James L. Holly, M.D.

Your Medical Record - Is It Secure?
By: Richmond E. Holly and James L. Holly

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.

To be valuable and available, medical records must first be found. Paper charts are often misplaced, because unlike EMR, when the paper chart is in one place, it can't be in another, at the same time. EMR answers the needs of availability. Are our medical records available when we need them? With EMR, the answer is, "Yes." Is the appropriate information going to be at the hospital when we come in for a broken arm, at the provider's office when we show up with the flu, at the pharmacy when we need to get a prescription refill, or the national laboratory when we go to get blood drawn? With EMR, the answer is "Yes." Availability is key to making the complex world of medical information systems worthwhile.

Yet, the next chapter in the history of medical records is going to address the issue of confidentiality of the record even more than availability and it is going to be guided by HIPAA, which stands for The Health Insurance Portability and Accountability Act of 1996. HIPAA's intent is to "improve the efficiency and effectiveness of the healthcare system by encouraging the development of health information systems that utilize Electronic Data Interchange for the administrative and financial transactions specified." This translates into three primary goals:

1. Availability (dealt with above)
2. Interchangeability -- Can our systems communicate with he systems of other partners and/or players in the health delivery community? One of the benefits of a giant like Microsoft is that they created and promoted a common platform through which we can all communicate and be assured of compatibility. This has not happened in the medical information systems world, and it will probably be sometime before it does. HIPAA is a driving force in this process.
3. Confidentiality. How do we safeguard private medical information from the prying eyes of hackers and other unscrupulous people?

SETMA's CIO has begun studying HIPAA, not only to make sure that we are compliant with Federal Law but also to improve the service which SETMA provides to its clients. In reality, HIPAA is going to impact everyone involved in patient care: clinics, hospitals, insurance companies, IPAs, laboratories, etc. Anyone who deals with patient information will have to make sure they are HIPAA compliant by the end of 2002. This is not much time considering what has to take place.

No one in the healthcare industry doubts that the result of HIPAA is going to be a milestone in the history of patient care and that it is going to be beneficial. However, there are those that are more optimistic than others about how long it will take and how expensive it will be to implement the requirements of HIPAA. In the opinion of SETMA's CIO, the healthcare industry will be nowhere close to implementing all of the issues related to HIPAA by the end of 2002. So much has to change before then. No small part of these changes will involve insurance companies. Without fundamental changes in the information which is being shared, some people are referring to HIPAA as simply a faster way of making the same bad information available. Without these changes, healthcare providers will still be faced with employers not reporting employee terminations to insurance companies, so when the clinic or hospital checks their

eligibility, when the patient presents themselves for care, the system will show them as covered. By the time the claim gets filed, the paperwork on their termination has been processed, and the claim is denied.

Only a small portion of HIPAA is going to involve new technology -- new machines or new software. The vast majority of HIPAA regulations involve internal, organizational policies, procedures, documentation, and the enforcement of those policies. Bill Braithwaite, senior advisor on health information policy with the U.S. Department of Health and Human Services, makes this point; he said, "Security technology is worthless if people continue to write down their passwords and post them on the side of their computers, or if the network administrator does not remove passwords from the account of an employee who has been terminated." At SETMA, we have begun adding to existing policies on this subject that will involve:

1. more education for our employees on what is expected in this area, and
2. clearly defined consequences if they do not do their best to maintain the security of our patients' information.

I am sure many people are wondering why we do not stay in the past? Why do we have to computerize everything making it possible for a hacker to remotely access patient information? Answering this question requires that we compare the security of computerized patient records and the security of the old systems. I have always said that with the old system, anyone in the world can break a window and steal a paper record, while the number of people in the world who could hack into a computerized system is much smaller. And, when the paper record was stolen, it is possible that it would not be missed for months or years.

Natural disasters also impact the security and durability of the old, paper medical record system. Under the old system, fire, flood, tornado or any other natural disaster could destroy your medical records, wiping out ten, twenty, fifty years of medical data, little of which could be recovered. With computerized patient records, a copy of your medical record is taken to a bank safety deposit box every day, ensuring the security, safety and longevity of your medical information.

Is any computer secure? Is any computer totally secure? In this day and age, as we hear in the news almost daily about the F.B.I. or E-Bay being hacked, it is safe to say there will always be someone out there who with enough time, money and talent could hack into any system. Our job is to make every effort we can to make it as difficult as possible within reason. SETMA has created firewalls and other security measures to ensure that our patients' records are secure and confidential. SETMA's Executive Management has attended conferences on confidentiality of medical records and has put into place standards, guidelines and safe guards to make sure records are never released to anyone who does not have a legal right to those records.

Whether examining the history of medical records, the content of medical records, the security of medical records or the confidentiality of medical records, the future is

electronic medical records. SETMA is proud to have the finest electronic medical records which exist today. Our ability to make valid, timely and beneficial recommendations to you for your health are supported by this system. If you have never heard of electronic medical records, make an appointment today. SETMA healthcare providers would be delighted to show you how your healthcare can be improved by the managing of health data rather than health documents.

Remember, it is your life and it is your health.