Grant Thornton
An instinct for growth™

Protecting patient information — Answers to your questions

February 18, 2014

Our webcast, "Protecting Patient Information: A Collaborative Approach Between Provider Organizations and Business Associates," generated many valuable questions from our audience and comments for the presenters.

In response, the following insights are provided by **Jan Hertzberg**, Grant Thornton LLP managing director of Advisory Services-Information Technology; **Cindy Davis**, Grant Thornton director of Innovative Services Development; **Lorna Koppel**, vice president and chief information security officer of Iron Mountain, and **Mike Hebrank**, vice president and CIO of University HealthSystem Consortium in Chicago. All four presenters contributed responses, with two answers provided by specific presenters as noted.

Download the webcast presentation (PDF) and replay the webcast, which gives all who process, manage, store or protect health information guidance in complying with HIPAA requirements.

State laws

Q: Which state law applies if the data is in state A and a hacker in state B breaches data?

A: What matters is the state where the company conducts business and the states where the residents of the breached PI (personal information) reside. Each state has different requirements for notification to those residents, so you should have a standard letter prepared for each state so you are meeting the notification requirements for that state.

Almost all state breach notification laws assert that the law applies to any person, business or state agency that acquires, owns or licenses computerized data that includes personal information of that state's residents. When it comes to maintaining information that they don't own, almost all state laws also assert that the provisions governing maintenance of PI are applicable to any entity maintaining information on that state's residents, whether or not they conduct business in that state.

California statute describes covered entities as: 1) Any person or business that conducts business in CA and owns, licenses, or maintains computerized data including PI; or 2) any agency that owns, licenses or maintains computerized data including PI.

Texas requires a company to notify residents in states where no breach notification laws exist: New Mexico, Kentucky, Alabama and South Dakota.

If you are maintaining information (even if you don't own it), it is important to understand both aspects of breach notification laws. You need to understand the laws in the states where you conduct business and the laws of the states where the customers reside.

Q: Whiat is the best resource that can track state laws??

A: There are several good resources:

State Security Breach Notification Chart
State Security Breach Notification Laws
Data Breach Charts

Electronic data

Q: What are the risks that should be considered with regard to the use of mobile devices and applications (domestically and internationally)?

A: We recommend you read the NIST Draft: *SP 800-164 DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices.* This is one of our favorite articles: "4 Mobile Device Dangers That Are More of a Threat Than Malware," by Robert Lemos (Sept. 11, 2013).

Q: We have a corporate entity with many subsidiaries and each subsidiary has its own email domain. Is additional security required for each domain?

A: It depends on the layers of network security in place. U.S. Department of Health and Human Services (HHS) expects that all communications sent over the internet be encrypted. To achieve safe harbor from breach notification, specific encryption algorithms should be used for all transport layers. See *SP800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.*

Breach notifications

Q: What is an appropriate time frame to require our business associates notify us of privacy/security incidents?

A: HIPAA requires 60 days from discovery of a breach to notify agencies and individuals. Discovery of a breach does not necessarily mean the same thing as determining that a security incident has occurred. It takes time to investigate a security incident that results in a discovery of a breach; an effective incident response program will have procedures that enable a timely investigation. All security incidents where data is exposed should be investigated quickly.

We notice that the common time frame a covered entity (CE) wants to be notified of a suspected breach by a business associate to be five days. A business associate should be able to notify a CE on the day they determine a security incident has occurred, but it's prudent to give them at least five to seven days to vet the discovery of the incident to make sure it has a high likelihood of being a reportable breach. It is not practical or advisable to be asked to be notified of every incident — only the ones that have been discovered to be a reportable breach. Otherwise, you could be getting notifications so frequently you might need a full-time equivalent employee to keep up with tracking them.

CEs have 60 days from the day they were notified by the BAA.

Q: Beside the patient, who needs to be notified of a breach?

A: For breaches of unsecured protected health information (PHI) involving 500 or more individuals, a CE will notify individuals and prominent media outlets serving the state or jurisdiction, and submit information to be posted to the HHS website. For breaches of unsecured PHI involving fewer than 500 individuals, a CE will maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification to HHS.

Due diligence

Q: As part of due diligence, you recommend taioring questionnaires and interviews to areas consistent with the service procured. Can you provide an example of such a questionnaire?

A: For a sample questionnaire, contact Mike Hebrank (hebrank@uhc.edu), vice president and CIO of University HealthSystem Consortium.

Q: How important is requesting/requiring a SOC 2 report from a third-party vendor?

A: A SOC 2 from a business associate gives you more insight into the risk to your data that is held or processed by them. A SOC 2 report should be incorporated into your risk assessment process to give you a comprehensive view of how your PHI is being managed throughout the information life cycle.

If you want to better understand the controls that your vendor has put in place to safeguard the PHI that they are creating, transferring, maintaining or destroying for you then it is essential you request a SOC 2 report from them. It requires them to be transparent and having a third party perform the attestation gives you confidence that the report is objective and performed under AICPA standards.

These reports also outline the controls that your company must have in place to make their controls effective. This piece in particular is very enlightening to many companies that outsource their data to third parties.

