The Truth about HIPAA-HITECH and Data Backup

Author: Bob Chaput, MA, CISSP, CIPP/US, CHP, CHSS
CEO and Founder • Clearwater Compliance, LLC

Date: October 29, 2012

The HIPAA Security Final Rule, the last of the three HIPAA rules, was published in the February 2003 Federal Register, with an effective date of April 21, 2003. Most covered entities (CEs), which include health plans, healthcare providers and health clearinghouses, had two full years (April 21, 2005) to comply with the standards within the rule. A majority of covered entities, especially providers, did not comply by that date and are not in compliance now.

Up until the 2010, HIPAA compliance has not been strictly enforced, which means very few covered entities have paid a price for non-compliance. The HITECH Act, which was enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, has changed everything. It is the largest and most consequential expansion and change to the federal privacy and security rules **ever**. Roughly fifteen change areas comprise new federal privacy and security provisions that have major financial, operational and legal consequences for all hospitals, medical practices and health plans. Notably, as of February 2010, *these same rules apply to covered entities' business associates – and even some vendors and service providers that were not previous considered business associates.* However, many business associates remain unaware of their obligation for full compliance with the regulations.

HITECH Act – Three Historic Changes

The HITECH Act has made three historic changes to the HIPAA Privacy and Security Rules.

1. The HITECH Act has significantly increased enforcement of the rules.
2. Organizations found non-compliant can be required to pay higher penalties and non-compliance fines return to HHS to fund even more enforcement.
3. The HIPAA Privacy and Security Rules now include business associates – and *soon* their agents and subcontractors.

Business Associates: A Primer

A business associate is an organization or individual who is not a member of a covered entity workforce yet performs certain functions or activities involving the use or disclosure of individually identifiable health information. Some example functions include:

- Quality assurance
- Utilization review
- Billing
- Practice management
- Data analysis, processing or administration
- Claims processing or administration
- Benefit management
- Re-pricing

Business associates provide services to or for a covered entity. Examples of services include:

- Legal
- Accounting
- Administrative
- Financial Services
- Data Aggregation
- Management
- Consulting
- Billing
- Actuarial
- Software-as-a-Service (SaaS)
- Accreditation

Business associates are statutorily obligated to comply with all applicable provisions of all HIPAA Rules and the HITECH Act. ***This obligation, therefore, includes the Standards and Specifications related to Contingency Planning, Data Backup and Disaster Recovery.*** Covered entities have explicit requirements to ensure that business associates who create, receive, maintain or transmit PHI for which the CE is responsible comply with the Privacy, Security and Breach Notification Rules. Beyond the laws and regulations, the ultimate legal liability for safeguarding the PHI rests in the hands of the covered entity. They cannot outsource responsibility.

HIPAA Rules | Privacy Rule | Security Rule

What's the general purpose for each of these rules?

- HIPAA requires organizations to protect the privacy and safeguard the security of patient information.
- The Privacy Rule covers all the Protected Health Information (PHI).
- The Security Rule protects electronic PHI (ePHI) whether it is stored in a computer or printed from a computer. The Security Rule was designed to protect the confidentiality, integrity, and availability of ePHI.

Standards and Specifications

The Security Rule is comprehensive, including 22 Standards defining what safeguards organizations must implement and 50+ implementation specifications that describe how organizations must implement them. In other instances, the Rule provides no guidance for how organizations must implement the standards.

A standard is a provision of the Security Rule with which all CEs and now BAs must comply, specifically with respect to ePHI. There are no exceptions. The HITECH Act has not changed the number of standards; however, more explicit guidance and clarity is provided in many areas of the Security Rule and the Privacy Rule. As required by the HITECH Act, HHS has issued guidance that states *there are two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction*. The guidance goes on to cite processes for encrypting *data in motion* and *data at rest*.

Myths versus Facts

The majority of organizational leaders responsible for both CEs and BAs are uninformed on how the HITECH Act has strengthened the privacy and security rules. The following table contains some commonly held beliefs that are actually myths. They are untrue. Within the table, the column on the right contains the facts.

MYTH	FACT
Our EMR runs in an ASP environment that is HIPAA compliant, so we're fine.	Environments cannot be HIPAA compliant. Only organizations can become compliant through a comprehensive process.
Our XZY Product is HIPAA compliant.	No product is HIPAA compliant. Organizations can only become compliant through a comprehensive process.
The HITECH Act doesn't change HIPAA; it just pushes electronic medical records.	The HITECH Act has significantly strengthened the HIPAA Rules in three specific ways: rule enforcement, penalties for non-compliance and the inclusion of business associates.
We're good. We've had all our patients sign that privacy paperwork.	That's not enough. The rules also include safeguarding patient information and much more. Non-compliant organizations will face penalties.
It doesn't apply to my small medical practice.	It applies to **ALL** covered entities – even solo practitioners.
It's only an *addressable* specification, it's not required. And we have chosen not to address it.	Addressable does not mean optional. The standards must be implemented. **No exceptions.**
Business Associates have to comply only as they did before.	Business associates are subject to the same standards as covered entities.
Installing an EMR doesn't change what we do in our office.	Installing EMR means you **must** comply with the Security Rule to protect the confidentiality, integrity, and availability of ePHI.
It's too complicated to enforce. They'll never come after my practice.	HHS / OCR has investigated and resolved nearly 18,000 cases (as of 9/2012). **Private practices** are the MOST COMMON among covered entities required to take corrective action.
Enforcement is only for covered entities. BAs just follow the contract.	Business associates are subject to the SAME standards as covered entities.

Contingency Plan Standard Language

The Contingency Plan Standard at 45 CFR 164.208(a)(7) is not a technical safeguard – it is a critically important business risk management matter, meaning a Board and C-suite issue. It is so much more than an IT problem.

