Politics and Patient Safety Don't Mix:
Understanding the Failure of Large-Scale Software Procurement for Healthcare Systems

C.W. Johnson,

Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK.

Telephone +44(141)3306053, Fax +44(141)3304913,
Email: Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

Keywords: Healthcare, Software Engineering, Patient Safety.

Abstract

President Obama has recently announced an additional $50 billion to support the development of healthcare informatics and electronic patient records systems. Public attention has, therefore, focused on ensuring that such investments do not suffer from the failures that have afflicted previous large-scale software procurements. This paper analyses a number of recent failures that have affected applications used by the Veterans Health Administration (VHA). The following sections describe the technical causes for these problems; tracing them back into the software engineering practices and project management techniques that have been used within the Department of Veterans Affairs (VA). However, the key argument in the paper is that these causes have been obscured by political arguments. In 2005, the VA centralized responsibility for IT infrastructure under a Chief Information Officer. Before this, each center had considerable autonomy in managing their IT budget and in organizing software development projects. We argue that attitudes to recent software failures are determined by individual perspectives on the political and organizational consequences of this reorganization. Some stakeholders have argued that recent software failures are due to the introduction of standardized development practices and centralized management techniques that ignore the end-user. They maintain that the changes of 2005 have obscured the clinical focus that is seen as essential for the successful development of healthcare informatics. In contrast, other agencies have argued that previous failures, which threatened patient safety, were often under-reported in the decentralized approach. They argue that standardization is essential for progress towards an integrated healthcare system and for ensuring accountability when failures do occur. We argue that these two perspectives have become so entrenched that they underestimate the complexity of software engineering and obscure the additional pressures that political uncertainty places on the technical development of healthcare information systems. It is concluded that by mixing politics and patient safety, there is a danger that we will waste the opportunities provided by new investments in healthcare informatics.

1. Introduction

This paper considers the interactions between the political and technical context of software development within large-scale national healthcare systems. Politics is defined to be the process by which groups make decisions. A key argument in this paper is that decisions about the technical development of large scale IT systems is often based more on political allegiances or shared views within an organization than on objective criteria. In particular, we examine the conflicts that have arisen over recent reforms in the software development practices being used within the US Veterans Health Administration. One group continues to support the clinician-focused development of software by cooperative agreements between local healthcare facilities based on an open source model. Other groups have opposed this approach arguing that a more centralized development process is required to ensure consistency with other national organizations, in particular with the Department of Defense. Unless readers understand the history and context behind these different viewpoints it is difficult to appreciate the detailed technical arguments that have been made both for and against architectures that have been proposed for future VA healthcare systems.

In one sense it should not be surprising that political decision making has a profound impact on the technical development and reliability of healthcare informatics. Hoffman & Podgurski (2008) note that “Politicians and government leaders have expressed great enthusiasm for the development and implementation of Electronic Health Record systems”. They trace recent political interest back to President Bush’s 2004 announcement that the National

Health Information Network will computerize 'most' American's health records within a decade. This led to subsequent support for healthcare informatics as key elements within the campaigns of Senators McCain and Obama. As we shall see, the subsequent passage of Obama's Stimulus Bill has further cemented this relationship between politics and technological innovation in healthcare informatics.

1.1 Successes and Failures in National Healthcare Systems

The public, media and political bodies often focus on failures in the procurement of large scale IT systems (Johnson, 2003). However, there are success stories. For example, the US Department of Veterans Affairs (VA), through its Veterans Health Administration (VHA), developed the Veterans Health Information Systems & Technology Architecture (VistA) that recently won an 'Innovations in American Government' Award (IAGA, 2006). The citation focused on the way in which clinicians could use the system when many of the 40,000 veterans who were affected by Hurricane Katrina had to flee the Gulf Coast without their medical records. The program's decentralized, flexible approach provided resilience even when records centers were destroyed by flooding. The award also praised the relatively low cost approach that had led to the distributed development of the VistA architecture with help from many centers across the country, rather than a centralized approach to procurement; "the system is designed and continually improved by front-line clinicians in the VA's 1,400 health care facilities nationwide". The involvement of clinical staff and of those involved in the local maintenance of the patient records systems supported the development of a successful product and contributed to a 'transformation' in the VA's quality of healthcare (Yano et al, 2007). The success of VistA has led to its adoption in countries as diverse as Mexico, Finland, Jordan, Germany, Nigeria, Egypt, Malaysia, India, Brazil, Pakistan and Samoa (Protti and Groen, 2008).

One of the complexities of healthcare informatics is that different stakeholders use different criteria to judge the success or failure of projects. At the same time as VistA was winning awards, the US General Accounting Office (1996, 2008, 2009) issued a series of reports that criticized software development practices across the Veterans Health Administration. A series of 'high-profile' failures also affected VA applications (Associated Press, 2009). Kuehn (2009) describes how a software 'update' at VA hospitals in August 2008 introduced a bug so that "health care workers at these facilities began to report that as they moved from the records of one patient to those of a second patient, they would sometimes see the first patient's information displayed under the second patient's name". This problem would only exhibit itself after a particular sequence of interactions; however, incidents were reported in 41 out of 153 VA medical centers. A notification about the problem was distributed in October and a bug fix sent out in December 2008. However, nine centers reported further issues with the electronic records system where physician's orders to stop medication were missed. Previously instructions to discontinue intravenous medications were displayed at the top of a screen. After another software update, these instructions were no longer displayed. Three patients are known to have received herapin for up to eleven hours longer than their clinician advised. Other patients received infusions of either sodium chloride or dextrose mixtures for up to 15 hours past the doctors' prescribed deadline (Associated Press, 2009).

