WHITE PAPER

1st Healthcare® Compliance

Defining Covered Entities, Business Associates, and HIPAA Breaches

WHITE PAPER

1st Healthcare® Compliance

Defining Covered Entities, Business Associates, and HIPAA Breaches

By Jill Brooks, MD, CHCO and Julie Sheppard, BSN, JD, CHC

Are you a covered entity? HIPAA defines a covered entity as one of the following: healthcare provider who transmits transactional information in an electronic form; health plan; or healthcare clearinghouse.

Most providers are covered entities, managing insurance-related transactions electronically, like submitting claims to a health plan.

Covered entities have severeal requirements under HIPAA, such as managing the business associate relationship and complying with the breach notification rule.

What Are Your Responsibilities as a Covered Entity?

Covered entities must comply with all of the HIPAA /HITECH rules and regulations. A covered entity must protect and secure individually identifiable patient information. Responsibilities of a covered entity also include the provision of records, compliance reports and cooperation with complaint investigations and compliance reviews by HHS including permitting access to facilities, records, accounts, and protected health information, if necessary, to determine compliance with administrative simplification. The covered entity has the ultimate responsibility for HIPAA compliance.

What constitutes PHI?

Protected Health Information (PHI) under the Privacy Rule is all individually identifiable health information held or transmitted by a covered entity or Business Associate (BA) in any form or media which includes the individual's past, present or future physical or mental health condition, the provision of health care to the individual, and past, present or future payment of health care to the individual. Individually identifiable health information includes a range of specified identifiers such as name, address, date of birth, fingerprint or full-face photograph, vehicle license, IP address etc. (45 C.F.R. §160.103)

Do You Meet the Privacy Rule Requirements for a Covered Entity?

Covered entities have several requirements under the Privacy Rule. The purpose of the rule is to protect and secure individually identifiable patient information. Compliance with the Privacy Rule was required as of April 14, 2003.

A couple of important aspects of the rule involve practical steps: assigning a privacy/security officer and staff training.

In a smaller practice, one individual may serve the roles of privacy and security officer, but the description of the duties should be well documented. Staff should be aware of who is serving these important roles. The privacy and security officer should develop, document and maintain policies and procedures, and work with the IT team and EHR vendors.

Staff training and education on the office HIPAA policies and procedures should be ongoing to make sure staff is aware of their responsibilities to keep the patient information private and secure. For instance, a covered entity must obtain an individual's written authorization for any use or disclosure of PHI that is not related to treatment, payment or healthcare operations with a few otherwise permitted exceptions. Reasonable efforts should be made by the covered entity to disclose the minimum amount of PHI necessary for the intended purpose, and the access to PHI should only be designated to those employees with duties requiring access.

Office policies and procedures should be reviewed and updated as needed to be sure that every possible system is in place to secure and protect all PHI, which under the Privacy Rule applies to any PHI-oral, paper or electronic. Most importantly, the staff must be continually educated about any changes to existing Privacy policies and procedures.

1st Healthcare® Compliance

WHAT ARE EXAMPLES OF A COVERED ENTITY?

- Physician
- Dentist
- Chiropractor
- Nursing home
- Pharmacy
- Health insurance companies
- Medicare/Medicaid
- Clearinghouse

WHAT ARE EXAMPLES OF A BUSINESS ASSOCIATE?

- A billing company
- An accountant
- An answering service
- A document shredding company
- A collection agency
- An attorney

Do You Meet the Security Requirements for a Covered Entity?

Covered entities should be aware of differences between the Privacy and Security Rule requirements regarding protected health information. One major distinction is that the HIPAA Security Rule only applies to electronic protected health information (e-PHI). A covered entity is responsible for maintaining confidentiality, integrity and availability of all e-PHI.

The HIPAA Security Rule is compromised of the following Administrative, Physical, and Technical Safeguards:

Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Technical Safeguards

- Access Controls
- Audit Controls
- Integrity Controls
- Transmission Controls
- Person or Entity Authentication

Under the HIPAA Security Rule, covered entities are required to do a risk analysis to document any risks or vulnerabilities to e-PHI. Any risks or vulnerabilities identified should be appropriately addressed and steps for mitigation documented, including necessary changes to policies and procedures. All documents should be kept for at least 6 years.

