

POLITICS AND PATIENT SAFETY DON'T MIX: UNDERSTANDING THE FAILURE OF LARGE-SCALE SOFTWARE PROCUREMENT IN HEALTHCARE

C.W. Johnson,[†]

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

Keywords: Patient safety, healthcare, information systems.

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 jeopardised patient safety in previous large-scale software procurements. This paper analyzes recent failures that have affected the Veterans' Health Administration (VHA); one of the United States' largest healthcare providers. The following sections trace the technical causes back to software engineering practices and project management techniques. However, the key argument in the paper is that these causes have been obscured by political arguments. 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

The US Department of Veterans' Affairs (VA) Veterans Health Information Systems & Technology Architecture (VistA) recently won an Innovations in American Government Award. The citation focused on the way in which the program's decentralized, flexible approach provided resilience even when records centers were destroyed by flooding during Hurricane Katrina; "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 [17].

At the same time as VistA was winning awards, the US General Accounting Office issued a series of reports that criticized software development practices across the Veterans Health Administration [5,6,7,8]. Kuehn 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" [10]. 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. CMU's Software Engineering Institute linked these and similar failures to specific software engineering deficiencies that threaten patient safety [8]. Each of the VA's 150 medical center directors had their own IT services, budgets and staff. They, therefore, exploited a distributed model of software development. Many different healthcare organisations contributed to the production of open source code. However, the SEI found that the VA did not attain level 2 of their maturity model in any of the 7 projects they studied. At this level, the success or failure of a project may be due to chance rather than the output of a recognizable process.

In October 2005, recommendations from Congress led to the creation of the VA's Chief Information Officer. The intention was to centralize control of the IT budget and standardize operations and systems development across this department. 6,000 posts were reassigned. The VA moved local responsibility for IT infrastructure to 4 regional data processing centers. This also had an impact on development practices. Before 2005, changes could be made to applications, such as VistA, on a local or regional basis. This was highly responsive to local needs. However, it also undermined the standardization critical for closer integration with other Federal organizations, including the Department of Defence. The reorganisation led to the introduction of 36 management processes in an Information Technology Infrastructure Library. A coding compliance tool was introduced. This ensured that VA facilities were running the same version of an application.

The centralization of software development was also intended to address more than 1,500 security incidents in the VA between 2003-2007 [2]. For instance, in December 2003, a VA laptop was stolen from an employee's home with data about 100 benefit appellants stored on it. This prompted VA staff to recall all laptops so that encryption software could be installed. Again in 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. Access control and

conformance to security management principles can be more tightly enforced in a smaller number of regional centres than in 150 medical facilities. The subsequent centralisation had the same organisational and socio-technical consequences that complicated other aspects of IT centralisation. The Director of one VA medical centre described how new security measures constrained activities that had been at the discretion of local facilities "... 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 12 minutes to log back on when we return... the clinician is thus forced to choose to 'do the right thing' for either the patient or the system, but cannot do both" [3].

The proponents of the VA's distributed model of software development argued that by focusing responsibility for data management in regional data centers, the VA 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. The process of centralization also moved IT support away from the 'sharp end' of clinical practice. The need for standardization –in terms of software development and the data formats that support exchange with other agencies, undermined clinician centered development. In the past, VA software was typically developed as open source, cooperative enterprises between programmers in different public healthcare organisations. This enabled the development of distinct versions of VistA by the VA, the Department of Defense in their Composite Health Care System and by the Indian Health Service in their Resource and Patient Management System. New ideas and concepts were then shared between these VistA communities.

The open source approach embodied within VistA supported the heterogeneous development practices that were so heavily criticised by the GAO and SEI. These practices have, in turn, been advocated as a model for large-scale IT procurement in other branches of government. The US Undersecretary of Defense for Advanced Systems and Concepts' Open Technology Development road map supports open source approaches to encourage reuse and reduce software costs. It does not consider the implications for the ensuring common standards across the distributed development of safety-critical systems. The proponents of the open source software also point to the loss of \$247 million when the VA's Core Financial and Logistics System was procured from a commercial defence contractor. 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. 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" [15].

2. Server Failure Case Study, 31st August 2007

A case study provides further insights into the interaction between political decision making and the technical development of safety-critical healthcare informatics. On 31st August 2007 the VA's Sacramento facility, one of the 4 data centers mentioned in previous sections, suffered the most severe failure in a succession of incidents involving the VistA/Computerized Patient Record System. It took more than 9 hours to restore services. Knock-on effects propagated to hospitals and clinics from Alaska to California, Hawaii, Guam, Idaho, Nevada, Oregon, Texas, American Samoa, the Philippines and Washington state. 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" [16].

