HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Twelve
Number Two
February 2010
Published Monthly

Meet

Meet Nancy Vogt, Director of Corporate Compliance, Aurora Health Care

PAGE 14

Feature Focus:

Medical identity theft: How is the health care industry responding?

PAGE 36

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ, SEE PAGE 45

Clarifying the confusing: The Anti-markup Rule made easy

PAGE 8

Business associate security and privacy programs: HIPAA and HITECH

By Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Editor's note: Rebecca Herold, The Privacy Professor®, is owner of Rebecca Herold & Associates, LLC located in Van Meter, Iowa. She may be contacted by e-mail at rebeccaherold@rebeccaherold.com or by telephone at 515/996-2199.

The Health Information Technology for Economic and Clinical Health Act (otherwise known as the HITECH Act portion of the American Recovery and Reinvestment Act of 2009) effectively widened the requirements for the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule to include the business associates (BAs) of covered entities (CEs). CEs are now accountable for more active validation of BA security and privacy program compliance, beyond just having a BA contract in place. It is more important than ever for CEs to take proactive measures to ensure BAs establish and maintain effective and appropriate information security and privacy policies and other supporting actions. Simply depending upon a security questionnaire answered once a year (or even less often), with no validation that the information provided is even accurate, is not effective. CEs must take a more proactive approach to ensuring BAs have effective and compliant programs in place. After all, CEs are ultimately responsible for ensuring the security and privacy of the information they collect from their own clients, patients, customers, and employees.

Business associates

I've done a great amount of HIPAA compliance work for CEs over the past decade, since just before HIPAA went actively into effect. In the past few years, I've done around 200 BA information security and privacy program reviews.

Many different types of BAs perform work for CEs. A large portion of them do business in other industries, in addition to the health care industry. In the BA information security and privacy program reviews I've performed, the BAs were of all sizes, provided a very wide range of services (some I had never even thought of before), and worked in many different industries.

I've been asked if a comprehensive list of BAs exists. Not only do I doubt that, I doubt if one even could exist; there is a constant turnover of companies that become BAs and cease being BAs.

The numbers of BAs used by CEs can be huge. As just one example, I did a BA security and privacy program review for one company that had approximately 15,000 employees. They had identified over 2,000 business partners, and of these, they identified around 600 "high risk" BAs – those with access to PHI.

Consider the statistics within the Health and Human Services (HHS) Breach Notice Rule which help to reveal the very widespread impact of the HITECH Act. HHS has determined that the HITECH Act impacts over 734,178 "small business" HIPAA CEs alone, and that doesn't include the medium and large CE businesses.

Consider the following data taken from the HHS website, based on US business census data provided to the Small Business Administration Office of Advocacy, which looks at how many "small" CEs will be impacted by the HITECH Act:

- 605,845 physicians, dentists, ambulatory care centers, hospitals, and nursing facilities
- 107,567 suppliers of durable medical equipment and prosthetics
- 3,266 insurance firms and third-party administrators
- 17,500 independent pharmacy drugstores

This represents a total of 734,178 small CEs. But, a large section of clearinghouses are missing from this list. There are more types of clearinghouses than what would fall under those shown. Now think about how many more thousands of medium-to-large CEs there are. The total number of CEs, as defined by HIPAA, in the U.S. is well over one million.

So then, think about how the HITECH Act has expanded HIPAA to effectively require all BAs to comply with the Security Rule and the Privacy Rule, and how many BAs are used by each CE. Consider a few numbers:

- One small CE I'm working with has five employees and five BAs.
- A little bit larger CE I've helped has around 50 employees and 15 BAs.
- A large CE (I've done over 150 BA security and privacy program reviews for them) has over 2,000 business partners, of which 600 are identified as BAs that have access, in some way, to protected health information (PHI).

Based upon just these limited examples, the HITECH Act has effectively expanded the reach of HIPAA by five to 600 times! The HITECH Act will be impacting literally millions of organizations. This demonstrates how the HITECH Act is impacting health care information security and privacy compliance

much more widely than even HIPAA did. Each CE now must widen their compliance purview significantly to help ensure that all their many BAs are appropriately safeguarding information and providing appropriate – and required – security and privacy protections.

Business associate services

BAs perform a very wide range of services. An example of just some of the activities performed by the 200 BAs I've reviewed include:

- Call center work
- Application development
- Archiving
- Backup vaulting
- Physical files maintenance
- Employee background checks
- Job candidate background checks
- Test data creation
- Transcription services
- Contracted laboratory and radiology departments
- Software development
- Hot site hosting
- Billing, and
- Home care services

So what is a "business associate"? HIPAA defines a business associate as follows within §160.103 Definitions:

"Business associate:

1. Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:
   i. On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
      a. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
      b. Any other function or activity regulated by this subchapter; or
   ii. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
2. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
3. A covered entity may be a business associate of another covered entity."

