Academia by FingerTec

5 DEC 2013

Safeguarding the Privacy of Patients' Data in the Healthcare Industry through Access Control

- By Johan Yusof, Marketing Executive, FingerTec Worldwide

T

The United States of America is known for having the largest healthcare services market in the world, which represents a significant portion of the U.S. economy. As written in an article on SelectUSA (2013), it has been noted that the healthcare services industry accounted for approximately $1.75 trillion in revenues and employed more than 14 million people, or nine percent of the U.S. workforce in 2010. Between 2008 and 2018, it was estimated by the U.S. Bureau of Labor Statistics that the growth in the industry will yield 3.2 million new jobs.

One of the biggest issues in healthcare is having to maintain the privacy of patients. Mandl et. al. (2001) noted that medical care increasingly depends on computerisation and in addition, both software engineering and marketing practices have become more relevant to issues of healthcare delivery and patients' rights. This could be simplified even more through the use of computerised and internet-based tools for decision support, communications and documentation.

In this article, we take a look at some of the challenges the healthcare industry faces with regards to safeguarding patients' privacy and ensuring that their data are being used in a proper manner.

Health is Wealth and So Is Safeguarding a Patient's Medical Data

Prior to the introduction of the Health Insurance Portability and Accountability Act (HIPAA), there never existed a set of security standards or general requirements for protecting health information in the healthcare industry. At the same time, new technologies were steadily evolving and the healthcare industry have started to move away from paper processes by relying more on the use of computers to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions. For example, in order to provide more efficient access to critical health information, covered entities are using web-based applications and other "portals" that give physicians, nurses, medical staff as well as administrative employees more access to electronic health information (Department of Health & Human Services, n.d.)

In addition, clinical applications are also used by providers, such as computerized physician order entry (CPOE) systems, electronic health records (EHR) and radiology, pharmacy, and laboratory systems. There are health plans that are providing access to claims and care management, as well as self-service applications for members. While this means that the medical workforce can be more mobile and efficient (for instance, physicians are able to check patient records and test results regardless of where they may be), the rise in the adoption rate of these technologies will result in an increase in potential security risks.

For patients, they believe that they have the right to know that their medical data will only be used in the way as intended. There is a need for them to have control over whatever medical information about themselves that have been recorded. Otherwise, they will fail to disclose important medical data or even avoid seeking medical care due to concern over denial of insurance, loss of employment or housing or stigmatisation and embarrassment (Mandl et. al., 2001).

Patients are poised to take control of their own personal medical information. We currently live in an age where people manage accounts, investments and purchases online and most people use the web in order to seek out information on various medical conditions. As such, patients will naturally expect to extend this control to their medical online portfolios.

Mandl et. al. (2001) continued that patients have trouble accessing their medical information and that very information is being used for unregulated secondary uses, which has caused concern for patients regarding the confidentiality and proper use of that record. This is due to many companies providing the record software or maintaining the record systems want in order to own the patients' data. The key to ensuring patients' access to their own medical information while protecting their privacy is to give patients control over permission to view their record, including its creation, collation, annotation, modification, dissemination, use and deletion.

Like all other industries, healthcare companies have also extend their business operations over the Web (Hu and Weaver, n.d.). Although most healthcare participants (e.g., hospitals, private physicians, insurance companies, pharmacies) have already implemented some type of computerized system to manage their business data, their implementations tend to be proprietary and interact loosely or not at all. Hu and Weaver noted that the idea of a more integrated system that helps to cross the various healthcare boundaries would clearly be of great benefit to patients. Rather than having four separate logins on four separate websites to conduct four separate transactions with four different entities, all that a patient needs is just a single, integrated portal in order for him or her to schedule an appointment, retrieve the results of a diagnostic test, refill a prescription and file an insurance claim. Such an approach has the potential to enable this single-portal scenario only if we can assure the privacy and security of patient data through the medical enterprise.

BIOMETRICS

The Solution to All Healthcare Concerns

In a report written by members of the Transparency Market Research (2013), the authors wrote that "rapid technological advancements in healthcare infrastructure, increasing accuracy and performance levels, along with reduced complexity and cost of biometric devices" are some of the major factors which drives the growth of biometrics in healthcare. Furthermore, there is a growing preference for reducing healthcare expenditure by minimizing the risk of security breaches and medical identity theft with the use of biometrics and this helps to support the growing acceptance of biometric systems in the healthcare industry worldwide.

