.W. Johnson, L. Fletcher, C.M. Holloway and C. Shea, Configuration Management as a Common Factor in Space Related Mishaps. In Proceedings of the 27th International Conference on Systems Safety, Huntsville, Alabama, International Systems Safety Society, Unionville, VA, USA. 2009.

C. Mellor, NHS SAN failure: Why did 80 NHS trusts lose access to SAN data? Techworld, 4th August 2006.

M. Mosquera, VA Revisits Data Consolidation Plan, Federal Computer Week, 12th October 2007.

M. Mosquera, VA Data Center Outage Hobbles VistA Again, Federal Computer Week, 15th April 2008.

NHS Connecting for Health, North West and West Midlands CSC Maidstone Data Centre Issue, 2006. Available on: http://www.connectingforhealth.nhs.uk/newsroom/news-stories/data_centre_issue, last accessed October, 2009.

NHS Connecting for Health, Report on the CSC Data Centre Incident 30th July 2006, Ref. GH185S07, 2007. Available on: http://www.parliament.uk/deposits/depositedpapers/2007/DEP2007-0080.pdf, last accessed October, 2009.

D. Schaffhauser, The VA's Computer Systems Meltdown: What Happened and Why. ComputerWorld, 20th November 2007.

R.E. White, Health Information Technology Will Shift the Medical Care Paradigm. Journal of General Internal Medicine, 23(4): 495–499, April 2008.