

**HIT Standards Committee**  
**Hearing on Health Information Technology Security Issues,**  
**Challenges, Threats, and Solutions**

**Building Trust Panel Testimony**

Chad Skidmore

Director, Network Services

Inland Northwest Health Services

1. Inland Northwest Health Services (INHS) provides IT services to 34+ hospitals in the United States, with most being located in the Pacific Northwest. In addition INHS operates a large air ambulance service, provides an extensive telehealth video network, maintains a wholly owned long term rehabilitative hospital, and provides community outreach and ongoing health education.

Our IT Division, Information Resource Management (IRM), maintains a large MEDITECH Hospital Information System used by our customer hospitals in addition to 300+ other applications used within those hospitals. For many of our customer hospitals we are 100% of their IT organization. In addition, we host and operate a GE Centricity Physician EMR and Practice Management system for 600+ physicians.

Given the size and breadth of our environment, security and trust are of high importance. Many of our customers are competitors, which adds an additional dynamic to our security approach. We not only need to protect customer and patient information from those who are not authorized to view it but we also have to insure proper segregation of data between hospitals and clinics in environments where the same clinician may practice at multiple competing facilities.

Building trust has come over time through successful execution, a sharp focus on security and integrity of data, and solid education for our customer base. We have also operated in a very open and transparent manner which helps to build trust. Not disclosing security issues and addressing them with precision and speed undermines the level of trust rapidly.

2. In 2009 INHS launched 1HealthRecord.com which utilizes the Google Health Record Bank to store personal health information that is originated from some select physician clinics that utilize our GE Centricity system. For this effort to be successful we had to build trust with the clinicians who were creating the data that would be visible to patients, and also build trust with the patients that their data was safe and secure. We commissioned full and highly unrestricted penetration testing of the interface software that we developed for this solution and in doing so found areas that could be improved in our code. We shared that information with the initial parties involved in the project and were very open about it. We also did extensive education for the clinicians and patients to help them understand the value of the product as well as the security that we provide. Most importantly we helped educate the clinicians and patients regarding what they need to do to help maintain the security of their data.

3. In clinical environments there are additional obstacles to providing higher levels of security due to the large number of people moving throughout the environment with most users being highly transient. This results in a large percentage of the user population not having specific workstations that they operate throughout the majority of their work day.

With the clinician's primary role being to provide patient care, they have a low tolerance for what they perceive as long delays to access information when they enter a patient room for example. This combined with requirements for hardware systems and processes that do not increase the likelihood of infectious disease, do not consume a lot of space in the clinical environment, and do not interfere with other medical systems make managing user logins and session timeouts far more difficult than in other industry sectors. As a result, user and session management is not as strict as we would like. This is an area where we are spending significant time and effort now to improve with different technology solutions.

4. While a more secure environment is less likely to incur stability issues due to security incidents, I do not believe that security standards directly translate to stability and reliability.

To improve stability and reliability we heavily leverage various virtualization technologies to abstract the application from the operating system, the operating system from the compute hardware, and the compute hardware and operating system from the storage hardware.

To improve security we utilize several different security standards such as SSL, AES, 3-DES, NSA Hardening Guidelines, OWASP Best Practices, two-factor authentication, etc. to help insure a more secure environment.

We also have moved from just performing compliance audits using outside auditors to more full penetration tests. We have increased our efforts to educate users and business partners regarding the value of penetration testing vs. vulnerability audits and compliance audits as well. This is a big shift in terms of our approach to security and we are no longer content to just be compliant with various standards and legislation. We are far more interested in being truly secure and feel that compliance does not always translate to secure.

5. Most customers and business partners have little understanding of cyber security. They are well aware of the existence of malware like viruses and Trojans but do not understand concepts like attack surface, infection/attack vectors, client side attacks, social engineering, etc. Until we do some education regarding what their true attack surface consists of they do not understand the value in full penetration testing vs. just being compliant. The other challenge has been to get support for penetration testing that is not tightly constrained. We have to educate the customers and business partners that real attacks will not be tightly scoped and limited and therefore our penetration testing process should be very open and unrestricted if we expect it to help identify security weaknesses.
6. The most important role and value of interoperable Infosec standards for us is the ability to easily scale. If we have to support various different infosec methodologies for each customer we will have significant challenges scaling our management of those methodologies. Inability to scale would likely have a negative impact on overall security, stability, and reliability as well. It also helps insure that the costs for implementing the standards are lower overall due to the ability to create once and replicate and also due to increased market competition from

companies that work with the various standards. By lowering the cost and complexity we can expect to see more widespread adoption in a shorter time span.

7. One of the larger challenges is that the healthcare software and hardware industry has historically been highly proprietary and there has been little emphasis placed on open standards. We see this in hardware systems from various vendors that are FDA Certified and cannot be changed or interfaced easily in a secure manner because it was not part of the FDA Certification. This impacts our ability to patch those systems as well and results in some critical FDA Certified systems sitting with known security vulnerabilities that the vendor will not address due to the fact that it would impact their FDA Certification.

We also see it with software that is not open enough to support various 3<sup>rd</sup> party encryption standards, user identity and security models, etc. and there is often a lack of willingness to adapt their products to improve that.

8. As electronic interactions with patients become more commonplace and move from just being information sent from the provider to the patient I think that patient identity concerns will emerge as more of a challenge. The financial sector is ahead of healthcare in many aspects of IT and we see rampant fraud in that space today due to stolen user credentials. In that sector the financial loss can be devastating but pales in comparison to the potential impact within healthcare where the user's life and well being are at stake.

As the exchange of electronic medical records increases it will be more important to have interoperable and centralized methods for verifying senders and recipients of that data and insuring that the data is correct and accurate. The margin for error is non-existent when the effect of erroneous data is patient safety.

For patients and clinicians to more readily adopt electronic medical records, personal health records, etc. they will need to trust the organizations that hold that data far more than they likely do today. Large scale data breaches are far too common today and work needs to be done to reduce that as well as to further harden healthcare systems.