VCPI

White Paper

The HITECH Act:

Protect Patients and Your Reputation

By: Donna Maassen
Director of Compliance, and Privacy & Security Officer
Extendicare Health Services, Inc.

Table of Contents

Ignorance no longer an excuse

A 2008 study by Dartmouth College showed that compromised data was often found in unprotected spreadsheets and Word documents, suggesting that many organizations are not adequately protecting data. In many cases, the entities leaking data were not even aware of the fact.

Executive Summary

On November 30, 2009, a series of regulations associated with enhancements to HIPAA enforcement called the Health Information Technology for Economic and Clinical Health (HITECH) Act took effect. These new guidelines address the privacy and security concerns associated with Protected Health Information (PHI), and extend the Privacy and Security Provisions of HIPAA to business associates of covered entities. Other significant changes include new breach notification and mandatory audit requirements. On February 22, 2010, the government began imposing penalties for noncompliance with Breach Notification Standards.

So, what does this mean for providers of post-acute care? Providers are required to report breaches, but if they don't understand the process, there is risk it won't happen properly or at all. The complexity of the new regulations can pose challenges, so a business and IT service provider that is prepared to help achieve regulatory compliance and drive higher quality care is a must.

This paper will highlight what you need to know as well as how you can protect yourself and those for whom you provide care.

The Bottom Line:

Your reputation is at stake: ***one stolen unencrypted laptop containing protected health information (PHI) constitutes a breach***, forcing you to publically disclose the breach to patients, potentially on your website, and the mass media.

What It Means:

The new guidelines for HIPAA compliance are complex and include enforcement that all providers must understand and practice in order to remain compliant. Providers must raise their awareness of privacy protection and doing so means taking all precautions necessary to prepare for potential breaches **before** they occur.

The Takeaway:

The benefits of working with a professional business and IT service provider with solid security controls in place, and policies and procedures to protect sensitive information are too significant to ignore. Your reputation depends on it!

What is a Breach?

Breach Does Not Include:

- Unintentional acquisition, access or use of Protected Health Information (PHI) by an employee or business associate if:
  - Made in good faith during scope of authority
  - Information is not further used and disclosed in a manner not permitted by law
- Inadvertent disclosures between authorized employees
- Disclosure to unauthorized person who is unlikely to retain information

The HITECH Act defines a breach as "the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

In order to determine whether a breach has occurred, covered entities and business associates must conduct a *risk assessment* to determine if there is a significant risk of harm to the patient as a result of an impermissible use or disclosure. HIPAA defines a business associate as a person other than a member of the covered entity's workforce or entity that performs a function using or disclosing PHI.[1] This includes the performance of financial, legal, actuarial, accounting, consulting, data aggregation, management, administrative or accreditation services to or for a covered entity. A covered entity may also be a business associate of another covered entity.

Examples of Breach

A breach can be difficult to determine, so below are some examples of actions that may result in a privacy breach.

- Employee "sneak peeks" patient files/documentation
- Email message containing PHI routed to the wrong recipient
- Fax containing PHI routed to the wrong recipient
- Posting of patient information on a social networking site
- Discovery of paper PHI by an unauthorized person
- Theft or loss of unencrypted electronic device

[1] HITECH Act of 2009, Pub. 160.103 of title 45, Code of Federal Regulations (2009).

Notification of a Breach

On September 23, 2009, the Department of Health and Human Services began enforcing a Final Rule that spells out what you must do when a breach occurs.

If the breach involves under 500 patients, you must:

- Notify all individuals in writing that a breach of Protected Health Information has occurred
- Notify the Department of Health and Human Services on an annual basis

If the breach involves over 500 patients, you must promptly notify the following that a breach has occurred:

- All affected individuals in writing
- The media, including a list of the state(s) in which the affected patients reside
- The Department of Health and Human Services within 60 days

Financial Risk

The HITECH Act defines the level of violation and financial penalties of noncompliance with breach notification standards as follows:[2]

	Instances where your organization…	**Fine per violation**	**Cumulative maximum per calendar year**
Tier A	didn't realize that it violated the act and would have acted differently had it known	$100	$25,000
Tier B	violated the act with reasonable cause, but not 'willful neglect'	$1,000	$100,000
Tier C	demonstrated willful neglect that your organization corrected	$10,000	$250,000
Tier D	demonstrated willful neglect that your organization did not correct	$50,000	$1,500,000

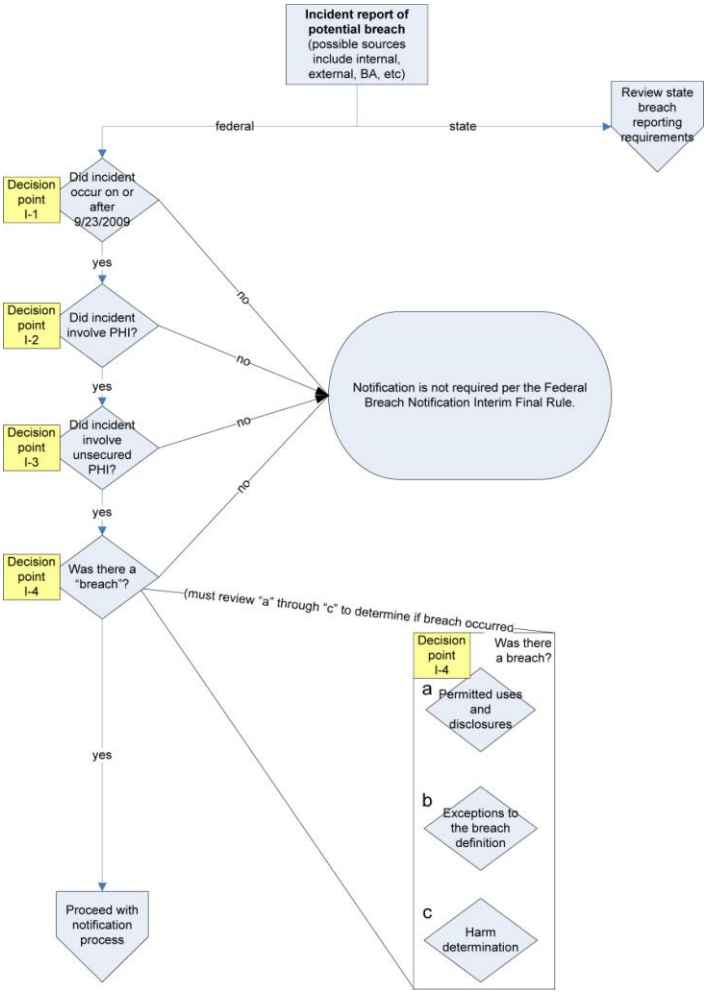
In addition to these fines, states' attorneys general can initiate a legal action on behalf of any harmed citizen of the state.

