Off-site Storage: No More "Out of Sight, Out of Mind"

April D. Robertson, MPA, RHIA, CHPS, FAHIMA, is vice president of customer advocacy at HealthPort. *Here she offers a look at the need to index inventory down to the individual record and suggests that the newly shared accountability conveyed by ARRA calls for a partnership between providers and vendors in getting this done.*

ARRA's modifications of HIPAA have shaken up many areas of HIM practice, including off-site records storage, where facilities often have indexed their inventory no further than by box.

Today's HIM departments face a montage of mediums: electronic health records, paper health records, and varying hybrids of the two. All require special handling and oversight to protect the confidential information contained within them. This we know.

What has changed is the extent of the responsibility. The HITECH Act within ARRA modified HIPAA, expanding the regulations to increase penalties, expand liability, and add responsibilities for protecting patient information and alerting patients if a breach occurs.

With the changes, all businesses covered by the regulations should take a thorough inventory of the records they store off-site. This is a level of detail they likely do not have, and providers and their vendors must work together to index each stored record and achieve a clear accounting of who is in possession of which records.

ARRA Ups Penalties, Extends Liability

Section 13400 *et. seq.* of ARRA provides for stricter enforcement and institutes increased tiered civil monetary penalties for violation of privacy and security measures, including a standard on safeguards (§164.530[c]).[1] Appropriate administrative, technical, and physical safeguards must be in place to protect the privacy of protected health information (PHI) for all forms of patient health information, not just in electronic forms.[2]

This standard thus protects PHI that is verbally expressed, written solely on paper, copied via a standard copy machine, sent through a paper-to-paper fax, discussed in a person-to-person telephone call or video conference, or left as a message on a voicemail system.[3] PHI, in any form or media, is covered by provisions of the HIPAA privacy rule.[4]

In addition, ARRA added breach notification provisions to HIPAA, making both covered entities (CEs) and their business associates (BAs) accountable for alerting patients whose PHI has been subject to a breach. Extending HIPAA to cover BAs addresses a significant security liability, because 44 percent of all breaches are due to third-party handling of data.[5] (In contrast, just 5 percent of incidents are the result of malicious cyber attacks.)

Thus off-site storage companies, along with the technology and service vendors that HIM departments employ, are now legally bound to the same extent as CEs. As such, they must be able to protect and account for every record in their possession at all times, regardless of medium.

Off-site Must Not Be Out-of-Mind

Six out of ten respondents to a PriceWaterhouseCoopers survey report that their organization still does not have an accurate inventory of locations or jurisdictions where personal data for employees and customers is collected, transmitted, and stored.[6]

Information stored off-site, in particular, can be easy to forget. However, it is almost impossible for an organization to effectively secure sensitive information when it cannot accurately locate it or identify the risks associated with it.

In order to prevent data breaches and effectively manage the associated risks and business impact, the CE must know all the personally identifiable data the organization holds and have a clear understanding of its lifecycle throughout the business

process. Failure to protect this information on the part of the CE or BA can have a wide variety of consequences, from legal liability to loss of trust, both of which can severely damage an organization's reputation and revenues.

Iron Mountain, a leader in records storage, suggests that organizations inventory each type of record and record-keeping system. A records inventory is a complete and accurate listing of the locations and contents of the organization's records—whether paper or electronic. Until a facility knows what it has, Iron Mountain notes, it is impossible to establish any type of records programs.[7]

Inventory beyond the Box

As originators of the PHI, it is imperative that CEs address their processes, policies, and education programs to curb data breaches, particularly with respect to third-party handling of data. To ensure they can comply with notification requirements should a breach occur, there must be an accounting of all records in storage, electronically indexed to the individual level, and both the BA and the CE must possess the inventory.

At Dallas Regional Medical Center in Mesquite, TX, old records stored off-site are only inventoried to the box, says Vickie Boyd, CCS, the facility's HIM director. The content is unknown other than a range of patient record numbers. Boyd has already negotiated with her off-site storage company the cost of having all individual records inventoried.

It is unlikely that a CE who is unwilling to pay to inventory its records will find a truckload of un-indexed records on its doorstep. However, it is in the CE's best interest to partner with the BA, because the off-site storage company is an extension of the hospital's own records library.

