ELECTRONIC MEDICAL RECORD AND REGULATORY IMPLICATIONS

Michele Person Madison, J.D.

ABSTRACT

Health care practices increasingly rely upon Electronic Medical Records (EMR). EMR systems impact the daily operations and generate additional legal obligations. Effectively implementing an EMR system requires review of the state and federal regulations.

EMR access, automation and aggregation of a comprehensive medical record benefit providers. However, each benefit poses substantial risk to the privacy and security of patient information. Vulnerable wireless or internet access, quick unsecured transferability and improper access of the patient's entire record are implicit within an EMR system. Therefore, providers should perform a risk assessment and implement legally directed safeguards.

The national implementation of an "electronic national health record" emphasizes the numerous risks and practical considerations arising through expansive access, automation and aggregation. The government is currently attempting to resolve such risks to ensure the effective use of EMR systems for all providers and patients. Protecting patient's privacy and security is a daily challenge.

"By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care."[1] Recognizing the benefits of an Electronic Medical Record (EMR), President Bush established a 10-year plan "to build a computer system that would provide every citizen of the United States with an electronic medical record that could be accessed from any location by 2014."[2] The idea of every individual patient's comprehensive medical record being accessible with the touch of a button may provide extensive benefits for the health care industry.

Reducing costs, minimizing legal liabilities and improving the quality of health care are fundamental goals of most health care providers (providers). Providers could reduce costs through operational efficiencies. Legal liabilities may be minimized by the use of best practice protocols and readily accessible medical literature related to specific patient symptoms and needs. Improving quality of care through direct access to a comprehensive patient record that fully informs the provider of any adverse allergies, family history, previous care and supports coordination of care with other providers, benefits both the patient and the provider while potentially reducing medical errors.

However, the benefits cannot be achieved without addressing the risks prior to implementation. Moreover, the health care industry is intensely regulated. Thus, the regulations governing patient records must be analyzed when developing and implementing an EMR.

APPLICABLE RULES AND REGULATIONS

On April 14, 2003, health care providers, health care plans and clearinghouses (covered entities) were required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy standards for patient protected health information (PHI). PHI includes identifiable information regarding the past, present and future health treatment and payment information. On April 20, 2005, covered entities that create, receive, maintain or transmit electronic protected health information (ePHI) were required to be in compliance with the HIPAA Security Rule.[3] The HIPAA Security Rule requires each covered entity to perform a risk analysis and assessment to evaluate risks and vulnerabilities in its operational environment and to implement policies and procedures to address the potential threats. Specifically, the covered entities must address administrative, physical and technical safeguards to protect the security and integrity of ePHI.[4]

In addition to the HIPAA regulations, the state laws and

regulations also apply to patient medical records in any format. HIPAA pre-empts the state laws unless the state laws are more stringent and protect patients' rights to a greater extent. Accordingly, state and federal regulations must be analyzed for the EMR implementation.

First, each provider must analyze its own state laws to determine if state laws supersede the HIPAA privacy and security protections. Typically, state laws address medical record retention, responses to judicial requests and proper means of disclosing patient record information.

MEDICAL RECORD DEFINED

The fundamental cornerstone to an EMR is defining what is included. The state law definition of "medical record" should be compared to the HIPAA definition of the "designated record set".[5] Medical records are generally defined as "a record of a person's illnesses and their treatment".[6] To further define the actual medical record elements, some states have specifically set forth required medical record components as a law. For example, in Georgia, the state promulgated a rule that defined what must be present in a hospital inpatient and outpatient record. Specifically, for an inpatient record, in order to comply with state law, the medical record must include 20 specific elements.[7] Likewise, outpatient records which are similar to physician office records have eight required elements.[8] Each state may differ with regard to the medical record requirements and each provider should review its state's rules and regulations.

Upon review of the legally required components of the medical record, providers should ensure that its EMR system contains proper modules to document and store the necessary information. Providers should maintain an EMR system that has the capability of documenting and storing the clinically relevant information that the provider believes is pertinent to the patient's treatment and quality care. For example, the EMR system should maintain software modules that allow at a minimum for the documentation of a patient's history, the physical examination, pharmaceutical treatments, medication history, order and testing information and progress note entries. Further, when evaluating state law requirements, administrative documents such as informed consents and advance directives may be required. Therefore, the EMR system should provide for an administrative module to maintain consent forms and health care documents that do not include clinically relevant information necessary for treatment.