Think about all the possible types of organizations you outsource different types of business activities to. If they have access in any way to PHI, then they are most likely considered to be BAs.

10 common indicators of problems

During the course of performing BA security and privacy program reviews, I have repeatedly run across similar problems when reviewing the completed questionnaires and other documentation, such as policies, website information, and so on. The following provides a high-level listing of the ten most common indicators that a BA information security and privacy program has some problems at best, and completely insufficient and risky programs at worst.

Indicator 1: Incomplete response

When a BA does not completely answer the information security and privacy questionnaire used during a review, it may indicate that no acceptable program in place. It may also indicate that the appropriate person did not provide the questionnaire responses. I have often had the BA's marketing contact try to answer the questions. The best people to answer the questions work in the information security and privacy areas. I have also found BAs often choose not to answer a question at all if it will look negative for them; perhaps they think not responding at all looks better.

Indicator 2: Inconsistencies between policy and response

Many times I have found the responses in the BA's completed questionnaire did not match the documentation provided. For example, the respondent for the questionnaire may indicate the passwords used are a minimum of six alpha characters, but the actual policy may indicate passwords must all be a minimum of eight alphanumeric characters. This shows that the BA is likely not enforcing their policies, that the systems are not configured to support the security policies, that compliance audits are not performed, and/or that

Continued on page 25

there is no training or awareness provided for the policies.

Indicator 3: No assigned security or privacy responsibility

The responsibility for security and privacy may be delegated to a "Jack/Jane-of-all-trades" or performed ad-hoc. Information security and privacy responsibilities need to be formally assigned and documented. Not only is this a requirement under multiple rules and regulations, including HIPAA, it is also good business practice to ensure personnel know their responsibilities with regard to security and privacy practices. A formally documented responsibility must be in place to ensure security is appropriately and consistently addressed.

Indicator 4: Response is provided by another company

Be sure to verify that the questionnaire responses apply to your BA and are not provided by some other entity. I have run across many instances when a completely different organization filled out the security and privacy questionnaire instead of the BA. For example, there have been multiple times the BA used an outsourced managed services provider to take care of their network, and got them to answer the questionnaire based upon the managed services security and privacy program, not upon the BA's program. It is important to know if your BA uses a managed services provider, but your BA still needs to answer the questionnaire and tell you about the BA's own security and privacy program. Your BA needs to have an information security and privacy program in place to address all the operational, physical facilities, and human issues, even if they have outsourced the network management.

Indicator 5: Subcontracting

Many times the BA was subcontracting the processing of my client (CE's) data to yet another company, and that subcontracted company did not have good security practices. In fact, in some instances, the subcontractor had basically no security practices! There have also been times when the subcontracted company was located in a different country. Be sure to cover the issue of having your BA subcontract within your organization's contract with the BA. In one very interesting case, I discovered that my client's BA had been subcontracting PHI management and processing to another company that employed an ex-employee of my client who had left under very hostile terms. This was certainly a high risk to have this person handling such sensitive information for a company against which he had a vendetta!

Indicator 6: No mobile computing controls

One of the most common ways in which security incidents and privacy breaches occur is through lost or stolen mobile computing devices, such as Blackberrys, laptops, notebooks, smart phones, and so on. An alarmingly large number of the BAs I've reviewed did not have security policies or controls in place for these types of mobile computing devices, or for their employees who work from remote locations. However, they often allowed the CE's data to be stored on the mobile devices, or allowed personnel who used these types of computers to process the CE data. Make sure BAs have appropriate security in place for such situations.

Indicator 7: No use of encryption

Another type of incident reported weekly, and sometimes daily, is the loss or theft of personal information, including large amounts of PHI, that was not encrypted. I have found most of the BAs do not use encryption to protect information in storage, in transit, or on mobile computing media and devices, such as laptops, backup tapes, USB drives, and so on. This is slowly changing, but in most cases, the BA will not spend the time and resources to encrypt data unless required contractually or by law to do so. Now laws in Massachusetts and Nevada require encryption of such personal information. Plus, the HIPAA Security Rule, which BAs must now be in compliance with, requires encryption to be used, based upon risk. Be sure encryption is used by BAs to mitigate the risk involved in such situations.

Indicator 8: Missing, incomplete, or outdated business continuity and disaster recovery plans

I never cease to be surprised when I find a BA does not have any documented business continuity or disaster recovery plans! It seems like such a common sense type of protection to have. However, in far too many cases, business continuity and disaster recovery plans are often either missing or were written several years ago and never tested. Recently, I found a BA with a very well-documented and detailed business continuity plan…from 1995! The plan had never been updated or tested! Needless to say, most of the BA systems and applications had been either replaced or changed dramatically since 1995. Be sure the BAs have up-to-date plans in place, and that they test them regularly.