There do not seem to have been any long-term adverse consequences before these software problems were corrected in December 2008. However, these previous incidents were widely publicised at a time when the Obama administration was promoting informatics as a corner-stone for healthcare reform. The apparent failings create concerns that future investments in healthcare informatics may be wasted (Wears and Berg, 2005). In particular, there is a danger that unless we learn from the problems in existing applications then the widespread adoption of electronic records systems may be undermined. The response to these failures can be understood at a number of different levels. Technical concerns were raised about specific software engineering deficiencies that threaten patient safety (Kuehn, 2009). The failures were also interpreted as symptoms of wider managerial and organisational problems, identified in the GAO reports (2003, 2008, 2009). However, these issues cannot be understood without some reference to the changing political environment that affects organisations such as the Department of Veterans Affairs.

1.2 Political Concerns: Relationships with the Department of Defence

Many politicians have urged closer cooperation between the VA and other healthcare services offered within the Department of Defence. They have sought both to reduce the costs associated with the development of parallel systems and also to improve functionality so that health records might be exchanged in a 'seamless' fashion when personnel move between the services provided by the VA and DoD. In April 2004, President Bush called for interoperable electronic health records by 2014. Secretary Eric Shinseki and Defense Secretary Robert Gates backed

initiatives to integrate VistA with the DoD's Military Health Systems Armed Forces Health Longitudinal Technology Application (AHLTA). However, there are considerable technical, philosophical and political barriers to this integration. As we have seen, VistA can be thought of as a suite of systems developed in-house by VA clinicians and IT personnel. In contrast, the DoD has traditionally relied on commercial software products that are customized for very specific uses (GAO, 2009). This creates barriers to integration where, for instance, the open source elements of VistA must interact with proprietary DoD applications. For instance, the DoD's Composite Health Care System (CHCS) captures pharmacy, radiology, and laboratory information while the Clinical Information System (CIS) provides a 'customized' commercial health information system to support inpatient treatment at military medical facilities (GAO, 2009). The roadmap for achieving the integration of these applications is through the HealtheVet initiative. This consists of eight software development areas. The most advanced is the Health Data Repository (HDR) database, which became operational in 2006 with a subset of health care data. At present, it contains standardized health data in areas that were given high priority by clinicians: vital signs, allergies, and outpatient pharmacy. This has enabled the VA and DoD to exchange pharmacy and drug allergy data on over 21,000 shared patients, an increase of about 2,700 patients between June and October 2008 (GAO, 2009). This process of standardisation supports data exchange with the formats used within the DoD. It is being extended to laboratory data, inpatient pharmacy data, dental, and ophthalmology (GAO 2003, GAO 2008). The importance of these initiatives can be illustrated by the scale of the financial commitment. Between 2001 and 2007, the VA spent some $600 million on the different strands of HealtheVet. The estimated cost for completion is in the order of $11 billion.

1.3 Political Concerns: Centralization, Standardization and Clinical Focus

The software failures, summarized above, have fueled a complex debate about the future of software development in the VA. Critical reports from the GAO (1996, 2009), by the VA's own Inspector General (2006, 2007) and by independent bodies, including CMU's Software Engineering Institute (GAO, 2008), identified weaknesses across the development lifecycle. In particular, the GAO/SEI (1996) review found that the distributed model of software development within the VA did not attain level 2 of the SEI maturity model in any of the seven projects that they studied. This is the most basic requirement for repeatable software development. At this level, the outcome of a project may be due to chance rather than the output of a recognizable process. There is no guarantee of success if a similar project were to be undertaken in the future. The VA was found to lack the discipline and control needed to mitigate development risks. The review concluded that they were "extremely weak in the requirements management, software project planning, and software subcontract management ... with no identifiable strengths or improvement activities. As a level 1 organization, VBA cannot reliably develop and maintain high-quality software on any major project within existing cost and schedule constraints, placing the VBA modernization program at risk" (GAO, 1996). This critical review triggered a range of organisational and technical changes across the VA. However, the SEI was again asked to review software development practices within the Veterans Health Administration as part of the HealtheVet program (GAO, 2008). This found further problems in the governance and management of software development. A programme was created to support decision-making processes by identifying areas of responsibility and levels of authority across the software lifecycle. However, a wider reorganization of the VA's IT management structure was triggered before many of the SEI recommendations could be acted upon.

In October 2005, the VA followed recommendations from Congress and created a Chief Information Officer. The intention was to centralize control of the IT budget and help 'standardizing operations and systems development across the department using new management processes based on industry best practices' (GAO, 2008). **It is impossible to understand the technical and organizational response to recent VA system failures without first considering the impact of these changes in the internal management of software development.** Prior to the centralization, IT funding and approval were controlled by each medical center director. The VA's 150 medical centers 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 process of centralization also had an impact on development practices. Before 2005, changes could be made to applications, such as VistA, on a local or regional basis. Hence there might be several parallel versions of applications running in different centers. Local IT officers liaised with the center 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 with external organizations including the DoD. These distributed development practices also created concerns over a range of non-functional requirements including security, infrastructure administration and disaster recovery.

The 2005 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. 6,000 posts were reassigned within a more centralized management framework. Within the IT function, the changes led to the introduction of a three part governance model (GAO, 2009, OIG, 1996). A technical component advisory council meets every weekly to discuss and prioritize projects. This is supported by a regional governance board that focuses on higher-level issues related to IT infrastructure. Finally, a monthly executive partnership council helps to coordinate IT work processes with stakeholders from the medical facilities being served in that region The acting director of the four regional centers described how before centralization "There was a sliver of an employee's [time] at every medical center that was supporting this application. There was no structure [for] maintenance and upgrades, no coordination in how we handled problem management. When a problem surfaced, 33 trouble tickets would be logged" (Schaffhauser, 2007). This led to the unnecessary duplication of tasks as each center looked for local solutions to common problems.

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 coding compliance tool was introduced across all of the 33 medical centers within Region 1 of the four mentioned above. This ensured that all of the VA facilities in that area were running the same version of an application. Such tools are critical if a central team is to respond to requests for support – without it they may not be able to identify whether a particular problem is common across all versions of an application or whether it is caused by a particular configuration of one local instance. The introduction of the coding compliance tool helped to monitor problem reports and develop coordinated responses. The acting director of the four regional centers went on to describe the difficult balance between centralized control and distributed support "the message I send to my folks in my organization is, 'You may work ultimately for me within Office of Information and Technology, but you absolutely work for the network or facility where you're stationed… The goal is to create that bench strength we've never had" (Schaffhauser, 2007).

