# Enterprise E-Signature: Managing Flourishing E-Signatures at the Organizational Level

by **Sandra Nunn**, MA, RHIA, CHP

In most organizations, e-signature functionality came about due to HIM professionals' larger work in developing electronic health record (EHR) functionality and policy. The first e-signature solutions frequently involved transcribed medical reports. Today, e-signatures are commonly used throughout healthcare facilities, and organizations would do well to manage them at an enterprise level. Those early policies developed for EHRs can make a sound starting point.

Managing e-signatures at the enterprise level requires identifying how and where e-signatures are used within multiple IT systems—both clinical and administrative—and standardizing and documenting policies. Included in this work is solving the challenges of new communication methods such as e-mail and establishing and synching appropriate retention according to record type and its system.

## Migrating E-Signature Policy

Formerly confined to healthcare providers, e-signatures are flourishing in applications for finance (e.g., signatures on financial instruments), contracting, and information services (e.g., collaboration technologies). It will eventually be part of electronic personal health records. Enterprise applications such as e-mail also require policies around authentication, particularly when an e-mail exchange meets the conditions of entering into a contract.

E-mail, e-signatures, and digitized signatures (scans of handwritten signatures) may only require a password to apply (e.g., logging on to an e-mail account), and they offer little assurance of the user's authenticity. In contrast, digital signatures are cryptographic signatures that authenticate the user and provide nonrepudiation.

In adapting to e-discovery requirements, many healthcare entities have begun creating inventories of all applications and databases supported by their IS infrastructures. Through these inventories, they document their ability to apply legal holds to records within each application or database. Most organizations also are looking at how to assign ownership and accountability on the business and IS sides of each of these applications and databases to ensure that the correct parties are creating good faith practices regarding the management of each of these information repositories. This work offers a basis for inventorying e-signature capabilities, also.

Organizations can begin centralizing their e-signature policies by capturing the functionality and use of e-signature in each application. With HIPAA security audits appearing around the country, healthcare organizations would be well served to be able to hand over a complete inventory of applications with attendant functionality including authentication information.

Organizations should also consider documenting existing organizational e-signature standards, policies, and procedures to get started. Taking the EHR as a jumping off point, HIM professionals should document the type of electronic signature chosen for authentication in the medical record (e.g., digitized, digital, password-driven, etc.). Those laws and regulations, both federal and state, reviewed to write e-signature policy for medical records could be amplified by other legislation that may govern e-signature in other sectors of the organization including those involving e-commerce.

Documentation should spell out the reasoning behind the selection of one type of electronic authentication over another. For example, digital signatures are often selected for authentication of electronic medical records because they provide higher levels of security assurance than other types of electronic signatures. If other authentication solutions are chosen either because of vendor limitations or because of other strictures on the organization, these limitations should be specified.

## Policy Decisions

As they catalog and migrate their e-signature policies, organizations must ask the following questions:

- When is authentication really required?
- What are the components of electronic signature and how does the user acquire e-signature rights?
- Can electronic signatures be cut and pasted from one record to another?
- What is the lifecycle of electronic signature?
- What are the privacy and security challenges involved?
- What cost issues must be considered?
- When and how does revocation occur?
- How does electronic signature occur in unconventional records?
- How are enterprise information management policies created that span information silos and business units?

In addition, exploring the following items helps organizations gain a global view of signature policy across the enterprise:

- Existing legislation governing e-signatures at the federal and state levels
- Existing standards that potentially influence e-signature policy creation
- Other required types of legal activity such as the application of electronic litigation holds as required by the Federal Rules of Civil Procedure or the application of date and time stamps to ensure medical record integrity and completion
- Audit trails and identity management
- Current business processes, including the need for countersignatures, multiple signatures, or notarized signatures

In addition to inventorying applications, organizations must also focus on documents and records. The organization's legal services or compliance department must spell out the types of documents and records that require authentication and how that authentication must be applied.

Whether a physician is authenticating a transcribed note online or a patient is updating personal information on a personal health record site, all requirements to authenticate electronically (or even physically if required by law) should be documented in a centralized policy, or a repository of centralized policies, referencing the legal or regulatory mandates involved. Those documents or records not requiring authentication should also be spelled out (e.g., common public information like marketing materials).

The components of electronic signature and the steps to acquire authority to use it must be part of a standardized process regardless of organizational sector and must be documented. For example, the identification materials required to sign authorizations to release information must be noted (e.g., the credentials necessary to sign medical records or the level of organizational authority achieved to sign financial instruments).

E-signature certificates that list the systems to which the owner has e-signature rights are a step toward signature authority centralization and ease the security cost of managing e-signature functionality across multiple systems. HIM professionals undoubtedly have developed processes that allow for the issuance of e-signature rights in the EHR. Building on those processes for other organizational domains is another step toward organizational best practices for electronic signatures. When and how the e-signature rights granted to individuals or groups are revoked must be a corresponding part of policy developed to grant rights.

## The E-Signature Lifecycle

The arc of e-signature policy begins with granting rights and ends with the revocation or termination of e-signature authority. In between, policy must also describe by applicable system whether the e-signature functionality is actually part of the electronic system or another piece of software attached to the system for authentication purposes. In either case, the signature must be retained the same length of time as the record to which it is appended. In other words, retention time frames apply equally to the signature file and its record.

The HIM custodian of the EHR carries responsibility to ensure that signatures applied to components of the EHR are retained for the required lengths of time. This applies equally to feeder systems that retain components of the legal EHR or the designated record set. If authentication occurs in those systems, the e-signature must become part of the retained file.

E-signature policy developed around the EHR and other conventional records is straightforward compared to policy creation concerning e-signature of records created through newer technologies. If the organization has established a retention period for e-mail messages as records, then policy must be developed for what constitutes authentication in an e-mail environment.

The very nature of a signature itself may change when e-signatures must be applied to unusual records created from instant messaging systems, VOIP exchanges, or electronic workflow management processes. Collaboration sites may require signature policy involving authentication by multiple participants in a team process potentially signing at different points in the process of record creation.

The HIM manager must develop e-signature policy to accommodate these technologies that are now novel but will soon be superseded by even faster and more technologically advanced ways of delivering patient care and performing healthcare business.

**Sandra Nunn** (snunn@phs.org) is enterprise records manager at Presbyterian Healthcare Services in Albuquerque, NM.

**Article citation**:
Nunn, Sandra L.. "Enterprise E-Signature: Managing Flourishing E-Signatures at the Organizational Level" *Journal of AHIMA* 80, no.5 (May 2009): 48-49.