HIPAA, HITECH & Meaningful Use

October 21, 2011

presented by

Helen Oscislawski, Esq.

Attorneys at
Oscislawski LLC

Overview - *What Has Changed?*

HITECH Act:

- **Increased Penalties** for non-compliance, effective 11/30/2009
- New federal requirements for **reporting Breaches** of health information
- Numerous **amendments to HIPAA**
- 2/17/2012 - Individuals will be able to **get % of CMPs** collected

Increasing Enforcement

- 2/17/2009 - **State Attorneys General** can enforce HIPAA & HITECH
- 2/17/2010 – HHS required to conduct ***periodic audits*** for compliance
- 2/17/2011 - Civil Monetary Penalties (CMPs) **MUST** be pursued by OCR for **willful neglect** of HIPAA/HITECH!!!

Meaningful Use:

- **EMR adoption**
- Electronic Health Information Exchange (HIE)

Civil Monetary Penalties

Type of Violation	Minimum CMPs**
Person/entity ***did not know*** (but by exercising reasonable diligence ***would have known***) of the HIPAA/HITECH violation	**Per violation** of a requirement – **$100** Annual maximum – **$25,000** {*these were former statutory maximums*}
HIPAA/HITECH violation due to ***reasonable cause***, but not willful neglect of the person/entity	**Per violation** of a requirement – $1,000 Annual maximum – $100,000
HIPAA/HITECH violation due to ***willful neglect***, but the violation is corrected within specified time period	**Per violation** of a requirement – $10,000 Annual maximum – $250,000
HIPAA/HITECH violation due to ***willful neglect***, and violation is not corrected	**Per violation** of a requirement – **$50,000** Annual maximum – **$1.5 million**

****Maximum CMP** for all categories: $50,000/violation, up to 1.5 Million annual

Enforcement Developments

- Office of Civil Rights (OCR), which now enforces both the HIPAA Privacy and Security rules, is asking for an increase of **$5.6 million in its Fiscal Year 2012** budget proposal, mostly to adhere to HIPAA compliance and enforcement.

- Nearly half **($2.283 million)** is needed because of **OCR's requirement to hire "regional privacy officers"** who offer guidance and education to covered entities, business associates, and individuals regarding HIPAA privacy & security.

- OCR requesting another **$1.335 million** to **help investigate HITECH breach** reports.
  - As of September, 30, 2010, OCR has received a total of **9,300 breach reports** -- 191 impact more than 500 individuals and 9,109 impact fewer than 500 individuals.
  - OCR says it needs help investigating the small breaches.
  - "Based on OCR's current HIPAA case load, almost all breach reports that impact [fewer] than 500 individuals are not investigated," OCR writes.

Enforcement Developments

- **Enforcement of the HIPAA Security Rule ($1 million).** Helps support OCR's new delegated authority for the administration and enforcement of HIPAA Security Rule.

- **Compliance review program ($1 million).** Supports OCR's establishment of a compliance review program designed to evaluate, educate, and ensure compliance within a sample of the expanded covered programs and providers each year**. OCR anticipates that FY 2012 will be the starting point for a steady increase in civil rights complaints requiring investigation and compliance reviews.**

- **OCR's periodic audits program** has yet to be released. The last update came last May when OCR announced it had hired an outside firm, **Booz Allen Hamilton**, to help build its HITECH-required HIPAA auditing plan. OCR told HealthLeaders Media it was "presently engaged in a contract to survey and recommend strategies for implementing the HITECH audit requirement.

- An "educational series" for Attorney Generals took place several weeks ago. Training of AG on when and how they can prosecute for HIPAA violations.

- RECENT ENFORCEMENT ACTIVITIES HAVE INCREASED!

Attorneys General

If State AG has reason to believe that an interest of ***one or more*** of the residents of that State has been or is threatened or adversely affected by any person/entity who/that violates a provision HIPAA/HITECH, the State AG may bring a civil action (*on behalf of such residents*) in district court to:

(1) ***enjoin*** further such violation by the defendant; and/or

(2) to ***obtain damages*** on behalf of such residents of the State

- OCR has to be given right to intervene
- In a successful action, court may award the State ***attorneys fees***!
- Penalties pursued by state AGs ***limited*** **to "old" $100 per violation** up to $25,000 annually for repeat violations of same provision

…… it can still add up!

