Digging Out from Data Hoarding: Using Governance to Manage Information Assets and Prevent Digital Data Avalanches

By Mary Butler

If a brazen television show producer were looking to cash in on the popularity of shows about hoarders, observing a health information management (HIM) department could be a good place to start.

Stories about hoarding records abound. Some hospitals have reinforced their floors to accommodate the weight of new boxes of records, while others have constructed whole new buildings to help contain records overflow.

As with the hoarders who pop up regularly on "Dr. Phil," records managers live with the constant fear that the files they've purged will be valuable down the line, whether that's in 10 weeks or 10 years. HIM professionals in these roles have a legitimate point—health records can be subpoenaed, help prevent allergic reactions, and chronicle the progress of chronic and acute disease processes. Conflicting federal, state, and organizational regulations offer little reassurance when purging clutter, particularly if a provider or vendor's service area crosses state lines.

Complicating the issue, the digital era of electronic health record (EHRs) allows mounds and mounds of information to be stored on computer servers—out of sight and hidden from scrutiny. But just because the data hoard is unseen doesn't mean that the issues that come with it—inability to quickly retrieve and reproduce vital information or legal implications of a lack of proper retention/destruction policies, for example—still have detrimental effects for healthcare organizations.

Information governance programs have been developed in healthcare to tackle these concerns and offer HIM professionals a much-needed framework for getting their own IG programs started. A joint study released this summer by AHIMA and Cohasset Associates demonstrated just how necessary a framework is. Only 37 percent of survey respondents said they had a program in place to retain only relevant information in response to a legal hold.

To grasp the challenges of enacting an information governance program, it's important to compare how healthcare measures up against other data-intensive industries. One also must examine how and why organizations amass the volume of data they do, study information governance programs, and fully understand the pitfalls and the benefits of retaining everything. Finally, one must understand just what HIM's role is in information governance.

But I Might Need It Later

An issue that HIM professionals encounter in their efforts to clean up databases is that enterprise-wide, everyone has a stake in retaining information. This is a phenomenon Seth Katz, MPH, RHIA, assistant administrator, information management and program execution, HIM department, at Missouri-based Truman Medical Center, sees a lot. He says that even when creating intake forms, departments such as nursing, finance, revenue cycle, social work, and case management request that their own data be captured up front.

All of these departments come to the table saying "We'd rather capture it than not," Katz says. "From their perspective it's just digital info on a server, 'How hard can it be?' They don't understand the long-term ramifications for storing all of this data."

Brent Bigelow, CISSP, CEH, a member of AHIMA's Information Governance Task Force and senior vice president of security architecture for Cardinal Health, has witnessed this play out in his professional and personal experience.

Working in a healthcare environment, he knows that organizations try to collect as much information about a patient as they can to properly diagnose them and justify a treatment plan for reimbursement. Gathering adequate data up front also prevents clinicians from having to call patients back into the office for unnecessary follow-up visits, and eliminates time consuming phone calls. Although healthcare organizations are collecting all this information, it is very rarely actually used. When Bigelow took his own kids to the doctor for school physicals, he was amazed by the number of questions their doctor asked.

"But from the professional perspective I'm thinking 'How are they going to deal with this? Where's all this data going? Where is it going to end up? Will it end up under the desk in a box? Is it on some sort of PC that's got a build up of dust? Or on a hard drive?'" Bigelow says.

Another very common, yet very daunting, governance concern in many organizations is e-mail backlogs. Melissa Martin, RHIA, CCS, CHTS-IM, chief privacy officer and HIM director at West Virginia University Hospitals, says that she and her colleagues struggle with the "I might need this" mentality about e-mail.

"I think the biggest area where we hoard digital information or digital data is actually e-mail. And much of that e-mail has very important information, whether it's patient information or business data, that we, for lack of a better term, hoard," Martin says. "It's not always the most up-to-date information."

Martin added that in legal cases where metadata is subpoenaed, information as presented in e-mails can be very misleading. "People tend to use e-mail more like a chat process and then they keep it. When they keep it and it gets subpoenaed as part of a legal case, it can get extremely detrimental to an organization," Martin says.

EHR Gold Rush Adds to Data Clutter

Because the evolution of EHRs developed so rapidly, with help from the federal government's "meaningful use" EHR Incentive Program, many organizations are scrambling to catch up, and that means they hang on to data in a variety of formats. Information is stored in paper records, electronic records, as images (CT imaging, ultrasound, etc.), audio files, and a myriad of other formats.

Retention laws can be slow to change and adapt, Katz says. For example, providers in Missouri are still required to offer the option of a telegram as a means of notifying a patient's next of kin about the patient's death.