Indicator 9: No corrective actions for prior breaches

Has your BA had an information security or privacy breach? This is definitely something you need to check on. Check multiple places. Use the time your BA is completing the security and privacy questionnaire to do research to see if they have had any publicized security incidents or privacy breaches. There are multiple services you can use to check on this, in addition to dozens to hundreds of good websites to search for news about the BA and any security breaches for which it was involved. I have found some BAs who indicated on their security questionnaire that they have never experienced a security incident or privacy breach, after I found through my own research that they have had significant incidents and

Continued on page 28

 ...continued from page 25

breaches! If you find the BA has had a breach, be sure to ask the company about it and find out what actions they have taken to prevent such a breach from occurring again.

Indicator 10: No independent assessment

If a BA has never had an independent security or privacy assessment of their organization, it is a warning sign. It could be indicative of many possibilities, such as:

- Lack of funding for the security and privacy program. Most organizations that are serious about security and privacy have an independent audit or assessment to ensure their controls and safeguards are appropriate.
- A false sense of security. Many of the BAs I've reviewed have indicated that they believed things were fine, so they didn't need someone to do a review. Ignorance is definitely not bliss when it comes to security, privacy, and compliance.
- Independent assessments have been done, but are not being shared. I've run across two very large BAs who did not want to share the results of their security and privacy program audit, because it had so many significant findings.

Of course, it is also possible that you will find upon investigation that the BA simply did not know that doing an independent assessment was advantageous, or they simply didn't want to spend the money to do one. However, it is still worth checking on.

Benefits of active BA compliance management

If you depend upon the use of questionnaires for doing BA security and privacy program reviews, as is typically done, you will likely reveal a very wide range of risks. I've done around 200 of these, and while they've been very beneficial to identify concerns within BA information security and privacy programs, they also have their drawbacks. Some of these include:

- Each review typically takes around four to eight weeks to complete, depending upon how timely the BA completes the questionnaire, provides documentation, and makes key contacts available for interviews.
- The review is an assessment of a point in time for the BA. As soon as the review is over, if anything within the BA operations, systems, networks, administration, or other signification factor changes, it will likely also change the information security and privacy posture for the BA.
- Most of the answers on the questionnaires are not validated. Many organizations answer the questionnaires in the way that will be most beneficial for them to "pass" the review, and they do not truly represent the reality of the BA information security and privacy program.

As I did more and more of these BA security and privacy program reviews, I became more and more convinced that there must be a better, more effective, accurate, and efficient, way for CEs to ensure, on an ongoing basis, that BAs have good information security and privacy programs in place. To meet this need I partnered with Jack Anderson, of Compliance Helper (http://www.compliance-helper.com), to create an automated way to allow CEs to see the documentation for their BAs at any time, on an ongoing basis, to validate appropriate documents, forms, and activities exist for BA security and privacy program compliance. By having a window into the key BA security and privacy program components, CEs will be able to ensure BAs:

- Are in compliance with legal and regulatory requirements and/or expectations
- Perform due diligence efforts during the contracting process or other risk management activities
- Are in compliance with CE contractual security and privacy expectations
- Resolve security and privacy issues promptly and appropriately

This is an effective and cost efficient alternative to performing the more time- and resource-intensive reviews based upon point-in-time questionnaires and documentation reviews. It also helps to quickly and effectively address and eliminate the ten BA security and privacy program problems.

Many benefits accrue from performing BA information security and privacy program reviews, or from choosing to have ongoing compliance monitoring capabilities:

- Meet compliance with multiple laws and regulations
- Demonstrate due diligence by your organization
- The resulting reports clearly detail for the BA what you want them to do to protect the information and system that you have entrusted to them
- Having such documentation also helps to motivate the BA and ensure the risks are resolved in a timely manner
- Ongoing monitoring, or doing point-in-time reviews, aids in a reasonable and appropriate evaluation of the BA's security and privacy program
- Security and privacy expectations for the BA are aligned with the CE's requirements
- Reviews and/or monitoring helps organizations define within their contract the issues and activities that are considered as grounds for termination of business relationship
- Vulnerabilities and threats can be identified and mitigated before bad things happen

Following formal information security and privacy review methodologies or using an ongoing program monitoring service will help to ensure BA compliance, which also helps CEs to ensure they are appropriately demonstrating due diligence, complying with all their compliance obligations, and doing all they can to prevent privacy breaches. ■