Shifting Risk Is Risky Business

The storage relationship is a collaborative one. There are benefits to partnership and dangers in failing to work together. Just as a CE would not undermine its on-site records library, it should not do so to its off-site library by attempting to unnecessarily shift risk to the BA.

According to Jim Booth, executive director of PRISM International, a nonprofit professional trade association for the commercial information management industry, for a vendor to accept more risk at the same negotiated price denies the economic reality of the free market system. In addition, Booth notes, attempting to establish a liability for missing information that was not initially verified as being present violates the most fundamental tenets of inventory management.

Shifting the risk unnecessarily from the CE to the BA is dangerous business. It does not foster high levels of patient service, security, and privacy. The CE will not benefit by undermining the records storage contract. Attempting to shift risk is even less justifiable now that ARRA has made the BA independently liable for its own regulatory compliance.

Finally, shifting liability from the CE to the BA could even be viewed as against public policy in a court of law, as is sometimes found in the construction industry in cases where general contractors require subcontractors to indemnify them without regard to fault. The BA may be willing to indemnify the CE against liability, but only for "known" records and only for its proportional share of negligence; all the more reason for both the CE and BA to work together to ensure all records are inventoried both on-site and off.

Smart for Retrieval and Retention

CEs and BAs also require inventories for effective record retention and retrieval.

An example comes from a recently retired HIM director for a large, multi-location healthcare facility who recounts an incident when the facility's tracking system crashed. With the system down, the facility did not know what was in storage, and the off-site storage vendor did not have a computerized list of all the charts. Shortly thereafter, a request was made for a chart and the facility was unable to find it. This led to a lawsuit resulting in significant monetary damage to the facility.

Not least in importance is the implication for litigation. The Federal Rules of Evidence and Federal Rules of Civil Procedure require potential litigants to produce documents relative to a lawsuit in a specified amount of time. Clearly, the CE must know who is in possession of the record in order to produce it in a timely manner. Ultimately, failure to produce a requested record could be held against the facility.

Detailed inventories also help manage complex retention requirements. A record may be subject to many different laws, with each law mandating a different length of storage. In California, for example, the MediCal Act and the Emergency Medical Services Fund require records be kept for a minimum of three years, whereas OSHA requires employee health records to be kept for the duration of an employees' employment plus 30 years if an employee could potentially have been exposed to dangerous substances.[8]

If the BA houses patient data that are to be destroyed in accordance with the CE's record lifecycle procedures, clearly the BA and CE must know who is in possession of the records.

Going Forward

With the CE and BA equally responsible for the protection of PHI, it is incumbent upon both to establish the location of each unique record.

Doing so will require that record storage companies spend the time to index the records and that the CE pay for the additional work that they likely waived during the initial transfer of records. The process will not be without cost, but legally they are accountable.

Furthermore, the regulatory climate will not become more lax as legislators and regulators attempt to protect privacy in light of advances in technology, and the need to store and manage physical records will continue for decades even with the implementation of electronic health records.

Without a mutual effort to inventory records, there will be much finger pointing in court and elsewhere for many years to come. Working together to fix the problem is the road providers and their vendors must travel.

Notes

[1] Dorfschmid, Cornelia M., and Michael Maffeo. "Managing Risks When Implementing the New EHR Disclosure Accounting Requirements of ARRA." *Compliance Today*, November 2009.

[2] *HIPAA Privacy and Security Rules Guide*. California Health Information Association, 2008.

[3] Amatayakul, Margret, et al. *Handbook for HIPAA Security Implementation*. AMA Press, 2004.

[4] HIPAA, Public Law 104-191. 45 CFR §164.500.

[5] Kam, Rich. "Five Steps to HITECH Preparedness." ID Experts. June 18, 2009.

[6] PriceWaterhousecoopers. "Trial by Fire." 2010 Global State of Information Security Survey.

[7] Iron Mountain. "Compliant Records Management: The New Corporate Imperative." White paper, 2005.

[8] California Medical Association. "Retention of Medical Records." January 2004.

April D. Robertson is vice president, customer advocacy, at HealthPort.

Original source:
Robertson, April D.. "Off-site Storage: No More "Out of Sight, Out of Mind"" (Journal of AHIMA website), May 25, 2010.