James L. Holly, M.D.

HIPPA and Security

- Medical Records: Is it Secure?

January, 2001 -- Once you are confident that your medical records contain all of the information needed (see Your Life, Your Health, Examiner, January 12th and 17th) , 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 medical records (EMR), this has changed. All of the functions and capacities which our previous articles identified as essential for 21st Century medical records can only be achieved with EMR. This means that now the issues of security of your medical record and the confidentially of that record requires new levels of access control.

While electronic medical records are more secure than the old paper charts, new initiatives are being undertaken to insure the continued improvement in that security and the guarantee of the confidentiality of those records.

A humorous anecdote illustrates these points. When making the decision to migrate to EMR, SETMA's founding partners attended the Medical Group Management Associates annual meeting in Washington, D.C. During one of the sessions at this 1997 conferences, a representative of an EMR 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.

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Tutorial

  If the Federal HIPAA requirements were not difficult to interpret and to comply with, the Texas Legislature in 2011 passed Texas HB300 which increased that complexity geometrically. Effective September 2014, all Texas Healthcare practitioners were required to renew their employee HB300 certification. That certification has to be renew every two years after that. The details of the requirements of Federal HIPAA Primacy and Texas HB300 are given below. The major problem faced by a large medical practice is the number of patient charts which are requested daily by insurance companies and other covered entities. If a practice receives 200 requests a day compliance with Privacy Regulations means we must examine every chart for information which requires special handling. That special handling may involve getting a more inclusive permission from the patient or patient's power-of-attorney before the information can be released even for the most common and simple reason. Because a chart can contain hundreds of pages and because the privacy issues apply even to Chronic Problem Lists, we needed an automated means of examining charts. Those which require special handling can be set aside while others can be sent out immediately. Because the Texas Privacy requirements are much more restrictive than the Federal Law, if you comply with Texas, you automatically comply with the Federal regulations.

- Is Your SETMA Medical Record Secure?: Part I

  September, 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.

- Is Your SETMA Medical Record Secure?: Part II

  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.

- SETMA's Provider Training for September, 2013

  September, 2013 -- A presentation by **SETMA's Chief Information Officer** on SETMA's extensive and continuing HIPPA Compliance Program and our IT information and data security program.

- Notice of Privacy Practices

  Southeast Texas Medical Associates, **Notice of Privacy Practices, Effective Date: February 1, 2015, Privacy Officer: Margaret Ross, RN, MSN, 2929 Calder Ave, Suite 100, Beaumont Texas, 77702, 409-833-9797,hipaaprivacy@jameslhollymd.com.** This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. Your Rights -- You have the right to:

  - Get a copy of your paper or electronic medical record
  - Correct your paper or electronic medical record
  - Request confidential communication
  - Ask us to limit the information we share
  - Get a list of those with whom we've shared your information
  - Get a copy of this privacy notice
  - Choose someone to act for you
  - File a complaint if you believe your privacy rights have been violated...

- Principles Contacting SETMA & Secure Texting

  iMessage traffic is encrypted, only readable for the two end users and therefore HIPAA compliant. You can tell when a message is being sent using iMessage because it will show in **blue** and not **green**...

- SETMA September Provider training HIPAA and Security

  The Security Rule: Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Requires Policies and Procedures Requires Annual Risk Analysis Requires Implementation of certain technologies.