A number of further arguments were put forward in support of the centralization process. By bringing IT staff under the control of a single administrative function, it was possible to create an appropriate career structure for systems professionals. In the past, many of the best staff in local VA centers left because there was little scope to extend their skills within local hospitals. In the new centralized approach, career progression could be mapped into more senior levels of project management enabling more coherent succession planning in an area where organizational experience is a key enabler. Similarly, the centralization of IT services helped to ring-fence training resources. Before 2005, local IT managers often found their budgets for staff development had come under pressure when other members of staff required training. . Above all, the centralization was proposed as a means of introducing a holistic approach to information management. The intention was to encourage a broader perspective that might not otherwise have been possible when core functions and staff were isolated within individual medical centers (Mosquera, 2009).

In contrast, the proponents of the previous, distributed software development model argued that recent failures are the result of centralization (Conn, 2009). By focusing responsibility for data management on regional data centers, the VA has created common points of failure. In the past, it was unlikely that a software fault would affect multiple centers at the same time given the looser coupling between each site. It has also been argued that the process of centralization has moved IT support away from the 'sharp end' of clinical practice. The need for standardization – both in terms of software development and in terms of the data formats that support information exchange with other agencies, including the DoD, have undermined clinician centered development. Before the reorganization, medical staff could arrange a meeting with local software teams to introduce changes that were specifically intended to support healthcare practices within their organization. Information technology was tailored for the local context. The reorganization introduced centralized control over configuration management. It arguably became more difficult to tailor specific applications for local needs given that greater consistency was required to ensure that all medical centers met the same requirements for security, data interchange, recovery etc. In consequence, Koppel et al (2005) maintain that clinicians must not be compelled to use the new generation of centralized applications until they are placed at the heart of software development practices. These comments cannot be understood without considering the political and organizational context of the VA. They must also be balanced by the opposing arguments from those who support centralization. For instance, arguments that centralization is incompatible with a

'clinician centered' approach are often contrasted with the 'patient centered' view that someone seeking medical support should receive the same standard of care no matter where they require it.

1.4 Technical Concerns: Security

The centralization of software development practices was identified as a means of addressing high-profile security breaches (OIG, 2006, OIG 2007). There were at least 1,500 reported security incidents in the VA that involved the loss of personal information between December 2003 and January 2007 (US House of Representatives, 2007):

- December 2003, a VA laptop was stolen from an employee working at home. This machine had data about 100 benefit appellants stored on it. This prompted VA staff to recall all laptops so that encryption software could be installed on them.

- November 2004, a software update made a disk drive visible outside the VA. This contained veterans' person information including names, Social Security numbers, dates of birth, and some personal health information including surgery schedules and diagnoses.

- December 2004, two personal computers were stolen from a locked research office of a medical center. One had files containing names, Social Security numbers, next of kin, addresses, and phone numbers of approximately 2,000 patients. The computers were password protected by the standard VA password system. Letters were mailed to all research subjects informing them of the computer theft and potential for identity theft. VA enclosed letters addressed to three major credit agencies and postage paid envelopes.

- March 2005, an individual reported e-mailing a list of 897 providers' names and Social Security numbers to a new transcription company. This was immediately reported, and the supervisor called the transcription company and spoke with the owner and requested that the file be destroyed immediately. Notification letters were sent out to all 897 providers. Disciplinary action was taken against the employee.

- October 2005, a personal computer that contained information on 421 patients was stolen from a medical center. The information on the computer included patients' names; the last four digits of their Social Security numbers; and their height, weight, allergies, medications, recent lab results, and diagnoses. The agency's Privacy Officer and medical center information security officer were notified.

- February 2006 a VA staff member accessed several co-workers' medical records to find date of birth. Employee information was compromised and several records were accessed on more than one occasion.

- April 2006 a former VA employee was suspected of hacking into a medical center computer system with the assistance of a current employee providing rotating administrator passwords. All systems in the medical center serving 79,000 veterans were compromised.

- May 2006 an office determined it was missing a backup tape containing sensitive information. Approximately 7,052 veterans were affected by the incident. 5,000 veterans received credit protection and data breach analysis for 2 years.

- August 2006, a desktop computer was stolen from a secured area at a contractor facility in Virginia that processes financial accounts for VA. The desktop computer was not encrypted.

- September 2006, a laptop attached to a medical device at a VA medical center was stolen. It contained patient information on an unknown number of individuals.

- January 2007, an external hard drive used to store research data with 535,000 individual records and 1.3 million non-VA physician provider records was discovered missing or stolen from a research facility in Birmingham, Alabama.

Just as costs savings and enhanced functionality have motivated politicians and the public to advocate a closer integration of the VA and DoD systems, security concerns have also motivated calls for the centralisation of information management. Access control and conformance to security management principles can be more tightly enforced in a smaller number of regional centres than in every one of the 150 medical facilities; "VA officials have said the consolidation will improve information security and help the department apply consistent and standardized management practices for critical information systems" (Mosquera, 2008). Following these failures, the VA looked to external companies to provide core security services. These included a $6.7 million contract to provide port monitoring software and device control to ensure that unauthorised hardware was not being attached to VA network infrastructure (Mosquera, 2007a). A further contract worth $5.2 million was awarded to develop a rights management service to implement access control functions, including the development of secure email attachments and file store protection for both PCs and BlackBerry's. $13.4 was devoted to secure Internet communications, including the development of a terminal emulator for remote connections. Steps were also taken to lease desktop PCs according to a standard configuration, again centralising aspects of local procurement that had been the practice before 2005. The VA's chief security officer argued that these changes represented a 'comprehensive plan' that avoided the previous 'piecemeal approach' to security (Mosquera, 2007a).

