CLARITY White Paper

Implementing Electronic Medical Records (EMR):

Mitigate Security Risks and Create Peace of Mind

The use of electronic medical records (EMRs) to maintain patient information is encouraged today and will soon be common practice in healthcare. Furthermore, the government is supporting the trend by advocating the implementation of EMRs — in 2004, President George W. Bush said his goal is for the majority of Americans to have computerized medical records by 2014[i] — and providing financial incentives to healthcare providers who make the conversion. The movement to create an electronic health record system nationally has physicians and hospitals increasingly abandoning traditional methods of record keeping and turning to EMRs with the expectations that the EMR will reduce costs, improve medical outcomes and increase data reliability. While the reasoning behind the transition to EMRs is justifiable, the change brings with it emerging privacy and security concerns that need to be understood.

The movement to create an electronic health record system nationally has physicians and hospitals increasingly abandoning traditional methods of record keeping and turning to EMRs … the change brings with it emerging privacy and security concerns that need to be understood.

The guidelines for the privacy and security of protected health information (PHI) contained within a patient's medical record were defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and expanded upon by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). HIPAA provides the compliance standards with how PHI should be safeguarded and protected, while HITECH specifically addresses the privacy and security associated with the transmission of PHI electronically and imposes civil monetary penalties in the event of a data breach.

8725 West Higgins Road Suite 810 · Chicago, IL 60631
T: 773.864.8280 · F: 773.864.8281
www.claritygrp.com

As with traditional records, the potential liabilities associated with EMRs arise when access to PHI has been breached. HITECH defines a breach as an impermissible use or disclosure (under the Privacy Rule) that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual[ii]. While healthcare providers may already have policies and procedures to defend against breaches of paper files, these measures would likely do little to protect against stolen laptops, lost blackberries, computer hackers and numerous other sources of potential liability that relate to electronic data. Additionally, the updated HIPAA/HITECH regulations further limit the disclosures as well as extend the requirements for business associates of covered entities in terms of who is permitted access.

Maintaining PHI electronically allows a single breach incident to potentially affect a greater number of individuals. This is significant because the violations correspond to the violator's level of culpability. The penalties are enforced by the Office of Civil Rights (OCR).

Maintaining PHI electronically allows a single breach incident to potentially affect a greater number of individuals - for example, one stolen laptop could contain the PHI for thousands of patients admitted to a particular hospital. This is significant because the violations correspond to the violator's level of culpability. The penalties are enforced by the Office of Civil Rights (OCR) and are as follows[iii]:

- Unintentional violations: $100 to $50,000 per violation
- Violations due to reasonable cause: $1,000 to $50,000 per violation
- Violations due to willful neglect that are corrected: $10,000 to $50,000 per violation
- Violations due to willful neglect that are not corrected: $50,000 per violation

The maximum penalty for all violations of an identical provision in a given year would be $1.5 million. However, entities that correct violations within 30 days of discovering an unknown violation may avoid the imposition of a civil monetary penalty.

8725 West Higgins Road Suite 810 · Chicago, IL 60631
T: 773.864.8280 · F: 773.864.8281
www.claritygrp.com

In addition to the possible fines in the event of a breach, the provider is obligated to provide notice to any individual who is potentially compromised no later than 60 days after the breach has been discovered. The notice must contain dates of the breach and discovery, description of the PHI involved, steps taken to mitigate harm, steps the individual should take to mitigate harm and contact procedures.

In addition to the possible fines in the event of a breach, the provider is obligated to provide notice to any individual who is potentially compromised no later than 60 days after the breach has been discovered.

In light of these new and potentially significant exposures, healthcare providers should take precautions to minimize the risk of violations. This should begin in their own practices and facilities with a review of the HIPAA/HITECH privacy and security rules with their staff, employees and others who have access to PHI. They also need to implement policies and procedures relating to how PHI is stored and accessed (both electronically and otherwise), properly train staff to follow them and schedule audits to ensure compliance on a continual basis. Also, providers need to consider the flow of PHI from their practice and have business associate agreements in place with all organizations or entities with which they share PHI, such as EMR software vendors. Providers and healthcare organizations that are eligible to participate in the EMR incentive funding programs under the American Recovery and Reinvestment Act (ARRA) of 2009 should review the meaningful use security requirements and technical capabilities outlined under HITECH.

In light of these new and potentially significant exposures, healthcare providers should take precautions to minimize the risk of violations.

One of the considerations healthcare providers may undertake is to gain insurance to provide them with protection before a breach might occur. The insurance coverage offers additional peace of mind and supports the internal processes undertaken to prevent a potential breach. In fact, some physician professional liability carriers currently offer the breach coverage to doctors in concert with their medical malpractice policies at no cost or for a minimal cost. Similar coverage is available for hospitals, long term care centers and other healthcare facilities. In evaluating the coverage available, it is important to consider what is covered (and excluded), limits of liability and premiums. Some of the features to consider include:

8725 West Higgins Road Suite 810 · Chicago, IL 60631
T: 773.864.8280 · F: 773.864.8281
www.claritygrp.com

- **Network security and privacy insurance** - including coverage for both online and offline information and coverage for defense costs and fines/penalties
- **Network asset protection** - coverage to replace or recover data that is lost, compromised, damaged or corrupted
- **Notification expenses** - coverage for the costs associated with having to notify individuals whose information has been compromised. This usually includes customer support and credit monitoring expenses for those individuals

While the emergence of EMRs exposes healthcare providers to a number of risks associated with the handling and transmission of electronic PHI, a proactive risk management approach can help mitigate potential liability.

Not all cyber liability insurance products are the same and healthcare providers interested in this coverage should carefully review the products and discuss them with their agents.

The ultimate goal of the privacy and security regulations is to enable health information to follow the patient wherever and whenever it is needed across the continuum of healthcare delivery. Safeguarding this process as well as building the confidence of patients and providers creates a real advancement in health information collection, exchange and technology. Further, while the emergence of EMRs exposes healthcare providers to a number of risks associated with the handling and transmission of electronic PHI, a proactive risk management approach can help mitigate potential liability. This includes:

- Staff training
- Policies and procedures that delineate what is collected and who has access
- Security plans in place in concert with the EMR vendor or partner
- Monitoring systems to ensure that any unsuspected attempted breaches can be detected
- Breach Disaster Plan in place to act quickly in the case of a breach to meet the notification requirements under HITECH

8725 West Higgins Road Suite 810 · Chicago, IL 60631
T: 773.864.8280 · F: 773.864.8281
www.claritygrp.com

Becoming aware of the risks and the privacy and security requirements outlined under HIPAA/HITECH, purchasing cyber coverage and instituting a proactive risk management plan can work in concert to create a peace of mind for healthcare providers utilizing EMRs.

Drew Becker
Manager, Physician Underwriting & Program Management
Clarity Group, Inc
Chicago, IL

For more information, please contact Drew Becker at 773.864.8280 or visit our website at www.claritygrp.com

[i] Associated Press (January 27, 2005). "Bush pushes computerized medical records." Retrieved from http://www.msnbc.msn.com/id/6876192/ns/health-health_care/t/bush-pushes-computerized-medical-records/
[ii] U.S. Department of Health & Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[iii] Federal Register, Vol. 74, No. 209 (October 30, 2009). "Rules and Regulations." Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf

8725 West Higgins Road Suite 810 · Chicago, IL 60631
T: 773.864.8280 · F: 773.864.8281
www.claritygrp.com