# Meaningful Use - Core Measure 15 Explained

*October, 2011*

Many practices are in the process of becoming "Meaningful Users" of their electronic health record (EHR) systems. Most of the initial measures involved with meaningful use involve some type of provider behavior (e.g. eprescribing 40% of the time) or turning on and using some aspect of the EHR (e.g. generate a list of patients by specific condition).

Core Measure 15 is different. Core Measure 15 asks the provider to "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." The objective here is to be able to prove the provider is protecting electronic health information created or maintained by the EHR technology through the implementation of appropriate technical capabilities. A significant benefit of adhering to Core Measure 15 is that any additional security that is implemented to comply will help keep your practice and your patients' PHI safe from any "bad guys" that are out there.


Risk analysis is not new – it has been part of the HIPAA Security Rule since 2003. It is something that practices should have been doing all along. 45 CFR 164.308(a)(1) is a subset of the HIPAA Security Rule that focuses on Electronic Health Record technology. CFR is short for "Code of Federal Regulations", which is the listing of all the rules and regulations of the various agencies of the Federal Government. The "risk analysis" referred to is the risk analysis spelled out in the HIPAA Security Rule: "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity" (see section (ii)(A) of 45 CFR 164.308(a)(1)).

There is not a lot of additional, easily obtainable or distillable information or guidance to go by. How do we know what the government is looking for here? Before we go forward, let's take a step back.

Most companies rely heavily on their internal computer networks to conduct their day-to-day business. Today's networks usually consist of fairly standard hardware including PCs, laptops, servers, wireless networking, routers, switches, firewalls, etc. Virtually all of these networks are connected to the Internet. For the most part, a connection to the Internet is a tremendous asset: employees can send and receive email, search for information, give web demonstrations and perform a myriad of other functions. However, an increasingly big issue is that of security. Just about every day there is an article in the newspaper about a major security breach of one type or another. Most companies take computer security very seriously, as it is not to their advantage to have their servers hacked or their email compromised. Despite all their efforts, however, corporate IT security remains an issue that companies must focus on every day. Although adding security to a network is an extra cost (both in the cost of the measures themselves and extra time it may take an employee to perform a certain task), it is a necessary and unavoidable cost of doing business.

When HHS developed the EHR Incentive Program, the need to insure that ePHI (electronic protected health information) was secure was a very high priority. Privacy is one of the core tenets of HIPAA, and is assumed by all Americans. We expect that when we go to the doctor, our medical records will remain private and secure. Intentional or unintentional breaches of this privacy are not acceptable and must be minimized. Sloppy privacy practices are not to be allowed. Therefore each practice must insure that it takes the proper steps to protect the privacy of its patients and their medical data. While most practices have done this, HHS wanted to insure that practices recognize the importance of continuing to keep medical records private and secure in the new electronic environment. Even though the HIPAA Security Rule was finalized over 8 years ago carrying a compliance deadline of 2006, some practices might not be aware of all the measures that need to be taken to insure privacy in the

new electronic age. After all, they might not have had any computer network in place before implementing an EHR. As a result, the prioritization of this is seen in Core Measure 15.

Now, an important point in Core Measure 15 is the following "protect electronic health information created or maintained by the certified EHR technology…" In fact, one of the available pieces of guidance from the incentive program states: "Eligible Providers must conduct or review a security risk analysis of certified EHR technology and implement updates as necessary at least once prior to the end of the EHR reporting period and attest to that conduct or review." Therefore, Core Measure 15 actually narrows the scope of a normal HIPAA risk analysis to the "EHR technology" which means the EHR system and the outside systems, programs, processes and tools that support privacy and security of the certified EHR technology. Note, however, this does not mean a practice does not need to comply with the entire HIPAA Security Rule – it simply means that for Core Measure 15 attestation the practice need only show proof of risk analysis of the certified EHR technology.

Networks take many shapes and sizes. So there is no "one size fits all" risk analysis. What might be appropriate for one network and practice, might not be for another. This is why HHS left the language as general as it is. But there are some common IT best practices that can be drawn upon. As examples, you should make sure that:


a) passwords are strong – for example, using "password" as your password is not recommended
b) user sessions time out after a reasonable period of time (so that access to the EHR is not available to just anyone who walks up to a PC)
c) access to protected health information is given to the right personnel (does your accounting manager really need access to ePHI?)
d) access to your wireless networking requires an ID/password and make sure the wireless networking is encrypted
e) the firewall on your network is properly configured to only allow approved Internet traffic in and out of your network
f) you use antivirus software on your PCs and servers (viruses are not good for computers or people!)
g) you encrypt protected health information as it is stored on the servers and as it is in moved between locations/computers

These are just some of the protections that need to be in place. But as you can see, many, if not all of these are security measures that most other businesses should implement as well.

For the purposes of Core Measure 15, HHS is asking each practice to review the security risks to their electronic health information and the protection measures that have been implemented on its network, versus what should be implemented for their network, and to correct any deficiencies that are identified. Each practice (probably in association with its IT department or its IT support company) should decide what is appropriate for its network. Some time needs to be given to thinking through the appropriate security measures based on the size, complexity and capabilities of the practice, the practices' technical/infrastructure/ hardware/software capabilities, the cost of the security measures and the probability and criticality of the potential risks to electronic health information. Once they have been identified, these security measures should be implemented and documented. It is not acceptable to implement security measures without documenting them.

HHS will be conducting random audits of providers that receive incentive money, so this measure should not be taken lightly. Proper documentation of the risk analysis and resulting security implementation is required. Also note that if there is more than one provider in a practice, the risk analysis does not have to be repeated for each one. A single risk analysis for the practice would be acceptable, assuming that each provider is accessing and using the same network.

## About BEI

BEI is a privately owned business that has been providing IT support services to organizations of all sizes throughout the Washington DC metro area since 1987. BEI provides network design, installation, support, maintenance and procurement services to hundreds of clients in the region, with a focus on healthcare IT. We are a Microsoft Partner with Gold Competencies in Server Platform and Volume Licensing. We specialize in Microsoft-based networks as well as other leading LAN/WAN technologies. BEI is a member of the VMGMA (Virginia Medical Group Management Association), the MCMS (Montgomery County Medical Society), the Northern Virginia Practice Management Association, HIMSS (Healthcare Information and Management Systems Society) and MS-HUG (Microsoft Health Users Group).

**To read other BEI Healthcare IT Whitepapers go to www.beihealthcare.com and select "Healthcare IT Whitepaper ARCHIVE".**