



HITECH for IT

What you **<now>** need to know..

A brief history..

- **2009 HITECH act** is part of the **larger** stimulus act (ARRA).
- HITECH def. (Health Information Technology for Economic and Clinical Health)
- HITECH made several changes to the HIPAA Privacy rules and applies to all “covered entities” – generally those practicing healthcare or related to healthcare.
- Applies as well to “**Business Associates**” of covered entities...**and their subcontractors.**

What the Government is Investing:

- As part of the ARRA stimulus package, the government is investing \$20 billion in Health IT infrastructure and Medicare and Medicaid incentives to encourage doctors and hospitals to use the HITECH Act to electronically exchange patient health information.
- With more electronic records comes more PHI (Protected Health Information) that needs...well.. protection!
- 2009 - \$197/per record breach cost, up to \$202 in 2010.

Aspects of HITECH:

- Breach Notifications
- E-discovery
- Business Associates
- Penalties
- “Certified Solutions” – defined
- “Meaningful use” – defined

Breach Notifications:

- Became effective Sept 23rd, 2009 – but no penalties enforced until Feb 22nd, 2010.

A – Breach – unauthorized access, use or acquisition or disclosure of PHI.

B – The PHI is considered “unsecured” – anytime PHI is not rendered unusable.

C – The breach “compromises the security of the PHI”.

A breach occurs when there is a significant risk of financial, reputational, or other harm to an individual.

New Security Provisions

- The Act includes new security provisions including:
- A. Requirement to notify patients and HHS of PHI (Protected Health Information) security breaches
- B. New HIPAA regulations regarding business partners (PHRs, HIEs) and enforcement of penalties
- C. Restrictions on the sale and marketing of PHI
- D. Ensuring that patients have access to their electronic health information
- E. Accounting of disclosures of PHI to patients
- In short, the privacy restrictions will be more stringent; with more stringent patient access and notification requirements should any breaches in security occur.

How to Secure PHI?

- HHS specified 2 guidelines to render PHI unusable:
 - **Encryption** – only secured where it has been encrypted.
 - Encryption must meet the NIST FIP 140-2 Standard. Technically, 128 bit cipher algorithm's may be feasible.
 - Encryption must comply with the HIPAA Security Rule which states CE's must implement 3 types of safeguards: Administrative, Technical, and Physical.
 - Encryption applies to the process of transferring the information from one system to another.
 - Encryption – HITECH is more interested in "data in transit" than in "data at rest".
 - **Destruction** – paper or film media is only secured where it has been shredded or destroyed such that the PHI cannot be read or otherwise be reconstructed.

Has a breach occurred?

- (1) Determine whether the use or disclosure of PHI (not just any data) violates the HIPAA Privacy Rule.
- (2) Analyze whether there is a use or disclosure that compromises the security and privacy of PHI – means “CE’s” and “BA’s” will need to conduct a risk assessment to determine this!
- (3) Assess whether any exceptions to the Breach Definition apply.

Breach Notification Requirements

- Triggered by the “discovery” of the breach of unsecured PHI.
- Notify individuals – the covered entity must send notice, within 60 days after the discovered breach occurred.
 - ** If the CE has insufficient contact information for 10 or more people, then a substitute notice must be provided via a posting for 90 days on their “home page”, OR conspicuous notice in major print or broadcast media. Also, a toll-free number must be active for 90 days.

- Notification to Media – if a CE discovers a breach affecting more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets without “unreasonable delay”, and in no case, later than 60 days after the date the breach was discovered.

- Notification to HHS – if more than 500 individuals are involved in the breach, then the CE must notify HHS concurrently with the individual notifications.
- For fewer than 500, the CE must maintain an internal log and annually submit such log to HHS.

Breaches by a Business Associate

- Following the discovery of a breach of unsecured PHI, a business associate is required to notify the CE of the breach so that the CE, can, in turn, notify the individuals.
- To the extent possible, the BA has the responsibility of identifying each individual whose unsecured PHI has been breached.

Encryption – the “Safe Harbor”

- Proper encryption provides a “safe harbor” from breach reporting.
- By undergoing such procedures of securing PHI, covered entities or businesses are hereby free from the notification procedure in cases when encrypted PHIs are compromised.

Enter ZIX...one of every seven hospitals use ZIXCORP for email encryption.

Two ZIX customers enjoy seamless encrypted communication.

How to PREVENT a breach:

- THE BEST way is to increase user awareness of the risks and provide proper, repetitive and timely training!!
- ?? Would THIS be a good enough reason to do social network background employee checks?