Contract negotiation

Q: How long is a business associate agreement (BAA) valid? Do BAAs need to be signed annually, biannually, etc.?

A: This is a question that is best answered by legal representation because it differs with each contractual situation. You might find the example Business Associate Contracts language on the HHS website helpful.

Q: What is involved in obtaining a third-party HIPAA attestation (time/cost)?

A: This answer is provided by Mike Hebrank, vice president and CIO of University HealthSystem Consortium: We hired Grant Thornton to do a readiness assessment first so that we understood where the gaps were in our HIPAA compliance program and to receive recommendations on how to address those gaps. Grant Thornton is now performing the attestation.

The time and cost was the greatest for us after the readiness assessment, which recommended additional controls be put in place to address the gaps. That took about a year for us to do as we needed to implement technology as well as processes that took time to develop, implement and mature.

The attestation is like most audits — we have to supply evidence to show that the controls we have implemented are operating effectively. Since we chose to have an opinion on six months of operations, we are pulling samples Grant Thornton selects that cover the last six-month period.

Operating

Q: Do business associates find covered entities are performing robust monitoring?

A: Robust monitoring by way of questionnaires has increased since September 2013, when the HIPAA Omnibus Rule went into effect.

Q: Do you recommend customizing the information provided to vendors to limit access to Social Security numbers, etc.?

A: All organizations that transfer information to another party should consider the data elements that are required by the recipient to meet the needs of the service requested. Only the data elements that are needed should be provided by either using limited data set criteria spelled out in HIPAA Privacy or by extracting and transferring only the data elements required for the purpose.

Q: Can you provide examples of controls and processes instituted by business associates regarding the items stored by health care clients?

A: This answer is provided by Lorna Koppel, vice president and chief information security officer of Iron Mountain: The short answer is that it depends on the services being procured and how the deployment is designed and negotiated. Our standard services (box storage, tape storage and shred/disposal) are typically sufficient to meet HIPAA requirements because we do not know what is stored inside or have access to the data in the box/tape/container. If a customer informs us of what data they are giving us with specific security needs, we can work together to ensure a compliant solution that meets their needs. This document, *What You Should Know About HIPAA and the Omnibus Final Rule,* goes into more depth. However, here are some high-level comments and some examples:

- Iron Mountain services have baseline controls that are generally sufficient for our health care customers: standardized workflows and tracking of information assets at each step of the process, physical access controls and monitoring such as badge controls, intrusion alarms, environmental/fire controls, cameras, sign-in/out for visitors, background screening of employees and contractors, strict policies against accessing inside customer containers, and frequent training on protecting our customer data. We also are very careful on chain of custody of the data throughout the transport/storage /disposal processes and have standard incident reporting processes.
- Standard box/tape storage: These depend mostly on our standard baseline controls mentioned above. Customers can order services where they can add additional security where they send the data in containers that are sealed/locked in a way to ensure that Iron Mountain doesn't have access to open them. If neededd, it is the customer's responsibility to make sure that tapes or electronic media are encrypted prior to sending to Iron Mountain.
- File retrieval services: An example of additional control is our policy that is applicable only to health care accounts. It requires one or more unique identifiers to be captured for new, incoming patient files that are stored on an open shelf or if files will be retrieved from cartons. This policy for individually listing files not only allows us to easily find and retrieve patient files that are needed for patient care, but it also helps our customer meet their HIPAA compliance obligations under the new HIPAA Omnibus Final Rules.
- Imaging services: The customer works with Iron Mountain to design the service based on what is to be handled, how the data is transmitted (including encryption) and access controls. Some features customers could order include a customer-dedicated room that has controls that are pre-agreed-upon such as restricted access to the area specific to the deal. Some additional examples can include no cell phones allowed in the room, cameras for monitoring or specifically no camera monitoring, etc. Depending on what is ordered, the equipment and network in these rooms may be dedicated to the customer, and the customer might control the configuration of software and electronic security controls.
- Medical image archiving: We offer digital record centers for medical images. These have a private network within the customer site and Iron Mountain, and all access to images is controlled by the customer login credentials within their picture archiving and communication (PACS) application. This includes encrypted transfer of data offsite to our secure data centers. The customer data is encrypted in transit and at rest while in the Iron Mountain data centers. We also leverage our strong physical security program to protect the data centers.

Discontinuing

Q: Medicare Access requires the business associate to preserve data, even at end of life. How does this impact the BAA?

A: A BAA should be in place for as long as the business associate holds the data.

Q: What evidence is generally provided to ensure destruction of records?

A: The evidence depends on the process that is being used to destroy the records. Many companies that provide record destruction services provide a receipt that is considered evidence. The contract with the company should spell out that they will safeguard the information, and if the records are not destroyed

the information, and if the records are not destroyed according to an agreed-upon method, they can be held liable if a breach occurs. To achieve safe harbor from breach notification, records should be destroyed in compliance with *NIST SP800-88_rev1 Guidelines for Media Sanitization,* which requires the following destruction techniques for paper records:

- Destruct paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL).
- Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.

Visit granthornton.com to read the article online.