

A White Paper for ...

Health Care Professionals, Covered Entity Execs and Business Associate Execs

By [Bob Chaput](#), MA, CISSP, CHP, CHSS

The Truth about HIPAA-HITECH and Data Backup

Executive Summary

As a healthcare executive, business owner and a service provider, few things irritate me more than ill-informed vendors, often HIPAA Business Associates, running around making assertions about regulatory or legal requirements that are simply not true and/or making assertions about their products and services being HIPAA -compliant when it is flat out wrong to assert that.

Many of these crazy assertions are reappearing around the HIPAA Security Final Rule and what is serving as its “after-burners”, The HITECH ACT. To be clear, there is no such thing as a HIPAA-compliant data center or a HIPAA-compliant server or a HIPAA-compliant data backup product or a HIPAA-compliant EMR software product or a HIPAA-compliant online data backup and recovery service. Only organizations become HIPAA-compliant through comprehensive processes. These organizations include Covered Entities (CEs) and Business Associates (BAs). BAs are now statutorily obligated to comply with all relevant sections of the HIPAA Privacy Final Rule, the HIPAA Security Final Rule and the HITECH Breach Notification (Interim) Final Rule. The HITECH Act “teeth” put into the HIPAA Rules.

This White Paper sets the record straight on a very specific aspect of the HIPAA Security Final Rule – the Data Backup and Disaster Recovery Implementation Specifications within the Contingency Plan Standard. We separate myth from reality about what exactly is required of whom, and by what dates CEs and BAs must comply with these Specifications.

Introduction – A Perfect Storm

We’ve written on the ‘perfect storm’ that is brewing in healthcare driven by, among other factors:

- Near-frantic EMR adoption pace
- Federal Government’s redoubled efforts to rigorously enforce the [HIPAA Security Rule](#)
- New Federal and state level enforcement and penalty “teeth” delivered via [The HITECH Act](#)
- General national concerns over the protection of personal information
- Major Transactions and Code Set conversions (4010-5010/ICD9-10)
- Absence of appropriate skills to get the EMR/EHR implementation job done well
- Lack of skills in and understanding of information security and data protection
- Historical behavior of ignoring the HIPAA Security Final

... as if, with national healthcare reform, there weren’t enough clouds on the horizon!

A recent study completed by the University College of London’s Department of Open Learning and published in The Milbank Quarterly concluded that:

"Depressingly, outside the world of the carefully-controlled trial, between 50 and 80 percent of electronic health record (EHR) projects fail--and the larger the project, the more likely it is to fail..."

Most medical practices and other smaller CEs and BAs have little or no skills, knowledge and experience when it comes to information technology in general and software projects with information security implications, in particular. Even in larger organizations, information security budgets lag greatly behind application development, business intelligence, networking and computing infrastructure and other IT line items. The Data Backup and Disaster Recovery Specifications are about information security. In a nutshell, information security is about ensuring three attributes of information or data: Confidentiality, Integrity and Availability. Remember CIA and you've got it!

HIPAA Security Rule and The HITECH Act

The HIPAA Security Final Rule, the last of the three HIPAA Rules, was published in the February 20, 2003 Federal Register with an effective date of April 21, 2003. Most CEs had two full years -- until April 21, 2005 -- to comply with these standards. A majority of covered entities, especially providers, did not comply by that date and are still non-compliant. Now BAs must comply fully with these laws as well.

However, since HIPAA compliance historically has not been enforced, very few CEs have paid a price for non-compliance. This has led to a widespread "false sense of security" which the perfect storm in healthcare and HITECH Act are about to shatter.

The HITECH Act, which was enacted as part of the ARRA of 2009, significantly modified and strengthened many aspects of the HIPAA Privacy and Security Rules, including the penalties that the U.S. Department of Health and Human Services (HHS) could impose for violations of the HIPAA Rules.

There are three absolute "game changers" under HITECH: 1) significant increases in enforcement; 2) higher penalties and non-compliance fines returning to HHS' coffers for even more enforcement; and 3) the much wider net being cast to include BAs and their Agents and Subcontractors.

In general, 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 covered by the Rule must implement and 50+ Implementation Specifications that describe how the standards must be implemented. The documentation requirements for the Security Rule are daunting. In fact, there are two separate Standards in the Rule covering policies and procedures (CFR 164.312(b)(1)) and documentation (CFR 164.312(b)(2)(i)). In some cases, no guidance is provided for how the standards must be implemented.

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. With HITECH, the number of Standards has not changed; however, more explicit guidance and clarity is provided in many areas of the Security Rule and the Privacy Rule as well.

One of the more “famous” examples of this guidance is around encryption. 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 and Mistruths about HIPAA Changes Specific to The HITECH Act

With the issuance of changes under the HITECH Act, as part of ARRA, it’s still surprising to hear the following circulating around:

- *“Our EMR runs in an ASP environment that is HIPAA-compliant, so we’re fine.”*
- *“Our XYZ product is HIPAA-compliant.”*
- *“The HITECH Act doesn’t change HIPAA Security, it just pushes electronic medical records.”*
- *“We’re good – we have all our patients sign that Privacy paperwork.”*
- *“It doesn’t apply to my small medical practice.”*
- *“It’s only an ‘addressable’ Specification, not required and we’ve chosen not to address it”*
- *“Business Associates have to comply only as they did before.”*
- *“Installing the EMR doesn’t change what we do in our office.”*
- *“It’s too complicated to enforce; they’ll never come after my practice.”*
- *“Enforcement is only for Covered Entities; BAs just follow the contract.”*

**ABSOLUTELY
INCORRECT !!**

Unfortunately, for the ill-informed and misspoken above, The HITECH Act 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 will have major financial, operational and legal consequences for all hospitals, medical practices, health plans, and now their BAs and some vendors and service providers that were not previously considered BAs.