The Penalties have increased

- First, HITECH expanded regulator's ability to impose criminal penalties for violating HIPAA.
- Second, the civil penalties that can be imposed were dramatically increased. **Ex.** A \$25,000 fine maximum per year in the previous HIPAA rule now permits up to \$1.5 Million for identical violations within the same year.
- Third, HITECH has eliminated certain defenses – no longer can parties avoid penalties by claiming they did not have actual knowledge of the violation.

E-Discovery and a lot less paper...

- In 2003, only 0.01 percent of *newly created* information was stored in paper format, with the newest information created in electronic format.
 - In 2009, digitally-stored data now totals 487 billion gigabytes world wide.
- ** This is the equivalent of 19 billion fully packed Blu-ray DVD's!

When “data” is more than data..

- Electronically Stored Information (ESI) – in a simple answer is “any information stored in an electronic format”.
- **However..**ESI also includes “metadata” – a set of data that describes and gives information about other data.

Other Legal Considerations:

- All electronic sources must be considered to hold potentially relevant, discoverable information.
- Zubulake v. UBS Warburg – addressed the scope of a Legal parties obligations to their client. The court found the defense counsel partly to blame for the underlying document destruction because they had failed in their duty to preserve and produce in timely fashion, the requested information.

Other Legal Considerations, cont..

- Attorneys should become familiar with CE's clinical systems and their capabilities!
- The court ordered that the attorneys are required to take “affirmative steps” to monitor compliance of their CD's clients.
- Attorneys should ensure that their healthcare clients have appropriate records retention and destruction policies in place.

Certified or “Qualified” Solutions

- Must be able to: have user identification recorded when electronic health information is created, modified, deleted, or printed; and an indication of which action(s) occurred must also be recorded.
- Such a solution is not simply one document – but *the culmination of all documents accumulated* from multiple office visits and hospitalizations over time.

Certified Solutions, continued..

- Patients must be able to obtain and view a copy of their medical records *in an electronic format, either that can be given to them at dismissal, or sent to them or a third party, at their request.*
- Incentives BEGIN in January 2011, with CE's needed to have at least a 3-month "attestation" period in 2011 for "Phase 1" meaningful use.
- Penalties and reduced payments begin in 2015.
- Certified solutions must have integrated triggers for "clinical decision support rules" and be able to track, record, and report on the number of alerts responded to by a provider.

“The Vision of Meaningful Use”

- Engage healthcare patients in a proactive way.
- Provide real-time access for patient data.
- Eliminate long waits and health care disparities.
- Use *new information technology* for open communication and timely treatment.
- Use tools (by practitioners and support staff) that will increase the safety and quality of medical care.

“Phases” of “Meaningful Use”

- Stage I – Electronic capture of health information in a coded format; tracking key clinical conditions and communicating outcomes for care coordinating; implementing clinical decision support tools to facilitate disease and medication management; and reporting outcomes for public health purposes.
- Stage II – Expands on stage I. Encourages the use of health IT to enhance computerized provider order entry; transitions in care; electronic transmission of diagnostic test results; and, research.
- Stage III – Expands on stage II. Promotes improvements to quality and safety; focuses on clinical decision support at a national level by encouraging patient access and involvement; and, improved population health data.

“Phase 1 Meaningful Use”

- Requires health care providers to collect data and integrate the data into an electronic format, which can be stored in one location, but shared by multiple health care providers.

2011 Goals - For Providers:

- Use CPOE for orders (at least 80% of orders)
- Implement drug-drug, drug-allergy, drug-formulary checks
- Maintain an up to date problem list of current and active diagnoses based on ICD-9 codes
- Generate and transmit prescriptions electronically (eRx)
- Maintain active medication list
- Record demographics: language, gender, race, insurance carrier, etc.
- Record advance directives

2011 Goals for Providers, cont.

- Record vital signs
- Record smoking status
- Incorporate lab-test results into qualified system as structured data
- Generate lists of patients by specific conditions for use with quality improvement and outreach
- Document progress notes with each encounter
- Check insurance eligibility electronically
- Submit claims electronically to public and private payers

2011 Goal for Hospitals

- Many are the same, but with some differences:
- 10% of all orders entered directly by provider(s).
- Implement one clinical decision rule related to a “high priority” hospital condition.
- Provide access to patient-specific education resources.
- Provide patients with an electronic copy of their discharge instructions, upon request or send to them, or named third-party.
- Must implement 5 clinical decision support rules relevant to clinical quality metrics.
- Certified EHR technology that includes 25 measures; 17 measures require attestation by the provider; eight require information submitted by the provider.

End Analysis..

- What's coming to the Healthcare sector can be expected to expand to other industries!
- It's never been more important for IT to be aware and involved in the procedures and policies.
- What priority is given to privacy and security in your organization?
- Like "cloud computing" the shift is for more specialized technologies to be sourced OUTSIDE the company's IT department while internal IT members increase their roles in business intelligence, goals and support of core functions.