"And there's some concern too that 'I've had this information in my chart for 10 years, am I OK to purge it according to state law? Because it doesn't say that I can't. So there's some uncertainty there," Katz says.

The healthcare industry is far from being an outlier in the realm of data hoarding, says Ed Hallock, director of marketing strategy of RSD Glass, a company that provides information governance platforms and solutions. The problem of hoarding electronic records and data occurs in many fields, including finance, banking, and especially highly regulated industries.

"We have cultivated this culture of 'keep everything' because storage is so cheap," Hallock says. This is because nobody wants to be in the position "where you can't find what you need to find," he says. "This is not unique to healthcare."

Hoarding electronic data is more problematic because any data steward can see the very visible, external cost to storing information on paper, whereas relatively inexpensive storage via cloud computing, external hard drives, thumb drives and products such as Dropbox aren't as tangible.

"I'm not convinced [storing electronic data] is cheap. Someone has to back it up, someone has to archive that data, and so there are a lot of other inherited costs," Hallock says.

He notes that digitized data are even more susceptible to being stored in a format that could potentially become obsolete. For example, health data or imaging tests are often burned onto compact discs, but new laptops or tablets already don't have the ability to read that type of data.

HIM to the Rescue

Every reality or talk show that features an exploited, heart-string-tugging hoarder also casts a professional organizer or psychotherapist (or both) in the role of a rescuer who can intervene and help the hoarder de-clutter. In the healthcare realm, that person, ideally, works in an organization's HIM department.

Whether they realize it or not, HIM professionals already analyze data and incorporate informatics skills and workflow management into their day-to-day activities, Martin says. She says HIM professionals' data stewardship duties should mirror those of a clinical documentation improvement specialist in a coding department. In both roles, HIM can combine their information governance skills with their clinical expertise to tell a patient—or record's—story.

"We need the HIM folks in the middle, whenever data is getting pulled together, whether it's for pro forma for a future business venture, or whether it's data we're gathering to negotiate a contract with an insurance company," Martin explains.

Data stewardship is a competency of any HIM professional's toolbox, Katz says. HIM employees know how data are created, where it lives, and how to find a specific piece of data upon request. Now that healthcare organizations have built giant databases of valuable health information, HIM professionals are well suited to manage data queries.

Katz was instrumental in implementing Truman Medical Center's information governance initiative, which in the last two years has transformed how data queries are handled in his organization. He attributes part of Truman's success to the fact that the information governance committee had three credentialed RHIAs.

"HIM professionals are well suited to be on those teams and lead some of those teams, and to really blaze the path on what information governance will look like in five years when people have built out programs," Katz says. "It's an emerging trend and topic that our skill set really aligns with."

Thanks to Truman's information governance activities, data requestors are seeing turnaround times of four hours instead of one business day or more. Very few data requests now fit the criteria for "complex."

"We've seen some improvement in satisfaction from staff. They can get their data faster, we've seen satisfaction from the analysts that are running that data because they're not getting 20 different tickets," Katz says. "They're getting those prioritized for them… Now people are asking for more detailed data and we're able to provide that much more quickly."

The following are examples of the types of data queries Truman's HIM department may receive:

- A list of all the patients within a certain zip code with a given comorbidity
- The number of patients who visited a primary care clinic during a certain period of time
- How many patients have sought pre-natal care at a clinic, typically if the facility is applying for a grant that requires the organization to quantify this data
- A physician's research project
- The number of babies born during a specific time period

Rooting Dark Data Out of the Shadows

Hiding in the dark recesses of healthcare information systems lurks the problem of dark data. Like data hoarding, dark data isn't unique to healthcare.

In the HIM world, dark data is also known as "shadow data," "shadow charts," or "convenience copies." Like the "dark" matter filling the universe that astronomers can't see or understand, but know exists, so too lurks dark data for HIM professionals.

Dark data is generated when a user accesses, for example, a patient chart to review clinical documentation for billing purposes. They may save that file to their own desktop computer or hard drive, save it to an internal SharePoint site, or e-mail the file to a colleague. Dark data also hides on employees' mobile devices if they bring them to work, and take home information to work on later.

This creates additional, untracked copies of information that may eventually work their way back into official record systems and cause versioning issues—or float out in the world unchecked but used to make business or care decisions. Dark data is also information being created independent from official record keeping processes, and apart from the watchful eye of an HIM professional.

Datskovsky compares dark data to the stuff in the bottom of your closet you don't want to sort through.

"Let's say you have a really, really old patient record system, and it was running on a mainframe, and the mainframe no longer works. But you still have a bunch [of data] to collect from that. However you don't really know anymore what data it is," Datskovsky says. "The problem is, if you dispose of it, you might be getting rid of something that's very important for regulatory reasons. And it's important for patient care, compliance, or for a lawsuit. And you might miss something."

