

## CONFIDENTIAL IS ESSENTIAL: HOW DO WE MAKE THAT HAPPEN?

*April D. Robertson, MPA, RHIA, CHP, FAHIMA*

How do WE raise awareness of the universal responsibility to safeguard personal health information? Everyone has a role when it comes to focusing on the importance of this awareness amidst changes we are currently experiencing in the healthcare industry transformation. **I encourage anyone employed in or interacting with the healthcare industry to recognize their privacy responsibilities.**

The importance of health information privacy is not a new topic for AHIMA members; we make privacy decisions every day. Neither is it a new topic to us as healthcare consumers, privacy laws have protected our health information for decades.

As the healthcare industry transitions from paper to electronic, it's critical to keep privacy responsibilities in front of us, especially since change can happen quickly...and we must maintain privacy programs that are trustworthy at all times. Confidentiality is possible only when everyone the entire workforce and consumers understand and do their part. Sometimes the right decision is clear; sometimes it's not as clear. What can an individual in the various roles do to help the transformation process which upholds confidentiality of personal health information?

### Where are we now?

- The Healthcare Industry is in the midst of an important healthcare industry transformation. We are taking steps to transition health information from paper to electronic, and are bound for technology-rich operations that enhance the quality of patient care.
- We are also working in collaborative circles to make advances with many industry stakeholders—such as caregivers, payers, vendors, and the government.
- At this time, the confidentiality efforts are largely controlled at the local level by the providers or creators of health information, and the laws governing the organizations that give the consumer the right to approve certain types of release of health information.
- Until the industry has a smoother electronic health information exchange process, we are learning from experience how to optimize technology within our organizations to maintain confidentiality.

### Who are we?

- When we say **“We,” that means “all of us.”** We all have activities and interactions within the healthcare industry that deal with personal health information in some way.
- First, we are all healthcare consumers. We and our families use healthcare services. Our personal health information is critical to the healthcare delivery process. Caregivers must have information to deliver care.

- Many of us who work in the healthcare field handle personal health information as part of our jobs and professional responsibilities. We care for patients, or carry out our responsibilities using health information.
- Some have jobs specifically working to administer privacy and security programs in healthcare. These individuals have responsibility for the program processes, compliance with law, policies and procedures, training delivery, and the communication needed for privacy and security functions.
- Whether we see ourselves in one of these roles or more than one, the message is the same: "Confidential is Essential." Each of us can help encourage the use of personal health information in a manner that keeps it confidential and effective.

As consumers, in order to have confidence or trust in our healthcare systems we expect these things:

- The information is accurate
- The information is available to assist in high quality care delivery
- Our personal health information is kept confidential and is not available to those who don't need to have it

All are critical. Yet, it's something of a challenge to ensure we make the information available each time it's needed and keep it confidential at the same time. For the best healthcare delivery, correct patient information must be available to the caregivers when it's needed. To do that we need to make sure it's quickly retrievable and that we can speed it along to the right place and the right people. Technology gives us speed. For confidentiality, we need to have systems and policies that offer security and caution before information is released. Technology gives us new options to lock down information so it can't leak out to the wrong places and the wrong people. We need to do both... lock it down for confidentiality, and speed it to the points of patient care. The healthcare industry is working to balance these important expectations.

#### What is the challenge?

- **Availability** – technology systems are being built that make efficient movement of health information possible
- **Optimal Care** – The industry is working on a universal language and standards to ensure the information is universally understood.
- **Privacy** – State and Federal laws have been in place for many years. Some are harder to comply with when health information becomes electronic. We don't have it all figured out yet.
- **Technology Safeguards** – Computers give us the ability to set locks where we didn't have or didn't need them before. Now we need to be sure we don't set locks that block information sharing needed for patient care.
- **Updates:** As electronic information gradually makes us paperless, we must continually update our systems any time a law changes, when new standards are introduced, and whenever we change the services we offer. We can have strong privacy and security programs only if we keep pace with industry change.

#### How do we make it happen?

##### Understand our participative roles

We are in the best position to support information privacy when we clearly understand our respective roles and take those roles seriously. Each of the roles looks a little different. We'll look at each of them.

## Stay informed

Change occurs in multiple ways within and outside healthcare organizations. Change creates a moving target. If we stay aware, we'll stay informed of the changes and know how to react.

## Be observant

With every change we are likely to see a ripple effect. A change triggers changes in other places, possibly somewhat distant from the initial change—and unrelated to the initial change purpose. Sometimes the ripple effect is anticipated, sometimes not. We can take note of the way information sharing practices occur, and ask ourselves if it appears appropriate to us.

## Speak up

We can ask questions freely! Don't be hesitant to ask for more information. If there's something you don't understand it may be that others don't understand either.

