The Compliance Newsletter

HIPAA + HITECH ACT

Compliance facts and updates for today's providers and their business associates

The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), signed into law on February 17, 2009, as part of the American Recovery and Reinvestment Act (ARRA or "stimulus act"), reshapes the regulation of the privacy and security of patient health information. The HITECH Act does this by imposing new privacy and security requirements under, and significantly altering key concepts and foundations of, the Health Information Portability and Accountability Act ("HIPAA").

One of the most significant changes is the regulation of business associates under HIPAA. Before the HITECH Act, the HIPAA privacy and security requirements applied only indirectly to business associates. Any privacy or security requirements were made applicable to business associates only through a Business Associate Agreement ("BAA") created between a covered entity and a business associate. Effective February 17, 2010, pursuant to the HITECH Act, many of the HIPAA standards were extended to apply directly to Business Associates.

The law now applies the same civil and criminal penalties to Business Associates that have always applied to Covered Entities. Business Associate Agreements (BAA) are also required for any person or entity that provides support to a Covered Entity (CE).

Calendar of Educational Events

October 18, 2012

Planning for compliance in 2013
Dulles,VA ($25)

October 25, 2012

HIPAA-HITECH Data Backup and Security in 2013

Leesburg,VA ($25)

November 1, 2012

Planning for compliance in 2013

Reston,VA ($25)

November 8, 2012

HIPAA-HITECH Data Backup and Security in 2013

Reston,VA ($25)

November 15, 2012

Planning for compliance in 2013

Frederick, MD ($25)

November 29, 2012

HIPAA-HITECH Data Backup and Security in 2013

Frederick, MD ($25)

Space is limited. Register today

www.TheComplianceDoctors.com

Or Call BeckITSystems, Inc.

(703) 433-0730

Myths and Facts about the HIPAA Security Risk Analysis

POPULAR MYTH	HIPAA-HTECH FACT
The Security Risk Assessment is optional for organizations.	Any organization that stores electronic health information is considered a "covered entity" under HIPAA. As such, they are required to perform a risk analysis.
Installing a certified EMR/EHR fulfills the security risk analysis requirement	Even with a certified EHR, you must perform a full security risk analysis. Security requirements address ALL electronic protected health information, not just what is in your EHR.
My EHR vendor took care of privacy and security.	EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security rules. It is solely your responsibility to have a complete risk analysis.
I must outsource the security risk analysis.	Small organizations can do the risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to compliance review will require expert knowledge that may be obtained through the services of an experienced outside professional.
A checklist will suffice for the risk analysis.	Checklists fall short of performing a systematic security risk analysis or documenting that one has been performed.
There is a specific method that I must follow.	A risk analysis can be performed in countless ways. The OCR assists organizations in identifying and implementing the most effective and appropriate safeguards.
The risk analysis only needs to look at the EHR.	ALL electronic devices that store electronic health protected information must be reviewed (mobile phones, copiers, tablet computers, USB drives, etc.)
I only need to do a risk analysis once.	To comply with HIPAA, you must continue to review, correct, or modify, and update security protections. This is typically an annual review.
I have to completely redo the analysis each year.	Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice occur, review and update the prior analysis for changes in risk.

THE HIPAA-HITECH AUDIT PROTOCOL

The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules that represent the separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the types of covered entity selected for review.

The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures. The protocol covers Security Rule requirements for administrative, physical, and technical safeguards. Contact The Compliance Doctors for a copy of the performance criteria for an audit.

Health Information Privacy Basics

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Learn more about which entities must comply with the Privacy and Security Rules, the requirements of the rules, and guidance available to help covered entities implement and maintain compliance with these requirements. (http://tinyurl.com/ComplianceDoctors)

Under License to BeckITSystems, Inc.

"Hey Doc, the Chief says posting pictures of your patients on your social media wall may be unethical and violates their privacy."

About The Contributors

ED BECKER - M.ED., M.A.

With over 35 years of operational and technology leadership in Information Technology for healthcare, government, and private industry. Ed writes and speaks on IT and HIPAA-HITECH compliance and security matters.

KIM BRADLEY - BSN, R.N.

With over 20 years of health care experience coupled with over 10 years of expertise in operational Health Information Technology and compliance practices, Kim presents a unique breadth and depth of expertise in HIPAA-HITECH compliance and IT operations.

THE COMPLIANCE DOCTORS

can help your organization achieve compliance with HIPAA and HITECH, create required documentation, and train your compliance officer.

HIPAA-HITECH Compliance Services:

- Virtual Compliance Officer (VCO)
- Onsite or Remote HIPAA Security Risk Analysis
- Assist the Security Official to develop and implement policies
- HIPAA Frameworks
- Emergency Mode Operations
- Data protection, & Encryption
- HIPAA Policies & Procedures
- HIPAA Security Officer Training
- Risk Management Plan
- Business Associate Agreements
- Security Breach Framework
- HIPAA/HITECH Staff Training Programs
- EMR/EHR Installation, support, security, and management

FOR COVERED ENTITIES

HEALTH CARE PROVIDERS & BUSINESS ASSOCIATES

The Privacy and Security Rules apply only to covered entities. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If an entity is not a covered entity, it does not have to comply with the Privacy Rule or the Security Rule.

This rule includes providers such as:

- **Doctors**
- **Urgent Care Centers**
- **Clinics**
- **Psychologists**
- **Physical Therapists**
- **Dentists**
- **Chiropractors**
- **Nursing Homes**
- **Pharmacies**

...and applies to these entities as they transmit personal health information in an electronic form in connection with a transaction for which HHS has adopted a standard.

Your 2012 Q4 HIPAA Newsletter has arrived!

BeckITSystems Inc.
The Compliance Doctors
22570 Markey Court #200
Dulles,VA 20166
(703) 433-0730

The HIPAA "Wall of Shame"

As required by section 13402(e)(4) of the HITECH Act, the Secretary of HHS must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers and Business Associates who have needed to report breaches of unsecured protected health information to the Secretary. See the current list at

http://1.usa.gov/Q5cku5