Beyond HIPAA: the Complexities of Electronic Records Management

by Randolph A. Kahn, Esq.

After all the planning and implementation, how can you ensure your electronic records hold up in court? Here's an overview of the many ramifications of electronic records. Learn how to protect your facility while preserving record integrity.

"Doctors Advised on E-Mail Visits" (*Wall Street Journal*, December 4, 2002)
"Computers Could Help Health Officials Detect Bioterrorist Attacks" (*Wall Street Journal*, November 26, 2001)
"Web Mishap: Kids' Psychological Files Posted" (*Los Angeles Times*, November 7, 2001)

The headlines above illustrate both the benefits and drawbacks of using computers for all facets of healthcare business. While computers can make the industry much more efficient, the application of digital information technology is not without risk, potential liability, and a variety of other business and legal consequences.

Recent laws such as the Electronic Signatures in Global and National Commerce Act (E-Sign) and Uniform Electronic Transactions Act (UETA) put electronic records and electronic signatures generally on par with their paper counterparts. Legal acceptance has provided the impetus for many organizations to move forward with e-initiatives such that many healthcare organizations rely solely on electronic records to document their activities. Indeed, for many organizations, the preponderance of data stored on their computers may never make it into paper form.

The information management challenges facing the HIM community go well beyond HIPAA and include topics such as legal admissibility, security, privacy, and a number of other issues. There are many legal and risk management issues that most institutions need to address regarding electronic records. The only way to fully appreciate the various and perhaps daunting legal issues facing the healthcare community is to consider the issues that have not gotten the attention of HIPAA, but nonetheless may affect you and your organization.

In this article, we'll explore how to ensure the viability and integrity of electronic records.

What to Manage?

Virtually every activity within your institution involves the use of computers that create electronic records that may need to be managed as business records. Every day, servers log thousands of network interactions, databases record gigabytes worth of transactions, and employees create millions of e-mail messages. Identifying the sources of electronic record creation, much less managing that information, is a complex task that increasingly requires our attention.

Today, the decentralized computing environment embodied by the Internet and the increased horsepower in conjunction with decreased cost of technology have spread information technology throughout our organizations. Such trends make it more difficult to manage sources of electronic record creation. Further, decentralization of creation and record retention into the hands of the drafter create evidentiary issues that likely did not exist in the same way in the paper world. If someone can alter an electronic record without obvious detection at any time and because the creator, who retains control of the record over its life, is most likely to have an interest in the content, there may need to be controls in place to ensure its trustworthiness.

How to protect your organization:

- Manage records according to their content

- Manage records centrally and electronically to the extent possible for efficiency and evidentiary benefits

Retaining "Conversations"

Organizations are increasingly adopting technologies that preserve communications that originally were meant to be transient. Businesses use technologies like voice mail, instant messaging, and especially e-mail for "conversations" that likely were not preserved in the past. And technology creates evidence of these business activities for every employee throughout an organization. E-mail use now is no longer confined to a temporal messaging role; rather, it has become the medium through which much business is conducted. As such, companies must institute policies to manage e-mail-based records like all other company records.

Don't overlook the danger of unchecked growth of certain forms of electronic records such as e-mail messages. Failure to cull them according to company policy or a retention schedule makes finding and producing them exceedingly difficult. Further, the sheer volume of electronically stored data is growing. For example, in 2001, approximately six billion e-mail messages were generated a day. In 2000, one source estimated that by 2005, that number would grow to about 18 billion e-mail messages a day.[1] After the September 11, 2001, terrorist attacks and the anthrax scare, growth of e-mail use will likely increase.

How to protect your organization:

- Records can be found on e-mail and other communications technologies, so manage records wherever they are located and managed by content
- Destroying all stored e-mail without regard to content does not promote real business interests
- Take on one challenge at a time: develop policies and retention guidelines for the technologies that are most heavily used for business purposes first

Growing Complexity

Technological complexity can make identifying and managing sources of e-record creation difficult. The knowledge required to create electronic information differs drastically from the knowledge required to understand how that information is created, what it means in its raw form, and how to interpret it. As computing systems grow in complexity, this knowledge becomes increasingly centralized and isolated from other parts of the organization. In other words, anyone can understand the technology behind the creation of a paper record, but relatively few understand the technology behind the creation of a digitally signed electronic form.

