The Basics of Protecting PHI

Best Practices when Working with Business Associates

Gelb, An Endeavor Management Company

1011 Highway 6 South
Suite 120
Houston, Texas 77077

P + 281.759.3600
F + 281.759.3607
www.gelbconsulting.com

Gelb
An Endeavor Management Company

The Basics of Protecting PHI

Note: We are not attorneys and this represents our experience in working with healthcare organizations. This should not be considered legal advice.

Overview

The Health Insurance Portability and Accountability Act (HIPAA) placed clear responsibility on healthcare providers to protect individually identifiable health information. Hospitals and healthcare professionals who work with this type of information everyday are familiar with HIPAA requirements. However, when external business associates are engaged for activities in which protected health information (PHI) is accessible or shared, there is often a lack of explicit discussion about how to protect PHI.

HIPPA rules stipulate that business associates are directly liable for following HIPAA requirements when working with PHI. For this reason, healthcare providers are required to employ a business associate agreement (BAA) or other written arrangement that specifies how the business associate will comply with HIPAA. Nevertheless, business associates may be unaware of the full breadth of regulations or lack the experience and/or resources to put proper safeguards in place. In fact, according to the U.S. Department of Health & Human Services, some of the largest HIPAA breaches have involved business associates. From Gelb's perspective as a small business that works with PHI, HIPAA has complex guidelines that require time and resources to fully understand and ensure compliance.

Privacy violations – whether the fault of a hospital representative or a business associate – can be a public relations nightmare and violate the trust of the community. For this reason, it is important for hospitals to go beyond a BAA when considering HIPAA compliance.

How can healthcare professionals be proactive in keeping PHI safe when working with business associates?

Despite the best of intentions, PHI breaches most often occur due to lack of awareness about HIPAA guidelines or failure to follow policies that are in place to prevent breeches. Particularly in the case of business associates who do not typically work with PHI, personnel may lack proper training and resources to protect the information. Even if policies are in place, there must be accountability to ensure the policies are being followed.

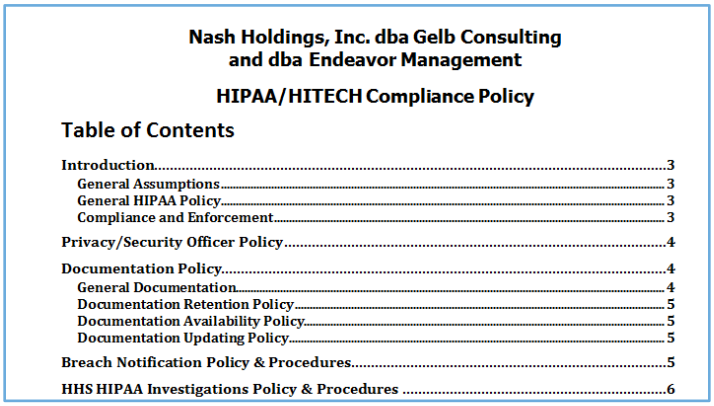
At Gelb, we work with PHI on a regular basis in situations such as in-depth interviewing of patients, conducting focus groups, conducting online patient surveys, and managing CRM dashboards. Based on our experiences, we would like to share some best practices for healthcare professionals to consider when sharing PHI with business associates.

Confirming Compliance: Basic Questions to Ask

Accountability and transparency is critical in protecting PHI. Even if a BAA is in place, prior to sharing PHI with a business associate, healthcare professionals should initiate discussion and ask questions to ensure best practices and regulations are being followed.

1. Do they have a HIPAA Privacy/Security Officer, and does that person understand the role he/she plays in protecting your PHI?
    - Organizations that work with PHI should designate and maintain a HIPAA Privacy/Security Officer.
    - This person should have in-depth knowledge of HIPAA regulations, and oversee compliance-related activities, training and policies.

2. Do they have a documented HIPAA compliance policy?
    - All internal compliance related policies, authorizations, training and other related documents should be clearly documented and updated.
    - The policy should explain what PHI is and how it will be handled to ensure compliance with the regulations.
    - The policy should be available to all employees and those who will be exposed to PHI must confirm that they have read it and will comply with it.
    - A copy of their policies should be provided to you if you request it.



Nash Holdings, Inc. dba Gelb Consulting and dba Endeavor Management

HIPAA/HITECH Compliance Policy

Table of Contents

3. Who will have access to PHI, and are they HIPAA trained?
    - Any personnel who have access to PHI should complete HIPAA compliance training. At Gelb, employees must go through several training courses and pass a written exam prior to working with PHI.
    - As a basic starting point, employees should understand what is considered to be PHI, and the importance of protecting the information. For example, it is a common misconception that it is not PHI if the patient's specific diagnosis is deleted.

4. How will PHI be stored?
    - Most documents saved on a company's shared drive or a cloud-based portal are accessible to the entire company. However, PHI should only be accessible on a

"need to know" basis. At Gelb, we have separate a web portal for each project that involves PHI, and each portal is only accessible to those who truly need access.