Around 07.30 on the morning of the incident, the end-users of the VistA system found that they could not log on to the Computerized Patient Record System 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. Staff, therefore, resorted to a 3-tier contingency plan. 2 of the 4 regional data processing centers were in the western United States. Region 1 was served from Sacramento, California and Region 2 from Denver. The first contingency plan was for the Sacramento services to be handled by the Denver data center. The second level of defense assumed that clinics and hospitals could read electronic patient records from central servers but that it would not be possible to save any changes to the shared system. In other words, they were to operate a 'read only' mode on the regional servers. Any changes would have to be logged locally and then updated when access was restored. The final fallback position was for healthcare facilities to use the local patient records that were stored on their own computers. These only provided brief summaries about individuals who were either on-site or who had appointments in the next 2 days. 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 from the Sacramento servers to Denver. The VA CIO had already witnessed 6 servers crash in the Sacramento data centre. They estimated it would take up to 2 days to restore services from the longer term backups in the Region 1 facility. There was a concern that by running the software necessary to support the Sacramento users from the Denver facility then any problems with the Region 1 code would begin to affect the Region 2 infrastructure. VA senior management were unwilling to risk the 11 remaining sites serviced from Denver without understanding the reasons why the Sacramento system had failed. The decision was taken, therefore, not to transfer services from the Sacramento centre using the first level contingency plan.

The remaining IT teams at 16 of the 17 VA facilities followed the second stage in their contingency plans when they

discovered that Sacramento would not be transferring support to Denver. This involved configuring local applications to rely on 'read only' access to the servers. 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. In consequence, local staff had to rely on the summary records that were cached on 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, known allergies and annotated problem descriptions. 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.

Staff at this 17th facility had to print out patient care records on local personal computers. While this was being done, 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. Ironically, those departments that made the most use of electronic information systems were worst affected by the failure. 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 to proceed without completing the appropriate documentation. 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'. The lack of integrated communications between different departments created delays in obtaining discharge medications. In consequence, some patients remained on the wards longer than would otherwise have been required. These delays, in turn, had consequences for admissions and transfers. This raised further concerns for patient well-being as procedures were postponed.

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 labelling 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.

The effects of the failure were exacerbated by consequences of centralization. In the past, local staff could call local support officers to estimate the duration of a disruption. Some of this personal contact was lost when the VA created 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, local management could not make informed decisions about the activation and support for contingency operations. 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, this created different problems when the Sacramento teams requested increasingly more detailed feedback on the success or failure of changes in the configuration of their servers. The software problems, therefore, exposed underlying communications weaknesses between local and centralized support teams across the VA.

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. A large number of people were, therefore, available to help diagnose the cause of the failure. This helped to share workload; however, it also increased the problems associated with maintaining shared situation awareness across large groups of co-workers. Together these support teams traced the cause of the outage to a change on the network port configuration for the servers that provided access to shared resources between 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 [1]. 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 [12]. 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 17 VistA systems that were hosted by the Sacramento center and bring them

back one by one. The aim was to restore those centers that were closest to the end of their peak working hours. 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 regions.

For all of the 17 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. Administrative staff worked for more than 8 weeks to catch up with the paper backlog from consultations and tests. 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; "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 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... the burden of this one failure will persist for a long time" [3].

Many commentators were quick to link this failure to the centralization of IT services [12,13,14]. These arguments were 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" [16]. 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 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.

Following the failure, some of the plans to migrate additional medical facilities to the regional centers were temporarily delayed. 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 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 from this incident was that centralization did not by itself provide the increased levels of resilience that some of its proponents had identified. Changes were introduced into the VistA application to ensure that the level 2 contingency plan offering 'read only' access to electronic records would be available following maintenance activities.

The deputy CIO in VA's Office of Enterprise Development was asked if the centralization of IT had played a role in the failure, he argued "Had the IT reorganization never happened, this error might have happened on Aug. 31 anyway because somebody didn't follow a procedure" [16]. The failure, therefore, highlighted competency and compliance amongst the several thousand members of staff who were caught up in the 2005 reorganisation. They were faced with considerable changes in their working practices, for instance, through the introduction of 36 new management processes in the VA's Information Technology Infrastructure Library. 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.

As mentioned, one site could not access centralised records during the failure; this facility had been disabled in order to create a number of new test accounts that were used to store the backup data. In the aftermath of the August 2007 failure, the VA hired an external company to review their contingency plans. 'Read only access' to VistA was reorganized to ensure that 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 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 of VA's Office of Enterprise Infrastructure Engineering, therefore created regional 'server farms'. Each of these supported approximately six hospitals. The intention was to localise future failures and make it easier to focus efforts on restarting services [1]. Concerns persist over the danger of bringing down a healthy server in the process of supporting a failed system.

The revised contingency plans have been tested by a series of subsequent failures. For example, a hardware problem affected the Region 2 centre in Denver during the afternoon of the 10th April 2008. This effected VistA services at 12 medical centers from Colorado to California for up to 7 hours. In contrast to the previous incident, it took longer to diagnose the precise circumstances leading to the failure. Secondary effects again propagated well beyond the primary user facilities. The recovery task was further compounded by a the near simultaneous failure of the VA's commercial telecomms carrier. This prevented connectivity checks that

might have helped support staff diagnose the VA's hardware problems. The April 2008 failure shows how significant investments following a previous incident are no guarantee of future reliability.

