Copy That? Meeting the Meaningful Use Objectives for Electronic Copies, Part 2

Save to myBoK

By Kelly McLendon, RHIA

Hospitals and providers seeking to receive payments under ARRA's "meaningful use" incentive program must prove their eligibility by meeting objectives and associated measures for the use of their EHR systems. Some of the requirements of most interest to HIM professionals are related to a provider's ability to produce, log, and disclose protected health information (PHI) to individuals upon request.

This column is the second of two that explores the issues. The first (April 2010) describes the three related program requirements and how they will be measured; this column discusses considerations for providing and securing the information.

Summary of the Access and Copy Objectives

In brief, the objectives require that EHRs produce electronic copies of data and documents in both human and machine-readable formats. The program requires two basic types of copies and access: electronic copies that are produced onto electronic media or e-mailed for disclosure and information posted for online access. Both providers and hospitals must provide a prescribed minimum of information in each case.

It should be noted that these requirements apply only to the meaningful use program and those providers that choose to participate. By 2014, however, all hospitals and providers must meet the meaningful use criteria or face reductions in Medicare and Medicaid payments in the following year.

Related Privacy and Security Requirements

Elsewhere in the meaningful use objectives are basic privacy and security requirements. These are not a part of the copy and access objectives, but they have direct bearing on them.

An objective related to ensuring privacy and security requires both eligible professionals and hospitals to "protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities" (see table). Providers will demonstrate their compliance by conducting a security risk analysis and implementing necessary security updates as described in HIPAA.

The interim final rule on EHR standards and certification, a companion to the meaningful use rule, identifies numerous security standards certified EHRs must include. Many are for encryption, addressing the safe harbor provision for secured PHI.

Considerations for Electronic Copies

Few providers are routinely providing patients with electronic copies of their information, and the meaningful use requirements will raise many questions for those that want to begin.

What media may be employed? The proposed rule does not specify the media that may be used to deliver PHI. Generally regulations avoid such specifics because the authors know that as soon as they name a technology it tends to become obsolete.

Providers are thus free to consider any media that will accommodate both the files containing the PHI and the security wrappers that will protect them. This could include CDs, DVDs, USB drives, patient portals, or personal health records. E-mail may be the preferred method in many instances, if it can be secured. Much of an organization's choice will depend on the file formats and media its current systems can support.

What file formats are acceptable? Likewise, the rule does not specify a file format beyond one that is "human readable." Certainly RTF, JPG, and PDF files are most easily produced from existing EHRs and managed by consumers.

An organization's first consideration in choosing file format is which format standard to employ: the ASTM Continuity of Care Record or the HL7 Continuity of Care Document. ONC's interim final rule on EHR certification standards did not specify format; it only requires that EHRs have the ability to interpret either and display the content in human-readable format.

There was some debate in the industry leading up to the March comment deadline on whether the rule should adopt a single format. It is possible that the comments ONC receives will influence the final rule.

The data and file formats will be important drivers in determining what information providers make available in electronic copies. Complicating this decision is the fact that not all EHR systems produce data in both human- and machine-readable files in the same ways.

For example, some products may produce only a CCR and an XML file; others may produce only a CCD and a PDF file. Determining each EHR vendor's capabilities will be a first step in determining what data may be presented in which format for both human- and machine-readable files.

What security is required? Providers will require the same standards that render PHI into secure 128-bit encryption. The security standards are listed in the interim final rule on certification standards and will require the input of the organization's IT staff (an example of why addressing the meaningful use criteria is best performed as a part of a team or workgroup). It will be necessary to encrypt data both in motion (while being transferred) and at rest (while on the medium, such as CD).

While in general the HIPAA security standards do not require entities to encrypt PHI, it is highly recommended that they do so. Thus the easiest way to deliver copies to patients will be either via secured e-mail or encrypted DVD or CD with a separate decryption key.

In order to encrypt PHI, providers will rely on either functionality within their EHR systems or third-party software. At present few EHR vendors include encryption functionality, so third-party tools may have to play a large role in enabling encryption until EHR products can catch up.

However entities choose to secure PHI, it is important they make decryption of the files as conveient to the patient as possible by including decryption software and readers with the files.

It should be remembered that decryption keys must be separate from the files themselves. Flash drives, DVDs, and similar media will require the entity to provide separate devices or decryption keys to maximize security. This is one good argument for secured e-mail or portal access, because the encryption and decryption processes are self -contained.

Securing Electronic Copies and Online Access

The meaningful use program requires participants to protect the privacy and security of information within their EHRs through appropriate technical controls. This requirement applies to the electronic copies and online access they provide to patients under separate objectives.

Objectives			
Care Goal	**Eligible Professionals (EPs)**	**Eligible Hospitals**	**Measures**
Ensure privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law.	Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement security updates as necessary.

Considerations for Online Access

What products or modules are necessary to post PHI online? This is a significant question given that most installed EHRs do not have the ability to provide patients online access to the results they incorporate (e.g., lab results) or the data and documents they capture and create.

Providers will require workflows for the capture of the external documents into EHRs, including reconciliation of exceptions and errors. Most will presumably turn to their EHR vendors or third-party services to provide online access though SAS, ASP, or other technologies.

Further, providers will require functionalities that manage, monitor, and track the copies and access they provide. To meet the electronic copy objective, professionals and hospitals must demonstrate they met 80 percent of patient requests within 48 hours. Professionals must provide online access within 96 hours to 10 percent of their patient populations. Measuring the latter may present operational challenges.

Meeting the requirements will require close work between HIM professionals, IT professionals, and their vendors. HIM professionals should also consider the law of unintended consequences: the objectives may generate more patient interest in HIPAA, more requests for accountings of disclosure, and more requests for amendments.

Kelly McLendon (kmclendon@go-iem.com) is president of Health Information Xperts.

Article citation:
McLendon, Kelly. "Copy That? Meeting the Meaningful Use Objectives for Electronic Copies, Part 2" *Journal of AHIMA* 81, no.5 (May 2010): 36-37.