Washington Healthcare News®

wahcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

Electronic Medical Records and Cyber Liability

By Janet Jay
Agency Sales and Service Representative
Physicians Insurance Agency

The electronic medical record (EMR) at its best is a great tool for medical providers needing to access patient files from wherever they are. A family practice physician can instantly send a patient's chart to an emergency room physician, who can then get instant access to results of an MRI from the radiologist so that important decisions about the patient's care can be made in a timely manner.

EMR has the potential to allow access to thousands of patient records at once for researchers to determine and predict trends, to see what treatment is or is not working for patients with similar fact patterns, and to assist in the diagnosing of new diseases and the tracking of new pandemic trends.

EMR is also the cyber criminal's dream. Medical records contain all sorts of data that could be valuable to a criminal looking for credit card numbers, patient medical histories, employee records, insurance information, addresses, and even social security numbers. In the days of paper files, someone trying to access patient files would have had to bring a large trailer and make multiple trips in and out of a clinic to get away with a fraction of the patient files that can now fit on a keychain jump drive.

Increased Regulation

Each year millions of medical records are inappropriately released. Some are due to the work of cyber criminals, while most are due to simple negligence. Legislators have responded to this alarming trend by increasing regulation. The HITECH (Health Information Technology for Economics and Clinic Health) Act has been enacted to promote the use and standardization of electronic medical records while maintaining patient privacy. It extends certain provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to third parties, such as EMR vendors, and mandates patient notification in the event of a data breach.

The HITECH Act calls for increased HIPAA violation penalties, both criminal and monetary. It also gives Health and Human Services (HHS) the authority to audit for HIPAA compliance. HHS has recently acted on this authority with a new pilot program that will audit up to 150 covered entities between November 2011 and December 2012. The pilot program will give HHS a broad assessment of HIPAA compliance issues, and through identifying and correcting HIPAA concerns found, HHS hopes to share what it learns and develop tools to help covered entities better protect health information.

Tools for Your Practice

While it is unlikely that your group will be one of the 150 entities audited this year, the new laws are a good reminder for your office to brush up on patient privacy. If you are a member of Physicians Insurance, you have access to HIPAA privacy

tools on the Risk Management section of our Web site, www.phyins.com. In addition, you or any member of your medical office can register for our no-cost risk management seminars, many of which currently review the new HITECH provisions of HIPAA.

Your office may also benefit from a new planning tool that the Federal Communications Commission (FCC) recently released at http://www.fcc.gov/cyberplanner to help small businesses develop a cyber security plan. In addition, the FCC has a wealth of information, tips, and other cyber security resources published at http://www.fcc.gov/cyberforsmallbiz.

Insurance Options

Cyber liability, network security, and data compromise policies vary greatly. When purchasing a policy, it is important to know what type of risk the policy affords. Some policies simply help you notify your clients of an inadvertent release of their private information. This coverage might include assistance in determining which records were released and provide your clients with credit monitoring services. Other policies are more comprehensive and can include additional features such as:

- Third-party liability coverage for claims alleging financial loss due to a network security or privacy breach;
- Coverage to replace your data that gets damaged, erased, or corrupted;
- Expenses associated with cyber extortion threats;
- Business interruption and extra expense for your loss of income due to a covered loss;
- Claims alleging copyright infringement; and
- Fines and penalties associated with HIPAA and the HITECH Act.

Whatever type of policy you choose, you and others in your office who may need to access the coverage at some point (e.g., IT personnel) should be aware of what the policy covers, as well as its limitations.

Janet Jay is the Agency Sales and Service Representative for Physicians Insurance Agency. She can be contacted by e-mail at janet@phyins.com or telephone at (206) 343-7300 or 1-800-962-1399.

Association Insurance Services, Inc., dba Physicians Insurance Agency, intends this article to be a useful reference. The information provided is obtained from or developed with the use of sources generally considered to be reliable, but the information may not be accurate and complete for all situations.

Reprinted with permission from the Washington Healthcare News. To learn more about the Washington Healthcare News visit wahcnews.com.