Meanwhile, it was discovered that hand, vein, face and iris recognition are expected to witness the fastest growth, proving how reliable biometrics are used in access control. The growing demand for these products will benefit from more strict government regulations and industry standards that cover the safety, security, and functional features of biometric systems. Logical access control, physical access control and transaction authentication are the three prime application areas of healthcare biometrics and the use of logical access is essential for a user's authentication in order to permit access to computer systems in hospitals and healthcare facilities. Thus, in terms of allocations, it is said that the logical access control segment is expected to dominate the global healthcare biometrics market during the given forecast period of 2013 to 2019 (Transparency Market Research, 2013).

Going back to the HIPAA, an understanding of the act is a great way to gauge the security requirements of a modern healthcare facility. Most healthcare services are now turning to stronger authentication methods and biometric methods. Biometric methods have been deemed useful for authentication and have been rapidly replacing passwords as the go-to authentication method, while non-biometric digital techniques, such as the use of RFID cards, have also proven useful as an authentication method (Hu and Weaver, n.d.).

According to a survey conducted among 3,700 physicians, the biggest concern when using tablets, mobile devices or other technology within their practice was ensuring patient privacy. The HIPAA Security Rule pertains to individuals' electronic protected health records (EHR) and in order to comply with these set of rules, a security risk analysis must be conducted. Regardless of what kind of software or application that is used to download or transmit EHR information, your practice will ultimately be responsible for the security of that information. A thorough security risk analysis can ensure the compliance of the hardware and software your practice uses, the staff knowledge of and compliance with security protocols and procedures and patient relations and communications. Especially with regards to patient relations and communications, it is through this where your patients need to be aware of the procedures your practice uses so that their information is kept secured and discover what their rights to their data are under the law (Webb-Morgan, 2013).

The HIPAA Security Rule also requires administrative, physical and technical safeguards in order to protect your patients' information. Through the security risk analysis as mentioned before, the results of the analysis will help to identify ways your practice can increase the confidentiality, integrity and security of electronic patient information. Administrative safeguards may include comprehensive staff training, limited access to electronic health records and contingency plans in case of emergencies while physical safeguards may include computer monitor privacy filters, locks to reduce equipment theft and limiting access to areas that house systems and data. Technical safeguards are used to limit access to electronic records through login restrictions, audit controls to monitor systems activity and transmission security measures to protect the integrity of your office's computer network.

Webb-Morgan (2013) stated that complying with the HIPAA Security Rule has its benefits. Sharing patient data with authorized providers can facilitate faster and more comprehensive treatment of patients. In the exam rooms, the use of tablets and other devices is a good way to educate your patients and facilitate better communication between the patient and physician. Compared to traditional paper records, electronic health records can actually offer patients even more protection. Using access control, in addition to passwords and user names, can help to reduce unauthorized access to medical records thoroughly since a secure system is far more difficult to break into than a locked file cabinet where paper records are usually kept.

There are two primary purposes as to why the security standards in HIPAA were developed. The first purpose is that implementing the appropriate security safeguards help to protect certain electronic health care information from being at risk. The second purpose is to protect an individual's health information, while permitting the appropriate access and use of that information. This ultimately promotes and stresses the importance of electronic health information in the industry, which is an important goal of HIPAA. (Department of Health & Human Services, n.d.)

The Answer Lies in FingerTec Products

Most doctors and nurses are known to have a lot of time on their hands and their hectic schedule have seen them constantly move in and out of departments and wards. Often at times, they won't be able to have the opportunity to resterilize their hands while some are usually seen with their gloves on as they rush from one department to another. Because of that, it can be a chore for them to verify their access through the use of readers that require verification through fingerprint, RFID card or password.

Therefore, face recognition is a surefire way to help verify access for medical personnel in order to facilitate smooth and swift movements within the premises. The reason for that is due to the terminal being contactless where the reader will scan the face in order to verify a person's access to a secured area. Realizing the needs for this kind of technology that is sure to prove beneficial for various industries, FingerTec has produced a line of face recognition devices through its Face ID series, which include Face ID 2, Face ID 3, Face ID 4 and Face ID 4d.

Face ID 4, FingerTec's facial recognition terminal for access control

The Face ID series are mainly used for access control and time attendance. Of the Face ID terminals that FingerTec has to offer, Face ID 4d is seen to be the terminal that would be ideal for use in most healthcare. The terminal has the ability to recognize a face in mere seconds for accurate door access solution and is loaded with the latest face recognition algorithm, Face Biobridge VX 8.0. Because of this, the terminal provides a swift detection of facial features during enrolment and verification is made more accurate that way. Even under minimal lighting, Face ID 4d can still detect your facial features with its high-resolution camera and infrared feature.