In addition to defining medical record components, state and federal laws and regulations may also affirmatively require providers to maintain a comprehensive medical record. Specifically, state laws often stipulate a provider owns the record while the patient has a right to access the record. The state laws require for the provider to maintain the medical record for a specific period of time and may address how to dispose of the records when the provider ceases to provide services.

Likewise, the professional licensure agencies may also establish rules and regulations that require the providers to maintain comprehensive medical records and comply with the applicable state and federal laws. Often failure to maintain records in accordance with the state and federal laws may be considered unprofessional conduct as defined by the licensure agencies. In the event a provider fails to maintain the medical record or fails to provide a patient with access as required by the applicable laws, patients may file a complaint with the professional licensure agencies. The licensure agency may then investigate and discipline the provider if appropriate.

Further, maintaining a comprehensive medical record is also impacted by the billing regulations. Specifically, the billing regulations require for providers to maintain an accurate and comprehensive medical record to support any and all claims or charges submitted. Submission of a claim for payment that is not supported by the documented services rendered may constitute submission of a "false claim". State and federal authorities have the authority to enforce false claim fines and penalties. Ensuring documentation of the treatment rendered within the EMR modules will support the submission of any claims and potentially prevent false claims allegations.

Because state, federal and licensure regulations define what constitutes a comprehensive medical record, providers must ensure that when selecting an EMR that all of the regulations are addressed. Some EMR systems may not include all of the modules or components required by the regulations. In that instance, providers may use multiple databases to ensure access to the comprehensive medical record. When the medical record components are located in different databases, providers may need to obtain computer programming for an interface to link the different databases together. Otherwise, providers must access each database in order to evaluate all of the medical record components. While it may be administratively difficult to maintain a comprehensive medical record using various databases, providers may still comply with the laws

and regulations as long as all of the medical record elements are maintained. Upon defining the components of the comprehensive EMR, the method of retaining the records should be addressed.

RETENTION

The time period for retaining records will vary depending upon the state and will apply to both electronic and paper records. HIPAA requires retaining records related to HIPAA compliance for six (6) years. Paper records are typically maintained on site in paper format; then downloaded onto alternative media, i.e. microfiche or scanned documents for long term retention. Saving paper records into alternative formats is typically a costly project.

Utilization of an EMR will enable the provider to directly document his or her treatment plans and any and all clinically relevant material into the patient's record. The information will be stored by a server or on an optical disk. The electronic storage can save more documents without taking up physical space. The information is readily accessible without having to search for paper records or concerns for lost charts. The benefit of having an EMR storage system may reduce costs for storage and ensure location of the relevant information for immediate review.

However, providers will not obtain the full benefit of cost savings, fast response and a comprehensive record immediately. Providers need to continue to maintain the paper record in accordance with the time period required by state laws. The state law requirements will apply to both the electronic and the paper record. Therefore, the retention time period for the electronic format and the paper records should be the same, regardless of format.

Although storing an electronic record should take less physical space, the HIPAA Security Rules specifically addresses the physical security of electronically stored PHI. Providers should address where the computers, including, but not limited to the hardware is located. For example, some providers may utilize EMR systems that are backed up and stored through hardware and on networks that are located outside of the physician's practice location. Other providers may store all of the EMR within the physicians' office on the computers and servers located within the facility. Therefore, the provider should assess how the PHI is stored electronically and the location of the computers.

Access to the locations of the hardware and network systems as well and the computer portals should be secure. Employees who need to have access to the ePHI should have access to the location of the computer. However, the general public and patient population should not have access to the computers. The provider should review or develop a facility security plan.[9] The provider should also validate employees and control their access levels to the software and hardware systems.

In addition, once the PHI is stored in an electronic format, the use of the computer workstations and their security should be addressed. The provider should ensure that the physical location of the workstation is in a location to be utilized only by employees who need access. The workstations should also utilize screen savers to prevent unauthorized access to ePHI when the provider or employee is away from the workstation. It is also recommended to password protect screen savers to further prevent patients or the general public from viewing patient's information on the computer screens when they are not in use by the appropriate provider.