[2] http://www.hcpro.com/HIM-229707-866/HIPAA-and-the-HITECH-Act-Know-the-level-of-penalties.html

Decision Tree

If a breach occurs it must be reported. The following chart helps determine if a reported incident involves a breach of PHI, which requires notification of the affected patients and what method of notification is required under the federal breach regulation.[3]

LTCC Unsecured PHI Federal Breach Reporting Decision Tree



[3] Long-Term Care Consortium, *Federal Breach Notification Decision Tree and Tools*. http://www.ahcancal.org/facility_operations/hipaa/Documents/Breach%20Reporting%20Decision%20Tree.pdf (November 2009). See full text for explanations of each decision point I-1 through I-4 above.

The Risk is Real

It only takes a misrouted email, and/or unauthorized access or loss of a laptop to compromise the security of confidential patient information.

Electronic Tools = Security Risk

Perhaps the biggest security risk for any provider is electronic media and tools. According to an article published by Computerworld, "Nearly eight months after new rules were enacted requiring stronger protection of health care information, organizations are still leaking such data on file-sharing networks," a study by Dartmouth College's Tuck School of Business found.[4] The study attributes this finding to the easy accessibility of sensitive health information on peer to peer networks.

It only takes a misrouted email, and/or unauthorized access or loss of a laptop to compromise the security of confidential patient information. There are a number of steps that can be followed to make sure all business laptops are secure and personal information is kept private. Both email communications and laptops can be encrypted. Internet monitoring and filtering will also strengthen privacy measures. Electronic role-based access controls enable a provider to control access to resources within a computer based information system and is of prime importance when working with confidential information.

[4] Vijayan, Jaikumar. "P2P Networks a Treasure Trove of Leaked Health Care Data, Study Finds." *Computerworld.com.* 17 May 2010. Web. 27 May 2010.

Protect Your Reputation

"If providers take steps to properly encrypt desktops and laptops they may be able to take advantage of the 'safe harbor' provision within the regulation."

Dan Jackson, Senior Security Engineer, VCPI

13 Tips

1) Assign a HIPAA Compliance Officer if you don't have one already, who is trained and well-versed with HIPAA, compliance, and the HITECH Act.
2) Incorporate the Breach Notification Standards into your existing HIPAA compliance program.
3) Take an inventory of all assets on which PHI resides. Be sure to include items like USB drives, portable devices (PDAs, cell phones, etc.), and all other mobile media devices.
4) Take an inventory of all roles and people who share PHI in various forms: paper, email, text messages, verbally, fax, etc.
5) Reduce the number of roles, people, and assets requiring PHI to a bare minimum.
6) Assign people to roles and create an electronic means of limiting access to PHI by these roles.
7) Ban text messaging involving PHI.
8) Make training a requirement of continued employment. Conduct training, track completion, and refresh training on a regular basis.
9) Encrypt portable devices and create a monitoring and maintenance program.
10) Create and enforce processes that prevent PHI from leaving your organization.
11) If an employee is taking backup tapes offsite to his or her house, that's a major risk. Ban the practice and contract with an encrypted, business-class service provider who is well versed in PHI.
12) Update your business associate agreements and educate them regularly.
13) Audit assets and document compliance regularly.

Navigating the System

There is no question that keeping patients' PHI secure is a key responsibility for any provider. Your reputation depends on it. The patient is any provider's most valuable asset and protecting them is a vital part of a successful operation. It is also an immense job that most providers can't tackle alone. Using a professional business and IT provider to help navigate the complexity of HIPAA guidelines will help you plan for success.

About the Author

Donna Maassen is the Director of Compliance, and Privacy & Security Officer for Extendicare Health Services, Inc. She has worked with Extendicare for more than 25 years and is an active participant in a collaborative long term care group called the Long Term Care Consortium (LTCC). The LTCC collaborates to reduce the compliance burden through sharing of ideas, tools and various resources. Ms. Maassen holds a CHC (Certified in Health Care Compliance) credential through HCCA.

About VCPI

Headquartered in Milwaukee, WI, VCPI helps clients solve business challenges with technology and beyond…without a staff. For more than 1900 communities across the U.S., VCPI takes care of technology, enabling clients to focus on taking care of patients. VCPI was founded in 2000 as a wholly-owned subsidiary of Extendicare REIT, one of the largest operators of long-term care, home health and assisted living communities in the U.S. and Canada.

Phone: 877.908.VCPI
Fax: 414.908.7393
Email: marketing@vcpi.com

www.VCPI.com

Special Thanks

Special thanks are due to the Long Term Care Consortium (LTCC) for providing data to make this paper possible.