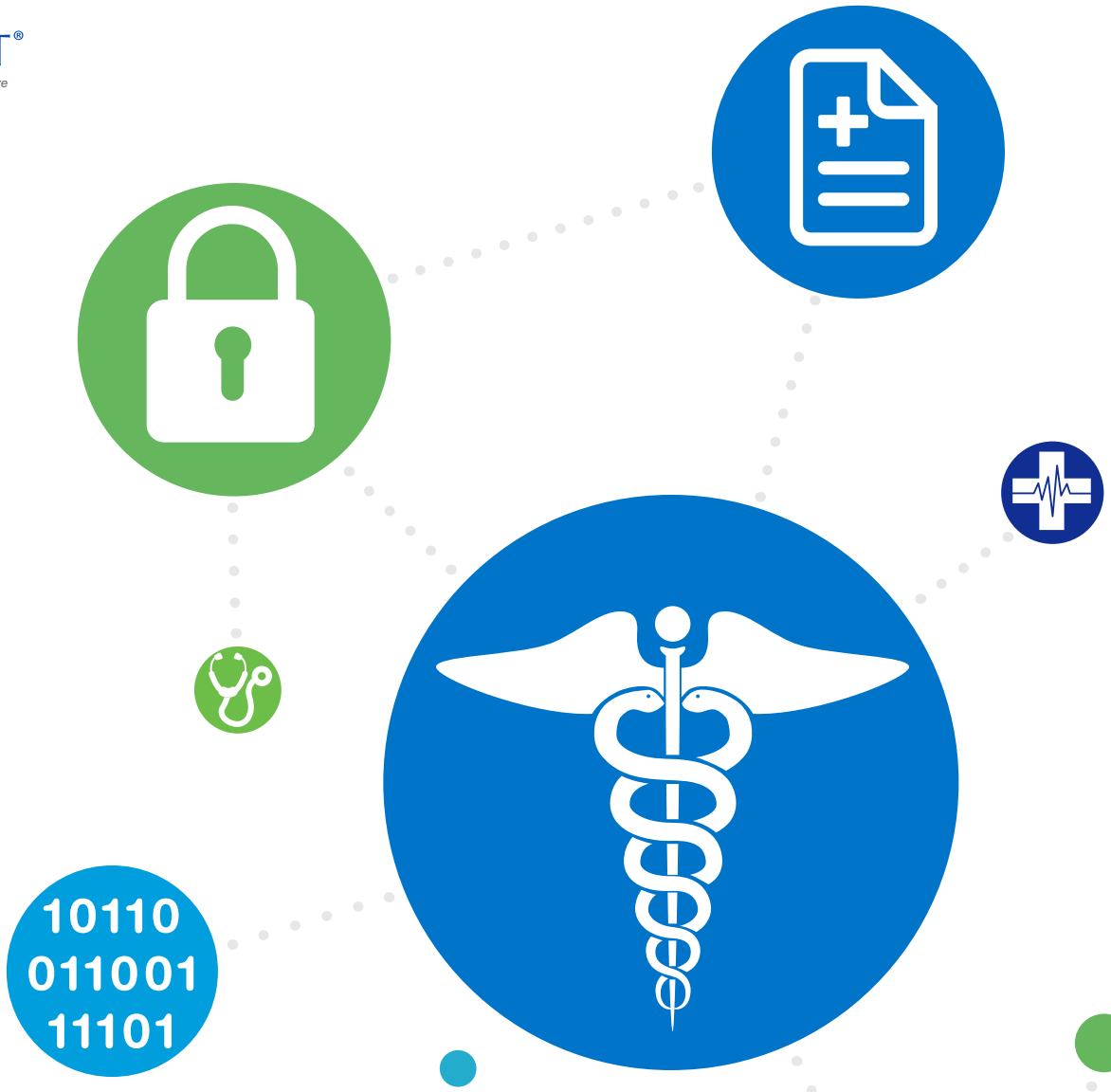
PREVALENT®
information anywhere, security everywhere



Getting the Facts **Straight** on **HIPAA** Compliance

TABLE OF CONTENTS

Getting the Facts Straight on HIPAA/HITECH Compliance

Covered Entities not only need to ensure they're protecting PHI and defending against cyber threats; they need to make sure their Business Associates are providing the same level of protection.

