POLICY AND LEGISLATION

Gerry Blass and Susan A. Miller, JD

HIPAA and HITECH Security in the New World

Accountable Care Organizations and Health Information Exchanges

IT'S A NUMBERS GAME WHEN IT COMES to information security risk management. The bigger the numbers the harder it is to manage the risk of unauthorized access to protected health information.

By "numbers" we mean the numbers of vulnerabilities that create risk. For example, in how many locations in an organization does identifiable health information exist and what controls are in place to protect it from unauthorized access? How many workstations, laptops, flash drives, servers, network devices, portable devices, smart phones, media, etc. exist in an organization? How about remote access, wireless access, email accounts? How about data stored in the cloud? The numbers grow when comparing a single practice physician, to an ambulatory clinic to a hospital, to a health system, to an accountable care organization (ACO) and health information exchange (HIE).

It is safe to say that as the industry continues toward a new healthcare world of ACOs and HIEs, the numbers will grow and the need for unified governance, standard information security controls and effective risk management will also grow.

The current number of individuals included in breach notifications by healthcare providers as of the date of the writing of this column is greater than 16 million. You can view which organizations reported breaches along with the reason why on the HHC website.

The most common reason for electronic breach is lost or stolen media, mainly portable devices. The biggest overall risk of breach continues to be from internal workforce either accidentally or intentionally, out of curiosity, for financial gain or other reasons looking at records that is not part of their role. If single organizations continue to experience breaches, how much information security risk vulnerabilities could there be at multiple organizations that are members of ACOs and HIEs? For starters, let's explore some history of healthcare information technology.

INCREASED TECHNOLOGY LEADS TO INCREASED RISK

When we started our careers in health information technology, it was called "data processing." Our experience included hospitals that housed their own mainframe computer or licensed shared systems. The users of the systems accessed and updated data via "dumb" terminals, which could not store information. Data communication was via analog phone lines. There was no Internet. There was much less motivation and opportunity for internal workforce members to steal or misuse information, and there was almost no risk for an external hack. The technology at that time resulted in low likelihood of breach of health information due to the low *number* of vulnerabilities. The biggest headache to healthcare organizations was software bugs and the high cost of hardware and storage.

1990 was a major turning point. Personal computers were getting more powerful every year. Systems were distributed to departments via servers. Dumb terminals were replaced by the more powerful and intelligent PCs. Users began to use desktop applications and stored health information on their PC. LANs and WANs and the Internet blossomed. Organizations that used to have all of their electronic health information located in one place now had it scattered across their organization, and beyond.

By the mid-90s and after a number of major breaches HIPAA became law and the healthcare industry began to focus on infor-

IT IS SAFE TO SAY that as the industry continues toward a new healthcare world of ACOs and HIEs, the numbers will grow and the need for unified governance, standard information security controls and effective risk management will also grow.

mation privacy and security. Today, the need to protect identifiable health information continues to be a major concern and effort as technologies and the exchange of healthcare information continues to advance.

GOVERNANCE

The starting point to managing increased vulnerabilities and risk is proper governance and standards. That applies to any size organization, and is especially important to managing risk at ACOs and HIEs. Proper governance requires a steering committee with excellent leadership, teamwork and work groups that focus on implementing organizational, administrative, physical and technical safeguards. The end result should be operational policies and processes that reduce the risk of unauthorized access to health information, along with legal documents such as business associate agreements, data sharing agreements, memorandums of understanding, etc. It is certainly easier said than done, and it is more complex in a multi-organization ACO / HIE. With all the breach notifications that have been documented to date, it is obvious that vulnerabilities still exist and that risk is still significant in many organinzations. Imagine how much more significant risk will be if ACOs and HIEs do not have proper governance and standards and controls in place to reduce vulnerabilities and risk to an "acceptable" level.

RISK ASSESSMENT AND MANAGEMENT

So no matter what size and complexity an organization is, a good starting point is to assess / analyze the potential locations and vulnerabilities of protected health information. This is something that must be done periodically in order to manage change. The objective should be to eventually limit the number of locations, lock down the majority of user workstations, and protect media that is vulnerable such as authorized portable devices with security controls including encryption that complies with HITECH / NIST standards. Remember that if lost or stolen protected health information is properly encrypted, there is no breach. There have been enough breach notifications involving lost or stolen portable devices to give all of us an understanding of the risk level. At some point, very soon, if not now, a breach due to a lost or stolen unencrypted portable device will be considered willful neglect, and the financial penalty will be substantial.

Next, assess/analyze the controls in place

BY CONDUCTING AN ELECTRONIC protected heath information (ePHI) risk assessment, and by analyzing access controls, organizations will be focused on reducing what has been proven to be the highest risk of unauthorized access to health information.

to authorize, establish, modify and terminate access to protected health information, and determine if they are operational. For example, if there are 7,000 workforce members, including business associates (BA), and subcontractors who are authorized to access an EHR and there are 8,000 active-user accounts, something is wrong with the access termination process. And, if something is wrong with the access termination process, there may also be problems with the access modification process. Keep in mind that the workforce normally includes BAs and subcontractors such as software vendors and billing companies who may have both onsite and remote access. There needs to be a process in place for proper notifications of access changes, especially terminations, of business associates and their subcontractors.

By conducting an electronic protected heath information (ePHI) risk assessment, and by analyzing access controls, organizations will be focused on reducing what has been proven to be the highest risk of unauthorized access to health information.

The bottom line, though, is that organizations (covered entities, BAs, and subcontractors) must assess all standards and implementation specifications of the HIPAA rule along with the additional HITECH requirements, identify gaps and risk and begin a never ending process of risk mitigation and ongoing assessments.

CONCLUSION

Vulnerabilities, threats and risk of breach of health information exist at any size organization. It is truly a "numbers" game. The complexity of managing risk increases geometrically along with increased organizational size and interconnections.

Imagine the complexity of managing risk at multi-organizational ACOs and HIEs. Imagine the impact of any breaches that occur at ACOs and HIEs and the potential impact on member organizations and patients that participate in them. We can certainly expect to see an increase in patients requesting an accounting of access and disclosure, especially when a breach is publicized. Technology continues to improve and healthcare delivery and structure keeps evolving toward electronic information exchange. The time to establish strong governance and standards and controls around the privacy and security of health information for the new healthcare world is now. **JHIM**

Gerry Blass has over 35 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services and software called ComplyAssistant that automates the management and documentation of healthcare compliance activities. Mr. Blass is the President & CEO of Blass Consulting and Compliance LLC.

Susan A. Miller, JD has 35 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Ms. Miller has provided independent consultation and legal services to numerous healthcare entities including NIST and HHS. Blass and Miller are co-founders of HIPAA 411, a linked-in group.