There is no magic in understanding a paper record. Understanding an electronic record, however, is no simple task. A typical electronic record may consist of several packets of data existing in various computers. Additionally, there may be various types of metadata (the data that describes the data) and audit records that provide important information about the record, its date of creation, its creator, and any changes made during its life cycle.

How to protect your organization:

- Technology professionals need to guide the organization about what can be retained as proof of business events
- Lawyers need to guide technology professionals about what will make good electronic evidence and what should be retained to protect the organization's legal interests

Records in All Forms

In addition to the complexity of the record itself, the process of electronic records management adds another layer of difficulty. Businesses routinely purge voice mail systems, in part because there is no simple way to manage the contents of the system. Perhaps no one has invented management solutions for communications technologies like voice mail because its original creators only intended it as a convenient communication tool, not a forum for conducting business.

Business evolution has changed the use of these technologies. Today, businesses use voice mail and other messaging technologies to respond to proposals, communicate with regulators, and enter contracts. In any event, a voice mail message may be needed as evidence. Healthcare organizations need to draft rules or procedures instructing employees on handling such

situations. For now, voice mail messages are normally forever lost when their contents are purged to make space for new messages. Obviously, organizations need not retain all voice mail messages; rather, they need rules so employees know what to keep and what to purge as well as how to retain a message.

How to protect your organization:

- For each new technology, provide simple rules to employees so that they know what to retain and what to purge
- Develop policy first and then, if necessary, build or buy technology to help manage new forms of information

Legal but Not Equal

In the days when there were only paper agreements, the non-testimonial evidence of the business transaction either existed or not. With today's reliance on electronic records for business there is a need to ensure that the electronic storage is evidentially sufficient given the value and importance of the transaction. That seems to presuppose that, while electronic records may be on par legally with paper records, there are different types of electronic records. In other words, some electronic records are more equal than others.2

Federal and state law has evolved over the years to accommodate the widespread use of and reliance on electronic records, whether they are "born digital" or created by scanning or imaging original paper records. Consequently, electronic records can be offered as evidence in most legal jurisdictions, for most purposes, without fear that they will be rejected merely because they are not in paper form or do not meet requirements for an original.

In fact, current evidence laws generally do not require records to be in any particular form and increasingly recognize that a requirement to provide a record can be met by a variety of electronic formats, such as a digital image of an original paper record that was converted to electronic form. Additionally, electronic records can be used to satisfy the record-keeping requirements of an increasing number of federal and state regulators.

Organizations should be aware that these laws do not reduce any requirement that electronic records be created and managed in a manner that promotes their authenticity, completeness, trustworthiness, and integrity. Just like paper records, electronic records can be attacked on these fronts and subsequently rejected by courts and regulators. In other words, a record of any form can still be excluded because it does not have integrity. Given the inherent complexity of managing electronic records and the many possible avenues of attack on their credibility, organizations need to ensure that records are properly managed from creation to disposition to ensure that they will satisfy their legal, regulatory, and operational needs.

How to protect your organization:

- Because not all electronic records are the same, for each new business use, employees should determine if the record retained will be sufficient
- Legal counsel should guide the organization on the type of evidence it is relying on as evidence of its e-business activities

Transmission Made Easy

Unlike paper-based information, electronic information can move around the world at the touch of a button. While ease of transmission has undoubtedly made business communications more efficient, it has also contributed to the unmanaged proliferation of electronic information and miscommunication of information, which has had serious ramifications. Additionally, the transmission component of the information life cycle encompasses two other areas of concern for those charged with managing electronic information: authenticity and confidentiality.

Confidentiality is a well-understood and managed quality in the paper world, with worldwide delivery systems in place that protect unauthorized parties from receiving and viewing confidential information (for example, couriers, registered mail, and even the envelope). However, there is no such widely available methodology in the digital world, though technology solutions exist and are getting better all the time.

