

*Testimony from Ryan Smith, Intermountain Healthcare  
“Systems Stability and Reliability Panel”*

**HIT Standards Committee – Security Hearing  
November 19, 2009**

Below are my responses for the HHS Standards Committee hearing questions on security.

1. Briefly describe your organization and your information security approach to system stability and reliability. “Intermountain Healthcare is a non-profit integrated system of hospitals, doctors, clinics, a medical insurance company, and homecare & hospice providers that serves the medical needs of Utah and southeastern Idaho. Key medical services include cancer, heart, women and newborns, orthopedics, sports medicine, and more.” (see: <http://www.intermountainhealthcare.org>). Intermountain’s information security approach has been structured using a single enterprise model to ensure security is implemented and managed consistently throughout the organization. We approach information system stability and reliability through IT risk analysis, utilizing the ITIL framework for change management, request management, incident management, and problem management. In addition, we actively employ network, hardware, and application level redundancy across core, enterprise systems, and make use of heterogeneous platforms and clients.
2. Provide one or two examples of information security issues you have faced recently related to system stability and reliability, and describe how you addressed these issues. Intermountain has near-real-time synchronization of authentication and authorization credentials between LDAP and Active Directory, and then integrates the access and authorization with many LDAP/AD enabled applications or systems. Centralizing the authentication and authorization for multiple vended applications or systems allows the authentication and authorization to be configured and implemented for a given application or system in a stable and reliable manner.
3. What kinds of trade-off’s have you had to make between security and usability, and other operational considerations?
  - a) Security – In general, we take a “business driven security approach” to help ensure that our security implementation is usable and acceptable to our end users. At the same time, we diligently pursue compliance with industry standards and regulations, working to educate end users and decision makers to the importance of information security. Involving users upfront helps to ensure “buy-in” to necessary changes to our information security infrastructure and applications. Security must never prevent clinical staff from providing acute critical care. This means that although roles, audit trails, separation of duties, and other security safeguards must be in place, there must always be a way for a caregiver to “break the glass” if necessary to provide critical care. Breaking the glass, however, must be audited and subject to post-incident review, etc.

- b) Usability – Applications and systems are occasionally selected by business and/or clinical users and then “turned over” to IT for implementation and ongoing maintenance. A fine line exists between preventing applications and systems from being selected without IT involvement, and allowing users to identify and select applications and systems to address their business issues.
4. What information security standards are you currently using to meet your business needs for system stability and reliability? Intermountain initially created and implemented an information security baseline based on HIPAA Security, then mapped HIPAA Security Policies and Procedures to each aspect of ISO 17799 (now 27001/27002), and now maps and correlates all other information security regulations and standards to this internally created framework. Intermountain continually reviews information security standards, and participates, as appropriate, in various information security standards bodies and organizations.
  5. What challenges have you had to address in implementing these standards (e.g., training)? Educating and training users of new standards and the corresponding policies and procedures is always difficult, as users sometimes don’t pay attention until the standard impacts them. One challenge is the end-user push back during the implementation of a standard or the corresponding policy or procedure, where users may not understand the compliance, legal, regulatory, or technical reasons behind the changes. Another challenge is operationalizing a front-line information security program where front line managers and application-specific administrators can effectively manage users in their systems with the “least privileged” role to get work done and to ensure only the right users have access to the system. This creates various provisioning/deprovisioning challenges for new hire, transfer, role escalation, and terminations. Across the breadth of systems/applications IT manages, as well as the large number of enterprise users, this can be a large challenge.
  6. What is the role/value of interoperable information security standards in helping assure system stability and reliability? The role would be to better standardize the product set or feature set for methods of interoperable information to be utilized. This also may lead to leveraged purchasing or shared costs, thus increasing the value. However, standardizing has its limitations and can eliminate emerging (and sometimes far superior) options from being used until the standard can be changed/updated, which can be months or even years. In addition, by centralizing and standardizing on our system interoperability, we can build greater operational redundancy into fewer systems to provide greater performance and availability/stability. A consolidated security infrastructure also affords us with fewer attack surfaces for malicious internal and external access attempts.

7. What are the current limitations or gaps in interoperable information security standards with respect to system stability and reliability? When sharing information with appropriate external parties, methods of sending/receiving, authenticating/authorizing, encrypting/decrypting, etc., must be negotiated, and many non interoperable standards exist. The sharing and exchanging of information is becoming very IT complicated, and the same data may be getting encrypted in various ways (and possibly at multiple levels), increasing the likelihood of the inability to communicate or to keep data/keys from becoming corrupt. In addition, interoperable standards (e.g. Single Sign-on, etc) can extend our attack surface and reduce uptime/availability if not implemented well, as more applications rely on the security infrastructure to perform reliability.
8. What new and emerging issues around system stability and reliability do you foresee over the next 2-3 years?
  - a) "The Cloud"
    - a. Audit – As more clinical and business information moves into the cloud, it will be increasingly difficult to have reliable, trustworthy access and audit records. As the physical location of the data becomes further virtualized, it will be difficult to identify "where the data is" from an access control and audit perspective.
    - b. Access Control – It will also be more difficult to provision appropriate access rights as you may not be aware of all applications or systems that may be able to access the cloud, or all the interfaces that may be interacting with that data. Who do you call when "the cloud is down"?
    - c. System Ownership – Who do you call when "the cloud is down"? The owner/provider of the API? Who maintains the hardware the cloud uses? Who is responsible for making and testing backups and verifying failure-resistant implementations?
    - d. IT Risk Management – Who is responsible when data goes missing, is not available, or an unauthorized disclosure occurs? The application owner, the hardware owner, the interface owner, the business itself, or the someone else? If the IT risk is shared, how is the appropriate amount of risk or damages assigned to each party?
  - b) General Purpose Operating Systems – In an attempt to be all things to all customers, commercial operating systems continue to become more complex and more difficult to secure in today's more inclusive network. This complexity means most hosts and applications are configured to supply far more access to data and services than is necessary for a given, specific implementation or purpose. This leads to larger attack (and failure) surfaces.
  - c) Patch Management – Patch management is increasingly at odds with customer requirements for decreased maintenance downtime. Distributing applications and data across server farms is of limited use if reliable interoperability and data sharing requires that all systems be at the same application and OS patch levels.

- d) Buzzword Compliance – It is the norm with vendors and customers alike, but verification of proper implementation of the requirement is often left to the vendor’s QA team or the customer’s initial implementation team. Who knows how thoroughly it has been tested, and what cases were tested?
- e) Virtualization – How do you prove that the data really IS protected from other virtualized sessions on the same hardware? How would you know if there were a session-to-session breach? Who assumes financial liability for the breach? Must you disclose the breach of data in just one session, or all sessions running on the same hardware if you can’t prove there was no interaction between sessions?
- f) Encryption – Encryption has become a requirement for many aspects of data protection. With encryption comes degraded performance (stability), if keys become corrupt, or bad key management is in place, the data may become inaccessible or even unusable.
- g) Enhanced Authentication – Enhanced authentication is becoming more of a common or recommended practice. Yet, in a healthcare industry setting, it’s difficult to do many types of enhanced authentication when clinical staff often only has one hand free while the other is gloved and ready to do work activities. For example, the typing of the password is a slow enough process when using one hand, and if the person has to de-glove to do a biometric scan or some other strong authentication method, the required or recommended process will significantly impact workflow.