Since 2009, the Department of Health and Human Services (HHS) has been gradually making comprehensive modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules ("the Rules"). Despite the various deadlines (e.g. by September 22, 2014 Covered Entities must bring all their Business Associate Agreements into compliance with the Rules) and with the Office of Civil Rights (OCR) set to resume compliance audits, many hospitals, doctor's offices, and other healthcare practices are struggling to make the necessary changes.

Compounding the pressure to develop and maintain substantial controls for data security and privacy, cyber criminals are levying unprecedented attacks on Covered Entity and Business Associate networks. Research from the Ponemon Institute revealed that criminal attacks on healthcare systems have risen 100% over the past four years.[1] Another study, conducted by the Identity Theft Resource Center, found that the healthcare industry experienced more data breaches in 2013 than it ever had before, accounting for nearly 44% of all breaches and surpassing all other industries. [2]

1. Fourth Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute, March 2014
2. http://www.idtheftcenter.org/images/

Healthcare data is more valuable on the black market than credit card numbers because the data contains information that can be used to access bank accounts, or obtain prescriptions for controlled substances.

Why do cybercriminals find more value in electronic protected healthcare information (ePHI) than financial services data? According to a private industry notification from the FBI released in early 2014[3] , healthcare data is more valuable on the black market than credit card numbers because the data contains information that can be used to access bank accounts, or obtain prescriptions for controlled substances.

In this whitepaper, we'll help Covered Entities identify best practices for complying with HIPAA/HITECH rules. Additionally, we'll demonstrate how they can protect their businesses from cyber threats by assessing the company's current state of compliance and security, comparing it to best practices, and implementing a plan to bridge the gap, beginning with the most critical threats.

Defining the Key Terms You Need to Know

One of the sources of confusion among healthcare administrators, managers, and executives stems from the various terms used by governing bodies when referring to mandates and compliance issues. Before delving into this matter any further, be sure to check out the glossary below to become familiar with the common terms that will be used throughout this article:

Covered Entity. Health plans, healthcare clearinghouses, and any healthcare provider that electronically transmits PHI (protected health information) or PHR (personal health records).

Business Associate. An entity that performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. (E.g. cloud providers and other IT vendors, third party administrators, billing and collections companies, shredding companies, EHR providers, medical equipment providers, etc.)

Business Associate Agreement. A contract between a covered entity and business associate that is used to protect PHI in accordance with HIPAA guidelines.

HITECH. The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

Meaningful Use. An incentive-based program that incorporates certified electronic health record (EHR) technology to:

i. Improve quality, safety, efficiency, and reduce health disparities.

ii. Engage patients and family.

3. "FBI warns healthcare firms they are targeted by hackers," August 2014, Reuters.com

iii. Improve care coordination, and population and public health.

HIPAA Omnibus Rule. A set of final regulations modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement various provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

OCR. Office of Civil Rights. The agency that enforces HIPAA privacy and security rules.

ePHI. Electronic Protected health information is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Start Here: Develop a Risk-Based Mindset

The decision whether to focus on complying with HIPAA rules or protecting your business from data breaches may seem akin to the age-old chicken and egg debate, but it's really not. A better analogy for these seemingly unrelated issues is a coin that has "compliance" on one side and "security" on the other side. The coin in this analogy represents risk, which is what Covered Entities ultimately are trying to reduce – and more realistically manage. With that goal in mind, the solution to your compliance and security challenges starts with the following question:

What's my risk environment? To help narrow down this broad question, we can hone in on three specific areas:

1. **Devices that capture, store, and transmit ePHI.** In addition to the usual suspects: desktop PCs, laptops, tablets, and handheld devices – including smartphones – don't forget about less obvious devices such as medical equipment. MRI machines, for example, often will include built-in computers to capture information from each test performed. If so, it's important that these devices are treated just like other computing devices and that access control systems and data encryption are used to ensure data doesn't get into the wrong hands. A health insurance provider learned this lesson the hard way after it returned a leased digital copier that was later found to have ePHI from more than 400,000 current and former customers stored on it.
2. **IT networks.** In basic terms, the network is what connects computers and other devices within a facility to one another as well as to outside entities via the Internet. In the past, an IT network could be adequately protected by antivirus software, but today's sophisticated cyber threats require multiple "layers" of security that add firewall protection and proactive intrusion prevention and detection appliances that monitor for suspicious behavior such as repeated hacking attempts or employees visiting harmful websites at work.

