

Consequences of Heightened Department of Veterans Affairs Information Security on Academic Medical Centers

Group on Information Resources

September 2007

Introduction

Threats to data and the systems that store them are ever-evolving. The cost of reducing the risk of data escape, both economic and social, must appropriately be balanced against the gains to be won through the use of those data. If a workable balance cannot be achieved, opportunities to work with our VA partners to advance knowledge through research will have been lost.

Public and private sector businesses as well as government agencies collect and store a vast amount of information about us. Our reputations and economic interests are jeopardized when personal information is poorly protected or inappropriately shared with others. One measure of the good stewardship of personal information was reviewed by the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization. Between January 1, 2005 and June 1, 2007 they documented that more than 155 million data records of U.S. citizens were lost, stolen or inadvertently released¹. The actual number of compromised records is undoubtedly much larger because not all organizations reported on the size of their data losses.

Each of the compromised records contained information identifying customers, employees, citizens, patients or anyone having a relationship with the organization involved. Names, social security numbers (SSNs), drivers' license numbers, and in some instances medical information was lost. Records were lost due to theft, carelessness, and occasionally through the unintended consequences of well-intended acts.

Incidents involving the VA

The four largest data breach incidents for which numbers are available were suffered by retailer TJM (45.7 million), credit card processor Card Systems (40 million), the Department of Veterans Affairs (VA) (28.6 million), and iBill (17.8 million), also a credit card processor¹. These four incidents account for 85% of the personal data that escaped from possession of organizations in the last 30 months.

Potential liability for the loss of personal information is enormous. It is estimated that through 2003 nearly 10 million Americans were the victim of identity theft or fraud. The average loss was \$4,800 per incident plus 30 - 60 hours of a person's time and an additional \$130 to repair their credit history².

On May 5, 2006 the VA lost a data tape in Indianapolis, IN containing veterans' names, SSNs, dates of birth, and other legal documents. The VA offered identity theft protection to affected veterans. Less than two weeks later, a laptop computer containing veterans' names, SSNs, dates of birth and, in many instances addresses and phone numbers, was stolen from the residence of a Veterans Affairs consultant. Three months later, a second Department of Veterans Affairs computer containing personal data from 15,000 veterans in the Philadelphia and Pittsburgh areas was stolen from a contractor (Unisys Corp., Reston, VA). Had these stolen computers not been recovered, the VA might have been forced to spend billions of dollars helping veterans protect against or possibly recover from identity theft.

Tightened Security Requirements

Taking steps to limit future liability and restore the reputation of the VA, the Secretary of Veteran Affairs, R. James Nicholson, issued a series of measures beginning August 4, 2006, stepping up information security practices throughout the Department. VA Directive 6500³ replaced the 1997 VA

Directive 6210 (“Automated Information Systems Security”)⁴. This new order made compliance with the Federal Information Security Management Act of 2002 (FISMA)⁵ mandatory throughout the Department. Directive 6500 applied not just to clinical systems but to “the security of all VA information and information systems, at all levels of sensitivity and at any location or facility.” Several weeks later, the Secretary broadened the focus of this directive by extending security efforts to data in motion, especially USB (thumb) drives.

To further tighten security of VA data, the Department began eliminating the use or connection of computing equipment and storage devices not owned by the VA on its computer networks. Until the phase-out is complete, non-VA equipment and the conditions of use are subject to the same policies and practices as VA equipment.

Data leaks continued to plague the VA. Three computer disks from McAlester Clinic and Veteran’s Affairs Medical Center in Muskogee, OK containing billing information on some 1,400 veterans were lost in the mail. On February 2, 2007, a portable hard drive containing personal information from more than a half-million veterans along with billing information from 1.3 million physicians went missing in Birmingham, AL. The VA has spent \$20 million in response to this incident.

