James L. Holly, M.D.

Is Your SETMA Medical Record Secure?
Part I I
By James L. Holly, MD, CEO and
Richmond Everett Holly, Sr, CIO
Your Life Your Health
The Examiner
October 4, 2012

This is the second in a two-part series about SETMA's electronic medical record security program. The first part was published September 27, 2012.

Scanning our System

The complexity of SETMA's systems requires that we depend on software produced by many different companies, like Microsoft Windows, Microsoft SQL, Microsoft Exchange, Adobe Reader, Adober Flash, Java, Cisco IOS, etc. Each of these products is used heavily in the IT industry. Keeping systems updated with the latest patches and firmware is critical but challenging. However, not doing it also increases the opportunity for data breeches, or for inappropriate access. It would take numerous employees to keep checking our system to make sure there are no security risks or updates we have overlooked. But, the problem created by technology, i.e., security can also be solved by technology.

SETMA has incorporated a device in our system which at regular intervals scans our system. This product is named Nexpose by Rapid7 and is considered the enterprise leader in vulnerability management and penetration testing. It continually looks at all software in our system. It regularly sends a report to SETMA's CIO about new versions or upgrades of the software that we use. It tells the CIO that SETMA is on one version and another is available. Included in that report, is an assessment of the value of the upgrade and the security risk of not upgrading to the new version. The risk is graded as moderate, severe and critical.

Since deploying this tool, SETMA has found almost 9,000 such security risks which were vulnerable to attack. Most of these were because outside entities we interact with do not keep their systems updated. In order to allow our systems to work together, we had to leave our systems on older software. SETMA's CIO was instructed by the SETMA Partners to secure our systems regardless of whether or not it broke our ability to interact with others. The others would either be forced to upgrade their systems, or we would find other vendors to replace them, i.e., vendors that properly secured their systems. Within one 27-hour weekend period, SETMA's IT department reduced the almost 9000 vulnerabilities to just under 2000. Within the next week, the vulnerabilities were down to 1100. That accounts for 87% of the vulnerabilities being eliminated in only one week. SETMA IT Department is actively addressing the remaining issues and expects to have them to zero within the next four weeks. Going forward, the scanning system will alert us to new issues which will be able to be remedied immediately.

Plugging and Playing

With multiple locations and hundreds of secure devises being used by SETMA, another significant risk to our security was the potential for an employee or someone else bringing an external device, such as a laptop, and plugging it into our system. Regardless of the intent, whether innocent or criminal, this presents a great risk to our systems. The risk could be a virus getting into our system, or someone trying to steal data. By upgrading our switches to state-of-the-art Cisco switches, we are now able to identify “unapproved” devices and refuse them access to our network.

Log of Activity

With a paper medical record, there is no way to know who has looked at the record. Maybe with finger printing it could be done but that is unreliable and expensive. With a robust EHR however, it is possible to know everyone who has looked at, accessed or entered data into a chart. With SETMA’s state-of-the-art EHR, an electronic log is kept of all activities related to a patient’s record. In the past several years, SETMA had occasion to need to know if a particular record had been inappropriately accessed by another person. This issue is so important that even as the CEO of SETMA, I do not look at any medical record unless I am involved in the patient’s care or unless I have a specific, legal need to do so. In fact, we are so serious about this issue that typically, even when there is a legitimate need to know something about a record, if that need is not involving patient-care or safety, that chart is not looked at without legal counsel and direction from counsel. In the case above, it was reassuring to discover that no one had looked at or accessed that chart inappropriately.

Now, SETMA is upgrading that ability. While various parts of our system created a log of activity, we did not have a cumulative log over our entire system. In our security analysis, we discovered that that was a HIPAA requirement and we are remedying that. Henceforth, if a patient raised a question or any other legitimate authority raised a question about access to any health information, SETMA will be able to comply with that legitimate and legal question via a log which contains information on all access and activity from all devices about a particular patient.

E-mail Security

Because we live in an electronic age, electronic communication is important. Where it is important to share patient information which is compliant with HIPAA, the connection between both ends of the communication must be encrypted. It is not feasible to encrypt traditional email between SETMA and the thousands of patients we serve. This is why we have partnered with our EHR vendor to offer ***NextMD*** to our patients. ***NextMD*** is a secure web portal that allows patients and SETMA providers to communicate securely.

Email continues though to present a security risk by employees accidentally sending emails out that might have protected health information (PHI) in them. SETMA has implemented Cisco’s ***Ironport*** product that provides data loss prevention (DLP) technology. All outgoing e-mail is scanned for prohibited information. For instance, if an e-mail includes a patient’s social security number or other confidential information, that e-mail is prohibited from being sent.