These security changes did not simply have a technical impact. They carried with them the same organisation and socio-technical consequences that complicated other aspects of the VA's IT infrastructure centralisation. The Director of one VA medical centre described how new security measures constrained activities that had previously been at the discretion of local facilities. Changes in security policy introduced new complexity, for example in scheduling teleconferences. "For example, to fully comply with security requirements on our examination-room PCs, we must log out of both a clinical application such as our Computerized Patient Record System and the Microsoft Windows operating system each time we leave the room even for a moment, yet it may take as long as 12 minutes to log back on when we return. Given a 20- or 30-minute visit with their veteran patient, the clinician is thus forced to choose to "do the right thing" for either the patient or the system, but cannot do both, the bad news is that centralization of physical IT resources to the (regional approach) has directly led to more system downtime for individual medical centers than they have ever had before, resulting in hundreds of simultaneous threats to the safety of our veteran patients" (Conn, 2007).

1.5 Technical Concerns: Open Source and Commercialisation

The organisational changes that have affected the VA IT infrastructure have fuelled a wider debate about software development practices. In the past, VA software was typically developed as a cooperative enterprise between programmers in different public healthcare organisations (Timson, 2009). This approach had its roots in the 1970s when John Chase, the VA's Chief Medical Director, established the precursor of VistA, known as the Decentralized Hospital Computer Program (DHCP). Congressman Gilbert "Sonny" Montgomery then worked to establish that VA code, derived from public healthcare projects, was legally in the public domain. Hence, VistA became an open source project for government healthcare organisations. The availability of the source code supported further decentralisation as distinct versions of the same system began to be developed by different organisations. At the same time as the VA supported the VistA core, the Department of Defense reused many libraries and routines in their Composite Health Care System, the Indian Health Service also extended their Resource and Patient Management System in a similar fashion. By 2004, this public sharing of the VistA core had created a situation in which a common code base was split between three or more principle variants. This created considerable strengths as new ideas and concepts could be shared between the VistA communities. However, it also added to the sense of decentralised organisation and heterogeneous development practices that were so heavily criticised in the GAO and SEI reports – which arguably paid insufficient attention to the relative strengths of open source development projects. For instance, the original developers of the VistA code called themselves the Hardhats and this informal self-help group continues to provide a focus for further development. Their work has also been supported by the WorldVista organisation, located at http://worldvista.sourceforge.net in March, 2009. WorldVista provides a legal entity as a non-profit corporation that can pursue grants, enter into contracts etc but with the same "spirit of initiative and volunteerism" that helped launch VistA.

The distributed cooperative model of software development promoted by the open source community has been widely advocated as a solution to the problems of large-scale IT procurement in government projects. For instance, in April 2006 the US Undersecretary of Defense for Advanced Systems and Concepts commissioned the Open

Technology Development road map. This advocated the use of open source approaches to encourage reuse and reduce software costs across the Department of Defence. The roadmap addressed the wider issues of intellectual property, licensing and valuing open-source solutions that had already been considered within the VistA community. The DoD report concluded that open source approaches would encourage industry to compete on ideas rather than rely on proprietary approaches that 'lock in' the customer to particular solutions. Unfortunately, there has been a relatively limited uptake of open source approaches across government. Typically, the code from a previous contractor is only made available when a new contractor takes their place. The open source model not only requires significant structural changes in the organisation of government contracts, it also requires a considerable 'shift in perspective' on behalf of numerous contractors who have significant investments in the proprietary models of procurement that are the norm.

The centralisation of IT procurement and development within the VA, therefore, occurs against a wider background of structural change in the acquisition and management of government information technology contracts. The proponents of the open source model point to numerous high-profile failures. In particular, the supporters of the traditional VistA decentralised approach have pointed to the $247 million write-off Core Financial and Logistics System (CoreFLS) procured from a defence contractor (OIG, 2004). The subsequent reports reveal the underlying tensions within the VA and similar organizations faced with decentralized development practices. The Inspector General was careful not to blame the problems on the use of proprietary development practices but instead identified problems in the local control of IT services – hence the issues of open source development cannot be understood in isolation from the political and organizational analysis presented in previous sections. The OIG (2004) concluded that the "success of CoreFLS is highly dependent on the ability of the software to integrate with existing VA legacy systems" including VistA and the Generic Inventory Package (GIP). The problems identified in the initial deployment of early versions of the CoreFLS arose because "most of the VA legacy systems contained inaccurate data because they had not been used properly, and that this may be a systemic problem throughout the Veterans Health Administration (VHA). The effect of transferring inaccurate data to CoreFLS interrupted patient care and medical center operations. We are concerned that similar conversion problems will occur at other VA facilities". There was insufficient training of staff to help hospital employees in the pilot sites prepare for the introduction of the new system. There was no plan for a phase or parallel introduction so that staff could fall back to a previous system if problems were encountered. This "resulted in unnecessary risk to patient care and the inability to monitor fiscal and acquisition operations" (OIG, 2004). Security concerns included a lack of background checks for the contractor's employees. The duties and responsibilities for the CoreFLS administrators were not adequately partitioned; individual users could acquire administrative rights. CoreFLS managers did not follow authorised procedures for the revision of the software and hence there were systemic concerns about the integrity of the application. Finally, it was argued that the security of the system was compromised because managers "did not have an effective contingency plan to protect CoreFLS assets and functionality. They might not then have been able to recover the system following any potential security incident or other emergency event. The investigation also argued that the VA's management of the CoreFLS software development did not protect the interests of the government. The contractor was the sole provider and the VA management accepted their statements of work and cost estimates without independent verification. Payments were made to the contractor for completion of work that had not been delivered. Modifications and updates were requested by the VA and paid for without sufficient justification or documentation to support external audit processes.

