SERCURITY

Gerry Blass and Susan A. Miller, JD

Accountable Care Organizations & Health Information Exchanges

An Information Security Survey

THE AUTHORS have written a number of *JHIM* columns regarding HIPAA-HITECH-Omnibus, etc., and have focused at times on the potential vulnerabilities that may exist with multi-organizational entities such as accountable care organizations (ACOs) and health information exchanges (HIEs). In exploring these vulnerabilities, we talked to a number of executives who work for healthcare providers and vendors and are active with their ACOs and HIEs.

We raised questions about information security controls implemented for ACOs and HIEs, and received answers that vary. In summarizing responses, it appears to the authors that there are no clear-cut standards and/or best practices being followed across the nation regarding information security controls within ACOs and HIEs.

RECENT GUIDANCE

Timing is everything, and at the time of the writing of this column, in early November 2014, the Office of the National Coordinator for HIT (ONC) published an initial report on ACO health IT infrastructure that includes the policy issues of:

- Privacy and Security
- Data Governance within the Accountable Care Entity
- Data Sharing with Community Partners
- Patient Matching Policies, and
- Consent Models

This report provides foundational concepts plus several case studies that will give ACOs and other entities a starting place to think through the necessary questions as they plan, implement, and lead an ACO.

CHALLENGES—SMALL AND LARGE

Single Organizations. Most of us are familiar with HIPAA–HITECH–Omnibus Security standards and implementation specifications. Many covered entities (CEs) and business associates (BAs) also follow the National Institute of Standards in Technology (NIST) guidance for implementing information security controls. These help to mitigate gaps and vulnerabilities that were identified during their HIPAA risk assessments and audits, which could threaten the confidentiality, integrity and availability of protected health information (PHI).

Even the largest organizational CEs and BAs are able to implement clear mandates and governance over responsibilities and accountabilities for complying with HIPAA. However, yes, there is still a prevalent lack of adequate money and human resources in many CEs and BAs, factors

EVEN THE LARGEST ORGANIZATIONAL CEs and BAs are able to implement clear mandates and governance over responsibilities and accountabilities for complying with HIPAA.

that have contributed to the large number of breaches of PHI.

The authors have contended in a number of JHIM columns that the highest risk to the privacy and security of PHI is a consistent lack of available money and human resources to address compliance. In addition, CEs now must monitor their BAs, especially their high and medium risk BAs. And, BAs must monitor their sub-contractors who are HITECH Act and Omnibus Rule downstream BAs. So the concept and difficulty of monitoring multiple organizations are major challenges facing CEs and BAs, even though clear-cut organizational mandates and governance can be implemented.

Multiple Organizations. Now add to the complexity of managing HIPAA Security the concept of ACOs and HIEs. The lack of adequate resources is still prominent, and mandates and governance are not easy to implement and manage, especially because governance is voluntary and not a legal or regulatory mandate. It seems to the authors that responsibility and accountability have the potential to be vague and unclear.

ACOs and HIEs are best defined as BAs to the member organizations that participate in the ACO and/or HIE, but which member organizations have the sense of being individually responsible and accountable? How are mandates and governance applied? A basic clarifying question could simply be – which organization is responsible for a breach of PHI? While that can be determined via audits and forensics, it is unclear to the authors how information security policies and procedures are implemented, monitored and how members of ACOs and HIEs are governed.

MORE QUESTIONS THAN ANSWERS

If you think that the authors have more questions than answers at this point, you are correct. We welcome the new ONC report (see previous discussion). In addition, we welcome insight and answers and more questions from our readers who work in ACOs and HIEs and manage HIPAA Security, and related Privacy and Breach Notification requirements. We have developed a series of questions and are seeking ACO and HIE HIPAA subject matter experts (SMEs) to answer the questions. We will follow up this column with one that provides answers to our questions, along with the SMEs' names upon their approval. We will also publish anonymous answers if we think they are valuable. We believe there is strong interest in hearing about the HIPAA Security controls in place at various ACOs and HIEs across the country.

SURVEY PARTICIPATION

Our survey will include questions in the following areas: legal documents, information security standards, best practices, audit, and a number of other areas. We encourage anyone involved in an HIE or ACO to participate in the survey. To participate, please send a request for the survey document to either of our email addresses: gerry@complyassistant.com or TMSAM@aol.com with the following in the subject line: "We would like to receive your ACO-HIE HIPAA Security survey questions." We may follow-up with a GoToMeeting or conference upon request to discuss and or clarify your answers.

CONCLUSION

We believe that many ACOs, HIEs, CEs, and BAs will be interested in reading the results of our survey, which we will share in a future *JHIM* column. Thanks in advance to all of you who participate in our survey. **JHIM**

Gerry Blass is President & CEO of ComplyAssistant and has more than 35 years of experience in healthcare IT and compliance. Blass provides IT and compliance consulting services and software (also called ComplyAssistant) that automate the management and documentation of healthcare compliance activities. To learn more, visit www.complyassistant.com.

Susan A. Miller, JD, has 40 years of professional leadership experience spanning college teaching, biochemistry research, and law. Since 2002, MIller has provided independent consulting and legal services to numerous healthcare entities including NIST, CMS [Centers for Medicare and Medicaid Services) and the OCR (Office for Civil Rights). Miller is the author and content manager of the NIST HIPAA Security Toolkit and has co-authored two OCR audit protocol prep books, HIPAA Security Audit Prep Book, and HIPAA Breach & Privacy Audit Prep Book You may reach her at TMSAM@aol.com. The prep books are published at http://www.malverngroup.com/New_Publications.html. Blass and Miller are co-founders of HIPAA 411, a LinkedIn group.