Enforcement by Federal OCR/CMS

- Massachusetts General: **$1 Million** Resolution (2/14/11)
- Cignet Health Maryland: **$4.3 Million** CMP (2/4/11)
- MSO: **$35,000** Resolution (12/13/10)
- Rite Aid Corporation: **$1 Million** Resolution (7/27/10)
- CVS Pharmacy, Inc: **$2.25 Million** Resolution (1/16/09)
- Providence Health: **$100,000** Resolution (7/16/08)

Enforcement by State Attorneys General

- April 2010, **California AG** convicts & incarcerates individual for misdimeanor counts of HIPAA violations. Fine of $2000, 4 months prison, 1 year probation.
- July 20, 2009, **Arkansas AG** convicts 3 people for violating HIPAA. 1 year probation, $5000 fine and $25 special assessment.
- August 2004, **Washington AG** convicts and sentences person to 16 months in prison.
- January 2010, **Connecticut AG** sue for violation of 446, 000 enrollees PHI, and files lawsuit to prevent further HIPAA violation by compelling encryption.
- December 2008, **Arkansas AG** convicts individual who is sentenced to 2 years probation and 100 hours of community service.

Individuals Convicted for HIPAA Violations

April 27, 2010. **Dr. Huping Zhou**, a licensed cardiothoracic surgeon in China, was employed in **2003 at UCLA Healthcare System** as a researcher with the UCLA School of Medicine. On October 29, 2003, Zhou received a notice of intent to dismiss him from UCLA Healthcare for job performance reasons unrelated to his illegal access of medical records. **That night, Zhou, without any legal or medical reason, accessed and read his immediate supervisor's medical records and those of other co-workers. For the next three weeks, Zhou's continued his illegal accessing of patient records and expanded his illegal conduct to include confidential health records belonging to various celebrities.** According to court documents, Zhou accessed the UCLA patient records system **323 times during the three-week period**. In his plea agreement, Zhou admitted that he obtained and read private patient health and medical information and acknowledged that he had **no legitimate reason, medical or otherwise, for obtaining the personal information.** Defendant was ordered to pay to the United States a special assessment of **$100 dollars** and pay a fine of **$2,000 dollars**, to be paid in full within 90 days of sentencing. The Defendant was ordered to be **imprisoned** for a term of **4 months on each count of violating HIPAA,** to be served concurrently! Upon release from imprisonment the defendant was orderd to be placed on supervised release for a term of 1 year.

HITECH Changes

HITECH Amendments to HIPAA

- Amends HIPAA Privacy, Security and Enforcement Rules
- Applies to Covered Entities and Business Associates, in most cases
- Affects Uses and Disclosures of Protected Health Information (PHI) for:
  - Business Associates
  - Accounting of Disclosures
  - Minimum Necessary
  - Marketing
  - Fundraising
  - "Sale" of PHI
  - Notice of Privacy Practices
  - Restrictions on Uses/Disclosures where paid in full "out of pocket"
  - Individual Access Rights for electronic copies of certain health information

- **Notice of Proposed Rulemaking (NPRM)** issued July 14, 2010

Business Associates

- **BAs** now **independently subject to** HIPAA and HITECH.

- HITECH and NPRM explicitly include as "Business Associate":
  - **Health Information Organizations (HIOs)**
  - **Health Information Exchange Organizations (HIEOs or HIEs)** and
  - **Regional Health Information Organizations (RHIOs)**

- **Revise Business Associate Agreements** (BAAs) necessary.