The failure of the CoreFLS challenged the adoption of proprietary software practices across the VA. As we have seen, however, the 'lessons learned' from this incident illustrates the contradiction at the heart of recent debates about the future of healthcare procurement. The proponents of a decentralised approach argue that the failure occurred because the developers did not take account of, nor did they support, the local context of operation within the VA facilities. In contract, the proponents of a more centralised approach to software development and procurement argue that CoreFLS failed precisely because those decentralised practices had enabled local variations that undermined the security and economy of previous applications. These are arguments that go beyond the narrow technical debates about open source software. They reflect deeply held, political and social views about the shape of government procurement in the field of healthcare informatics.

It is against the background of the failure of CoreFLS that the VA launched their initiatives to modernise the VistA application. The 2009 budget argued that this application "was created more than 20 years ago and is inefficient, limits revenue collection, does not meet current regulatory requirements, potentially jeopardizes patient safety, and is

unable to support planned quality improvements to patient care." As might be expected from the previous analysis of the GAO, SEI and OIG reports, the VA leadership focused on centralised and proprietary approaches rather than open source, federated development practices. In 2006, the decision was taken to replace the VistA laboratory information systems module with proprietary software purchased from a commercial vendor. The contract requested the development, testing and national implementation of the vendor's lab system throughout the VA. It was awarded following an analysis of the cost estimates between proprietary outsourcing and an internal upgrade to existing VistA lab module. As we write, the new lab software still has to be integrated within the other blocks that will be carried forward into the HealtheVet architecture with national deployment scheduled to start in 2010.

As might be expected, concerns have been raised about these changes almost from the time at which they were initiated in 2005 (Conn, 2007). A Director of Clinical Informatics in one of the VA centers presented evidence to the House of Representatives committee on Veterans' Affairs (2007) in which he described how "I believe that employees at some medical centers expressed a number of concerns about the details of the plan. In particular, I believe they felt that the regionalization of IT resources would create new points of failure that could not be controlled by the sites experiencing the impact, and that the system redundancy required to prevent this was never listed as a prerequisite to centralization of critical patient-care IT resources. From my point of view as the director of clinical informatics, it was clear to me that the focus of reorganization/realignment was on technical relationships and not on how the missions of the Veteran's Healthcare Administration would be communicated to the new Office of Information and Technology (OI&T) structure. For example, realignment success metrics were focused on (regional data processing center) deliverables rather than facility needs. Finally, key facility-based IT staff had been tightly integrated into local committees and planning groups as subject matter experts, but could no longer be tasked directly by the facility director to participate, and had no clear OI&T-driven incentive to continue. Ultimately, the concern was that in trying to create a new structure in the name of 'standardization,' support would wane to a 'lowest common denominator' for all facilities, no matter how diverse their actual needs were...In my view, there remains a tremendous uncertainty about how to work with our long-standing IT colleagues to address local or regional clinical care, research or educational needs...There is a sense of great inertia that overrides the anticipation of great opportunities in the new OI&T structure."

1.5 Macro-Politics, Obama's Stimulus Bill and the Centralization of Big Government

The previous paragraphs have sketched the complex interactions between the political and technical context of healthcare software development within the Department of Veterans Affairs. It is difficult to separate these different issues. One cannot simply look at the choice between proprietary and open source development techniques without also considering the debate between centralised control and distributed development. These debates also influence the perception of external agencies. For example, SEI's critical analysis of software project management shaped the reporting structures that led to the creation of four regional centres and the post of Chief Information Officer. Hence the technical advice that is provided by these agencies is often viewed in the context of previous reports that have had both a managerial and a political impact on the VA's healthcare provision.

It is important also to recognise that political views over open source and proprietary software development continue to shape the technical decisions that are being made across the Department of Veterans Affairs. The importance of understanding these influences cannot be underestimated given the scale of the resources that have been earmarked for healthcare informatics by the in-coming administration. It might seem as though the centralising tendencies of the VA senior management is in the ascendancy, supported by the findings of successive SEI and GAO reports. However, other groups within Congress continue to advocate the development of open-source IT systems for healthcare. President Obama recently signed a $787 billion economic stimulus package into law. This included provisions for tax cuts and also for investments in health care, infrastructure, energy and education as a means of pump priming job creation. The bill had mixed support, with minimal backing from Republican groups in Congress. The House Minority Leader John Boehner (R., Ohio) stated that "The flawed bill the president will sign today is a missed opportunity, one for which our children and grandchildren will pay a hefty price." This Stimulus Bill included incentives for health care facilities to replace paper records with electronic systems. Page 488 of the 800+ pages in the bill is particularly relevant in the context of this paper. This provides for a 'Study and Report on the Availability of Open Source Health Information Technology Systems'. By the 1st October 2010, the Secretary of Health and Human Services is instructed to present to Congress a report that describes:

(i) the current availability of open source health information technology systems to Federal safety net providers (including small, rural providers);

(ii) the total cost of ownership of such systems in comparison to the cost of proprietary commercial products available;

(iii) the ability of such systems to respond to the needs of, and be applied to, various populations (including children and disabled individuals); and

(iv) the capacity of such systems to facilitate interoperability.

These provisions within the Stimulus Bill illustrate how the micro-level political debates within the VA are only part of a wider debate between Republicans and Democrats over the nature of government across the United States. The provisions that focus on the creation of a national electronic patient record system have revived Republican concerns over the centralizing tendencies of 'Big Government'. These are a direct parallel to debates over the centralization of HealtheVet and VistA. A recent opinion piece described how 'Billions will be handed to companies creating these databases. Billions will be handed to universities to incorporate patient databases into the initial and ongoing training of health professionals' (McCullagh, 2009). It went on to argue that many Americans may not want to have their medical histories, including information about race and ethnicity, stored in an electronic format that is easily shared and searched for "bio-surveillance and public health" or "medical and clinical research". Particular privacy concerns have focused on differences between the Senate bill and the version presented to the House of Representatives. The Senate version includes a section that may permit marketing literature and direct mail to be sent to individuals based on the contents of a patient's e-records.

