Testimony of

Patrick Heim

Chief Information Security Officer

on behalf of the

Kaiser Permanente Medical Care Program

Clinical Operations Workgroup

Medical Device Hearing

March 28, 2011

Good afternoon members of the Clinical Operations Workgroup, HIT Standards Committee. Thank you for the invitation to discuss the security challenges related to biomedical devices faced by the industry, as more and more medical devices become connected and interoperable. I am Patrick Heim, Chief Information Security Officer of Kaiser Permanente.

The Kaiser Permanente Medical Care Program is the largest private integrated healthcare delivery system in the United States, providing comprehensive healthcare services to 8.7 million members in nine states and the District of Columbia.

Kaiser Permanente is deeply committed to the adoption and advancement of health information technology, and we continue to make substantial investments in capital and human resources to improve the performance of our information technology capabilities. These capabilities are essential to our mission to deliver high quality healthcare at an affordable cost, and we take seriously our obligations to provide necessary information security safeguard.

General Comments

As medical devices become more integrated into the enterprise network, security capabilities and defenses of the devices will need to keep pace.

Definition and adoption of granular security standards for functional security capabilities (e.g. logging), data protection (e.g. encryption and integrity hashes), authentication and authorization of devices and users (e.g. identity directory integration and mutual authentication), device security maintenance (e.g. configuration, patch and vulnerability management), and quality of the application implementation (e.g. robust design and software code) will help address many common security concerns.

In some areas, mature industry standards, such as secure wireless network protocols and central authentication, already exist but should be more widely adopted and implemented in a manner that enables integration into existing infrastructures at customer sites.

In the area of information security, standards or standards-related capabilities that are most relevant and important to the meaningful use of EHR technology would include standards targeted at manufacturers of biomedical devices. Such standards would define functional security requirements, data protection, authentication and authorization, device security maintenance, and quality of application implementation.

The desired outcome of standards development would be certification that assures customers that standards requirements are met. These standards should also require periodic reassessment on the effectiveness of the controls with the understanding that any computing system faces dynamic threats and vulnerabilities.

From a security perspective, a key barrier to effective use of health care devices to advance health and wellness is the lack of sufficient protection against privacy and security threats to prevent unauthorized modification and interruption to direct patient care, which could impact patient safety and quality of care.

Moreover, widely publicized privacy or security incidents related to biomedical devices could negatively impact the confidence that patients have in relying on these devices and therefore inhibit the adoption of telemedicine devices.

One change that would enable more effective and widespread use of health care devices would be for the healthcare industry to differentiate itself from other industries by ensuring that security controls for devices are integrated as up-front capabilities rather than waiting for dramatic failures to motivate implementation of these features.

Device Security & Data Security Panel

Care Settings

Different care settings, such as SNF, hospital, home (or other remote site) present heterogeneous user, clinical, technical, environmental and regulatory characteristics that contribute to different security risks with medical devices.

Devices used at a provider-managed care setting, such as a hospital or a SNF, are usually shared among multiple clinical users in caring for different patients. Devices used in these provider-managed settings are typically operated by trained professionals; they are used to provide more critical or acute care, may be (increasingly so) connected to an enterprise network, of clinical grade rather than consumer grade, and subject to greater regulation.

In a provider-managed care setting, there is a greater likelihood that robust confidentiality controls will be implemented because of regulatory requirements, or ganizational policy and more widespread access to the devices. When a medical device is employed in an acute or critical care setting, it typically requires higher availability protection. Clinical grade devices may contain critical decision support functions (e.g., dosage checks in smart infusion pumps), thus illegal tampering will present higher threats to patient safety. Therefore, devices in these settings require higher level security protection for data integrity.

Additionally, as medical devices become components of the enterprise network, infrastructure controls such as intrusion prevention become mandatory with provider-managed devices.

Different provider-managed care settings also require different risk management approaches. For example, frequent inactivity time-out is commonly enforced at ambulatory, SNF and other episodic care settings, but much less frequently within a highly critical and tightly control environment such as an Operationing Room or ICU, where regular provider monitoring is routine.

In the home environment, there are different threats and vulnerabilities. User authentication may be optional or minimal. However, because users of those devices are not trained professional or necessarily technology-savvy, controls aimed at reducing user errors become important. Some examples include easy and effective ways to identify the patient, and removal of higher critical clinical functions to limit the attack surface. Additionally, consumer privacy preferences vary widely, and consumer devices should provide affordable privacy protecting security options such as encryption.

Existing Security Standards and Network-enabled Devices

We see two major opportunities for improvement: security standard development specific to medical devices, and certification processes that validate that the standards are appropriately implemented.

Medical device technical security standards exist today mostly to meet medical device interoperability related needs such as network transport security. While some address HIPAA related confidentiality issues, few appear to be constructed to tackle a broader set of security requirements. Other industry efforts also exist to define best practices with medical device security controls, but most are overly general and vague, and not conducive to tangible improvement of security controls with network-enabled devices. Furthermore, end-to-end use cases that test the validity and sufficiency of the security controls have not been developed and analyzed.

An industry effort, similar to the Biomedical Device Innovation, Safety and Security consortium co-led by the VA and Kaiser Permanente, would be necessary to identify and prioritize security use cases that reflect a variety of threat models with networked biomedical devices; overlay the use cases with existing security standards; and identify and bridge any critical gaps that might impact confidentiality, integrity and availability. Those technical standards must be sufficiently specific for vendor testing and adoption.

Security assessment, including control validation and penetration testing with networked medical devices, require highly skilled professionals. The outcome of such assessment could benefit a large population of care providers, patients and manufactures. Currently such assessments are conducted, if at all, by individual providers, involve high cost and low consistency, and present very limited incentives for device vendors to improve their security design. Improvement in the testing and certification area will help drive better security standard definition as well as adoption. Security needs to become a competitive advantage for device manufacturers.

Network and Connectivity Issues - Remote Monitoring

The primary issue with intermittent connectivity relates to the integrity of data, which is represented by risks of incomplete data and corrupted data. An optional store-and-forward protocol is recommended. The design of remote monitoring systems should also consistently time-stamp all data entries, time synchronize with authoritative time sources, and provide a message digest (such as cryptographic hash or digital signature) to detect any corruption/modification before and after the network interruption.

Thank you for the opportunity to testify. I would be happy to answer any questions from the Committee.