By the same token, methods for protecting the authenticity of a paper-based transmission are well established and are based primarily on the known delivery mechanisms and the physical qualities inherent to paper that make alteration relatively easy to

detect. However, electronic communications have neither standardized methodology nor inherent qualities that protect their authenticity.

An unprotected e-mail message is like a postcard written in pencil—anyone who receives or intercepts the message can easily compromise both its confidentiality and its authenticity. While most organizations address these facts by creating policies that dictate the types of content that are appropriate for e-mail, policies alone may not be enough for protection.

How to protect your organization:

- Develop classification rules that help employees properly protect confidential company information
- Use technological solutions to secure transmission over the Internet, but only after policy is developed

When Integrity Is Challenged

Management of electronic information to ensure integrity, completeness, and trustworthiness requires a great deal more effort than what the paper world required. Paper records were rarely attacked because there were few avenues through which an attacker could advance. Either a signature was authentic or forged. Electronic records are substantially easier to attack because there are so many ways to do it. Consider the following ambiguities:

- How can an organization prove the date of creation when paper printouts of all electronic records look like originals?
- How can an organization recreate the original records when software changes or the hardware used to create them is no longer available? Of course, changes in software can change presentation or access altogether. Mere changes in presentation may create questions about what the original looked like.
- What procedure limits access to the system or record that provides confirmation that the record was not altered or could not have been altered after creation?
- What evidence will be needed to overcome the argument that the record remained in the control of the creator who could have changed it at will? System access control becomes integral to record trustworthiness. Metadata and audit information become central to proof on integrity. But what is being retained?

In many cases, paper records are centrally managed by a records management department that controls the records after creation. Central to records management is the application of retention schedules. At the end of a retention period, the department may destroy the records, absent any reason otherwise to continue to retain them, such as an imminent or pending audit, investigation, or lawsuit.

How to protect your organization:

- Develop electronic record policies that address integrity, retention, and ownership issues
- Manage software and hardware with the records to ensure that retained records will be accessible and reproducible over time

Can’t Keep Everything

Electronic records present unique challenges that make central management and application of retention rules difficult at best. Today, businesses rely on a variety of computer systems, networks, legacy systems, mainframes, servers, backup computers, personal computers, laptops, and hand-held computers. Each computer system generates vast quantities of data. For example, there are roughly 25 million tape drives in use today. The tape drives store approximately 2.5 exabytes of electronic data (one exabyte is the equivalent of about 600 trillion 500-page books). Imagine trying to find a needed patient’s medical record among this growing volume of information. It’s alarming to consider that tape drives represent only one type of data storage and retrieval mechanism.

Businesses rarely regard this growing mass of information as they did paper records. Not surprisingly, the retention schedules authorizing destruction of paper records do not routinely get applied to electronic records. The electronic information continues to grow unobstructed.

How to protect your organization:

- Develop and apply retention rules to e-records now—this task won't get any easier as more electronic content is created and retained
- Don't destroy records without an established retention policy in place. Without a retention policy, this practice could be attacked as improper destruction of evidence, for which there can be personal and corporate liability, even criminal sanctions

Explore Central Management

In the paper world, central control is the lynchpin of records management. Records are physically moved to a centralized storage facility and perhaps off site when they become inactive. In the electronic world, businesses typically have no centralized management of data (though that will change as more companies implement electronic records), but rather a decentralized ownership by default by the manager of the system or technology housing the data. Limitations of electronic record software complicate the problem further. Software currently cannot manage all electronic record formats and all types of data. Simply put, while records management computer program solutions are getting better, they are still far from a panacea.

How to protect your organization:

- Harness technology wisely: companies that need to retain records in electronic form should consider software applications to help in the process

Litigation Is a Good Reason

You can only fully appreciate the complexity and enormity of finding and producing electronic evidence in the context of a request to produce everything potentially relevant to a lawsuit, investigation, or audit. The burden created by requests for the production of electronic records includes a number of both obvious and hidden costs that clearly differentiate the production of electronic records from the process for production of paper records.