Finally, retaining the records through a server or the network hardware is imperative in order to comply with state and federal retention requirements.[10] However, when a provider must dispose of a workstation or obsolete computer equipment, the provider should ensure that any and all PHI be completely removed from the media prior to disposing of the computer software and hardware. In addition, the media should not be re-used without ensuring that PHI is not embedded in the computer workstation or in the media. In addressing the security safeguards, the provider must comply with the disposal and media re-use safeguards. Providers are only required to address the accountability and data backup standards based upon providers' needs and scope of the practice operations. The computer networks, servers and software should be backed up to a server or backup storage media or a separate storage location to ensure that the ePHI is not lost in the event of a disaster. The provider should assess what data backup storage methods are most appropriate and reasonable for the provider's office. For example, in smaller offices using backup tapes stored off-site may be sufficient to address the practice's needs. Larger integrated health systems with hundreds of thousands of records may seek to maintain an off-site duplicate network server and a comprehensive disaster recovery plan.

PRODUCTION OF RECORDS

Once you have defined and retained the medical record, providers are often asked to produce the record. State law

normally governs when and how records may be disclosed or produced. Likewise, HIPAA privacy rules specifically address the permitted methods for disclosing and producing medical records. One such request for production arises from court proceedings or subpoenas. When a provider receives a judicial request, the provider must consider both the paper and electronic records and comply with the regulations. Pursuant to HIPAA, when responding to a judicial request a covered entity may disclose PHI in response to a subpoena, discovery request or other lawful process if satisfactory assurances are provided that the individual who is the subject of the PHI has been given notice of the request and has had an opportunity to object to the request and that no objections were filed or that the court has ordered production through a qualified protective order.[11]

The paper records and the electronic records should all be reviewed for potential relevancy and whether they fall within the scope of the request. Therefore, providers must evaluate both the paper and electronic records. The paper records may be produced in paper format, provided the proper authorizations and process are followed as required by state and federal laws. Further, if the records are maintained in multiple databases, each database must be reviewed to determine if it contains records relevant to the request. Failure to evaluate each database may result in the production of an incomplete record which may result in complaints and enforcement proceedings by professional licensure agencies or the state or federal authorities for violation of patient's right to have access to the complete medical record.

On a daily basis, providers receive request for production of records from attorneys or patients that are pursuing medical malpractice claims. When a malpractice claim is being pursued, the patient is reviewing the provider's care in hindsight. However, the provider's care was rendered at a specific point in time based upon the information available on the date treatment was rendered. At the time the record request is received, the medical record may contain more information from consultations or subsequent treatments that was not available at the time the treatment in question was rendered. Therefore, it is important for the EMR to document the dates and times of medical record entries. The dates and times within the EMR will establish what information was available to the provider on the date the treatment was rendered. Unlike an EMR, paper records are merely filed into the medical record and the record may not document the actual date it was entered which may imply that the provider had access to all of the information at the time the treatment was rendered. Thus, the EMR's date and time accounting may be beneficial in defense of malpractice claims. The EMR systems vary with regard to time entries and should be evaluated prior to implementation.

ELECTRONIC PRODUCTION

Responding electronically is impacted by the HIPAA security rules because the provider is electronically transmitting protected health information (ePHI) as defined by HIPAA. The security rules set forth specific technical safeguards that must be addressed to prevent the unauthorized use or disclosure of ePHI.

The electronic record should be transmitted in accordance with the transmission security safeguards. Depending upon the individual provider's practices and procedures, encryption may be necessary to prevent unauthorized access. In addition, providers must ensure that the information transmitted is intact and un-alterated when it is received by the receiving party. Therefore a proper means of transmission security and data integrity tests should be utilized within the EMR system.

Although electronic transmission may be convenient and efficient, electronic production of a medical record may be operationally difficult. In addition to the potential need for encryption and ensuring that the information received is the same as the information transmitted, there are multiple software platforms and it may not be possible for the receiving party to access the transmitted records. Currently, the federal government is sponsoring initiatives to establish a standard platform for the electronic exchange of health information. However, at this time, not all individuals may have a software program with the same standards to access the records. One means of addressing this concern is for the EMR system to download the records into a simple software format that may be transmitted across encrypted lines to the receiving party.[12] Providers should avoid merely e-mailing patient records to patients in light of the fact that the patients may not have encrypted e-mail systems and the documents may be intercepted or altered. In the alternative, providers may utilize an encrypted web portal to transmit records to patients. When evaluating an EMR system, providers should evaluate the ability of the system to download the records in accordance with the security regulations, the EMR process for electronic transfers and whether a separate web portal will be necessary to ensure the security and

privacy of the patient's information.

