James L. Holly, M.D.

Is Your SETMA Medical Record Secure?
Part I
By James L. Holly, MD, CEO and
Richmond Everett Holly, Sr, CIO
Your Life Your Health
The Examiner
September 27, 2012

This two-part series explains SETMA‟s active program for securing the medical information entrusted to us by our patients. It is critical that the safety, security and the confidentiality of that information be kept safe and available. This is both a professional and a legal obligation. This review lets all of patients know how seriously we take this responsibility.

What is HIPAA? It is the acronym for the **Health Insurance Portability and Accountability Act** that was passed by Congress in 1996. HIPAA does the following:

- Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;
- Reduces health care fraud and abuse;
- Mandates industry-wide standards for health care information on electronic billing and other processes; and
- Requires the protection and confidential handling of protected health information

Meaningful use (MU), in a health information technology (HIT) context, defines the use of electronic health records (EHR) and related technology within a healthcare organization. Achieving meaningful use also helps determine whether an organization will receive payments from the federal government under either the Medicare EHR Incentive Program or the Medicaid EHR Incentive Program.

In order to receive the Federal funds for EHR, a medical practice must attest to having completed a "security analysis" and to having remedied any deficiencies discovered in that analysis. Already Federal investigators are examining medical practices for compliance with this requirement and in several notable cases have levied six-digit fines and penalties.

The amount of money which the MU program will pay a practice is based on the number of physicians in the practice who have met meaningful use standards. Unfortunately, nurse practitioners and physician assistance are not considered to be "eligible providers" (EP) under the law. The incentive is to motivate reluctant providers to invest in EHR. Of course, SETMA started this process in 1997 and has invested ten times more that the MU payments in building a world-class electronic record foundation in Southeast Texas.

Attestation to HIPAA and Meaningful Use

Obviously, all practices have been concerned about "attesting" to having satisfied the security requirements of HIPAA and Meaningful Use. This issue of Your Life Your Health will discuss

SETMA‟s response to these security requirements. We believe that all of SETMA‟s patients will be pleased to know how safe and secure their records are:

In reality, SETMA has always been concerned about the security of the information which is contained in our EHR. The January 24, 2001, Your Life Your Health was entitled, *Your Medical Record, Is It Secure?* Co-authored by SETMA‟s CIO, Richmond Holly and SETMA‟s CEO, James L. Holly, the article addressed the security of our medical records. It stated:

“Once you are confident that your medical records contain all of the information important for the management of your health, you want to be sure that only those who have the „right or responsibility‟ to know your medical history have access to it. In the past, the security of your medical record consisted of the lock on your doctor's office door and the receptionist who sat at the front desk in the doctor's office. No one thought much about how many people had uncontrolled access to the medical records because in reality most people are honest and wouldn't read someone else's record. With the advent of electronically stored data, i.e., electronic health records (EHR), this has changed…now issues of security and the confidentially of that record requires new levels of access control.

“…electronic health medical are more secure than the old paper charts…A humorous anecdote illustrates this. When making the decision to migrate to EHR in 1997, SETMA's founding partners attended the Medical Group Management Associates annual meeting in Washington, D.C. During one of the sessions at this conference, a representative of an EHR company related her experience while making a presentation to a group of hospital administrators in a large mid-western city. Close to the end of her discussion, the elder statesmen of the administrators confronted her and said, „Young lady, you can't make your electronic stored medical records more secure than our paper records!‟ He was aggressive, adamant and loud. Realizing that her success potential was waning rapidly, she assured this gentleman that the electronic records were more secure than his paper records. He persisted, repeatedly making the same point: your electronic records can't be as secure as our paper records.

“She attempted to convince him without success. Finally, with an instantaneous change in his facial expression -- a smile now broke out on his face -- he said, „Young lady, we can't find our medical records, you can't make them more secure than that!‟ The entire audience broke out into laughter, and the speaker breathed a sigh of relief.”

That really was true. With paper records someone could walk into a medical office pick up a chart, conceal it, walk out and no one would ever know. And, even when the chart couldn‟t be found, it would not be apparent that it had been stolen and there would be absolutely no way to know who had it.

