INFORMATION SECURITY AT NATIVIDAD MEDICAL CENTER: A MODEL OF BEST PRACTICES

INFORMATION SECURITY AT NATIVIDAD MEDICAL CENTER: A MODEL OF BEST PRACTICES

SUMMARY

In 2009, the Monterey County Board of Supervisors separated the Information Technology (IT) systems of Monterey County and Natividad Medical Center. As a healthcare system holding patients' Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Natividad has requirements for privacy and security that are different from those regulating the other County Departments. The Monterey County Civil Grand Jury (MCCGJ) 2013-14 report, *Privacy and Security of County On-Line Data and Information Systems*, focused on the County's IT Department and not Natividad Medical Center's IT Department. This report looks at the protections in place for those who utilize the services of Natividad Medical Center.

BACKGROUND

The need to protect PHI is significant. Theft of personal information can be used to infiltrate finances, damage reputations, extort money, or risk physical harm. Theft of medical information can allow persons and businesses to fraudulently obtain medical goods and services, whether by over billing Medicare, generating false records, abusing patient information to obtain prescription drugs, or contaminating an individual's medical history. There are serious penalties to health institutions reporting breaches. Because Natividad Medical Center is a county hospital, any breaches expose the County to exorbitant penalties.

The Ponemon Institute, a premier independent research organization on privacy, data protection, and information security policies, noted in its *Fourth Annual Benchmark Study On Patient Privacy and Data Security* (March 2014) that:

> Data breaches continue to cost some healthcare organizations millions of dollars every year. While the cost can range from less than $10,000 to more than $1 million, we calculate that the average cost for the organizations represented in this year's benchmark study is approximately $2 million over a two-year period. This is down from $2.4 million in last year's report as well as from the $2.2 million reported in 2011 and $2.1 million in 2010. Based on the experience of the healthcare organizations in this benchmark study, we believe the potential cost to the healthcare industry could be as much as $5.6 billion annually. [p. 2]

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) imposes penalties of $100 to $50,000 per incident up to $1.5 million per year for privacy/security breaches depending on whether the breach was unknown, willful, corrected or not corrected.

METHODOLOGY

During the investigation, the MCCGJ interviewed several key personnel of the following offices and departments:

- Administrative Offices of the County of Monterey and of Natividad Medical Center
- Departments of Information Technology of Monterey County and of Natividad Medical Center

The MCCGJ also read and reviewed extensive published materials on the subject from the

- California Attorney General's Office
- Ponemon Institute
- U.S. Department of Health & Human Services Office of Civil Rights (OCR)
- American Hospital Association Solutions (AHA)
- ID Experts -Data Breach Response Experts
- International Association of Privacy Professionals

DISCUSSION

With the monetary penalties for breaches in excess of $1 million per year and the potential harm to patients' privacy, the MCCGJ investigated the readiness of Natividad Medical Center to thwart hackers and malware from invading its IT system. The report considers the following four areas of interest in connection with HIPAA breaches that most concern the California Attorney General and the Ponemon Institute and which can be controlled by Natividad Medical Center and its IT Department.

Annual Risk Assessments and Updating Privacy and Security Practices Based on the Findings

Natividad's IT Department conducts internal risk assessments annually, and if flaws are found, the department formulates an action plan to remedy the threat. The impact of the threat, the probability of the threat, and the cost to mitigate or fix the threat are weighed. If the system is locked down too tightly, functionality is lost.

All HIPAA breaches must be reported to the California Department of Public Health within five days of the breach. All incidents of breach that involve 500 or more California residents are required to be reported to the California Attorney General. To the credit of the IT Department, Natividad Medical Center has had no reportable breaches since the 2012 law requiring the reporting of such breaches.

To ensure privacy and security rules are followed, all health care facilities are on notice that the U.S. Department of Health & Human Services Office of Civil Rights (OCR) may conduct random audits at any time. To date, OCR has not audited Natividad, but the IT Department represents it is prepared for any such audit when and if it is contacted by OCR.

MEDITECH is the IT system used to manage electronic health records at Natividad Medical Center. All storage of electronic data is held "in house". It is backed up every night to disk and magnetic tapes. It is backed up every week and stored in a vault-protected location. Some electronic data at Natividad Medical Center is stored in a "cloud", but storage of PHI data in a cloud is not technically available yet.

Strong Encryption to Protect Personal Information in Transit

Natividad Medical Center currently has approximately 200 network servers and approximately 1,200 laptop computers for its employees. There are multiple networks for storing data of different departments. Each network has its own dedicated servers. MEDITECH uses 12-13 servers. Before each laptop computer is assigned to an employee of Natividad Medical Center, it undergoes a total volume disk encryption, which prevents unauthorized access to data storage. If the user is unable to connect with the system, the laptop becomes unusable.

Every night the workstation computers are scanned for security. All websites accessed by staff are content filtered and scanned for viruses on an ongoing basis. Some have USB ports turned off. Users have access only to those networks for which they have a need to access. Smart phones can only access a guest network; they have no internal access. Employees can be set up to access their Natividad network email via their smart phones, but users must give permission for phone wipes by the IT Department, which would completely eliminate all storage data on the user's cell phone.

The IT Department staff through its system can determine who accesses data, what data is accessed, where and when it is accessed, and what is printed. All accesses to patient records are logged. Any suspicious activity can be traced to a specific workstation for follow-up.