PORTABLE ACCESS

As technology develops, EMR systems make health records more accessible to patients and treating providers. Patients may gain access to their PHI[13] via the Internet or e-mail. Physicians may receive lab reports or diagnostic tests results from remote locations on portable devices without ever entering the office or hospital. Physicians access patients' records through a PDA or Internet portals to the EMR. The PDAs can receive and store medical record information. In addition, physicians may document in the PDA and transmit the information to another provider, the hospital or the office. The PDA is storing medical records. Therefore, implementing administrative, physical and technical safeguards should be performed.

First, the administrative access controls should be addressed.[14] If the physician is gaining access to a hospital's EMR system via the PDA, the hospital should maintain policies and procedures to ensure that the physicians are responsible for having the PDA reviewed by the hospital information technology department and approved for use. Access to the PDA should be restricted by a unique password and log in. The hospital should have a process for verifying that the log in from the PDA into the hospital EMR is tracked and monitored. Further, the hospital may set forth policies and procedures limiting the amount of information that may be stored on a PDA, i.e., no more than three (3) days of information.

Next, the physical safeguards should be addressed via policies and procedures. Specifically, the hospital may maintain policies and procedures for its administrative and medical staff that any and all PDAs must be maintained in a secure location and any user of a PDA is responsible and accountable for the security of the PDA, as well as the password used for access. PDAs maintain numerous health records within its memory. Therefore, the physical location of a PDA presents a serious threat to security because the PDA can store more information than one paper medical chart. It is compact and extremely portable, thus making it much easier to misplace than a large patient chart. PDAs should not be left behind in restaurants, cars or areas where unauthorized access may be gained to an individual's health information. PDAs should be maintained by the practitioner in a secure location and protected by a unique password to prevent unauthorized disclosures.

Finally, the technical safeguards should be addressed. The PDA should only be accessed by unique user identification and may be required to have an automatic log off. The PDA transmission of information should also be through a secure transmission mechanism addressed by the hospital. The hospital may require that the physicians ensure that their PDAs do not utilize analogue transmissions and securely transmit information.

WIRELESS NETWORKS

Another technology advancement that promotes quality and safe care is the use of wireless EMR networks within health care facilities. For example, hospitals may use a wireless network to enable its employees to utilize laptops and travel throughout the facility while still being able to log into the network. Nurses utilize laptops at the patient's bedside to document patient care. In those instances, the hospital normally maintains a wireless network over the facility to ensure that the information is being downloaded to the secure server. The wireless network has multiple access points throughout the facility. The hospital must secure the access points so that only individuals who have an appropriate and authorized user name and password can access the system.[15] For patients who enter into the hospital and bring their laptops, it is possible that they may also have wireless software loaded on their personal laptop and it is important to ensure that the wireless network governing the facility is secure and prevents individual patients from gaining access. If there is a web portal or wireless access point that is open to the public, an individual patient could gain access to all the patients' information within the facility. Each wireless access point must be secure.[16] The information technology department may audit the wireless access points to ensure that a wireless access point has not been compromised and that all of access points are secure.

ELECTRONIC COMMUNICATION

In addition to accessibility, EMR provides greater automation to patient's PHI. It enables the patients and the physicians to forward or send patient health information across state lines, outside of facilities and to remote locations to treat patients and reduce medical errors. Likewise, patients may e-mail their providers for medical advice and treatment from remote locations. E-mail transmission of information between covered entities and patients should be addressed for compliance with HIPAA security rules. Specifically, when a patient e-mails his/her health care provider for medical advice, the individual should already be an established patient so that the health care provider can identify the patient and ensure the physician-patient

relationship has been established. In addition, the patient should have previously received a notice of privacy rights from the health care provider or the covered entity. Otherwise, the provider may post the notice of privacy rights on the Internet site and the patient may submit acknowledgement via the Internet. The administrative safeguards provide a framework for the administrative policies and procedures that should be established.[17]