A plan should be developed based on the risk analysis results and should include how the practice uses the administrative, physical and technical safeguards to mitigate risks. This risk analysis should be an ongoing process and to achieve Meaningful Use, a review is required periodically. This is not a "one-size fits all" so the security measures are scalable to any size practice.

The Administrative, Physical and Technical Safeguards are the focus of the OCR Audit Program Protocol for the Security Rule. These safeguards include required and addressable implementation specifications.

Addressable does not mean optional. The covered entity will decide if the addressable implentation specification is "reasonable and appropriate" for their practice. If it is not considered "reasonable and appropriate", the reason must be documented.

With the enactment of HITECH, the HIPAA Enforcement Rule allows Civil Monetary Penalties (CMP) for violations of the Privacy and/or Security Rules. A covered entity could be assessed a fine of up to $1.5M for identical violations in one calendar year even if the covered entity did not know about a violation and if known, the correction must occur in 30 days from discovery or be subject to maximum penalties.

Who are your Business Associates?

Most providers realize the importance of having Business Associate Agreements (BAA) in place. However, many find it challenging to determine which vendor relationships require a BAA.

By definition, a business associate (BA) is any individual or entity that a covered entity allows to create, receive, maintain or transmit Protected Health Information (PHI). As required by HIPAA, a covered entity must have a written business associate agreement (BAA) in place for any of the following BAs:

- Practice or benefit management
- Answering service
- Billing company
- Collection agency
- Document shredding company
- Claims processing, accountant, legal, utilization review, actuarial, healthcare clearing house, medical transcriptionist, electronic health record (EHR)
- E-prescribing gateway.

Examples of those not considered to be a BA of a covered entity include: health plans, laboratories, pharmacies, janitorial services or conduits such as a telephone service provider, US Post Office, UPS, or Fed Ex.

Below are a few questions heard frequently from physicians and practice managers.

What about the phone company or the Internet provider? They could access my patient information, so we need a BAA with them, right?

BAAs are not necessary with certain organizations considered to be mere conduits. Examples are the US Postal Service, some private couriers, telephone companies, and Internet Service Providers. This is because a conduit transports the information, but does not access it. No disclosure is intended by the covered entity and there is low likelihood of disclosure of PHI in these situations.

What about the landlord or the cleaning service? They have access to the office where we keep PHI.

It is unnecessary to have a BAA with the cleaning service because they are not contracted to perform services involving use or disclosure of PHI. However, you need to have reasonable safeguards in place to protect PHI. Ideally, you should store paper PHI in a locked cabinet.

Do I have to have a BAA with _____? She's been doing our accounting for years, but she isn't an employee.

It is common to overlook a business associate who has been working in your organization for a long period of time. However, if an independent contractor is providing services such as accounting or anything that involves PHI, then you must have a BAA in place.

Hopefully, your practice has BAA's at the top of your priority list this month. If you don't have appropriate BAA's in place, your procrastination could be expensive. Every time a BA accesses your patients' information without the proper agreement, your practice is potentially exposed to very large fines.

HIPAA Breach: To Be Or Not To Be?

Under HIPAA, a breach is any impermissible use or disclosure of PHI that does not fit into one of the following exceptions (45 C.F.R. §164.402):

- Unintentional access, use, or acquisition of PHI by an employee of covered entity or BA made in good faith and would not result in further use or disclosure;
- Inadvertent disclosure from one authorized person to another authorized person;
- Disclosure where the covered entity or BA has a good faith belief that the unauthorized person who received the PHI would not likely retain the information;
- Low probability of compromise as determined by a risk assessment of the following factors:
  - Nature and extent of PHI involved including likelihood of re-identification;
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether PHI actually was acquired or viewed;

– The extent to which risk to PHI has been mitigated.