VA Directive 6504, Restrictions On Transmission, Transportation And Use Of, And Access To, VA Data Outside VA Facilities, issued June 7, 2006 defined sensitive information to include “information whose improper use could adversely affect the ability of an agency to accomplish its mission...”. This broad interpretation made it extremely difficult for VA researchers to determine whether or not all of their data might be considered sensitive. However, the checklist made it clear that sensitive research data must not be removed or transmitted outside the VA.

In a February 6, 2007 memo, William Feeley, Deputy Undersecretary for Health for Operations & Management, and Joel Kupersmith, MD, Chief Research & Development Officer broadened these security protections to research information involving either humans or animals, although subsequently, the inclusion of animal research was lifted. VA researchers were directed to complete a checklist and certify to the best of their ability that all VA research data in their possession were used and stored in accordance with these directives.

Although the Feb. 6, 2007 memo allowed VA sensitive data to leave the premises, it set stiff conditions. Permissions and property passes must be obtained; devices and media must be encrypted and/or password-protected, and names, addresses and SSNs must be replaced with codes. The memo also asserted that if VA data resided on non-VA servers, those servers and their environments must be FISMA-certified and accredited.

Potential Impact on Research

The Principal Investigators checklist and the behaviors it requires represent a threat to research projects involving VA patients at an academic medical center (AMC). It imposes restrictions on where VA data can be used. One of the attractions of an academic faculty appointment for VA physicians is the opportunity to collaborate with colleagues who augment their capabilities. Collaborators often bring to a project different expertise and additional resources not found in the local VA facility. AMCs often provide space, new research methodologies, and access to highly specialized equipment. Limiting VA

faculty to working with VA data inside the walls of their VA facility may hamper those researchers' ability to conduct their research.

In addition, requiring researchers to use only VA-owned servers and workstations presumes there is a suitable physical environment with adequate room to store research data and with ample computing power to process these data. It also presumes that the necessary software tools and support expertise are available for use within the VA. While these assumptions may be satisfied at some VA institutions e.g. the Baltimore VA Medical Center, it is unlikely to be the case at many other facilities. Research data processing needs put on local VA facilities the extra burden of reproducing the necessary information processing capabilities that are readily available at the neighboring AMC. For those VA facilities fortunate enough to have ample space and resources, it is possible to come close to reproducing the desired research environment. For other facilities, VA researchers must hope their AMCs will create a pool of FISMA-certified and –accredited resources so that their data may be allowed to reside outside the VA's walls. The FISMA compliance process imposes a financial burden on the affiliated medical center that may exceed the VA's cost for additional hardware and software.

FISMA is the VA's Answer

FISMA is a federal law enacted as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899) that is meant to strengthen computer and network security of systems operated by federal departments and their contractors. FISMA creates a set of processes and controls that all such information systems must follow. The processes are based on a combination of Federal Information Processing standards (FIPS)⁶ and the National Institute of Standards and Technology (NIST) special publications SP-800 series. The controls are based on the Privacy Act of 1974, the Health Insurance Portability and Accountability Act⁷ (HIPAA), and other relevant federal regulations.

AMCs are very familiar with HIPAA Privacy and Security rules that went into effect in 2003 and 2005, respectively. They have written policies and have operated their healthcare delivery activities as a Covered Entity (CE) to comply with HIPAA's requirements. Scientific research involving patients or human volunteers conducted by AMCs is not regulated under HIPAA. To simplify recordkeeping and minimally disrupt research, some AMCs elected to become a HIPAA Hybrid Entity. A Hybrid Entity is composed of two parts: a CE that delivers health care and a non-CE that performs other functions. Moving research into the non-CE exempted investigators from HIPAA's requirements. Other AMCs chose to apply their HIPAA policies and practices to research activities as well. Doing so extended the same protections to research subject and patient data as those data enjoyed when used for treatment, payment and health care operations. As a result of these different approaches, information security measures protecting human (or animal) research data vary from one AMC (or laboratory) to the next.