Minimum Necessary Access

One of HIPAA's primary requirements is that "minimum necessary access" to patient information be established so that a specific employee can do his/her job without having access to patient information which is not required for the performance of that job.. All of SETMA's employees do not need to have the same access, or perhaps any access to all to SETMA's patient records. Therefore, SETMA's executive staff reviewed the responsibilities of each employee and has set up their account in SETMA's system to allow access only to what they need. This is also true of external organizations which have a HIPAA-compliant need to know information and which have an encrypted access to our system; their access is limited only to that which they need in order to serve our mutual patients' needs and interests.

Back up of all of SETMA's system and information

Another aspect of security relates to what happens if SETMA's systems are destroyed by fire or natural disaster. SETMA has state-of-the-art, encrypted, digital tape backup of ALL SETMA system information, as well as the integration of the various parts of our system. Daily a copy of that tape is taken off premise and monthly a copy is placed in a safety deposit box in a local bank.

If a medical practice using paper records is destroyed, the records are lost. Most practices have insurance which will pay $5,000 for record restoration. When SETMA integrated five medical practices at its founding the paper products to create a new charting system – this was before electronic record – cost $20,000. You can see how inadequate the insurance is for record restoration, even if you could find copies of the information.

For SETMA, we have in place a "disaster recovery plan" so that all of SETMA's systems and information can be restored within a few days, even if our IT Department and server room were totally destroyed.

HIPPA Policies and Standards

SETMA's Information Technology Department has developed and established comprehensive policies and standards by which to guide the department and all of SETMA in the maintenance of HIPAA Compliant, secure and confidential medical records and medical information in an electronic environment. Security and compliance is not just the responsibility of SETMA's IT Department but includes all departments and providers. There are several dozen such policies and standards. SETMA has introduced all of SETMA's staff and providers to these policies and each staff member and provider has signed a compliance agreement document which affirms their understanding of the policy and their pledge to be guided by it and to comply with it.

Policy

" This policy is established to ensure all SETMA facilities, practices and personnel: Comply with federal HIPAA privacy and security regulations; adopt and enforce appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of protected health information (PHI); Safeguard confidential information from unauthorized access and use; and Maintain the confidentiality, availability and integrity of electronic information assets for which SETMA is the custodian according to SETMA Policies and Standards."

Each policy and standard has a "scope" which relates to the specific issue addressed by the particular policy. The intent of each policy is stated in the "policy section" of each of the policies and standards:

> "The Health Insurance Portability and Accountability Act (HIPAA) is a federal law. As part of compliance with HIPAA regulations, SETMA has defined policies and procedures for handling the privacy and security of health information. Information assets are valuable, and thus their integrity, availability, and confidentiality are essential to the business and to the patients we serv Information assets shall be protected commensurate with their defined value, risk, and legal requirements.
>
> "All SETMA facilities must apply prudent measures to protect the confidentiality, availability, and integrity of electronic information assets. In addition to implementing the SETMA information security policies and standards, each facility must implement and oversee procedure to support the SETMA Information Security Program and to comply with applicable federal and state regulations. Facilities in states with additional requirements must gain SETMA Corporate assistance to implement policies that address state-specific requirements.
>
> "Information Security Program Elements
>
> "The SETMA Information Security Program consists of policies, procedures and standards provided by the Corporate Information Technology Department. Each SETMA facility will implement the Corporate Information Security Program and any additional facility-specific information security procedures necessary to support compliance with applicable federal and stat requirements."

SETMA Policies include an explanation of the penalty for non-compliance. This section of the policy manual addresses:

Compliance Violations

"Suspected violations of this policy must be handled in accordance with this policy, the SETMA Code of Conduct, and with SETMA Compliance Policies. Each facility must implement and enforce the SETMA process for promptly reporting violations. Violations must be reported to the Facility Security Officer, Facility Privacy Officer and the Corporate Security Officer, as warranted. (See policy on Security Incident Reporting and Response).
Policy Exceptions

"The Chief Information Officer (CIO) approves information security governance processes and exceptions. Exception approval is based upon risk management reflecting appropriate, reasonable, and effective information security measures for a given situation.

Security Program Policies and Standards

"Refer to the currently-approved list of SETMA security policies and standards. These policies and standards will be reviewed and updated at least annually."

Conclusion

This is only a summary of SETMA's security systems. It lets everyone know we are serious about the safety and security of our patients' health information. And, it suggests that security is not a point you reach but it is a mind-set which drives SETMA to continually find new and better ways to secure our systems.

As the article from twelve years ago, so this article is co-authored by SETMA's CEO and CIO. The collaboration between clinicians, technologists and administration creates a strong environment for excellence in SETMA. These are exciting days in healthcare. Technology helps us do a better job, but ultimately it is about persons – real people – and these tools only allows us to treat people with respect, with compassion and with excellence.