Face ID 4d also boasts some additional features to make it a complete door access solution. While face recognition is its main form of verification, verification can also be done using card or password. The ergonomically-designed nature of the terminal also allows easy positioning and alignment of your face for a hassle-free way of verification. Perfect for doctors and nurses to get around the hospital easily without much delay in their activities. At the same time, the latest software update to Face ID 4d ensures that those wearing glasses are also able to verify their access without the need of having to remove them when they want to verify through face recognition.

FingerTec OFIS-Y Scanner

Logical access controls have also been known to aid in the verification of access to a computer or any form of medical data. A device that would be of great benefit for this would be FingerTec's Online Fingerprint Identification System (OFIS), a biometric solution for online verification and enrolment. The FingerTec OFIS runs on a Browser/Server (B/S) Environment, in which users can enrol their fingerprint through the FingerTec OFIS-Y Scanner that is connected to a PC. What the OFIS-Y Scanner does is act as a capturing station for a variety of applications, the most prominent being a station to login to your computer without the need of a password. Just a touch of a finger is possible to be used as a verification tool. In addition, the OFIS-Y Scanner supports 64-bit windows and with the OFIS SDK (Software Development Kit), the system can be integrated seamlessly into any solution and system to enhance its threshold security, not to mention solving loose remote and online verification problems with its biometric features. This is especially useful in order to reduce access of your patients' medical data while also gaining trust from your patients regarding their data being secured without the chance of potentially being leaked out.

FingerTec Ingressus II, which supports a two-door environment. Both Ingressus I and II come bundled with Ingress

As hospitals and medical centres tend to be large in order to accommodate a great number of patients, it is vital to have a device that helps to monitor the activities of all healthcare personnel within the premises. With features such as surge protection to prolong the lifespan of access control terminals, antipassback features and real-time door status monitoring, FingerTec Ingressus is the perfect solution for hospitals and medical centres in order to strengthen access control within the premise and ensure that all personal data and items are safeguarded well. The controller is bundled with the powerful Ingress software, which comes with additional features to heighten access control, such as graphical floor maps, centralized management, data analysis and reporting and IP camera software integration.

There is no doubt that privacy towards a patient's data is crucial in order to maintain a degree of trust between the patient and physician. With the advancement of technology, there are now many ways to ensure that no personal data gets leaked out easily. The idea of heightened access control through biometric terminals have become a very important part of the healthcare industry and further development of these products will continue to play a prominent role in maintaining and increasing the level of access control that the industry needs in order to ensure that all medical supplies and personal data belonging to patients are safeguarded.

References

- Department of Health & Human Services, USA, 2004, *Security 101 for Covered Entities, HIPAA Security Series (2007).*
- Hu J. and Weaver A. C., n.d., Dynamic, Context-Aware Access Control for Distributed Healthcare Applications, *Department of Computer Science, University of Virginia.*
- Mandl K. D., Szolovitz P., Kohane I. S., 2001, Public standards and patients' control: how to keep electronic medical records accessible but private, *BMJ: British Medical Journal / BMJ Group*. [ONLINE] Available at: *http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1119527/*. [Accessed 18th November, 2013]
- Planet Biometrics, 2013, *A strong pulse for biometrics in healthcare.* [ONLINE] Available at: *http://www.planetbiometrics.com/article-details/i/1745/.* [Accessed 20th November, 2013]
- SelectUSA, 2013, *The Health and Medical Technology Industry in the United States.* [ONLINE] Available at: *http://selectusa.commerce.gov/industry-snapshots/health-and-medical-technology-industry-united-states.* [Accessed 21st November, 2013].
- Transparency Market Research, 2013, *Healthcare Biometrics Market (Fingerprint, Face, Iris, Voice, Vein, Signature and Hand Recognition Technologies, Logical Access Control, Physical Access Control and Transaction Authentication Applications) - Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2013 - 2019.*
- Webb-Morgan M., 2013, How to safeguard patient info in the digital age, *Ragan's Health Care Communication News.* [ONLINE] Available at: *http://www.healthcarecommunication.com/HIPAA/Articles/How_to_safeguard_patient_info_in_the_digital_age_9857.aspx*. [Accessed 20th November 2013]