HIPAA - The Eight Hundred Pound Gorilla in Meaningful Use

As most medical practices hone in on meeting their Meaningful Use measures and attaining electronic health record (EHR) stimulus payments, many are underestimating the effort involved in developing their HIPAA Security program involved in Meaningful Use Measure 15, the Security Risk Analysis. Practices typically spend most of their effort on Core and Menu Set measures that require workflow changes such as smoking status, vital signs and visit summaries. Most practices don't realize that the security risk analysis presumes that the HIPAA Security Rule, which went into effect in 2005, has been implemented within their organizations. Until now, there has been almost no enforcement of the security aspect of HIPAA, only privacy. That is all about to change.

The HITECH Act, which established the EHR incentive program, placed a heavy emphasis on HIPAA when it included Core Measure 15. It states that eligible providers (EP) must "conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1)". This is the HIPAA Security Rule that was put in place in 2005. Measure 15 also states that EPs must "implement security updates as necessary and correct identified deficiencies…". There are many aspects of the Security Rule that require a practice's time and effort to remain in compliance.

The HIPAA Security Rule also involves the development of policies and procedures that ensure safeguards are in place for all electronic protected health information (ePHI). ePHI is considered any protected health information (PHI) which is stored, accessed transmitted or received electronically. PHI, under HIPAA, means any information that identifies an individual and or relates to one of the following: 1) a person's past, present or future physical or mental health, 2) the provision of health care to an individual, 3) the past, present or future payment for health care. Information is determined to be identifiable in nature if it includes either the individual's name or any other information that could enable someone to determine his/her identity. There are eighteen types of "individually identifiable" data that comprise PHI and they pertain to an individual, their employer or family members.

The safeguards that are required to be in place under the HPAA Security Rule fall into four categories: administrative, organizational, technical and physical. Each category has specific elements that must have documented policies and procedures (identified below). It is also the responsibility of the medical organization (covered entity or CE) to provide education for their employees. The expectation is clearly that CEs create cultures of privacy and security within their organizations and not simply place a binder with canned HIPAA policies and procedures on a shelf to collect dust. The expectation

is that the following safeguards be in place and/or a documented action plan that addresses the requirement:

Administrative Safeguards (164.308)

- Identify security official; conduct risk analysis; create risk management plan; develop a sanction policy; review information system activity; establish workforce authorization, clearance and termination procedures; foster security awareness and conduct training; protect systems from malicious software; establish a data backup plan, an emergency mode operations plan, a disaster recovery plan complete with testing and revision procedures, applications/data criticality analyzed and security incident response and reporting.

Organizational Requirements (164.314)

- Business associate contract compliance with rules about the length of time that documentation is maintained and its availability to staff.

Technical Safeguards (164.312)

- Access control, unique user identification, emergency access procedure, automatic logoff, encryption and decryption, audit controls, integrity controls, authentication, and transmission security.

Physical Safeguards (164.310)

- Facility access controls, including contingency operations, a facility security plan, access control and validation procedures, and maintenance records; workstation use and security; devices and media controls such as disposal, media re-use, accountability, data backup and storage.

To meet Meaningful Use, the Security Risk Analysis, which is a review of an established security program, must be performed within an EP's reporting period. Many practices underestimate the scope of this effort and are left scrambling to address requirements before the end of the period in order to secure their incentive payments.

The HITECH Act also includes a substantial HIPAA Security enforcement component which is the responsibility of The Office of Civil Rights (OCR). OCR has engaged the KPMG consulting firm to conduct random audits, which are currently underway. These will be relatively few in number and are intended to focus on education in this early stage of enforcement. However this should not lead EPs into complacency because the intention is clearly to increase accountability over time. The law entails substantial penalties for non-compliance which range from $25,000 (maximum) for "unknowing" violations to $1.5 million (maximum) for "uncorrected willful neglect".

As we enter a new age of electronic heath information we will need to expand the way we think about protecting patient information. In time, the primary enforcer for doing so will not only be the government, but patients, too.

The EHR Advisory Group, LLC provides an array of EHR & Meaningful Use, as well as HIPAA privacy, security, breach and risk management services.

Visit us at: *ehradvisorygroup.com*
6443 Ridings Road, Suite 130, Syracuse, NY 13206
315-437-4377 (Phone)
315-410-5552 (Fax)