For SETMA, the complexity of the security issue is much greater than the typical practice. The ideal of EHR is achieved when every healthcare encounter is documented in the same record.

For years, SETMA has used the EHR in the clinic, at the providers‟ homes, in the emergency department of all hospitals in our area, in all nursing homes in our area, in all hospitals in our area, in hospice, home health, physical therapy and from remote sites when providers are on vacation and want to keep up with their patients and/or to answer questions which arise. This is the ideal of healthcare and one of the first places it existed was in Beaumont, Texas at SETMA.

The question of security is complicated by all of this access. Since the beginning all information has been protected by 256 bit encryption and by security codes. In fifteen years of using EHR, SETMA has not had a security breech. As improved security tools have become available, SETMA has upgraded our system to improve the security of your medical information. The following will summarize some of the state-of-the-art tools which SETMA uses. Hopefully, you will l "get the idea" that we both take your healthcare-information confidentiality seriously and that we have invested a great deal of time, energy and money to give you the confidence that your information is secure.

Two Factor Authentications

Previously, access in the clinic to SETMA‟s EHR was via usernames and passwords. Usernames and passwords while still the standard security measure for most systems in the world are showing signs of age. Hackers are getting better at guessing them, breaking them and compromising people accounts. Also, because most people use the same username and password for everything, once one account is compromised they are all vulnerable.

SETMA has taken what most in the industry consider to be the next iteration of security. It is called "Two Factor Authentication. Two factor authentication means you have to have something you physically possess combined with something you know. The physical device is called a "smart card". It is a card that has a small computer chip in it and it is programmed and tied to a specific users account. The something you know is similar to a traditional password. Someone can steal your smart card, but if they don‟t have your password it is worthless. Conversely, they can know your password, but unless they have the physical smart card it does them no good.

SETMA‟s system now requires that each employee use two factor authentications to log in. The card is placed in the specially designed key board. Once the "smart card" launches the system, the user has to place their password into the system in order to access patient information. Another security benefit of the smart card is that a provider or staff member can only use it on one computer at a time. It cannot be shared with other people to allow others to log on. A provider cannot forget to log out of a computer, leave the room and continue on about their day. They can forget, but not for long. As soon as they get to the next exam room, they will remember they need to go get their card.

Currently, neither HIPAA nor MU require two-factor authentication but SETMA believes that in the future it will be. When it is, SETMA is ready; meanwhile, SETMA‟s data is much more secure than ever before. But, what if someone loses their "smart card"? SETMA has a security policy that requires employees to report a misplaced, lost or stolen card. But, remember without

the password, the “smart card” is of no benefit. However, when a card is reported missing, SETMA‟s Information Technology (IT) Department can inactivate that card rendering it useless and our system safe.

Remote Access with Random Number

Another risk these days is remote access to medical records. Remote access is critical to ensure the best care for our patients. It allows our providers to access records from the emergency department, the hospital, the nursing home, providers‟ homes, etc., for the sole purpose of providing continuity of care. The ultimate goal in all health care is to have all encounters with a patient documented in the same database. This requires remote access.

Remote access to SETMA‟s EHR, like the clinic until recently, was controlled by a username and password. SETMA has added a new and elegant improvement to this system. The product is published by RSA and it is named SecurID. RSA is considered the industry leader in their field. Like the “smart card,” RSA is a physical device that is tied to the users account. This device generates what is known as a one-time password. It is a password that is only valid for sixty seconds. Now to gain access remotely, our users have to enter in their username, password and the one-time password, the RSA device generates for them. The providers have to have possession of their unique device in order to log in remotely. Even if someone‟s username and password is compromised, no one can log in remotely without their RSA device.

Controlled Access to Patient Care Areas

All of SETMA‟s clinics have controlled access to all patient-care areas and all areas where medical records are stored. This includes all exterior doors to SETMA‟s clinics. All employs have identification cards which provide them electronic access to the clinics. Based on their needs, that access is for clinic hours or clinic hours and for after hours. A log is kept of when any person enters any of SETMA clinic. Except for patients with appointments a log is kept of all people who enter SETMA‟s clinics and no unescorted persons are allowed in patient-care areas, or areas where medical records are accessible.