These concerns over privacy and centralisation extended to the procurement of the proposed national records systems. In particular, questions have been raised about the ways in which government might (ab)use its economic power to force companies and healthcare organisations to meet the 'standards and implementation' specifications that have been approved by government but which might not be fit for purpose given previous failures in the procurement of national IT systems. The centralising power of government was also criticised as short-circuiting a gradual move toward e-health records in terms that are strongly reminiscent of those used to support decentralised development across the VA. Before the publication of the Stimulus Bill, old systems were gradually being replaced or upgraded with solutions that were well tailored to their local context of use 'questions about security find better answers, and doctors and their staff become more familiar with the technology' (McCullagh, 2009). This decentralised process is being undermined by the centralising proposals in the Stimulus Bill, which envisages minimum standards for procedures and for data formats that will be required before local data might be introduced into a national system. This process will be backed up by financial sanctions – from 2015, physicians who do not participate as 'meaningful users' in the federal e-record initiative will receive less funding.

There are further parallels between the political debates at a national level over the Stimulus Bill and the controversies over software development within the VA. As mentioned previously, the post of Chief Information Officer was established to act as a focus for centralization within the Department of Veterans Affairs. The recent proposals for the development of a national patients' record system include provision for a National Coordinator of Health Information Technology. Just as the proponents of a decentralised approach within the VA attacked the post of CIO, others have attacked this more recent national proposal. The accusation is that the new post is part of a wider political programme that will force doctors to give up their autonomy (Daschle, 2008). The raw nature of the political divide is apparent when commentators argue that the National Coordinator will "monitor treatments to make sure your doctor is doing what the federal government deems appropriate and cost effective... The health-care industry is the largest employer in the U.S. It produces almost 17 percent of the nation's gross domestic product. Yet the bill treats health care the way European governments do: as a cost problem instead of a growth industry. Imagine limiting growth and innovation in the electronics or auto industry during this downturn. This stimulus is dangerous to your health and the economy" (McCaughey, 2009). Very few commentators pause to consider the implications of these political debates for patient safety. Unfortunately, recent experience shows that the risks to the end-users of healthcare services can be profoundly affected by the outcome of political decision making.

2. The Nexus between Politics and Patient Safety: Server Failure Case Study, 31st August 2007

The first half of this paper has provided an overview of the political pressures that are influencing technical software development practices both within the VA and more widely across the US healthcare industries. As we have seen, these pressures are helping to shape decisions that favor centralization and standardization over local cooperative enterprises for the development of healthcare informatics. The same influences are strongly tied to proprietary rather than open source solutions – although the complexity of the situation is revealed by groups arguing in favor of closer centralization using non-proprietary approaches to software development (Daschle, 2008). In contrast, the second half of this paper looks in more detail at a software related failure where patient safety was placed at risk. This case study is analyzed to identify lessons that can be learned from the interaction between political decision making and the technical development of healthcare informatics.

The case study focuses on an unscheduled system failure on 31st August 2007 involving the VA's Sacramento facility, one of the four data centers mentioned in previous sections. This was the most severe in a succession of more than fourteen failures that occurred since April of 2007 after the 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 centers 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 center 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 centers; they also affected local pharmacies. Many of these used VistA applications to automatically produce orders and labeling. 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).

The problems experienced at the Sacramento facility led to renewed questions about the process of centralizing the software development infrastructure across the VA (Brewin, 2007). In particular, a subsequent hearing of the Committee on Veterans' Affairs in the US House of Representatives (2007) reviewed the ways in which local development practices had been brought under the control of the Chief Information Officer and his staff. Several witnesses told representatives that the VA had created new points of failure. By establishing large regional centres, there had been a loss of redundancy as critical IT resources for patient care were removed from local facilities. However, as we shall see, this failure stemmed from a failure to follow the procedures for configuration and change management (Johnson et al, 2009). This is exactly the type of informal development practices that centralisation was intended to avoid, following the critical reports by the SEI, GAO (2009) and OIG (2004).

2.1 End-user Perspective

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 centers 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 three tier contingency plan. 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 center in Region 2. The second level of defense 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). The intention had been that both 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 Sacramento to Denver. However, The VA 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. 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. The final facility 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.

As mentioned, one facility had to rely on the 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. This created further problems for those areas where the facility had made most progress in the adoption or integration of electronic information systems. In several instances, the parallel paper based forms were no longer available and more recent staff 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. 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.

It is difficult to recreate the uncertainty that both technical and clinical staff 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 centers. Support officers in the Sacramento center 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 center

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.

2.2 Systems Support Perspective

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.

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."

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).

2.3 Lessons Learned and the Political Response

Many commentators were quick to link the failure to the centralization of IT services (Mosquera, 2007, 2009). 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).

Following the failure, some of the plans to migrate additional medical facilities to the regional centers were temporarily delayed. The Region 1 management organized an internal review with that reported to the assistant secretary of the Office of Information and Technology. This was extended to consider a number of alternate contingency 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 centers or risk propagating an undiagnosed error to the neighboring region. A key lesson learned from this incident was that centralization did not by itself provide the increased levels of resilience that some of its proponents had identified. In the immediate aftermath of the 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 centers 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. Section 1.3 has 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.

2.4 Epilogue

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 neighboring 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 center 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 centers from Colorado to California. As we have seen, however, the secondary impact of these interruptions propagated well beyond the primary user facilities. Different centers 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).