FISMA's reach is broader than that of HIPAA. FISMA applies to all data and information processing systems, not simply to those engaged in particular activities such as the direct delivery of health care, and it calls for classification of information and systems based on their sensitivity (i.e., the degree to which their loss, compromise or malfunction interferes with an agency's mission or with national security). FISMA relies on the guidance of FIPS-199⁶ to specify three levels of sensitivity: Low, Medium and High, and it requires correspondingly greater protections for the more sensitive data and systems.

Are FISMA certification and accreditation the right course for AMCs?

If AMC research information systems were to comply with FISMA, they would have a formal set of policies and processes defined to govern access to and protection for their research data. For some AMCs, this might represent a leap forward in protecting research information. For other institutions that have already applied HIPAA's policies and practices to their research arm, FISMA represents another layer of bureaucracy and recordkeeping that would provide little or no practical gain. Significant costs, time to achieve certification, and re-certification requirements add to the challenge.

Is the VA's requirement that its partners implement FISMA the best solution for their information security concerns? FISMA is primarily an administrative framework. By itself, it is not a security recipe. Within that framework, organizations must assess their data value and system vulnerabilities and then implement appropriate defenses to mitigate risks. The VA chose to specify particular products and methods to be employed at all local VA facilities. When an AMC implements FISMA, it will perform a similar risk assessment but may well reach different conclusions. The AMC may choose to mitigate risk using a very different combination of technologies and practices. Furthermore, FISMA does not govern the operations standards outside the server environments. Therefore, there is no certainty that solutions employed by the VA will be compatible with or offer the identical degree of protection as those instituted by each AMC. Moreover, despite attaining FISMA certification and accreditation, it is still unclear if this certification will allow AMC researchers to store or access veterans' data outside a local VA's firewall.

Hypothetical Case Studies Illustrating Possible Approaches

AMCs and local VAs will undoubtedly seek a variety of solutions to the problem of data security and use. Three hypothetical situations that illustrate different ways of achieving compliance are outlined below.

Case A. The VA medical center closely partners with its AMC on dozens of research protocols that involve health care data on tens of thousands of veterans. In response to recent directives, the local VAMC identified dozens of investigators affiliated with the AMC who would be subject to the VA Research Survey and the new VA security requirements. Inspection revealed that hundreds of gigabytes of VA patient data resided outside the VA medical center's building. Working closely with the VA medical center's Chief Information Officer, Information Security Official, Associate Chief of Staff for Research and individual investigators, the AMC migrated all VA patient research data to an existing VA server. That server in the local VA's data center had enough extra storage capacity and computing power to host investigator activity. The local VA set aside space for additional research workstations and provided complete technical support for that equipment. These actions allowed AMC as well as VA investigators to work with these data more readily. Commitments were made to reproduce the necessary data analysis software if those applications were not already available. This solution rapidly achieved compliance with VA directives. It did not slow the pace of research or place undue strain on the local VA or the AMC.

Case B. The AMC has contracts from various federal agencies. Some of them require particular servers and workstations located at the AMC to be FISMA compliant. Although the AMC's HIPAA Security policies and procedures addressed many of the items called for under FISMA, other areas had to be addressed differently or for the first time. During those contract negotiations, the AMC included the time and cost for establishing and maintaining FISMA compliant data systems. The security level

required for these contracts is less than that mandated by the VA. Instituting a higher security level to handle VA research data meant additional policies and practices had to be integrated into the AMC's FISMA framework. The new VA-compatible research system had to be separately certified and accredited. The local VA agrees that the level of security protection for clinical data stored by the AMC under its HIPAA policies and practices are satisfactory for FISMA compliance. The AMC decides to pay for FISMA certification in the hope that it will give it an advantage over other AMCs when competing for future government contracts and grants. There is no additional cost for the local VA partner; however, research continues, and the local VA remains out of compliance until the AMC's systems are certified and accredited.