Quick Refresh: Business Associates

A business associate (BA) is an organization or individual who is not a member of a CE workforce yet performs certain functions or activities involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing. BAs provide services such as legal, actuarial, accounting, consulting, data aggregation, billing, management, transcription, software-as-a-service, administrative, accreditation, or financial services to or for a covered entity.

BAs, again, 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.

CEs have explicit requirements to ensure that BAs 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 CE. CEs cannot outsource responsibility.

Let's Look at the Exact Language of the Contingency Plan Standard

It is important to note that the Contingency Plan Standard at 45 CFR 164.208(a)(7) is not a Technical safeguard; this underscores the importance of contingency planning as an important business risk management matter and not simply an "IT problem." It's a boardroom, C-suite 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*. Remember, addressable does not mean "optional."

The exact wording in the Rule is:

§ 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.

From the above explicit language, other parts of The HIPAA Security Final Rule and clarification provided by The HITECH Act and ensuing HHS guidance, one can derive "the truth" about data backup and recovery requirements. We do so in the next section.

The Truth, then, and Nothing But the Truth about HIPAA-HITECH and Data Backup

1. It's not optional -- all CEs, including medical practices and BAs must securely backup “*retrievable exact copies of electronic protected health information.*” (45 CFR 164.308(7)(ii) (A))
2. Your data must be recoverable – well, duh!, why else are you backing it up? 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 – **call it common sense or risk management**, as required by the HIPAA Security Final Rule (45 CFR 164.308(a)(1)), how could one defend a data backup / disaster recovery plan that stored backup copies of ePHI in the same location as the original data store?
4. You must back up your data frequently – again, call it common sense or 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 erasure of data by a disgruntled employee at 4:40pm 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 – CEs and BAs cannot let their guard down. (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 transmissions. (45 CFR 164.312(e)(1)(B)) Many CEs and BAs fail in this area because tape- or disk-based backups are moved around freely, unencrypted. Unfortunately, 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 and may require notification to patients (always required) and, in addition, notification to HHS and local media as well. 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 a huge 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 increased significantly 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 – CEs have been subject to the HIPAA Security Final Rule since April 2005. BAs are now statutorily obligated to comply by February 2010.

Last Line of Defense

We believe that having a rock-solid data backup and recovery solution in place may serve as a last line of defense for many CEs and BAs 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 in a court of law following a data breach event that one has no way to notify affected individuals because one has no idea who they are... **because there is no back up copy.**

Choose Your Service Provider Carefully

Recently passed state privacy legislation (including the Nevada statute, which is effective January 1, 2010, and the Massachusetts Regulation, which is effective, March 1, 2010) is trend setting in many ways including their prescription for choosing service providers.

The Massachusetts law states that you 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, and you must *“take all reasonable steps to ensure that such third party service provider is 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. We agree and we can help you!

Disclaimer:

This discussion and its references are not legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance.



About the Author: Bob Chaput, MA, CISSP, CHP, CHSS

Mr. Chaput 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 no stranger to protecting large amounts of healthcare data – his experience includes responsibility for some of the world’s largest healthcare databases, requiring the highest levels of security and privacy while a senior executive at GE, Johnson & Johnson and Healthways, Inc.

Over the years he has also built, grown and sold a number of businesses serving industries with strict regulatory requirements, with deep experience in HIPAA and HITECH rules. He speaks and writes extensively on HIPAA and HITECH security matters and is a recognized HIPAA-HITECH data security expert. His 30-year career includes 25 years of responsibility in regulated industries, with 20 of those years spanning the highly security- and privacy-regulated healthcare industry. He holds undergraduate and graduate degrees in mathematics, numerous technical certifications and is a Certified Information Systems Security Professional (CISSP), Certified HIPAA Professional (CHP) and a Certified HIPAA Security Specialist (CHSS).

bob.chaput@ClearwaterCompliance.com

(800) 704-3394

Follow Bob on Twitter: twitter.com/AboutHIPAA



Are you still betting your healthcare business on a data backup system that **fails 50% of the time?**

In fact, 77% of the respondents to a recent *Storage Magazine* survey found their homegrown tape- or disk-based recoveries failed while testing their backup. Don't bet your healthcare businesses' or medical practice's future on those odds.

Get a Jump On HIPAA Security Rule and HITECH Compliance.

Many sections of the Final Rule cite data protection. Section 106.308(a)(7), Contingency Plan, specifically calls for data protection.

“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.” Two key REQUIRED standards call for a “Data Backup Plan” and a “Disaster Recovery Plan”. Data Mountain, a leading provider of digital data backup solutions for healthcare organizations, can provide secure, automated “set and forget” solutions that provide exact, readily retrievable copies of ePHI that will help you meet these required HIPAA and HITECH standards. **Our solutions help both CEs and BAs.**



Eliminate Tape and Disk Gymnastics = Eliminate Risk.

With the **LiveVault Online Backup Service** you can eliminate business risk and the daily hassle of homegrown tape and disk backup solutions. The LiveVault Service will continuously backup your critical server data, archive it securely at two off-site data centers, and make it immediately available for recovery 24 hours a day.

Best of all, it's completely automated and online, so you never touch those unreliable tapes or disks again!

Explore Hassle-Free Data Backup.

Learn more about our hassle-free online data backup and recovery services by calling us today at **(800) 704-3394**. Or visit our data backup services web site, www.DataMountain.com.