Linking Anti-fraud and Legal EHR Functions

Save to myBoK

by Michelle Dougherty, RHIA, CHP

The following statement could easily come from any material written on the legal electronic health record: "EHRs and information available through the NHIN [nationwide health information network] must fully comply with applicable federal and state law and meet the requirements of reliability and admissibility of evidence."[1] However, this is a key recommendation from the "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities." The statement highlights that principles to detect and prevent fraud in EHR systems overlap with those designed to maintain a legally sound electronic record.

In 2005 AHIMA's Foundation of Research and Education, under contract with the Office of the National Coordinator for Health Information Technology, researched and published a report on the use of health IT (HIT) to prevent and detect fraud. Five work groups were formed to focus on key issues, with one group looking specifically at law enforcement and prosecution issues. The law enforcement and prosecution work group came to consensus on two key guiding principles:

- EHRs and information available through the NHIN must fully comply with applicable federal and state law and meet the requirements of reliability and admissibility of evidence.
- A standard minimum definition of the legal health record must be adopted for electronic health records.

This article focuses on the first recommendation and excerpts key principles for electronic systems as outlined in the report. The foundation for the principles is derived from the Government Paperwork Elimination Act (GPEA), which establishes criteria to submit or exchange information electronically when conducting business with the government. Although GPEA is not limited to healthcare, there is a clear overlap with core HIM principles for maintaining a legally sound health record.

The anti-fraud report identifies the following key principles:

- **Completeness**: In developing required, mandatory, or custom data fields of information in EHRs and billing records, the information must include complete information and be sufficient to fully satisfy, support, and communicate decisions made about services rendered and facilitate automated coding and billing purposes.
- **Accountability**: Users of the EHR (in moving from a paper or hybrid environment to an interoperable HIT system) agree that the EHR/NHIN system must contain executed "terms and conditions agreements" as necessary among all the parties to the electronic process to ensure that all conditions of submission and receipt of data electronically are mutually known and understood, including potential criminal, civil, and administrative penalties for making fraudulent claims or false statements.
- **Access and availability**: Access must be restricted (closed) to only approved, identifiable users for approved, identifiable purposes. Access to any backup databases must be appropriately maintained and restricted and made available at all times.
- **Traceability**: Access must be restricted (closed) to only approved, identifiable users. The system collects and preserves all transaction (and/or clinical or encounter) information.
- **Auditable (verifiable)**: The system's electronic processes can be shown to gather, retain, and reproduce data that can be audited and verified to be accurate and to do so reliably and without alteration.
- **Identification**: The EHR and/or interoperable HIT system includes processes to identify and verify the identities of authorized users who input, alter, and/or transmit information as well as the identity of each individual who is a party to an EHR entry or transaction.
- **Authentication**: The system must authenticate the parties and the specific individuals involved in creating, modifying, or transmitting an EHR or transaction. Authentication is defined as a system that enables a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.

- **Biometric authentication**: Authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable. This includes authorization of electronic signatures. Furthermore, this applies to records stored off-shore in addition to those maintained electronically in the United States.
- **Nonrepudiation**: The EHR and/or interoperable HIT system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.
- **Integrity**: The EHR and/or interoperable HIT system must ensure that the recipient, or a third party, can determine whether the contents of the document (EHR and/or electronic transmission) have been altered during its transmission or altered or amended or sought to be amended by any party.
- **Storage and security**: EHRs and/or data transmitted and retained in an interoperable HIT system must be stored and be secure from access by unauthorized and unidentified persons or users. This applies to data stored in the United States and offshore. Records must be retained-unaltered, readable, and retrievable-and record retention must comply with all applicable laws and regulations. Records are to be readily available and in a readable format in the English language. Regardless of the physical location where the EHR is stored, the EHR must at all times be actually available, by legal process or as otherwise authorized by law, to patients, governmental and private payers, and law enforcement.
- **Record retention**: Record retention requirements must be a minimum of 10 years. Presumably, patients would want their EHRs to be preserved forever since they represent patient medical history, but this would not be true for transactional/billing records. Law enforcement would need, at a minimum, to replicate current retention requirements for transactional records (i.e., 10 years for civil enforcement purposes).
- **Reliability**: Unique EHRs and the interoperable HIT system must reliably and consistently do what they are supposed to do, perform as they are supposed to, use redundant or backup (of all transactions and changes) systems as necessary, and therefore be reliable. If the IT system fails, there is a goal of always having access for law enforcement and all other purposes. Either redundant or backup information must be available if the system fails.
- **Digital certificate**: A digital certificate is a data record that, at a minimum: (1) identifies the certification authority issuing it; (2) names or otherwise identifies the certificate holder; (3) contains a public key that corresponds to a private key under the sole control of the certificate holder; (4) identifies the operational period; and (5) contains a serial number and is digitally signed by the certification authority issuing it.
- **Digital signature**: An EHR or transaction record in an interoperable HIT system must include a digital signature record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using a private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensures that the signer's identity and the integrity of the file can be confirmed. This relates to the transmittal, which creates a record and authenticates that it was an unaltered transaction.
- **Electronic signature**: A method of signing an electronic message that identifies a particular person as the source of the message (or record) and identifies the person's approval of the information contained in the message. Electronic signatures are key to traceability of an individual or organization.
- **Public key infrastructure (PKI)**: A structure under which a certification authority verifies the identity of applicants; issues, renews, and revokes digital certificates; maintains a registry of public keys; and maintains an up-to-date certification revocation list.
- **Private key**: The key of a key pair that is used to create a digital signature.
- **Public key**: The key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed records or transactions from the holder of the key pair.

Follow-up work is currently being conducted that uses these principles to further work supporting the legal EHR. The Office of the National Coordinator has issued a second contract to develop model anti-fraud requirements for EHRs. This contract was awarded to Research Triangle Institute with a subcontract to the Foundation of Research and Education. A report will be delivered by March 31.

Work is also under way to develop functionality standards for a legal profile in conjunction with the Health Level Seven EHR system functional model standard (watch the Journal for more information on this project). Although both efforts seem different in nature, they share aspects rooted in the core principles for the security and reliability of electronic systems.

The principles overlap in three key areas: security and reliability, the legal EHR, and anti-fraud. They also support data quality and integrity-providing a compelling reason for inclusion in EHR systems. HIM professionals can use these principles to evaluate current and future systems. Where a principle is lacking, organizations can work with their vendor to improve functionality and develop a mitigation strategy. The bottom line-organizations shouldn't settle for a system that inadequately protects their critical health information resources into the future.

Note

1. Foundation of Research and Education. "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities." September 30, 2005. Available online at www.hhs.gov/healthit/documents/ReportOnTheUse.pdf.

Reference

Government Paperwork Elimination Act. Pub. L. No. 105-277, §§1701-1710 (1998) (codified as 44 U.S.C.A. § 3504 n. (West Supp. 1999)). Available online at www.whitehouse.gov/omb/fedreg/gpea2.html.

Michelle Dougherty (michelle.dougherty@ahima.org) is a practice manager at AHIMA.

Article citation:
Dougherty, Michelle. "Linking Anti-fraud and Legal EHR Functions" *Journal of AHIMA* 78, no.3 (March 2007): 60-61.