3. **Software.** There are two types of software that can put a Covered Entity at risk. The first is unauthorized software infected with spyware that's installed on a Covered Entity's networked devices (e.g. a peer-to-peer program such as uTorrent). Another type of unauthorized software could also include a legitimate program that is installed and used outside the Covered Entity's business policies (e.g. a cloud storage and collaboration program such as Dropbox is installed by an employee without IT's knowledge or permission). The second software threat category entails legitimate applications (e.g. EHR and Microsoft Office apps) which are not regularly updated with the latest patches.

The HIPAA Omnibus Rule requires Covered Entities to ensure their Business Associates are also in compliance with industry standards and able to properly address IT risks, too.

In addition to addressing their own IT risks, Covered Entities need to be mindful of how their Business Associates address those risks as well. This category of risk is specifically addressed in the HIPAA Omnibus Rule, which defines Business Associates as subcontractors who work with Covered Entities and handle ePHI. Not only are Business Associates expected to treat ePHI with the same care as Covered Entities, the HIPAA Omnibus Rule even goes so far to say that a Covered Entity is not in compliance with the standards if it is aware of a pattern of activity or practice of the Business Associate that constitutes a breach of the contract, but the Covered Entity doesn't take reasonable steps to cure the breach or end the violation.[4] So, in addition to "minding their own businesses," The HIPAA Omnibus Rule requires Covered Entities to ensure their Business Associates are also in compliance with industry standards and able to properly address IT risks, too.

Identify Your Business Associates and Validate PHI Protection Processes

Within a large hospital or health system, there are a myriad of Business Associates. For example, there typically are various specialists such as anesthesiologists, physical therapists, neurologists, occupational therapists, and each group is a separate subcontracted company (i.e. Business Associate). In addition to those clinicians providing hands-on care for patients, there are many others that provide indirect care, which would also qualify as a Business Associate based on the HIPAA Omnibus Rule. Some examples of Business Associates that might not be readily obvious include: equipment repair companies, outsourced billing providers, medical transcription companies, and answering services.

Covered Entities now have the additional responsibilities and challenge associated with user access management, change management, and data stewardship of these Business Associates – even though some Business Associates may never visit the Covered Entity's premises.

4. HIPAA Privacy Rule, section 164.504(e)(1)(ii); www.hhs.gov

As if that weren't enough, consider this: some Business Associates subcontract work to other organizations, thereby extending Business Associate responsibility to yet another company.

To get a firm handle on these new business challenges, Covered Entities should seriously consider contracting with a third-party risk management provider that specializes in these matters.

As you might expect, the process of identifying all vendors and developing risk profiles can be a daunting undertaking for Covered Entities, which may already have been resource restrained before the HIPAA/HITECH rules went into effect. Additionally, managing external resources requires a special skill set that's different from the skills required to manage IT infrastructures or even one's own employees. To get a firm handle on these new business challenges, Covered Entities should seriously consider contracting with a third-party risk management provider that specializes in these matters.

Conduct a Third-Party Risk Assessment

Up to this point, we've primarily focused on identifying risks. The next step is to validate potential risk points by conducting a third-party risk assessment. Through this process, a Covered Entity will:

1. Evaluate risks across multiple evidence sources and determine who is responsible for mitigating risks in each area.
2. Identify all of the Covered Entity's Business Associates and determine the type of data and systems those Business Associates can access.
3. Determine the risk associated with access to the data and systems by an outside third party, and the Covered Entity's tolerance for such risk.
4. Create a risk classification system that places a risk score for each type of risk and the necessary/required protections to mitigate that risk.
5. Create risk scoring per vendor. Apply the risk classifications determined above to each Business Associate. This practice allows Covered Entities to rank Business Associates based on system/data risk and organization importance, ensuring attention is paid to the biggest, most immediate threats first.
6. Sign Business Associate Agreements (customized for each Business Associate) only with subcontractors who demonstrate a commitment to following HIPAA/HITECH standards and immediately correct any compliance issues that are identified or may arise in the future. Those who don't demonstrate these qualities should be immediately replaced with more competent business partners.
7. Organize relevant IT and business risk information into a single repository that allows all parties (Covered Entity and Business Associates) to view assessment results and provide feedback on corrective action plans. A central repository is also helpful at enabling Covered Entities to leverage shared assessments (e.g. assessments conducted on larger Business Associates may be conducted by multiple people) and avoid information silos.