The covered entity also should address who will receive the e-mails from patients to ensure that the e-mails are only sent to an authorized recipient.[18] The physical location of the devices used to answer the e-mails is also a security concern. For example, physicians may attempt to receive and answer e-mails from computers in hotels, coffee shops or remote locations. The computers that are not controlled by the provider may have malicious software that could breach the security of the information, the computers may record the e-mail transmissions, or the information exchanged may be inadvertently stored on the memory of the remote computer.[19] Therefore, the covered entity may establish policies that prohibit transmitting patient information, including e-mailed information, from a remote site or computer that is not owned and maintained by practice. Reasonable precautions should be taken to minimize the risk.

Further, the technical safeguards should address how the patient and providers may transmit information.[20] The e-mail transmission should be over secure lines. Many times, individuals do not utilize e-mail systems that are secure and encrypted. If this is the case, the individual's health record information may be accessible. One technical consideration is to require patients who wish to e-mail the health care provider to e-mail via a Web portal from the physician's web page. The Web portal may utilize programs to encrypt the transmission of the information.[21] This type of mechanism should be evaluated and addressed for covered entities when evaluating whether or not they intend to directly e-mail PHI.

Although automation of the medical record is a great benefit there are costs involved in complying with the laws. The sensitive nature of the medical record information requires implementation of administrative, physical and technical safeguards. Implementing each safeguard requires time, computer programming and funding. Initially, the time and costs required to implement the appropriate safeguards may outweigh the benefits of the automation. The benefit-cost analysis will depend upon the size of the provider. As the federal government establishes standards for the electronic exchange of information and computer companies focus upon creating a comprehensive, secure EMR system that satisfies the federal standards, the costs will decrease. Competition in the EMR industry will also reduce the costs. Therefore, the benefit-cost analysis will change as EMR systems become more available and standardized. Providers should continually evaluate the costs and benefits to its practice.

LIMIT ACCESS TO AUTHORIZED PERSONS PERMITTED BY LAW

Two of the main processes for EMR, whether it is in a stand-alone hospital or integrated with other networks, are access and termination of access. Although this seems to be a fundamental component of the EMR (i.e., access and termination), it is an area that is often overlooked. For example, covered entities must maintain a password management system to ensure that any individual, who is gaining access to the system, is an authorized user who has been granted a password because of his/her job functions or his/her role in the organization.

Covered entities should maintain a policy or procedure for granting passwords. It is recommended for passwords to be maintained by the information technology department. Passwords should be required to be a specific length to include numbers and letters. Passwords should not be shared or disclosed. It is recommended for the information technology department to perform regular and random audits to ensure that there are no unauthorized users utilizing or gaining access to the system.[22] It is also important to verify that there is a termination procedure to retire a password when an individual is terminated. Randomly auditing passwords utilized by previously terminated employees to ensure that they are not currently being used to gain access to the secure system would also promote security and prevent unauthorized disclosures.

AGGREGATE DATA FOR QUALITY MEDICAL CARE

Improving quality care is an industry goal. The ability to integrate information and aggregate a patient's information into one comprehensive source supports quality care, but poses significant security risks. This benefit promotes quality and safe care for patients as the medical information is aggregated and a practitioner will have the full overview of a patient, including any allergies or history readily available. The integration of information may also reduce medical errors. However, having all of the information accessible by one source means that all of the patient's records

may be breached by one single access versus the paper records which are normally located in varied and multiple locations, i.e., hospital and physician offices.

As the industry moves more towards an integrated network between hospitals and physicians to reduce medical errors, there are numerous legal barriers that must be addressed. The following will highlight a couple of prominent issues. As the records are integrated with other providers, it is more difficult to evaluate who is gaining access to the provider's network as other individuals may be gaining access to the record via their own network. Accordingly, it is important to ensure that any and all integrated networks have security mechanisms in place to ensure that only the proper providers or health care plans are gaining access to the appropriate modules or subcomponents of the EMR. It could potentially be a breach if a physician office had integrated its records with a hospital and the physician was terminated by the patient, but the physician continued to access to the patient's record. The physician's access is unauthorized as he/she is no longer the treating physician and has no need to access to that patient's information. This scenario would be a breach of the security standards and the privacy standards. Therefore, it is important for any termination procedures to terminate access on an individual patient basis. The integrated networks may evaluate integrating each individual patient on a patient-by-patient basis and not on a network-by-network basis to provide proper termination.

