Metadata You Need: Determining What Must Be Collected and Retained

Save to myBoK

by Patricia Trites, MPA, CPC, CHP, CHCC, CHCO

Metadata are not inherently good or bad, they just are. Metadata have been defined as "data about data."[1] They can be further described as the "who, what, where, and when" of electronic documents.[2] Their importance depends on who is viewing the information—prominent among their users are regulators, defendents, and prosecutors.

The metadata underlying an electronic record can serve as proof that an individual or organization has complied with the law, participation agreements, accreditation standards, or contracts. They can also prove the opposite. For this reason, the courts have put an increased focus on metadata within electronic records.

For HIM professionals, the challenge is understanding the types of metadata generated within their organizations and when they must be collected and retained as part of document retention policy.

Retention Requirements for Metadata

A simple example of metadata can be found in a Microsoft Word document. Selecting the "Properties" feature displays metadata elements such as author, creation date, accessed date, and modified date. Functions such as "Track Changes" reveal what information has been altered, who made the alteration, and when.

Most departments use some type of word-processing, spreadsheet, and e-mail software. Documents relating to human resources, accounting, finance, contracting, and clinical data are all subject to some form of retention requirements. Metadata are included in these requirements.

The impact can be significant. Envision how the metadata in the situations below might help or hurt an organization:

- A clinical document is provided as evidence. The accompanying metadata indicate that the author of the chart note was actually another physician. The metadata indicate that the data were created a year before the date of service and then modified on the date of service. They also indicate that the "author" was in the record a total of three minutes.
- E-mail sent and received between human resources employees and department supervisors about a misclassification of exempt employees shows received and read receipts for all recipients.
- Spreadsheets used in contracting contain data accessible through the "Track Changes" function that indicate a higher payment amount to another competitor contractor.
- Comments in a document that may or may not be flattering are discovered through the track changes function.
- A disgruntled employee alleges that nonphysician providers are providing patient services and that the documentation indicates the physicians are rendering the care. However, the metadata tell a different story. They show that those who have signed into the computer system are nonphysician practitioners and physicians. The metadata show each type of provider performed different parts of the documentation, and the time stamps indicate the electronic documents were created at the beginning of the patient's appointment and not at the end.

The above information could lead to an organization's downfall or defense, depending on its metadata retention requirements and maintenance.

Why retain this type of possibly incriminating information? Why not delete the files or scrub the metadata so it cannot be a liability? That is possible, unless the organization has a regulatory or legal mandate to retain the electronic documents.

Legal Requirements for Metadata

Electronic document retention is not new by any means. It is law in some cases. However, the inclusion of hidden information does make things more complicated.

The courts have not determined the specific metadata required in all instances, but case law has established that metadata are necessary for outputs to be admitted into legal proceedings; the federal e-discovery rules outline procedures for identifying and submitting electronic data and its supporting metadata.[3]

The federal Civil False Claims Act, which can be applied to any and all claims for services provided to federal health plan beneficiaries, states:

> The term "documentary material" includes the original or any copy of any book, record, report, memorandum, paper, communication, tabulation, chart, or other document, or data compilations stored in or accessible through computer or other information retrieval systems, together with instructions and all other materials necessary to use or interpret such data compilations, and any product of discovery.[4]

Healthcare organizations that must adhere to FDA regulations have the responsibility to maintain their electronic documentation in accordance with Title 21 Code of Federal Regulations (21 CFR part 11). These FDA regulations establish criteria under which electronic records and signatures can be considered equivalent to paper-based records and handwritten signatures and include:

- Security controls to prevent unauthorized access to documents (to protect from unauthorized disclosure, alteration, or deletion)
- Time- and date-stamped audit trails recording changes to records
- Electronic signatures on documents with name, date, and purpose of signature
- Policies that hold users accountable for documents
- Audit trail documentation that must be retained for a period at least as long as required for the subject electronic documents[5]

These requirements may seem familiar, as they are quite similar to the HIPAA security rule. All covered entities have a legal obligation to maintain the confidentiality, integrity, and availability of electronic protected health information.[6] This encompasses requirements such as:

- Implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- Implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident-tracking reports
- Implementing hardware, software, or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information
- Maintaining this documentation for at least six years from the date of its creation or the date when it was last in effect, whichever is later

Depending on the legal structure of the organization, other laws may affect the capture and storage of metadata. For entities that are publicly traded, the Sarbanes-Oxley Act applies.

