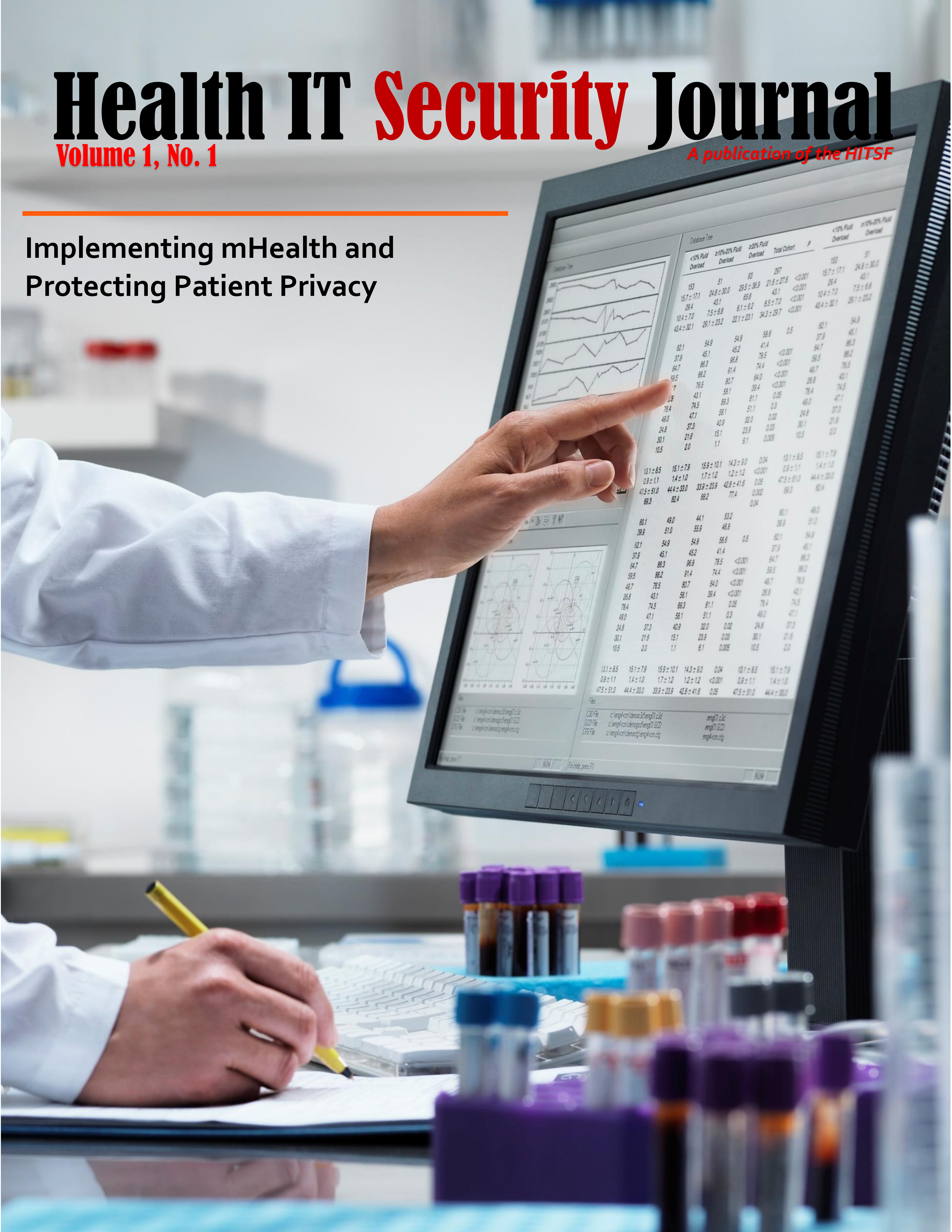
Health IT Security Journal

Volume 1, No. 1

A publication of the HITSF

Implementing mHealth and Protecting Patient Privacy



Health IT Security Journal

Volume 1, No. 1

HITSF

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Letter from the editor

Dear readers,

This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

www.healthitsecurity.org

IN THIS ISSUE

Implementing mHealth and protecting patient privacy

by Eric Vanderburg

Mobile phones, PDAs and other mobile devices have long been promoted as an essential tool for health care. In 2010 such initiatives were given the term "mHealth" which describes mobile technologies and supporting infrastructures used in health care.

The two main barriers to this initiative have been mobile computing power and security. We are now at the point where one of these has been resolved; that of computing power. Mobile computing devices are much more powerful today and capable of not only sending and receiving data but also processing and displaying that data in a usable and intuitive way but many are still uncomfortable with the use of mobile devices that have access to sensitive Protected Health Information (PHI) in a heavily regulated industry. The consistent flow of health care breaches further increases this feeling in both companies and consumers causing doubt as to whether mHealth can be used securely.

Initiatives around mHealth desire to lower health care costs and improve quality. For example, with mHealth, there is potentially less delay in the administering of medicine or procedures and the documentation of such activities leading to a lower patient documentation error rate. It also increases the information available to health care staff when working with patients so that they can make more effective decisions. Lastly, mHealth caters to a generation more comfortable working with portable devices; who expect to be able to use such technology in the workplace and to see that technology used by their health care providers.

In order to realize these advantages without compromising patient privacy, health care providers need to implement policies and a layered set of security controls followed by training mHealth users on appropriate handling procedures so that policies and procedures are followed consistently.

The first step in securing mHealth is to inventory, manage and track mobile devices that have access to PHI. Devices should be centrally inventoried and tracked using location services on the phone. In order to protect the integrity of location data and security configuration settings, mobile devices should be locked down so that users cannot disable location features or security controls in place on the device. Mobile devices also need protection against newly discovered software vulnerabilities so updates should be centrally deployed, managed and enforced throughout the organization. Malicious applications can be used by attackers to gain access to data accessible to the device so users should be restricted from installing additional applications or "apps" on the mHealth devices.

Second, encryption is vital to the protection of PHI. Encrypted channels using technologies such as Secure Sockets Layer (SSL) should be used to transmit data to and from the device. Organizations should avoid storing patient data on the device itself but any data that is on the device should be encrypted. Encryption does little to protect patient data if an unauthorized user can access the device and through it the rest of the information system so additional layers of controls are necessary to protect PHI in mHealth.

Augmenting other controls to promote a proper layered approach is authentication controls. These controls are essential to protect the device against unauthorized access. Users should be required to use a complex password and devices should be configured to automatically lock when not in use. Passwords can still be broken so devices should be configured to automatically wipe if an incorrect password is entered too many times and administrators should be able to remotely wipe a device that is reported lost or stolen.

As can be seen from the guidelines so far, one control is not enough. It takes a number of controls layered together to provide an effective set of controls to protect PHI. As such, BYOD is not a good choice for mHealth because of the control needed to implement layered controls is not available on devices that are owned by employees. Rather, mHealth devices need to be treated as organizational assets and protected just like medicine and other resources are. They should be checked out when used and kept on hand. They should be stored in a secure location and distributed by authorized personnel.

More detailed information for implementing mobile devices security can be found in standards from organizations like the National Institute of Standards and Technology (NIST) and, of course, HIPAA, but the above requirements provide a good overview of what is needed to implement mHealth and take advantage of the quality improvement and cost savings it provides. When implemented properly, mHealth can go a long way in improving patient care and the bottom line.

About the Author:
Eric Vanderburg

Director, Information Systems and Security, JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.