The other potential barrier is that in many states the provider or health care practitioner who created the record is the owner of the record and the patient has a right to access and copy the record as the information belongs to the patient. In those instances, when there is an integrated network, it is important for the EMR to maintain the integrity of the physician's record separate from the hospital's record. Simultaneously, separate modules must also grant access to view the records to reduce medical errors and ensure proper and complete communication between providers. Further, the records may be transmitted across state lines and multiple state laws regarding privacy and security must be analyzed in addition to the HIPAA rules and regulations for compliance.

Moreover, in many cases hospitals comply with the Joint Commission standards and physician offices do not have the same requirements. The documentation in a hospital record is scrutinized by the Joint Commission and specific abbreviations are prohibited. If the physician's record is integrated into the hospital record, the hospital should address how to require each physician integrating his/her records to comply with the documentation requirements set forth by the Joint Commission. This is often addressed by the documentation selections available in the EMR system.

As integrated networks span from hospital to physician and from state to a national level, the secure transmission of the information must be evaluated and the software platforms that are being utilized for the integrated network must be interoperable. The transmission of the information in an integrated network should be protected through secure encryption or other secure means.[23] The transmission should also protect the integrity of the record and prevent erroneous information from being relayed.[24] Developing interoperability standards should assist in promoting efficient and accurately transmitted records.[25]

Maintaining and retaining the integrated EMR should also be addressed by developing a comprehensive disaster recovery plan.[26] Specifically, being able to backup the EMR on an optical disk or media that can be utilized in the future is important and required by the HIPAA security standards. Therefore, if an entity has an integrated network, there must be an entity that is backing up or providing disaster recovery for the EMR. There is always a risk that the optical disk may corrupt or there may be other problems with regard to the backup mechanisms. If backup tapes are being utilized, the backup tapes should be stored in a remote and secure location. It is important to recognize that stolen or lost backup media would constitute a breach of the privacy and security of PHI. Accordingly, there should be duplicate types of secured backup and alternative plans for disaster recovery.

These considerations are especially important in light of the hurricanes and natural disasters that recently occurred. For example, as Hurricane Katrina flooded New Orleans, many of the individuals whose health records were on paper in the different hospitals were lost forever. If the system had been electronic and backed up at a different site outside of Louisiana, then the individuals' health records would be readily accessible when they were transplanted to other areas and their physicians or health care providers in other areas could have electronically accessed the records. This also would have provided health care backgrounds such as allergies and previous medication information on patients who were being transported out of New Orleans to other sites.

In light of the aggregated information in an integrated network, access and termination of access as discussed also is critical.[27] Because information is aggregated through EMRs, all of the patient's information is located at one source. Failure to maintain physical security for laptops, PDAs and other devices that store the information may result in security breaches. For example, many of the security breaches related to personal and confidential financial information has been caused by lost or stolen laptops that contain personal information.[28] Therefore, administrative, physical and technical safeguards should be implemented, reviewed and continuously improved upon to prevent potential vulnerabilities and risks to the security of EMR systems.

CURRENT CHALLENGES

Notwithstanding compliance with the rules and regulations, developing broad benefits of a national EMR system faces many practical challenges. The impediments to a national EMR are creating a uniform interoperable record, ensuring the same standards are used by all vendors, ensuring secure transmissions and enabling all health care provider access to EMR systems. The federal government is attempting to address the impediments through the Office of the National Coordinator for Health Information Technology, rules and regulations to permit donations of EMR software and hardware systems to providers and presidential executive orders requiring standards and interoperable electronic medical record technology for government payor plans and its participants. All of these efforts are aggressive and push for realization of an EMR by 2014. As each new step is taken by the state and federal governmental agencies, providers must continually assess their daily operations and consider their unique needs to comply with the laws and protect patient's rights.

In summary, the electronic health record is a new fundamental standard or component of the health care industry. As covered entities move towards implementing and developing their EMR and integrated health networks, the security standards must be addressed. Although the security standards appear to be a global requirement, they are very detailed and will affect the operations right down to the passwords that are provided to individuals who gain access and in the termination of this password to cease access to health records. As the national health information network expands and develops over the next several years, the security standards will also expand and each individual provider should be aware of his/her responsibilities to maintain the administrative, physical and technical safeguards to protect the privacy and the integrity of the electronic health records.