Section 404 of Sarbanes-Oxley mandates that all publicly traded organizations demonstrate due diligence in the disclosure of financial information. They must implement internal controls and procedures to communicate, store, and protect that data.[1] Many organizations are using the ISO security standard ISO-17799 as a framework for implementing their information security program.[8]

There are certain legal requirements regarding information technology security to which federal agencies must adhere and that are recommended for the private sector. Many come from legislation, while others come from presidential directives or the Office of Budget and Management circulars.[9]

For example, the Minimum Security Requirements for Federal Information and Information Systems, similar to the HIPAA security rule, cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.[10]

The Payment Card Industry Data Security Standard requires all entities that accept credit cards to comply with 12 security-related requirements. These call for, among other things, encrypted transmission of cardholder data, periodic network scans, logical and physical access controls, and activity monitoring and logging.[11]

The list of standards, both recommended and legislated, continues, but those that appear here are applicable to many healthcare organizations, from solo practitioners to hospitals and pharmaceutical companies.

The audit requirement and the retention of the audit data are where the metadata come back into focus. The audit information, specifically the metadata—the who, what, where, and when of an electronic action—is the information that will be reviewed for compliant behavior.

Ensuring Proper Retention

Unfortunately not all software and information systems have the ability to capture and retain metadata as required. Many EHR systems do not have this capability, or they may enable audit features to be turned off. Product certification does not ensure system compliance at this time. Current CCHIT certification requirements do not capture all of the legal requirements of the HIPAA security rule.

It is up to each provider and organization to perform as part of its risk analysis an assessment of what information is captured and retained. Once identified, this information should be made part of the entity's document retention and destruction policies.

Additional analysis of other organizational electronic documentation (e.g., financial, personnel, e-mail, and instant messaging systems) creation, maintenance, and retention should also be undertaken to ensure compliance with applicable regulatory standards.

Notes

1. The Linux Information Project. "Metadata Definition." March 21, 2006. Available online at www.linfo.org/metadata.html.
2. Davey, Carrie. "Find It Fast: Leveraging Meta Data." *The Applied Discovery Orange Pages Electronic Discovery Newsletter.* August 2003. Available online at www.applieddiscovery.com/lawLibrary/newsletter/TheOrangePages_Aug03.pdf.
3. Gelzer, Reed D. "Metadata, Law, and the Real World: Slowly, the Three Are Merging." *Journal of AHIMA* 79, no. 2 (Feb. 2008): 56–57, 64.
4. False Claims Act § 3733. Civil investigative demands; (l) Definitions subsection (5).
5. Food and Drug Administration. "Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures." March 20, 1997. Available online at www.fda.gov/ora/compliance_ref/part11.
6. HIPAA. Public Law 104-191, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards. February 20, 2003. Available online at www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf.
7. SOX-online: The Vendor-Neutral Sarbanes-Oxley Site. "The Connection between SOX and Security." Available online at www.sox-online.com/security.html.
8. Ibid.
9. National Institute of Standards and Technology, Computer Security Division; Computer Security Resource Center. "By Legal Requirement. Publications." Available online at http://csrc.nist.gov/publications/PubsByLR.html.
10. National Institute of Standards and Technology, Computer Security Division. "Federal Information Processing Standards Publication: Minimum Security Requirements for Federal Information and Information Systems." FIPS PUB 200. March 9, 2006. Available online at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.
11. Jaikumar Vijayan. "Credit Card Data Security Standard Goes into Effect." *Computerworld Security*. June 30, 2005. Available online at www.computerworld.com/securitytopics/security/story/0,10801,102913,00.html.

Acknowledgment

The author thanks Reed D. Gelzer, MD, MPH, CHCC, for his continued assistance and support.

Patricia Trites (patrites@docintegrity.com; pati@complianceresources.com) is president of Advocates for Documentation Integrity and Compliance, LLC, and CEO of Healthcare Compliance Resources, LLC, in Augusta, MI.

Article citation:
Trites, Patricia. "Metadata You Need: Determining What Must Be Collected and Retained" *Journal of AHIMA* 79, no.7 (July 2008): 52-53;60.