In one recent case, the court concluded that it was not "unduly burdensome" for a pharmaceutical company to spend millions to see if any electronic records they retained were responsive to a lawsuit or produce millions of e-mail messages. In that same case, the court imposed sanctions on the drug company for destruction of evidence because the company disposed of back-up tapes kept for disaster recovery purposes, which should have been disposed of long ago, without first checking to see if anything on them was needed in the current lawsuit. Due to the Sarbanes-Oxley Act of 2002, which aims to protect investors by improving the accuracy and reliability of corporate disclosures and came about in part due to numerous record destruction problems, an organization is well served to develop and follow business information management and legal hold policies to protect itself from devastating penalties.

How to protect your organization:

- Prepare for the inevitable: if your organization gets sued, anything electronic that exists may need to be looked through and produced
- Develop policies now so that your organization will be able to respond to requests for information from regulators, courts, and litigants in a timely manner
- Develop a "legal/hold" mechanism to ensure the organization is preserving potentially relevant information for lawsuits, audits, and investigations

Can You Find It?

The content of a paper record is clear and obvious. Electronic records are identifiable only through use of a computer and software. Further, because storage media does not display its contents, there is no simple way to know what is inside a computer, a file, or a magnetic tape without inspecting the storage device with the use of a computer.

In the world of electronic records, locating a needed record first requires finding the storage device on which someone stored the record. Even if someone finds the right unit of media, failure to have an adequate index regime or uniform naming convention may prohibit finding the precise record needed. Some electronic records are searchable only by their file name,

used by the author or creator of the record. Without knowing what the creator called it or how he or she indexed it, finding it among the content itself becomes a challenge.

How to protect your organization:

- Create and implement indexing regimes, classifications coding, labeling, proper storage, and back-up of electronic records: proper management demands it

Start Now to Protect Yourself Later

In this world in which technology seemingly makes everything happen, its output is a variety of electronic records and digital information requiring management from not only technological or operational perspectives, but from a legal perspective as well. Information is neither inherently good nor bad but mismanagement of information can only be bad. The good news is that for every problem there is a solution. The immediate task is to address it now. u

Notes

1. Battey, Jim. "By the Numbers." *InfoWorld* 22, no. 39 (2000): 22.

2. Kahn, Randolph A. and Diane J. Silverberg. "From Mt. Sinai to Cyberspace: Making Good E-Business Records." *The Business Lawyer* 57, no. 1 (2001).

What Are Your Information Issues?

Healthcare organizations need to understand the types of information issues that have legal, compliance, or risk management implications. Use the following questions to generate discussion within your organization:

- What type of information should be transmitted via unsecured e-mail?
- What liability will be attached to an errant message improperly disclosing personally identifiable health information?
- What metadata should the technology department retain to prove authenticity and completeness of electronic records?
- Should adulterated records be acceptable to regulators? What if the veracity of your organization's electronic records can't be proved in court?
- How can an organization reduce the likelihood that a disgruntled employee will make public innocent third parties' health information or even abscond with the facilities' information stored on disks that fit easily into his or her pocket?
- How can an organization demonstrate that an electronic contract has not been altered and that it has remained in its original form from the date of creation?
- How can an organization prove the date of creation and transmission of an important submission to a regulator?
- What electronic records should companies retain? Which ones can they destroy and when?
- How can an organization methodically retain electronic records in accordance with records retention policies?
- How can an organization protect itself from the liability associated with electronic record discovery or a judge's order?
- How can an organization prevent electronic records destruction that is innocent but nonetheless gets the company in trouble?

Randolph A. Kahn *(rkahn@KahnConsultingInc.com) is an attorney and consultant with expertise in the legal, risk, and policy issues of records, digital information, and e-business processes. As a principal of Kahn Consulting Inc., he directs a team of consultants who advise business executives, corporate counsel, information technology*

professionals, and records managers in both government and corporate institutions. Clients include pharmaceutical companies; federal, state, and local agencies; federal and state courts; Fortune 500 corporations; and information technology companies. He teaches "Legal Issues in Records and Information Management" at George Washington University and writes, lectures extensively, and conducts corporate training seminars around the country.

Article citation:
Kahn, Randolph A. "Beyond HIPAA: the Complexities of Electronic Records Management." *Journal of AHIMA* 74, no.4 (April 2003): 31-36.