AFFILIATIONS

Michele Madison is a health care attorney who represents hospitals, providers and integrated health care delivery systems and specializes in health care regulatory advice including Stark II, Anti-kickback, Compliance and HIPAA. She may be contacted at mmadison@mmmlaw.com.

REFERENCES

1. President George W. Bush, State of the Union Address, January 20, 2004.
2. http://www.whitehouse.gov/infocus/technology/economic_policy200404/
3. 45 *Code of Federal Regulations* (C.F.R.). Parts 160, 162 and 164.
4. *Id.*
5. 45 *C.F.R.* §164.501, "Designated Record Set. means (1) a group of records maintained by or for a covered entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used in whole or in part, by or for the covered Entity to make decisions about individuals; (2) for the purposes of this paragraph, the term record means any item, collection or grouping of information that includes PHI and is maintained, collected used or disseminated by or for a covered entity."
6. *Merriam Webster's Medical Desk Dictionary*, (1996).
7. *Rules and Regulations of the State of Georgia* Section 290-9-7-.18.
8. *Id.* Outpatient record must include 1. A unique identifying number and a patient identification form, which includes the following if available: name, address, date of birth, sex, and person to be notified in an emergency; 2. Diagnosis of the patient's condition; 3. The name of the physician ordering treatment or procedures; 4. Patient allergies; 5. Physician's orders or orders from another practitioner authorized by law to give medical or treatment orders as applicable; 6. Documentation that the patient has been offered the opportunity to consent to procedures for which consent is required by law; 7. Reports from any diagnostic testing; and 8. Sufficient information to justify any treatment or procedure provided, report of outcomes of treatment or procedures, and, as appropriate,

progress notes and the disposition of the patient after treatment.

9. 45 *C.F.R.* 164.310(a)(1).
10. HIPAA Security Rule, Physical Safeguards, Device and Media Controls 45 *C.F.R.* 164.310(d)(1).
11. 45 *C.F.R.* 164.512(e), Disclosures for Judicial and Administrative Proceedings.
12. For example, the provider may download the records into a pdf format and transmit the documents through an encrypted and password protected format to prevent alterations to the original record.
13. Protected Health Information generally includes individually identifiable health information that is transmitted by electronic media; maintained in any medium; or transmitted or maintained in any other form or medium. See 45 *C.F.R.* §164.501.
14. See 45 *C.F.R.* §164.308.
15. See 45 *C.F.R.* §164.310(a)(1) Facility Access Controls; 45 C.F.R. §164.312(a)(1) Access control.
16. See 45 *C.F.R.* §164.312(a)(1) Access Control; 45 C.F.R. §164.312(d) Person or Entity Authentication.
17. See 45 *C.F.R.* §164.308. Administrative Safeguards.
18. See 45 *C.F.R.* §164.308(a)(4) Information Access Management.
19. 45 *C.F.R.* §164.310(a)(1) Facility Access Controls.
20. 45 *C.F.R.* §164.312(e)(1) Transmission Security.
21. There are software programs that can secure e-mail and ensure that any e-mail that is sent or received is encrypted. It is recommended to discuss encryption with any EMR vendor or Webpage operator.
22. See 45 *C.F.R.* §164.308(a)(7) Security Awareness and Training.
23. See 45 *C.F.R.* §164.312(e)(1).
24. *Id.*
25. Currently, there are many different regional health information organizations (RHIO) that are attempting to facilitate an integrated health record. Those systems have different models and are currently being evaluated. (Nine state-level regional health information organizations have been selected to participate in the development of RHIO-related best practices, according to the Foundation of Research and Education of the American Health Information Management Association.) As the RHIOs develop, the security standards must be addressed by each covered entity and ultimately by the RHIO.
26. 45 *C.F.R.* §164.308(a)(7) Contingency Plan.
27. See 45 *C.F.R.* §164.308(a)(4), Security Awareness and Training; 45 *C.F.R.* §164.312(a)(1) Access Control.
28. See http://www.privacyrights.org. Since Feb. 15, 2005, there have been approximately 93,754,336 records containing sensitive personal information involved in security breaches.