The high level commitment to privacy and security happens at the Board of Directors level. High level commitment to quality healthcare occurs at the same place – the Board of Directors level. The executive team turns the mission and vision into directives and operations expectations. Privacy and security officials administer the privacy and security programs. The medical staff and clinical staff carry out direct quality of care treatment functions. Everyone in the workforce weaves these commitments into the culture and daily decision-making.

After 5-plus years of working under the federal HIPAA privacy and security rules, we know the application can seem complicated or overwhelming. The amount of detail and degree of change within our policies and procedures may be intimidating, even scary. We ask: "Will we make the right decision?" "Will we do it right?" When we are in doubt about how to find the balance between confidentiality and patient care needs we think, if in doubt, don't give it." Ask instead, "Have I given this enough consideration? Am I interpreting this correctly?"

Questions such as those listed here can help you decide whether the best decision is to enable information sharing or to hold it confidential:

- Am I interpreting the request correctly?
- Will patient care be impeded?
- Does the patient have a voice?
- Is the policy or procedure flexible and clear?
- Is it law or practice?
- Who's my go-to person in this situation?

Privacy and security responsibilities can't be carried out effectively without specially trained staffs who administer the programs. These individuals understand everything from high-level compliance with the law to the detail of daily operations for access and release.

In our respective organizations these positions are held by the privacy officer and security officer. These individuals have responsibility for the program's compliance with the law, policies and procedures, training delivery, and the communication needed for privacy and security functions to be carried out.

It takes many perspectives from key positions within the organization to arrive at the most protective and balanced privacy and security approaches. Key positions include: members who serve on privacy and security policy-making committees such as CIO, HIM director, risk manager, legal counsel, quality improvement manager, and so on.

Historically, healthcare organizations have complied with many different sets of privacy directives when managing patient health information. Some common US laws and directives are listed here. Not all organizations are governed by the same directives. The laws and standards are written for different purposes. This calls for balance too as they are not always consistent.

According to the legal parameters governing an organization, the privacy and security programs are designed, and the policies and procedures are written and carried out. Most likely it is different across town and across state lines.

When health information is on paper only, the release of information process is slower and typically handled by several people. Generally the Health Information Management Department staff is responsible for knowing the laws and processing information for external release in a compliant manner.

**There are advantages and disadvantages to paper privacy:**

- The file room is locked
- Keys are controlled
- Involved staff is trained in confidentiality
- Nursing staff monitor chart viewing activity on care units
- HIM professionals monitor post discharge medical record access

However, except for physically observing someone reading a medical record or report, we have no retrospective way to know who viewed the information when no one was looking. In an electronic environment we “lock doors” and “control the keys” in very different ways:

**Technology gives us many new options:**

- We can keep people out completely
- We can let them into only a few systems
- We can let them into only a few applications and in certain locations—such as Laboratory and Unit 3 East
- We can track what a user has accessed—which patients, and what specific information details about a patient they accessed
- We can capture exact dates and time of system activity
- And we can set the system to alert us to unusual activity
- We can run reports to check system activity against our policies to see if users are compliant with our own policies and the laws. This is called Auditing and is carried out behind the scenes and may be a surprise to system users. By law—healthcare organizations must use system auditing capabilities to evaluate privacy.

Having these technology capabilities makes it possible to move information to many locations and to many different people while still controlling what they are allowed to “see.” At this time, the healthcare industry is more sophisticated internally within our organizations than we are externally with moving information electronically. Privacy has been in the healthcare industry spotlight much longer than security. Physical security requirements were limited in number with paper. Now the word “security” is largely used to refer to technology features.

- The first healthcare security law was implemented in 2005.
- The Security Rule came two years after the 2003 implementation of the federal Privacy Rule but decades after many other privacy laws were enacted. The delay was logistical—they weren’t ready at the same time.
- However, these two rules are designed to work together regardless of the delay in their launch.

Privacy and security working together is the key to the way we manage confidentiality in healthcare. In the electronic world we can’t have privacy without security. Privacy policies set the requirements and Security safeguards help “make” privacy happen. When changes are made in an organization, it requires careful analysis of the impact on the privacy and security programs. New and additional healthcare services may require compliance with laws we weren’t under before. New technology and system upgrades may offer stronger protections than before, calling for new procedures or new workflow design.

Any one of us may be the first one to detect the unfortunate impact of change by the way we observe privacy and security operating together. We are all in a position to make a difference. It is all of us who are showing the way to an effective balance in healthcare between privacy and appropriate information availability for patient safety and quality of care.

Health Information Privacy and Security Week takes place April 19 through 26, 2009. During this week we make a special point to recognize the importance and the impact of privacy and security of health information and the importance of those who help make it happen. Please take this message out there with YOU and apply it every chance YOU get!

References:

[www.AHIMA.org](http://www.AHIMA.org)

[www.MyPHR.com](http://www.MyPHR.com)

**April D. Robertson, MPA, RHIA, CHP, FAHIMA**