The VA's Office of Enterprise Development 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); the successor to the Capability Maturity Model that was used in the earlier critical reports of the VA's software development practices. 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. There have also been projects to introduce model-based requirements engineering together with elements of rapid application development and agile software engineering. These 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 is increasingly based on risk assessment techniques that help management identify possible contingencies, including problems in configuration management, hardware reliability and the failure of network infrastructure.

The safety implications of the network failures in 2007 and 2008 raise numerous questions about the supervision and regulation of healthcare informatics. Kuehn [10] argues that these incidents reveal a need for additional Federal oversight. The Certification Commission for Healthcare Information Technology's certification programme lacks the technical and organization resources to monitor hundreds of recent initiatives in healthcare informatics. It also, arguably, lacks the sanctions to enforce recommendations. Hoffman and Podgurski [9] argue that "The benefits of Electronic Health Records (EHR) systems will outweigh their risks only if they are developed and maintained with rigorous adherence to the best software engineering and medical informatics practices and if the various EHR 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".

President Obama recently signed a \$787 billion economic stimulus package into law. This included provisions for tax cuts and also for investments in infrastructure, energy and education to pump prime job creation. The Stimulus Bill included incentives for health care facilities to replace paper records with electronic systems. 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 VistA. As mentioned, the VA's Chief Information Officer was appointed to direct the centralization of their healthcare systems. The Stimulus Bill provides 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 [4]. 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 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" [11]. 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 are determined by political decision making.

3. Conclusions

This paper has analysed recent failures involving information systems operated by the Veterans Health Administration (VHA); one of the United States' largest healthcare providers. The technical causes can be traced back to problems in monitoring software engineering practices and in supporting project management across complex national infrastructures. A key lesson from this incident was that centralization did not by itself provide the increased levels of resilience that some of its proponents had identified. Changes were introduced into the VistA application to ensure that the level 2 contingency plan offering 'read only' access to electronic records would be available following maintenance activities. Previous sections have also described a number of communications issues. Initially it was difficult for local engineering teams to get information on the failure as centralised staff struggled to diagnose the nature and extent of the problem. Communication between the data center and the local facilities quickly increased once staff believed they had identified the cause of the problem. However, this created different tensions when the Sacramento teams requested increasingly more detailed feedback on the success or failure of changes in the configuration of their servers. The software problems, therefore, exposed underlying communications weaknesses between local and centralized support teams across the VA.

These technical issues were compounded by political arguments over the strengths and weakness of centralised control over information technology and about the role of commercial contracting versus open source development. In particular, previous sections have argued that recent failures involving VistA stemmed from inadequate configuration

management. However, the consequences of this were exacerbated by underlying political decisions to increase central control over their information architectures. Unless we understand these interactions between politics and the technical causes of systems failure then there is little prospect that we will be able to maintain patient safety as governments increase public spending on national healthcare information systems.

Acknowledgements

Discussions with the members of the US AHRQ project Reducing Risks by Engineering Resilience into Healthcare Information Technology for Emergency Departments (grant number R18 HS0 17902) provided the initial idea for this paper and have helped to shape the arguments.

References

- [1] B. Brewin, August VA Systems Outage Crippled Western Hospitals, Clinics, GovernmentExecutive.com, 5th October 2007. http://www.govexec.com/story_page.cfm?articleid=38235&dcn=basics_coop, last accessed March 2009.
- [2] 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).
- [3] J. Conn, California System Faced Epic Vista Failures: Report. Modern Healthcare, 1st October 2007.
- [4] 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.
- [5] US General Accounting Office, Software Capability Evaluation: VA's Software Development Process is Immature, GAO/AIMD-96-90, Washington DC, June 1996.
- [6] US 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] B. M. Kuehn, IT Vulnerabilities Highlighted by Errors, Malfunctions at Veterans' Medical Centers, Journal of the American Medical Association, 301(9):919-920, 2009.
- [11] B. McCaughey, Ruin Your Health With the Obama Stimulus Plan, Bloomberg.com, 9th Feb 2009. http://www.bloomberg.com/apps/news?pid=20601039&refer=columist_mccaughey&sid=aLzDxfbwhzs, accessed March 2009.
- [12] M. Mosquera, VA Revisits Data Consolidation Plan, Federal Computer Week, 12th October 2007..
- [13] M. Mosquera, VA Defends its IT Recovery Plans, Federal Computer Week, 4th October 2007a.
- [14] M. Mosquera, VA Data Center Outage Hobbles Vista Again, Federal Computer Week, 15th April 2008.
- [15] 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.
- [16] D. Schaffhauser, The VA's Computer Systems Meltdown: What Happened and Why. ComputerWorld, November 20, 2007.
- [17] 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.