The Risks of Unsecure PHI

The Office of Civil Rights (OCR) provides guidance for keeping PHI secure. In the event there is a breach of unsecured PHI, the covered entity is required to follow the Breach Notification Protocol. Therefore, it is critical for providers to take the appropriate safeguards for securing PHI. Below is a list of examples of unsecure PHI that increases risk of a HIPAA breach:

- Lost or stolen laptops, desktop computers, tablets, and other devices containing unsecure PHI
- Discussing patient information in public areas
- Leaving patient files in public areas
- Leaving a computer unattended in an accessible area with unsecured PHI
- Employees that inappropriately access patient information
- Sending patient information to the wrong patient
- Discussing patient information with friends, family or co-workers
- Improperly disposing of patient records
- Texting or emailing unsecure PHI
- Posting photos or information regarding patients on social media sites
- Releasing unauthorized PHI due to incomplete or invalid HIPAA forms
- Failure to adhere to expiration dates specific on HIPAA forms
- Impermissibly disclosing PHI in response to a subpoena that does not meet the requirements of the Privacy Rule
- Being the victim of a cyber attack that compromises PHI

Unfortunately, cyber attacks are on the rise. Utilizing ransom ware and phishing scams, hackers are able to victimize those with encryption, password protection, and/ or a VPN. A couple of recent breaches such as MedStar in DC and Hollywood Hospital in LA resulted in taking EHRs offline, resuming paper processes and subsequently disrupting and delaying patient care.

The Security Official has determined a breach has occurred, now what?

The covered entity is required to notify the affected individuals of any unauthorized access, use, disclosure or acquisition without reasonable delay in writing within 60 days after discovery of breach (some states within 30 days).

If a breach of unsecure PHI is determined to have occurred:

- Notify affected individuals in writing without unreasonable delay and no longer than 60 days from discovery and post on covered entity's website
  - If ≥500 affected individuals notify HHS at same time as notification of individuals
  - If <500 affected individuals notify HHS within 60 days of Calender year end

- Notify media if >500 residents affected from one location (state, county, city)

The Notice to affected individuals should contain the following:

- Description of Breach
- PHI involved
- Steps taken to investigate, mitigate harm and prevent further breaches
- How to protect themselves from any possible harm as a result of the breach

What is the Wall of Shame?

As part of HITECH, any breach of over 500 individuals will be posted on "The Wall of Shame" on the Department of Health and Human Services website. It is important for covered entities to be aware of the necessary steps to avoid joining this list and to become familiar with the HITECH Breach Notification Protocol in the case of a breach.

Headlines of credit card security breaches at Target, Home Depot, Kmart, Ebay and JP Morgan Chase are all too common these days. A wake up call to all health care facilities arrived with the recent hacking incident into Community Health Systems' network. An increase in the black market value placed on stolen credit card information and social security numbers associated with PHI makes it even more important to assess potential threats and vulnerabilities in a healthcare organization.

Healthcare entities have enhanced visibility of privacy and security breaches due to the HHS "Wall of Shame." To avoid joining this list, continually monitor your organization for vulnerabilities and threats and mitigate any potential risks to PHI to prevent avoidable breaches.