This Standard is very explicit about, among other risk management actions, backing up ePHI and ensuring its recoverability in the event of a data loss event, disclosure or corruption. Like almost all others, this standard has implementation specifications, which are *required* or *addressable*. **Addressable does not mean optional.**
The exact wording in the Rule is as follows:

§ 164.308 Administrative Safeguards.

(7) *Standard:*

(i) *Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures (Addressable).* Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis (Addressable).* Assess the relative criticality of specific applications and data in support of other contingency plan components.

Putting it Together: Understanding what's needed for compliance with the HIPAA-HITECH rules and data backup involves three key factors: (1) reviewing the explicit language in the rule (2) understanding the other key parts of the HIPAA Security Final Rule and (3) adding clarification provided by the HITECH Act and the ensuing HHS guidance.

The Top Ten Truths about HIPAA-HITECH and Data Backup

1. **It's not optional.** All covered entities, including medical practices and business associates must securely backup *retrievable exact copies of electronic protected health information.* (45 CFR 164.308(7)(ii) (A))
2. **Your data must be recoverable.** You must be able to fully *to restore any loss of data.* (45 CFR 164.308(7)(ii) (B))
3. **You must get your data offsite.** This is **common sense risk management** and required by the HIPAA Security Final Rule (45 CFR 164.308(a)(1)). It is not possible to defend a data backup/disaster recovery plan that stored backup copies of ePHI in the same location as the original data.
4. **You must back up your data frequently.** Again, this is **common sense risk management**, as required by the HIPAA Security Final Rule (45 CFR 164.308(a)(1)). In today's real time transactional world, a server crash, database corruption or data erasure by a disgruntled employee at 4:40 p.m. would result in a significant data loss event if one had to recover from yesterday's data backup.
5. **Safeguards must continue in recovery mode.** The same set of security requirements that apply under normal business operations must also apply during emergency mode. (45 CFR 164.308(7)(ii) (C))
6. **Encrypt or Destroy.** HITECH says encrypt or destroy data at rest. (Section 13402(h) of Title XIII HITECH Act) HIPAA Security Rule says encrypt data in transmission. (45 CFR 164.312(e)(1)(B)) Many covered entities and business associates fail in this area because tape or disk-based backups move around freely, unencrypted. If that media is lost or stolen, it will likely be a direct violation of the HIPAA Security Rule, and a growing number of state privacy laws. Depending on the number of patient records compromised, it will also trigger the Breach Notification Rule of

HITECH. The Breach rule requires patient notification and may require notification to HHS and the local media. The business reputation risk is far greater than the compliance risk, and the latter is no longer trivial.

7. **You must have written procedures related to your data backup and recovery plan.** Policies and procedures (45 CFR 164.312(b)(1)) and documentation (45 CFR 164.312(b)(2)(i)) are an integral part of the HIPAA Security Final Rule.
8. **You must test your recovery.** Backup is useless if your recovery fails, therefore the law requires that you *"Implement procedures for periodic testing and revision of contingency plans."* (45 CFR 164.308(7)(ii) (D)). Unfortunately, testing tape-based or disk-based recovery can be time-consuming, and most companies rarely do it.
9. **Non-compliance penalties are severe.** Penalties are significantly increased in the new-tiered Civil Monetary Penalty (CMP) System with a maximum penalty of $1.5 million for all violations of an identical provision.
10. **Now is the time to act.** Covered entities have been subject to the HIPAA Security Final Rule since April 2005. As of February 2010, business associates are statutorily obligated to comply.

Last Line of Defense

Clearwater Compliance's position is that having a rock-solid data backup and recovery solution in place may serve as a last line of defense for many covered entities and business associates striving to be compliant with the laws. Losing data is one matter; not having *exact retrievable copies* as required by law is another. The ultimate embarrassment may be, however, trying to explain a data breach event in a court of law. Especially when a covered entity or business associate has no way to notify affected individuals since they have no record of who the individuals are… **because a back up copy of ePHI does not exist.**

Choose Your Service Provider Carefully

Recently passed state privacy legislation (including the Nevada statute and Massachusetts Regulation passed in 2010 and Texas House Bill 300 in 2011), is trend setting in many ways, including their instructions for choosing service providers.

The Massachusetts law states that companies must take *all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information"* in compliance with the regulation. Companies must also *take all reasonable steps to ensure that such third-party service providers are applying to such personal information protective security measures at least as stringent as those* required by the regulation. In other words, Massachusetts puts a premium on careful selection of reputable vendors. Smart organizations will do the same.

About the Author

Bob Chaput, MA, CISSP, CIPP/US, CHP, CHSS, is CEO and Founder of Clearwater Compliance, LLC. Clearwater Compliance helps covered entities and business associates meet stringent HIPAA-HITECH Security Rule requirements and address one of five health outcomes policy priorities in the Meaningful Use Stage 1 guidelines dealing with privacy and security. Having served on operational and technology assignments in large healthcare enterprises, Mr. Chaput is an expert in protecting large amounts of healthcare data. His experience includes senior executive positions responsible for the privacy and security of some of the world's largest healthcare databases, including GE, Johnson & Johnson and Healthways, Inc.

Chaput has also built, grown and sold a number of businesses serving industries with strict regulatory requirements. He speaks and writes extensively on HIPAA-HITECH security matters and is nationally recognized HIPAA-HITECH data security expert. Chaput holds undergraduate and graduate degrees in mathematics, numerous technical certifications and is a Certified Information Systems Security Professional (CISSP), Certified Information Privacy Professional (CIPP/US), Certified HIPAA Professional (CHP) and a Certified HIPAA Security Specialist (CHSS).