Privacy and Security - More Important than Ever

By Carlyn M. Choate, MSHI, RHIA, CHPS
HealthInsight-HIT Project Coordinator

HealthInsight and the Nevada Regional Extension Center want all physicians to be apprised of the complexity of meeting the requirements for Core Measure 15- Privacy and Security. As we know from the recent security breaches across the country, organizations, physicians, covered entities, and their business associates must maintain vigilance in protecting health information. Taking these requirements seriously will ensure Meaningful Use payments and protect practices, patients, and organizations from potential breaches.

If you are one of the many providers who have successfully reached Meaningful Use, you may not be aware, but early adopters to the Electronic Health Record (EHR) Incentive Program have been subject to Meaningful Use Attestation audits to verify the accuracy and validity of core and menu measures reported to the Centers for Medicare and Medicaid Services (CMS). These audits have initiated recent changes to the Meaningful Use attestation process and CMS is conducting "pre-payment" audits for eligible providers preparing to receive Meaningful Use incentive payments. Practices in violation of federal and state regulations are subject to potential penalties including fines, penalties, and even jail time if appropriate safeguards are not implemented.

Increasing privacy and security are also critical to maintaining important relationships with patients. Patients and families want to know that their healthcare community is taking privacy issues seriously in this digital age. Core Measure 15 of Meaningful Use is the foundation for building a successful Privacy and Security Management program.

What are the Requirements for Core Measure 15?

Eligible Professionals Meaningful Use Core Measure 15: Protect Health Information	
Objective:	Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities
Measure	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process. Eligible professionals (EPs) must attest YES to having conducted or reviewed a security risk analysis in accordance with the requirements prior to or during the EHR reporting period to meet this measure.
Exclusion:	None

In order for eligible providers to successfully attest "YES" to this measure, they must have conducted a security analysis or review and update an existing security analysis. In addition, eligible providers must implement changes to address deficiencies. Many physicians are still confused and unsure of what this measure entails and how they go about conducting a security analysis.

Assuming that your electronic health record vendor has completed a security analysis on your behalf or installing an anti-virus software does not meet the necessary requirements for attesting to Core Measure 15. Physicians must not assume that simply because their EHR software is ONC certified and meets the certification criteria, that this is sufficient for attestation. A security risk analysis must still be conducted, implemented, and documented to satisfy the requirement. Keep in mind that the size of the organization and the complexity will determine the depth and approach to meeting Core Measure 15.

Privacy and Security - More Important than Ever

By Carlyn M. Choate, MSHI, RHIA, CHPS
HealthInsight-HIT Project Coordinator

What are Risk Assessment, Risk Analysis, and Risk Management?

In order to understand Meaningful Use Core Measure 15, first you need to understand the difference in Risk Assessments, Risk Analysis, and Risk Management. Many individuals use these terms interchangeably, however there are significant differences in each of these.

Risk Assessment*:* A risk assessment is a term used to identify the overall risk analysis process. This consists of the evaluation of the environment and assesses the potential threats to the organization.

Risk analysis*:* A risk analysis is the detailed granular process of identifying the weaknesses that make the organization vulnerable to threats.

Risk management*:* This is an ongoing maintenance process that includes the practical application and implementation of making corrections, developing policies and procedures, monitoring, evaluating and communicating risk.

Each of these terms is the stepping stone for the other; for example, you cannot "*analyze*" a situation without first "*assessing*" what it is you want to analyze, and you cannot "*manage*" something without knowing what it is you are trying to control and prevent.

Steps to Meeting MU Core Measure 15

Step 1 System Characterization-This is the process of collecting inventory and identifying which critical assets need protection or increased level of security. Inventory includes hardware, software systems, software applications, networks, and identifies all primary users and owners within the system.

Step 2 Threat Identification-This step identifies the possible threats to availability, integrity, and availability of information within the system. Examples of these threats include acts of nature (earthquake, hurricane, etc.); acts of man (unauthorized access, identity theft, workforce and staff, etc.); and environmental (hardware/software failures, power outages, etc.).

Step 3 & Step 4 Vulnerability Identification and Control Analysis- Because of the relationship between vulnerabilities and control, these steps are often combined depending on if the application is new or currently in use by the organization.

Vulnerabilities- is defined as the weakness within the system that leaves the data or information vulnerable to attack, loss, or destruction.

Control-is defined as the lack or inadequate control over the access, use, or availability of the software or hardware that contains the information.

Step 5 Likelihood Determination-This step includes determining the probability of a threat in successfully penetrating the system and determines the how likely a potential threat will occur.

Privacy and Security - More Important than Ever

By Carlyn M. Choate, MSHI, RHIA, CHPS
HealthInsight-HIT Project Coordinator

Step 6 Impact Analysis-The next step is to address the impact of those threats to the organization of systems are compromised. If an impact to the organization is categorized as HIGH, it may cause significant financial loss to the organization.

Step 7 Risk Determination- This step encompasses a scoring method based on the likeliness and impact to the organization allowing the organization to determine the priority at which the threat should be addressed.

Step 8 Control Recommendations- This step identifies each vulnerability found and addresses solutions to remedy the threat.

Step 9 Results Documentation- This step includes any forms, documents, spreadsheets, inventory, checklists, notes, etc. gathered during the risk analysis process. Documentation is required by HIPAA to be maintained for six years and is critical during an audit and for Meaningful Use Attestation requirements.

Eligible Providers must be aware that meeting Core Measure 15 is required for each attestation year. They must be prepared to provide documentation to support that a security analysis was conducted as part of the CMS EHR Incentive audit process.

Meeting Meaningful Use Core Measure 15 is a multi-step and continuous process that requires planning, resource, and support from others with experience in privacy and security in a quality conscious healthcare environment. It is not sufficient to assume that your vendors and contractors will ensure PHI is protected in your practice. You must take steps to ensure that risks are addressed and document it thoroughly. Failure to do so can not only cause failure to comply with Meaningful Use Objectives and Measures but could also open your practice up for HIPAA violations and their related fines.

HealthInsight and the Nevada Regional Extension center can provide assessment tools and support to eligible practices. Contact us at 1-800-483-0932, REC@healthinsight.org or at http://healthinsight.org/nevada

References

Mehta, P. (2008, November 11). *Risk Assessment vs. Risk Analysis vs. Risk Management*. Retrieved April 18, 2013, from Security: http://security.networksasia.net/content/risk-assessment-vs-risk-analysis-vs-risk-management

NIST. (2012, September). *Special Publications (800 Series).* Retrieved April 18, 2013, from National Institute of Standards and Technology (NIST): http://csrc.nist.gov/publications/PubsSPs.html

Walsh, T., & Amatayakul, M. (2011, January). *Practice Brief: Security Risk Analysis and Management: an Overview (updated)* . Retrieved February 2013, from American Health Information Management Association: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048622.hcsp?dDocName=bok1_048622