Accounting of Disclosures through EMRs

- **HIPAA - Accounting of Disclosures (AOD)** within **six (6) years** from date of request. Disclosures for **treatment, payment and health care operations (TPO)** exempted.
- **HITECH requires AOD for ALL disclosures, including TPO IF**
  - Disclosure was made through an **EHR** and
  - Within previous (3) years.
- Covered Entities can either:
  - **Provide AOD, including those made by BAs**; OR
  - **Provide list with contact information of BAs.**

Accounting of Disclosures through EMRs

- **Effective Date:**
  - **Effective 1/1/2014** if EHR adopted before 1/1/2009
  - **Effective 1/1/2011** if EHR adopted on/after 1/1/2009

- **BUT!!!**
  - The NPRM explicitly **does not address AOD**s
  - Public comment solicited by HHS as to:
    - the **benefits** of AODs for individuals;
    - the **burden** for covered entities and BAs;
    - the **elements** that should be included in an AOD.

Minimum Necessary

- HIPAA - **only the minimum amount of PHI necessary to accomplish intended purpose of use/disclosure/request.**
- HITECH - Covered Entities and BAs must limit use/disclosure/request to **limited data sets** OR if not feasible, to **minimum amount of PHI necessary** to accomplish use/disclosure/request.
  - Minimum Necessary **policies and procedures** to dictate determinations **until guidance issued** from Secretary of HHS.
  - **BUT!!! No guidance in NPRM.** Public comment solicited as to how to determine the minimum necessary for purposes of complying with Privacy Rule.

Marketing

- **HIPAA** - **valid written authorization** for **"marketing" communications** where PHI was used/disclosed.
  - **Covered Entities** prohibited from **selling PHI** for such purposes.
  - **Covered Entities permitted to receive money** from outside entity WITHOUT OBTAINING AUTHORIZATION only where:
    - Communication describes products/services offered as part of a health benefit plan or "value added" services for plan enrollees;
    - Communication is for treatment of the patient; or
    - Communication is for case management, care coordination or to direct patients to alternative treatments, therapies, providers or settings of care (certain health care operations)
  - **<u>OR WITHOUT OBTAINING AUTHORIZATION</u>** where:
    - Face-to-face communication
    - Promotional gifts of nominal value

Marketing

- **HITECH:**
  - **Prohibits direct or indirect payment** in exchange for sending "marketing" communications UNLESS **prior written authorization is obtained.**
  - **Removes HIPAA exception** for certain health-related communications.
  - **Exception** for:
    - Communications describing **only** a drug/biologic currently being prescribed to the patient **so long as payment received is reasonable in amount.**

Marketing

- **NPRM** replaces "**direct or indirect payment"** language from HITECH with **"financial remuneration"**
  - **Financial remuneration =** "direct or indirect payment from or on behalf of a third party whose product or service is being described."
  - **Health care operations communications** where **"financial remuneration"** is received are now **marketing.**
  - Requires "**notice**" and **"opt-out"** conditions for **written treatment communications** where **financial remuneration** is received.
  - Provides additional exception from remuneration prohibition for **prescription refill reminders.**

Marketing

Key Points for Understanding "Marketing"

- **Written authorization** required **before** marketing communication sent IF financial remuneration received.
- **IF exception applies,** financial remuneration must be **"reasonable in amount."**
- IF financial remuneration received for **written treatment communications,** MUST provide:
  - **Notice** and **Right to Opt-Out** - statement in Notice of Privacy Practices that Covered Entity or its BA may send marketing communications AND that individual has right to **"opt-out"**.
  - **Disclosure of fact of remuneration** in marketing communication AND **clear and conspicuous opportunity** for individual to **"opt-out".**

Fundraising

- **HIPAA** - use/disclosure of PHI for fundraising purposes **without authorization** only where:
  - **Demographic information** or **dates of care** of individuals; and
  - Statement in **Notice of Privacy Practices** of intent to conduct fundraising; and
  - **Description in fundraising materials** how to "opt-out" of future communications.
- **HITECH** adds:
  - **"clear and conspicuous"** opportunity for individuals to opt-out of receiving future fundraising communications.
  - **No conditioning of treatment/payment** on individual's choice to receive/not receive fundraising communications.
  - Election **not to receive fundraising** = revocation of authorization.