8. Schedule regular vendor risk evaluations. In addition to evaluating a Business Associate before they are provided with access to data and systems, ongoing monitoring to determine if risk controls are properly maintained is essential. This step should include assessments to ensure that ePHI confidentiality, integrity, and availability remains intact.

What to Do When a Breach Occurs

Even the best security and compliance strategies aren't 100 percent "fool" proof. After all, despite good intentions, humans make mistakes from time to time and at some point a mistake will occur with your PHI (e.g. during a network scan a firewall port is discovered to be open). Having a plan in place ahead of time will help you quickly correct the problem and minimize damage. Following are four steps to follow when addressing a suspected data breach.

Having an action plan in place before a breach strikes makes it easier for Covered Entities to adhere to the 60 day disclosure laws imposed by the HIPAA/HITECH act.

1. **Detect.** Determine whether a suspected breach actually occurred by asking the following questions:
   - Does the incident involve an acquisition, access, use, or disclosure of PHI that would not be permitted under the Privacy Rule?
   - Is the PHI unencrypted or unsecured?
   - Does the incident fall into one of the exceptions?
     - Did the PHI access occur in good faith by an employee of a Covered Entity or Business Associate within the scope of employment and the PHI is not further accessed, used, or disclosed?
     - Inadvertent disclosure by an authorized person within a facility operated by a Covered Entity or Business Associate, if there is no further use or disclosure.
     - Disclosure involved limited data set (e.g. without date of birth and zip code).
     - Disclosure of PHI where the Covered Entity or Business Associate has a good faith belief that the unauthorized person to whom it was disclosed would not reasonably been able to retain it.

2. **Notify all appropriate parties in a timely manner.** The HIPAA/HITECH Act requires covered entities to notify the individual(s) affected by the breach within 60 days as well as the OCR, and in some circumstances the media (e.g. if the breach affects more than 500 individuals in the same state or jurisdiction) concerning breaches involving unsecured PHI. It's also important to note here that most states have their own breach notification laws, which may include additional requirements beyond those defined by the HIPAA/HITECH Act.
3. **Investigate.** After being notified, the OCR will conduct an investigation into the matter. Covered Entities are required to cooperate by being responsive and providing relevant documents and other information.

4. **Remediate.** Respond quickly and cooperating with investigators, providing documentation to demonstrate how the problem was remediated is very important. In addition to addressing a technology fix (e.g. implementing a more robust firewall) or human resources issue (e.g. terminated a negligent employee or contractor), it's important to show additional steps put into place to provide added protection (e.g. the firewall is being managed by a HIPAA-certified security company) and education (e.g. re-trained employees and contractors in the department about procedures for handling PHI).

Just because a security breach hasn't happened to your organization isn't a good reason to skip the advice outlined above. The OCR has indicated that it will be conducting audits and enforcing HIPAA privacy and security rules shortly and if there's one trend that's been made clear it's this: pleading ignorance or waiting until a problem happens to develop PHI security policies and procedures only compounds the matter – and the fines.

Another mistake is focusing on compliance alone, which entails meeting only the minimum requirements defined in the HIPAA/HITECH Act and HIPAA Omnibus Rules. The best rule of thumb is to face privacy rules and security threats head on by adopting a risk-based business culture. This approach not only enables Covered Entities to proactively combat the myriad of threats that face their businesses, but it allows them to experience the true benefits Meaningful Use was really intended for, which is providing patients with better care through the use of technology.

About Prevalent, Inc.

Prevalent is an industry-leading vendor risk and cyber threat intelligence innovator.

Since 2004, Prevalent has worked diligently with leaders in information security, compliance, and risk management to develop solutions that are proven to help organizations reduce, manage and monitor the security threats and risks associated with third-party business relationships. This close collaboration has led to the development of award-winning technologies, enabling Prevalent to create value for their customers.

Follow us on Facebook, Twitter and LinkedIn.

Prevalent meets the need of its customers by developing cloud-delivered, managed services based on industry-leading technology. This service is hosted in Prevalent's cloud environment and administered by their knowledgeable and experienced staff. The result is reduced time to value, reduced infrastructure requirements, dramatic reduction in operational cost, and increased security and compliance readiness.

Today, Prevalent remains the leading innovator in the third-party risk management and monitoring market, creating powerful software and service solutions like Prevalent Vendor Risk Manager and Prevalent Vendor Threat Monitor, while delivering compliance and risk solutions in the cloud via Prevalent Compliance as a Service (PCaaS).