- PHI should not be downloaded or saved to an individual computer or portable device, but instead edited or accessed through the portal. In a rare situation in which PHI is downloaded (such as due to lack of internet access during the research), the device should be encrypted, and the downloaded PHI should be deleted as soon as possible. PHI saved to portable devices is the cause of many news stories in which privacy is breached due to a loss or theft.
- When working with business associates, it is best to avoid sharing hard copies of PHI. However if hard copies must exist, they must be stored under lock and key with documented control of who has access.

5. How will PHI be shared between the project team members?
    - Team members should not use email to share PHI documentation. They should share documents via a secure server or online portal. Although hospitals might have specific security measures in place that allow them to email PHI, most business associates do not have this capability.
    - The business associate team should maintain a log of PHI sensitive information – who it was received from, who it is accessible to, any situations in which it is transferred or shared, and when it was destroyed.

Interview Schedule Date: Monday, 03.09	
Time	**Patient Code**
8-9 a.m.	Patient 234
9-10 a.m.	Patient 433
10-11 a.m.	Patient 653
11-12 a.m.	
12-1 p.m.	Patient 321
1-2 p.m.	
2-3 p.m.	
3-4 p.m.	Patient 431
4-5 p.m.	
5-6 p.m.	

Tip: The number of documents that contain PHI should be limited. For example, if the team is working on a schedule for interviews or focus groups, PHI can be protected by assigning each patient a code. The code is included on the scheduling documents and research notes rather than the patient's name. This allows the documents to be emailed and shared with the team without compromising privacy.

6. How is privacy maintained when recruiting or speaking with patients?
    - In marketing research, it is common that patients need to be recruited for interviews or focus groups. It is important that those contacting the patients can clearly communicate how they obtained their name and information to dispel concerns that patients might have about their privacy.
    - Team members should also be aware of how much information they share via a voicemail or message left with another person who answers the phone. For example, at Gelb we leave ambiguous messages or voicemails along the lines of "We

are conducting a project with [name of hospital] that you might be interested in participating in." Rather than explaining that we are calling to ask about their experience with the Lung Cancer Program.

Tip: For consistent messaging, it is helpful to have a client-approved recruiting and voicemail script. It is also helpful for the research team to avoid using full names on any of the research materials (such as within an interview transcript or within the file name) and instead use the patient's code so that the transcript does not become PHI.

7. Will the business associate be utilizing additional subcontractors or service providers? If so, are they HIPAA compliant?
    - Business associates may need to use subcontractors or service providers for purposes that require them to share PHI – such as recruiting for research or distributing online surveys. In these situations, the business associate must execute a BAA with the other entity to ensure that it is HIPAA compliant as well.
    - At Gelb, all subcontractors and service provider must complete training and enter into a BAA that outlines safeguards for protecting PHI. Gelb project managers reinforce these guidelines during the project.

8. What happens to PHI after the project is completed?
    - All PHI should be shredded at the completion of a project.

Tip: At the end of a project, ask the business associate team to conduct a "PHI Check" to ensure all PHI documentation related to the project has been destroyed. This includes checking servers, online portals, portable devices and hard copies.

Key Takeaway – Transparency and Accountability are Critical

Sharing PHI with business associates is often necessary, and can result in valuable information and technology. However, a lack of explicit discussion between healthcare professionals and business associates about how PHI will be handled makes a breech more likely. Prior to sharing PHI, healthcare personnel should initiate conversation and ask detailed questions about the business associate's HIPAA-related policies to ensure that best practices and regulations are being followed. Ultimately, transparency and accountability are critical for both organizations in not only following the law, but also in maintaining patient trust and confidence.

About Endeavor

Endeavor Management, is an international management consulting firm that collaboratively works with their clients to achieve greater value from their transformational business initiatives. Endeavor serves as a catalyst by providing pragmatic methodologies and industry expertise in Transformational Strategies, Operational Excellence, Organizational Effectiveness, and Transformational Leadership.

Our clients include those responsible for:

- Business Strategy
- Marketing and Brand Strategy
- Operations
- Technology Deployment
- Strategic Human Capital
- Corporate Finance

The firm's 50 year heritage has produced a substantial portfolio of proven methodologies, deep operational insight and broad industry experience. This experience enables our team to quickly understand the dynamics of client companies and markets. Endeavor's clients span the globe and are typically leaders in their industry.

Gelb Consulting Group, a wholly owned subsidiary, monitors organizational performance and designs winning marketing strategies. Gelb helps organizations focus their marketing initiatives by fully understanding customer needs through proven strategic frameworks to guide marketing strategies, build trusted brands, deliver exceptional experiences and launch new products. Gelb can help you to develop and implement the right strategies. Using advanced research techniques, Gelb can help you to understand the complexities of your market, to develop your strategic decision frameworks and to determine the best deployment of your resources and technology to monitor your successes.

For over 50 years, Gelb has worked with marketing leaders on:

- Strategic Marketing
- Brand Building
- Customer Experience Management
- Go to Market
- Product Innovation
- Trademark/Trade Dress Protection

Our websites:
www.endeavormgmt.com
www.gelbconsulting.com
www.gulfresearch.com