Sale of PHI

- **HIPAA** – "sale of PHI = "marketing"
- **HITECH** separates from **definition of marketing** into **"Sale of PHI"**
  - Covered Entity or BA prohibited from receiving "direct or indirect remuneration in exchange for disclosure of PHI unless **valid authorization is obtained by Covered Entity."**
- **NPRM** requires authorization to **state that the disclosure of PHI will result in remuneration** to the Covered Entity.

Sale of PHI

- **HITECH retains HIPAA exceptions**
- **No authorization needed** where "sale of PHI" for:
  - Public health activities (NPRM adds limited data set forms)
  - Research purposes (NPRM adds limited data set forms)
  - Treatment (NPRM adds payment purposes)
  - Sale, transfer, merger or consolidation of all/part of Covered Entity
  - BA Services pursuant to valid BAA
  - Individual's request for access to his/her PHI (NPRM adds AODs)
  - Use/Disclosure required by law (NPRM only)
  - Any purpose permitted by Subpart E of HIPAA Privacy Rule (NPRM only)
  - Other purposes determined **necessary** and **appropriate** by the Secretary.

Notice of Privacy Practices

- **HIPAA** - must describe:
  - Covered Entities' uses and disclosures of PHI
  - Covered Entities' privacy responsibilities and obligations
  - Individuals' rights with regard to their PHI
- **HITECH** and **NPRM –** describe ALL uses/disclosures requiring **authorization** from the individual, including
  - Sale of PHI
  - Marketing & Fundraising
  - Disclosure of psychotherapy notes
  - Drug/alcohol rehabilitation information
  - HIV/AIDS information and other state-regulated sensitive information.

Restrictions on Uses/Disclosures

- **HIPAA** did not require Covered Entities to agree to restrictions on uses/disclosures of PHI.
- **HITECH** and **NPRM require** Covered Entities and their BAs to grant restrictions where use/disclosure of PHI:
  - for carrying out **payment/health care operations** and not otherwise required by law**;** AND
  - Restriction on the PHI would relate **solely** to health care items/services for which Covered Entity has been paid **in full and out of pocket by the individual.**
- Statement in **NPP** must notify Individuals of this right

Individual Access Rights

- **HIPAA** - access to and copies of PHI in a Designated Record Set (DRS).
- **HITECH** - includes **electronic copies** of PHI used/maintained **in EHRs** by Covered Entities and their BAs.
  - **NPRM** - all PHI used/maintained in **any electronic DRS**, **regardless** of whether part of the Covered Entity or BAs EHR.
  - **NPRM** – copy in electronic form and format **requested by the individual**, or if not readily producible, in **readable electronic form and format agreed upon by the Covered Entity and individual.**

Security Breach Notification

HHS Posts Breaches on-line

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
- HHS required to post a **list of breaches** of unsecured PHI affecting 500 or more individuals.
- Posted information includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary.

Security Breach Notification

HHS Interim Final Rule for HITECH Breach Notification

- Effective September 23, 2009
- Detailed process for analyzing when a Security Incident constitutes a reportable "Breach" triggering notice requirements.
- Enforcement delayed when rule pulled. Likely tweaking "Harm" threshold.

New Jersey Identity Theft Prevention Act (NJITPA)

- In effect since 2006
- Includes breach notification requirement

Breaches: Importance of Federal-State Law Analysis

Element	HITECH	NJITPA
Who is covered?	Covered Entities & Business Associates	Businesses & Public Entities
What Info?	"Personal Health Information"	"Personal Information"
What Medium?	Electronic, Paper & Oral	**Electronic** only!

When is a Security Incident a "Breach"?