Cardinal's Bigelow agrees that dark data is a problem across industries, including healthcare. In his experience, dark data is usually archived data stored to someone's desktop as a shortcut, or it can be legacy data. And in some cases, dark data can be paper records stored in unofficial areas.

"The data stored on a desktop, there's no clear understanding of what's valuable and what's not. There's no retention flags on said data. There's a lot of areas that have that. Finding it can be a bit tricky," Bigelow says. He adds, however, that his organization has a process in place to scan computers and databases for certain criteria.

"It's sort of like storing my kids' pictures for 15 years. It's there, I know I back it up. I'm not sure where everything's at, three computers later I just keep moving it over. So operationally, we tend to move that data without really interrogating it and looking at it from an analysis standpoint," Bigelow says.

How Data Hoarding Hurts

Healthcare organizations can't afford to waste any time forming and enacting information governance programs and practices. Health data—particularly in the electronic realm—are susceptible to breaches and litigation, and unchecked data hoarding can make these situations worse. Lawsuits, breach notifications, and compliance violations can damage an organization's reputation as well as their finances.

With its framework document, Information Governance Principles for Healthcare, AHIMA provides guidelines for helping organizations develop sound policies around how long certain health data is retained by an organization and how and when it can be purged.

The principles AHIMA has developed follow the association's definition of information governance, which is: "The adoption of an organization-wide framework for managing information throughout its lifecycle and supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements."

Sandra Wolfskill, FHFMA, director of healthcare finance policy at the Healthcare Financial Management Association (HFMA), and member of AHIMA's Information Governance Task Force, says that the task force is working to elevate responsibility for information governance to the executive level and clearly apply IG principles throughout the organization.

"The biggest risk [in having ungoverned data] besides accidental breach is that the data may be used against the provider in a legal action," Wolfskill explains. "Organizations are perfectly within their rights to destroy information that qualifies for destruction based on policy and state or federal law. If qualifying data is destroyed, it cannot be breached or used against the provider or discovered.

"So in that sense, managing retention and destruction is just good business practice."

With regard to data retention, AHIMA's principles recommend that organizations need "an information retention program that defines what information to retain, how long to maintain it, and how to dispose of it when it is no longer required. This is based on the concept that information has a lifecycle, which begins at its creation and ends at its final disposition."

West Virginia does not have any state health data retention regulations, which has its pros and cons, according to Martin, from the University of West Virginia Healthcare.

"The pro for us in West Virginia, with not having one, means WVU Healthcare can establish our own, and as long as we follow that we should be covered from a legal perspective," says Martin, noting that it becomes more complicated when her organization has to coordinate or partner with providers with different policies.

"Now, there's some states worse off than we are. They say you have to keep it forever, or you have to keep it for 40 or 50 years," Martin says. "We established 20 years here at WVU. So I don't know if it's a good thing or a bad thing that we didn't have a state law, because in a university setting you're allowed to set your own retention. But some people might look at that a little bit differently."

For those who do keep records for longer than 50 years, recent changes to HIPAA enacted as part of the HITECH Act have changed the rules on protecting and managing old information. HITECH states that records 50 years old or older are no longer formally protected by HIPAA and open to public viewing. Although HIPAA's regulation may have changed, organizations can still enact their own rules regarding the release of this information. But if no policy is in place, the records must be released, meaning providers should revise their release of information and retention policies if they keep records past 50 years.

As Galina Datskovsky, PhD, CRM, a member of AHIMA's Information Governance Task Force, points out, AHIMA's principles dictate that each healthcare organization should follow state and federal regulations. Organizations should look at each internal system that creates or generates data, figure out which ones are most vulnerable, and then rank the systems based on which of the data need the highest level of protection and management. Using this ranking system will allow organizations to prioritize which ones to improve and strengthen first.

"Then organizations will know what they have and properly decide how to apply principles to each collection in accordance with that information," Datskovsky says.

Consider the following Dr. Phil-like advice: The sooner an HIM department identifies (admits) they have a data hoarding problem, the sooner they can apply information governance initiatives to fix it—and actually start enjoying the benefits of well-maintained information.

Reference

AHIMA. "Information Governance Principles for Healthcare." 2014. http://www.ahima.org/topics/infogovernance.

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA*.

Article citation:
Butler, Mary. "Digging Out from Data Hoarding: Using Governance to Manage Information Assets and Prevent Digital Data Avalanches" *Journal of AHIMA* 85, no.10 (October 2014): 24-28.