Case C. VA research data are stored on two 4-yr old servers and 20 workstations at the AMC, none of which are FISMA-compliant. The AMC agrees to transfer possession of these devices to its local VA partner. The local VA partner operates a FISMA-compliant data center with workstations. It has adequate space and enough support personnel to accommodate these older devices. VA personnel reconfigure the old AMC devices in accordance with their FISMA security policies and practices and grant AMC researchers access to them again. The devices will be provisionally certified until they become fully accredited during the local VA's next FISMA review cycle. VA patient research continues with only a brief interruption at both institutions.

Other Potential Scenarios

Other scenarios may arise at AMCs as a result of the VA's current policies about securing veterans' health care data. In addition to the hypothetical cases described above, other possibilities include:

1) Since FISMA applies only to Federal agencies and their contractors, a research contract like the one presented in Case B could include payments from the VA to the AMC to cover costs incurred for FISMA compliance. This would impose an additional burden on an already financially stressed VA health care system. Local VA facilities may not be able to afford payments great enough to encourage AMC participation.

2) The VA and AMC could sign HIPAA-like Data Use or Business Associate Agreements between the parties. These are contracts that among other conditions stipulate the duration of data use and level of data protection required. For example, a contract might require that VA data be retained by the AMC or researcher only for the duration of the project. If those data were stored on AMC mobile devices or mobile media, the contract might call for its encryption using any method that meets the FIPS 140-2 standard. However, the actual devices used and methods and procedures employed would be the sole discretion of the AMC. The VA would have the right periodically to inspect and verify the AMC's compliance with the terms set out in the contract. By not requiring AMC to receive FISMA certification and accreditation, the costs incurred by the AMC and the VA could be substantially lower. AMC research studies using VA patient data could continue.

3) Considering the cost and effort involved, AMCs may cease recruitment of VA patients and avoid using their data for research. This could jeopardize many ongoing research projects and have detrimental consequences for future collaborative research efforts. It may also limit the availability of AMC studies to VA patients and the inclusion of VA patients into community-based studies.

None of these outcomes is ideal. However, a common solution is unlikely to satisfy the needs of every AMC- VA partnership pair. It is our hope that through a dialog, nationally and locally, a collection of mutually agreeable solutions will be identified that will allow fruitful research collaborations between AMCs and the VA to continue to flourish.

Conclusions

The VA's efforts appear to be directed at the improbable goal of stopping rather than slowing the leak. By assuring that veterans' data never leave VA control or FISMA jurisdiction, they restrict information flow to others, yet despite all the VA's efforts; research data will escape from VA control and diffuse into the hands of others. Endeavors to prevent this will require ever greater safeguards and more burdensome procedures for researchers to follow. The danger is that at some point VA researchers will decide the gain is no longer worth the extra effort.

In the interest of preserving an incredible pool of research prospects, many of whom would choose to be part of a joint AMC/VA research study if given an opportunity, we recommend continued dialog and communication with the VA to arrive at a workable solution that is in the best interest of the patient.

Bibliography

1. Privacy Rights Clearinghouse, <http://www.privacyrights.org> (Searched June 1, 2007).
2. Federal Trade Commission – Identity Theft Survey Report”, September 2003, <http://www.ftc.gov/os/2003/09/synovatoreport.pdf> , (Searched August 2007).
3. VA Directive 6500, http://www.research.va.gov/resources/data-security/policies_cyber.cfm. (Searched June 1, 2007).
4. VA Directive 6210, http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=12&FType=2, (Searched June 1, 2007).
5. Federal Information Security Management Act of 2002 (FISMA), <http://csrc.nist.gov/policies/FISMA-final.pdf> , (Searched June 1, 2007).
6. Federal Information Processing standards (FIPS),<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> ,(Searched June 1, 2007).
7. Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), <http://www.hhs.gov/ocr/hipaa/>, (Searched June 1, 2007).