Element	HITECH	NJITPA
"Breach" defined	▪ **Unauthorized** acquisition, access, use, disclosure i.e., violation of Privacy Rule ▪ **Unsecured** PHI. ▪ **Compromises** the security of PHI	▪ **Unauthorized** access to electronic files, media or data containing ▪ **Unsecured** PI ▪ **Compromises** the security, confidentiality or integrity of PI
Unauthorized Access	A use or disclosure in violation of the Privacy Rule	Not specifically defined
"Secured" vs. Unsecured	Unusable, unreadable, indecipherable by: – *Encryption* – *Destruction* – *Per NIST's standards*	▪ Encryption or "**any other method or technology** that renders PI unreadable or unusable." *[if not recognized under HITECH would be preempted]*
Compromises	Significant "**Risk of Harm**"	"Misuse" reasonably possible

Exceptions & Knowledge

Element	HITECH	NJITPA
Unintentional	▪ Acquisition, access or use ▪ *By* Employee or agent of CE or BA ▪ Good faith ▪ Within scope of authority ▪ No further violation of Privacy Rule	▪ "Good Faith Acquisition" by ***employee*** or ***agent*** ▪ Legitimate business purpose ▪ Not further used or disclosed
Inadvertent	▪ Disclosures ▪ ***By*** Employee or agent of CE or BA ▪ ***To*** employee/agent **at the same** CE/BA ▪ No further violation of Privacy Rule	
Retention Not Possible	▪ Disclosure to unauthorized person ▪ Good faith belief that unauthorized recipient would not be able to retain the PHI	
Knowledge	▪ Actual knowledge (including ***imputed knowledge*** of employees and agents!) ▪ *"Should've known"* with reasonable diligence	▪ Actual discovery of breach ▪ Upon notice of breach

Notice: *Who?*

Element	HITECH	NJITPA
Individual	**YES**	**YES**
HHS	**YES** Annual Log for 500 > Immediate for 500 ≤	No
Media	**YES**	No
NJ DCA	No	1000 > document and make available to NJDCA upon request
State Police	No	**YES** (must report before individual notice)
Consumer Reporting Agencies	No	**YES** **1000 ≤** must notify CRAs

Notice: *How?*

Element	HITECH	NJITPA
Timing	▪ ***No unreasonable delay*** ▪ 60 days is maximum threshold	▪ No unreasonable delay ▪ Most expedient time possible
Delay	▪ For Law Enforcement. ▪ Must receive written communication ▪No more than 30 days	▪ *Wait for law enforcement to make a determination -- **may be preempted by HITECH…***
Content	What happened; Type of PHI involved; Steps to take; What is being done to investigate & mitigate; Contact information (i.e,. toll-free number, e-mail, website or postal)	Categories of PI involved; **FTC website and toll-free number**; Steps to take; What is being done to investigate & mitigate; Contact info (i.e,. toll-free # or other)
Form	▪ U.S. Mail (or E-mail, ***only if*** agreed) ▪ Substitute notice *only if* - info **Out Of Date**; **Missing** for 10≤; or **Urgent**	▪ U.S. Mail or e-mail ▪ *Substitute notice - if cost is $250K≤ or 500,000 < persons – **preempted***

State Law

- ***Devil is in the details!***
- Security Breach tools included in Manual include:
  - Breach decision-making algorithm
  - "Model" Notice to affected individuals that satisfies HITECH and State law requirements
  - "Model" Security Breach Policy
  - Breach Log
- Other risk areas exist due to lack of understanding how **federal law and State law** are reconciled. Examples:
  - Responding to Subpoenas
  - Patient's Right to Access their own information
  - Sensitive Categories of Information (e.g., NJ HIV/AIDS statute has a Private Right of Action if a person handing HIV/AIDS information uses/discloses it improperly)

Health Information Exchange

Getting Connected

- Meaningful Use
- Hospital-based Health Information Exchanges
- ACO s - Accountable Care Organizations
- NJHIN – New Jersey Health Information Exchange

Getting Prepared

- **HIE Participation Agreements** will require compliance
- Must demonstrate **Security Gap Assessment**
- Responsible for acts of **End Users**
- **Liability** for misuse by third parties

Consequences?

Failure to meet standards could result in possible:

- Termination from participating in an HIE
- Loss of Meaningful Use payments
- Loss of business
- Penalties from OCR, or (in future) possibly from State of New Jersey

Thank you. **Any questions?**

Attorneys at Oscislawski LLC

Helen Oscislawski, Esq.
Principal, Attorneys at Oscislawski LLC
helen@oscislaw.com
609-835-0833