E-Mail: Treat It as Just Another Record

By Deborah Kohn, RHIA, CHE, CPHIMS

April 2009

In the electronic (i.e., digital) world, everything learned about traditional, paper (i.e., analog) records management has been thrown into disarray. For example, the distinctions between original and duplicate or copy are irrelevant. File folders and labels are as anachronistic as graven stone tablets. But, for health information management (HIM) professionals who currently have to juggle managing digital and analog patient health records, isn't e-mail "just" e-mail?

Absolutely not!

E-mail is no longer "just" a messaging system or the electronic equivalent of the Post-it note. It has become a record-generating, communication system vital to a health care organization's business processes. It has replaced most of the organization's analog processes, and it is being used increasingly for a number of non-traditional e-mail activities: sending secured, digital reference lab results to the unit, attaching secured, digital discharge summaries to the physician's office, etc. Therefore, it is essential to do away immediately with misconceptions about this Internet-derived technology and start to manage it with the same thought and attention that have gone to managing other patient record-generating media.

The fact is e-mail is "just" another record. It is subject to the same course of evidentiary discovery as any other health care organizational business record, such as the patient medical record, patient financial record or employee record. In addition, e-mails have a lifecycle just like any other record. They are created, indexed, searched, retrieved, routed, stored and purged. More importantly, e-mail is now one of the health care organization's largest and most vital information assets. Therefore, like any other business records or documents, e-mail records and the information or data contained in the e-mail records require management.

Already e-mail management is an enormous, complex problem. Unfortunately, the problem is expected to get worse as the number and type of senders and receivers increase exponentially.

The first step in e-mail management should be to retain e-mails within an overall electronic document management strategy. For example, most often, the information contained in e-mails is interconnected (e.g., regarding Mary Smith's diagnosis, the privacy official's recent meeting minutes, etc.). To ensure that all the e-mails relating to Mary Smith or the organization's privacy meetings can be located, it makes sense that the strategy includes identifying those existing, enterprise-wide repositories that securely store (or should store) e-mail records and attachments that merit evidentiary handling.

Next, to reduce the legal risks of e-mail records, it behooves the health care organization to develop or acquire an e-mail management system. This system should include a centralized archive. In addition, the system must be easy to use, providing intuitive methods for identifying e-mail classification (such as patients) and retention rules. Also, the system must provide fast and efficient access to the archive, including tried-and-true search capabilities. Finally, the system must work with the popular e-mail systems, such as Lotus Notes and Microsoft Exchange.

For example, the system should enforce e-mail archiving policies. When an individual closes an e-mail and is ready to discard or save it, a prompt should appear with a YES

or NO choice asking if the user would like to make this a part of any of the health care organization's "business" records. If the health care organization declares ahead of time that the e-mail must always be retained to comply with a regulatory, legal or business need, then this "opt in/out" e-mail capture function can be eliminated. In addition, this function can be managed in the background using Web technology so that, for example, each new patient added to the master patient index triggers a domain name with all inbound and outbound mail captured for patientname.com.

Also, retention rules should be triggered automatically by actions. This includes automatically deleting or encrypting a "patient class" of e-mail after X number of days/months/years so it cannot be accessed. (NOTE: Never archive encrypted e-mail records for fear of losing the algorithms or keys!) This can include issuing an e-mail notification to all authorized users when e-mail records one through 100 for patientname.com are approaching the seven year retention mark or just issuing an e-mail notification when user mailboxes contain more than, for example, 100MB of messages.

There is little doubt that e-mail management is a vital HIM issue. Just like other records, e-mail presents a huge opportunity to reduce the risks of enormous legal costs in evidentiary proceedings. On the other hand, its anticipated, explosive growth and its growing significance in the legal process present formidable challenges. The opportunities for HIM professionals to manage the organization's patient e-mail records just like other records will allow HIM professionals to oversee the aspects of many enterprise-wide information repositories and focus on both the digital and analog patient record repositories inside and outside their existing domains.

Response to the article above from “Peter”

Some interesting information, but email should be retained based upon its content. What was not mentioned was the issue of holds whether for litigation, audits or investigations. Finally the term "archiving" is a misnomer. In the IT world 'archiving' means storage and not something of historical or permanent value to the organization.

I suggest that anyone interested in managing emails or any other type of electronic message should obtain a copy of the ANSI/ARMA standard "Managing Electronic Messages as Records" which can be obtained from the ARMA Internation bookstore www.arma.org