The VA's Office of Enterprise Development (OED) has continued to drive many of the changes that started in 2005. There has been an increased use of Enterprise Architectures as a mechanism to support the integration of the Office of Information and Technology with the end-user and business requirements. They have also worked hard to introduce industry leading practices for systems engineering across the VA. These include Capability Maturity Model Integration (CMMi); this is the successor to the Capability Maturity Model that was used in the earlier critical reports of the VA's software development practices (SEI, 1996). The OED have also promoted the 'leading' management processes defined in the Information Technology Infrastructure Library (ITIL), mentioned in previous sections. Further initiatives have sought to promote the Control Objectives for Information and related Technology (COBIT) within the VA. This provides a framework of best practices for information technology procurement and maintenance created by the Information Systems Audit and Control Association and the IT Governance Institute (ITGI). There have also been projects to introduce model-based requirements engineering together with elements of rapid application development and agile software engineering. Agile techniques include 'Test-Driven Development' where progress is continually assessed against a suite of verification requirements that are derived from user requirements in the earliest stages of a project. Project management has increasingly been based on risk assessment. These techniques are intended to help management identify possible contingencies, including problems in configuration management, hardware reliability and the failure of network infrastructure. However, all of these technical innovations are being integrated into a five step organisational design strategy that reinforces political and organisational objectives that have persisted since 2005:

1. Centralize development community;
2. Standardize the organization to greatest extent possible;
3. Merge remaining development activities into Organisational Enterprise Development;
4. Evolve the organization as OI&T establishes and matures new processes;
5. Integrate capabilities.

It is important not to underestimate the wider, cumulative impact of successive failures involving the VA information infrastructures. The combined effects of the security breaches, mentioned earlier, and the network interruptions during 2007 and 2008 have raised numerous wider questions about the supervision and regulation of healthcare

informatics. For instance, Kuehn (2009) has argued that although the makers of electronic records and information systems, such as VistA, have conducted rigorous tests on their implementation, there is a need for additional Federal oversight. The Certification Commission for Healthcare Information Technology has developed a certification programme. However, it lacks the technical and organization resources to monitor the many hundreds of new initiatives that have recently been launched in healthcare informatics. It also, arguably, requires additional sanctions to enforce recommendations. In particular, it may be necessary to transfer oversight to the US Food and Drug Administration, the Centers for Medicare & Medicaid Services, or a new governmental agency (Kuehn, 2009). Hoffman and Podgurski (2008) summarize the key issues when they argue that "The benefits of EHR systems will outweigh their risks only if these systems are developed and maintained with rigorous adherence to the best software engineering and medical informatics practices and if the various Electronic Healthcare Records systems can easily share information with each other. Regulatory intervention is needed to ensure that these goals are achieved. Once EHR systems are fully implemented, they become essential to proper patient care, and their failure is likely to endanger patient welfare".

7. Conclusions and Further Work

This paper has argued that technical decisions in the development and architecture of national healthcare information systems are profoundly influenced by political decisions both at a national level and within the organisations that must operate them. We have illustrated this argument by a detailed analysis of the changes that have occurred in the Veterans Health Administration's information infrastructure between 2005 and 2009. Prior to this time, information systems were largely maintained by healthcare facilities under the direction of their local directors. This provided a direct interface with the clinical and administrative staff that used these services. This helped to reduce the delays associated with configuration management and the tailoring of information technology to local requirements. Development of major infrastructure programmes could be distributed as a collective effort that, arguably, avoided many of the overheads associated with proprietary and 'off the shelf' commercial solutions that cannot easily be tailored to the diversity of VA requirements. However, this distributed approach also created concerns about resource management and the delivery of high-quality services across all VA sites. A number of security incidents were seen to be the result of lax local controls. There were also concerns about the need to deliver the data integrity and consistent interfaces that would be need to merge VA infrastructures with other branches of government, in particular the emerging DoD applications as part of the HealtheVet initiative. These concerns motivated the centralisation initiatives that were embodied in the creation of a Chief Information Officer. They had multiple objectives and were intended to: focus IT resources by reassigning more than 6,000 technical professionals with a unified management structure; strengthen oversight and compliance with information systems polices; implement 36 management processes defined in the Information Technology Infrastructure Library (ITIL); provide architectures that were better suited to meet a range of non-function requirements including security, infrastructure administration and disaster recovery. The political and organizational consequences of the centralization were profound. Budgetary control for information services moved from individual VA facilities to four data centers and beyond that to CIO's staff.

The second half of this paper analyzed a failure that helped to focus concerns over the provision of information services across the Veterans Health Administration. This incident stemmed from problems in the configuration management of the servers that were used within one of the four regional data centers, mentioned above. The impact of this failure was exacerbated by problems in implementing the available contingency plans. The idea of moving services from the failed center to another region was rejected on the day of the incident. There were concerns that this would propagate the failure to servers that were working normally. Further problems arose because one of the healthcare facilities could not access the accounts that were used to store 'read only' copies of critical patient data that provided a second level of contingency support. This case study was chosen for a number of reasons. It helped to illustrate the technological consequences that arise from organizational and political changes in complex organizations, such as the VA's Office of Information & Technology (OI&T). The proponents of centralization pointed to the failure to document configuration management changes and argued for closer supervision of IT processes. For them the failure of some existing contingency plans helped to reiterate the need for central control over these aspects of infrastructure service provision. The opponents of centralization argued that the failure demonstrated that the development of regional data centers had removed the redundancy, which was a key benefit of the distributed model. They also argued that this and subsequent problems undermined claims that

proprietary and commercial procurement models could provide levels of reliability that would not have been possible using cooperative or open source techniques.

Above all, the recent history of healthcare informatics within the VA has demonstrated the challenge of implementing large scale changes within complex organisations. The VA's Chief Information Officer had been under no illusion about the scale of the tasks that they faced; "This will not be an easy or quick transformation. There will be a few difficulties along the way, and it's natural for some people to be uncomfortable with change on such a scale. But the prospect of more standardization and interoperability we can harness through this centralization is exciting" (Schaffhauser, 2007).

Acknowledgements

One of the benefits of analyzing the implementation of healthcare policy in another country is that it provides a different perspective. Distance creates a certain degree of isolation from the different political and organizational factions involved in particular debates. However, it can also create difficulties in interpreting the policies and programmes created by complex organizations such as the VA. We have tried to guard against this by obtaining input from various individuals directly involved in the events described in this paper. 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. However, if any errors persist then these 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. Available on http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20090114/REG/301149994&nocache=1, last accessed March 2009.