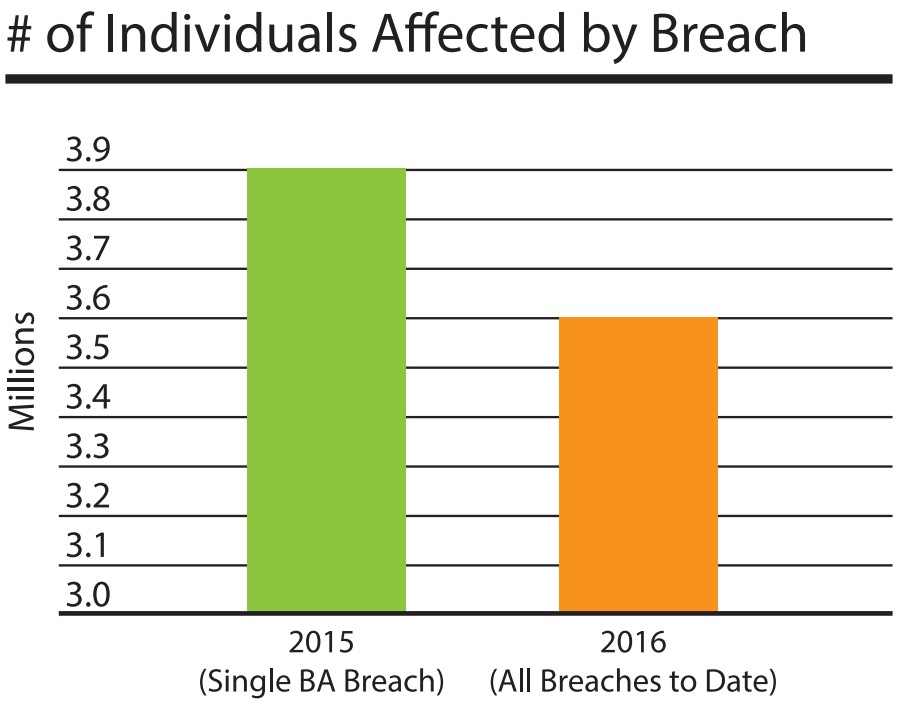
Don't Be Unprepared for a Breach by a Business Associate

Covered entities should be very concerned about the possibility of a major breach of PHI originating from a BA. According to the HHS' Wall of Shame, a single breach in 2015 by a BA in Indiana affected more than 3.9 million individuals which is more than all individuals affected by breaches from covered entities and BAs listed to date in 2016.

The covered entity is ultimately responsible for the Breach Notification protocol, but this can be the BA's responsibility if part of the BA Agreement. A recent $750,000 settlement for a HIPAA violation by an orthopedic practice demonstrates the need to have BA Agreements in place prior to disclosing PHI to a BA.

Last year's breach by a BA occurred as a result of hackers gaining unauthorized access into an EHR, compromising PHI at 44 locations in 3 states. This may seem small compared to the largest breach ever reported, the Anthem breach in 2014 affecting over 80 million individuals. Similarly, this incident was the result of a cyber attack on a server such that the full extent of this breach remains under investigation and the actual numbers are still yet to be determined.

What if Anthem had been a large EHR provider instead of a covered entity? Let's not find out. To this end, healthcare providers need to be ready for any size cyber security incident and this should be reflected in your BAA. The April 2016 OCR Cyber-Awareness Monthly



Update highlights important measures every covered entity should take when dealing with business associates:

- Defining in their service-level or BAA how and for what purposes PHI shall be used or disclosed in order to report to the covered entity any use of disclosure of PHI not provided for by its contract, including breaches of unsecured PHI, as well as any security incidents.
- Indicating in the service-level or BAA the time frame they expect business associates or subcontractors to report a breach, security incident, or cyber attack to the covered entity or BA, respectively.
- Identifying in the service-level or BAA the type of information that would be required by the BA or subcontractor to provide in a breach or security incident report.
- Finally, covered entities and BAs should train workforce members on incident reporting and may wish to conduct security audits and assessments to evaluate the BAs' or subcontractors' security and privacy practices. If not, e-PHI or the systems that contain e-PHI may be at significant risk.

Healthcare providers need to be ready for any size cyber security incident.

Keep in mind that not all breaches are related to hacking incidents. For this year, breaches by BAs are overwhelmingly attributed to theft and unauthorized access or disclosure. Fortunately, these types of breaches should be much easier to prevent than trying to avoid a sophisticated cyber attack. Just like covered entities, BAs must have appropriate physical, technical and administrative safeguards in place.

Our Solution:

Confidently manage compliance with the First Healthcare Compliance comprehensive compliance management solution which provides you the visibility, oversight, controls and tools to manage your organization's compliance program from the topdown and from the bottom-up. Confidently manage your risk and drive compliance with our customized, scalable cloud-based solution coupled with live support from our team of experts in healthcare compliance.

1st Healthcare® Compliance

First Healthcare Compliance

www.1sthcc.com
888.54.FIRST
3903 Centerville Road
Wilmington, DE 19807