The Natividad IT Department is working with other county hospitals to create a Health Information Exchange (HIE) where patient information can be shared electronically. Salinas Valley Memorial Healthcare System, Natividad Medical Center, and Community Hospital of the Monterey Peninsula are close to being able to connect with each other. Mee Memorial Hospital will follow. The HIE will be inclusive of county clinics and

GLOSSARY

Health Insurance Portability and Accountability Act of 1996 (HIPAA): a law enacted to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

Office for Civil Rights (OCR): an arm of the U.S. Department of Health & Human Services that investigates complaints, enforces rights, and promulgates regulations, develops policy and provides technical assistance and public education to ensure understanding of and compliance with HIPAA privacy and security laws.

Health Information Exchange (HIE): the mobilization of healthcare information electronically across organizations within a region, community or hospital system.

Information Technology (IT): the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise encompassing computer hardware, software, electronics, semiconductors, internet, telecom equipment, e-commerce and computer services.

Protected Health Information (PHI): any information about health status, provision of health care, or payment for health care that can be linked to a specific individual, including any part of a patient's medical record of payment history.

the Monterey County Health Department. Even without the HIE in effect, the IT Department reported that paper breaches are more common than electronic breaches at Natividad. When requested, printed medical information is physically given to a patient for transmittal to another service provider, because Natividad Medical Center is not yet able to transmit data through an HIE.

Training of All Staff, Employees, and Third Party Vendors

All staff are trained in their IT responsibilities when they are hired, and they receive security training regularly. Before being hired, each must pass a background check. Third party vendors must also go through training and execute contracts drafted by counsel for the IT Department to ensure compliance with Natividad's patient PHI policies and procedures.

All users have unique passwords to log on to workstation laptops. There are separate passwords for the various networks. They must be changed frequently, and no similarities to former passwords are allowed. The system will lock out the user on multiple failed login attempts. All passwords and account information are kept in a vault for access by IT staff when necessary.

The IT system scans email coming in and going out of its networks. It blocks spam and any unauthorized links. It examines any suspected infections to the networks.

Policies and Procedures to Achieve Compliance and Secure Sensitive Information

Natividad Medical Center staffs its IT Department 24 hours a day, 7 days a week, every day of the year. A minimum of two (2) IT staff are on call at all times. Natividad Medical Center devotes 5.5% of its budget, approximately $10 million to IT.

Currently, Natividad's IT requires one factor (password) for access to the networks. The IT Department is moving toward two factors (badge and password) as a single access for all authorized platforms and auto logout users. This will eliminate the need to open multiple platforms and speed workflow.

There is a formal handbook containing specific information for compliance with policies and procedures. Troubleshooting occurs regularly, and IT Department staff monitor the system 24 hours a day to protect the community that utilizes the services of Natividad Medical Center. MCCGJ was pleased to learn of the standards and quality of care by Natividad's IT Department.

One important aspect of Natividad's service to the community is its readiness to communicate medical diagnoses and treatment in languages of the people it serves, including multiple dialects. Persons with language skills are on call to translate for patients and their families when no staff can. Currently Natividad has legally required written notices to persons who are impacted by PHI breaches in English and Spanish. If there are other languages commonly used by a large number of its patients, those notices should be translated for their understanding, as well.

FINDINGS

F1. The separation of Natividad's IT Department from the County's IT Department in 2009 was warranted, due to unique regulations and auditing standards for health provider institutions.

F2. Natividad Medical Center is exemplary of best practices in its protection of patients' PHI.

F3. Natividad Medical Center has 24/7 IT Department staff well-equipped to prevent cyberattacks.

F4. Natividad Medical Center minimizes downtime of its IT networks by dedicated, continual monitoring.

F5. Language translation services should be utilized in preparing written notices to persons impacted by PHI breaches whose common language is other than English or Spanish.

F6. A weak link exists in security of PHI with hand-delivered paper documents.

RECOMMENDATIONS

R1. Natividad Medical Center share its IT Department model with other county hospitals as a standard of excellence when appropriate at all upcoming opportunities.

R2. Natividad Medical Center immediately review and ensure that its notices to the public about HIPAA breaches are written in languages commonly understood by the impacted persons.

R3. Natividad Medical Center continue to improve and update best practices for secure physical delivery of PHI documents to other healthcare providers and individual patients while awaiting an active HIE for secure transmittals.

RESPONSES REQUIRED

Pursuant to Penal Code Section 933.05, the Grand Jury requests a response to all Findings and Recommendations from the following governing body:

- Monterey County Board of Supervisors

APPLICABLE PRIVACY LAWS AND ENFORCEMENT MEASURES

Notice Laws

California's Data Breach Notification Statutes provide that agencies (Civil Code §1798.29) and businesses (Civil Code §1798.82) who maintain computerized data that includes personal information of others must notify individuals of any breach of their personal data immediately upon discovery. Personal information is defined to mean (1) a person's user name or email address in combination with a password or security question and answer that would allow access to an online account or (2) a person's name and one of the following:

- Social Security number
- Driver's license or California identification number
- Account number, credit card number, debit card number, with any required security code, access code, or password that would allow someone to access the individual's account number
- Medical information[1]
- Health insurance information[2]

The HIPAA Final Omnibus Rule of 2013 requires agencies and businesses sending notices for a breach that effects 500 or more residents of California to send a copy of the written Notice to the California Attorney General, thereby making a record of the crime. As of February 20, 2015, there were 18 reported in 2015 throughout California.

Law Enforcement

The OCR arm of the U.S. Department of Health and Human Services is tasked with enforcing the privacy and security laws. It has three functions. (1) It teaches health and social service workers about civil rights, health information privacy, and patient safety confidentiality laws that they must follow; (2) It educates communities about civil rights and health information privacy rights; and (3) It investigates civil rights, health information privacy and patient safety confidentiality complaints to find out if there is discrimination or violation of the law and takes action to correct problems.

[1] Medical information as defined by the Civil Code is any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

[2] Health insurance information as defined by the Civil Code is an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.