B. Brewin, August VA Systems Outage Crippled Western Hospitals, Clinics, GovernmentExecutive.com, 5th October 2007. Available on http://www.govexec.com/story_page.cfm?articleid=38235&dcn=basics_coop, last accessed March 2009.

B. Brewin, Veterans Affairs Aims To Update and Centralize IT Systems, GovernmentExecutive.com, 21st February 2008. Available on http://www.govexec.com/dailyfed/0208/022108bb1.htm, last accessed March 2009.

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? September 26, 2007, Serial No. 110–47 (2007). Available on http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:39456.pdf, last accessed March 2009.

J. Conn, California System Faced Epic Vista Failures: Report. Modern Healthcare, 1st October 2007.
Available on http://www.modernhealthcare.com/article/20071001/FREE/310010001, last accessed March 2009.

J. Conn, Rewiring the VA: Decision to use outside contractors to replace key pieces of vaunted VistA IT system draws criticism from experts, original architects. Modern Healthcare, 2nd February 2009.
Available on http://www.modernhealthcare.com/article/20090202/REG/901309967, last accessed March 2009.

T. Daschle, S.S. Greenberger, J.M. Lambrew, Critical: What We Can Do About the Health-Care Crisis, Thomas Dunne Books, February 2008, ISBN-10: 0-312-38301-0.

United States General Accounting Office, Software Capability Evaluation: VA's Software Development Process is Immature, GAO/AIMD-96-90, Washington DC, June 1996.

United States General Accounting Office, Computer-Based Patient Records: Short-Term Progress Made, but Much Work Remains to Achieve a Two-Way Data Exchange Between VA and DOD Health Systems, GAO-04-271T , Washington, D.C.: Nov. 19, 2003.

United States General Accounting Office, Veterans Affairs: Health Information System Modernization Far from Complete; Improved Project Planning and Oversight Needed, GAO-08-805, Washington DC, June 2008.

United States General Accounting Office, Electronic Health Records: DOD's and VA's Sharing of Information Could Benefit from Improved Management, GAO-09-268, Washington DC, January 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, 2008;22[1]:104-165, 2008.

Innovations in American Government Awards, Healthcare Program Serving U.S. Vets Wins Government Innovation Award Hi-Tech VistA Program One Of Two Federal Initiatives To Win $100k Grant, Council for Excellence in Government, J.F. Kennedy School of Government, Harvard University, Cambridge, MA, July 10, 2006. http://unpan1.un.org/intradoc/groups/public/documents/UNPAN/UNPAN027875.pdf, last accessed March 2009.

C.W. Johnson, Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting, University of Glasgow Press, Glasgow, Scotland, October 2003. ISBN 0-85261-784-4.

C.W. Johnson and G. Amar and 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, USA 2009, International Systems Safety Society, Unionville, VA, USA. Submitted 2009.

B. M. Kuehn, IT Vulnerabilities Highlighted by Errors, Malfunctions at Veterans' Medical Centers, Journal of the American Medical Association, 301(9):919-920, 2009.

R. Koppel, J.P. Metlay, A. Cohen, B. Abaluck, A. R. Localio, S.E. Kimmel, B.L. Strom, The Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors, Journal of the American Medical Association, 2005;293:1197-1203.

D. McCullagh, U.S. Stimulus Bill Pushes E-Health Records For All, 10th February 2009. Cnet News: Opinion Piece, Available on http://news.cnet.com/8301-13578_3-10161233-38.html, last accessed March 2009.

B. McCaughey, Ruin Your Health With the Obama Stimulus Plan, Bloomberg.com, 9th February 2009. Available on http://www.bloomberg.com/apps/news?pid=20601039&refer=columnist_mccaughey&sid=aLzfDxfbwhzs, last accessed March 2009.

M. Mosquera, VA Revisits Data Consolidation Plan, Federal Computer Week, 12th October 2007. Available from http://fcw.com/Articles/2007/10/12/VA-revisits-data-consolidation-plan.aspx?Page=1, last accessed March 2009.

M. Mosquera, VA Defends its IT Recovery Plans, Federal Computer Week, 4th October 2007a. Available from http://fcw.com/articles/2007/10/04/va-defends-its-it-recovery-plans.aspx, last accessed March 2009.

M. Mosquera, VA Data Center Outage Hobbles VistA Again, Federal Computer Week, 15th April 2008. Available from http://fcw.com/articles/2008/04/15/va-data-center-outage-hobbles-vista-again.aspx, last accessed March 2009.

Office of Inspector General, Issues at VA Medical Center Bay Pines, Florida and Procurement and Deployment of the Core Financial and Logistics System (CoreFLS), Department of Veterans Affairs Report No. 04-01371-177, 11th August 2006, Washington, DC 20420, 2004.

Office of Inspector General, Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans, Department of Veterans Affairs Report No. 06-02238-163, July 11, 2006, Washington, DC 20420, 2006.

Office of Inspector General, Administrative Investigation Loss of VA Information VA Medical Center Birmingham, AL, Department of Veterans Affairs Report No. 07-01083-157, Washington, DC 20420, June 2007.

D. Protti and P. Groen, Implementation of the Veterans Health Administration VistA Clinical Information System around the World. ElectronicHealthcare, 7(2) 2008: 83-89

D. Schaffhauser, The VA's Computer Systems Meltdown: What Happened and Why. ComputerWorld, November 20, 2007. Available on http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9047898, last accessed March 2009.

G. Timson, The History of the Hardhats, Accessed from http://www.hardhats.org/history/hardhats.html, March 2009.

B. Wears and M. Berg, Computer Technology and Clinical Work: Still Waiting for Godot, Editorial, Journal of the American Medical Association, 2005—Vol 293, No. 10 **1261.**

E.M. Yano, B.F. Simon, A.B. Lanto, L.V. Rubenstein, The Evolution of Changes in Primary Care Delivery Underlying the Veterans Health Administration's Quality Transformation, American Journal of Public Health, (97)2: 2151-2159, Dec 1 2007.