HIPAA/HITECH
Omnibus Final Rule

HCCA Compliance Institute
April 21, 2013

Christina Heide, JD
Senior Health Information Privacy Policy Specialist

David Holtzman, JD, CIPP/G
Senior Health Information Technology and Privacy Specialist
### Omnibus Components

<table>
<thead>
<tr>
<th>Omnibus Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• HITECH Privacy &amp; Security</strong></td>
</tr>
<tr>
<td>- Business associates (BA)</td>
</tr>
<tr>
<td>- Marketing &amp; Fundraising</td>
</tr>
<tr>
<td>- Sale of protected health information (PHI)</td>
</tr>
<tr>
<td>- Right to request restrictions</td>
</tr>
<tr>
<td>- Electronic access</td>
</tr>
<tr>
<td><strong>• HITECH Breach Notification</strong></td>
</tr>
<tr>
<td><strong>• HITECH Enforcement</strong></td>
</tr>
<tr>
<td><strong>• GINA Privacy</strong></td>
</tr>
<tr>
<td><strong>• Other Modifications</strong></td>
</tr>
<tr>
<td>- Research</td>
</tr>
<tr>
<td>- Notice of privacy practices (NPP)</td>
</tr>
<tr>
<td>- Decedents</td>
</tr>
<tr>
<td>- Student immunizations</td>
</tr>
</tbody>
</table>

### Not in Omnibus

<table>
<thead>
<tr>
<th>Not in Omnibus</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• HITECH Accounting of Disclosures Rule</strong></td>
</tr>
<tr>
<td><strong>• HITECH Distribution of Penalties/Settlements to Harmed Individuals Rule</strong></td>
</tr>
<tr>
<td><strong>• HITECH Minimum Necessary Guidance</strong></td>
</tr>
<tr>
<td><strong>• HIPAA/CLIA Patient Access to Laboratory Test Reports Rule</strong></td>
</tr>
</tbody>
</table>
Important Dates

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period to Conform BA Contracts – Up to September 22, 2014, for Qualifying Contracts

Business Associates

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; directly liable for violations
- BAs must comply with the use or disclosure limitations expressed in BA contract and those in the Privacy Rule; directly liable for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of BA are now defined as BAs
  - BA liability flows to all subcontractors
Marketing

- Communications about health-related products/services by covered entity (CE) to individuals now marketing & require authorization if paid for by third party
- Applies to receipt of financial remuneration only; does not include receipt of non-financial benefits
- Authorization must state that communication is paid for
- Authorization can be obtained to make subsidized communications generally
  - Scope of authorization need not be limited to single product/service or products/services of one third party

Marketing

- Limited exception for refill reminders (and similar communications)
  - Includes generic equivalents, adherence communications, drug delivery systems
  - Payment must be reasonably related to cost of communication
- Face to face marketing communications and promotional gifts of nominal value still permitted without authorization
Fundraising

• CE may use additional information to target fundraising communications
  – Demographic information
  – Dates of service
  – Department of service*
  – Treating physician*
  – Outcome information*
  – Health insurance status

*Newly permitted

Fundraising

• Each communication to individual must include “clear and conspicuous” opt out – no undue burden or more than nominal cost to exercise

• CE may not condition treatment or payment on individual’s decision

• CE must honor opt out (no further fundraising communications permitted)

• Flexibility provided in scope of opt out and method to opt back in permitted
Sale of PHI

• Even where disclosure is permitted, CE is prohibited from disclosing PHI (without individual authorization) in exchange for remuneration
  – Includes remuneration received directly or indirectly from recipient
  – Not limited to financial remuneration
• If authorization obtained, authorization must state that disclosure will result in remuneration

Sale of PHI

• Exceptions:
  – Treatment & payment
  – Sale of business
  – Remuneration to BA for services rendered
  – Disclosure required by law
  – Public health
  – Research, if remuneration limited to cost to prepare and transmit PHI
  – Providing access or accounting to individual
  – Any other permitted disclosure where only receive reasonable, cost-based fee to prepare and transmit PHI
Right to Request Restrictions

• CE must agree to individual’s request to restrict disclosure of PHI to health plan if:
  – PHI pertains solely to health care for which individual (or person on behalf of individual other than health plan) has paid CE in full out of pocket
  – Disclosure is not required by other law

Right to Request Restrictions

• Preamble guidance
  – Scope of restriction extends to health care item or service paid for out of pocket
  – Can’t require individual to restrict all or none of a provider’s health care items or services; however, recognize issues with bundled items or services
  – If original form of payment dishonored, must make reasonable efforts to obtain payment prior to billing health plan
  – How to address other legal requirements
Electronic Access

- If individual requests e-copy of PHI maintained electronically in designated record set, CE:
  - Must provide access in electronic form/format requested, if readily producible, otherwise in readable electronic form/format as agreed to by CE and individual

- If requested, CE must transmit copy of PHI to individual’s designee (not limited to electronic access)
  - Request must be in writing & signed
  - Must clearly identify designated person and where to send

Electronic Access

- CE may charge for:
  - Labor for copying
    - Time attributable to reviewing request and producing copy
  - Cost of electronic media
    - CD, USB drive, or similar portable media/device, if individual requests copy on portable media

- CE has 30 days (with one 30-day extension) to act on request for access
  - Provision allowing initial 60 days for off-site PHI removed
Definition of Breach

• Harm standard removed
• New standard – impermissible use/disclosure of (unsecured) PHI *presumed* to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least:
  – Nature & extent of PHI involved
  – Who received/accessed the information
  – Potential that PHI was actually acquired or viewed
  – Extent to which risk to the data has been mitigated

OCR 17

Definition of Breach

• Exceptions for inadvertent, harmless mistakes remain
• Exception for limited data sets without dates of birth & zip codes removed

OCR 18
Breach Notification

- Makes permanent the notification and other provisions of the 2009 interim final rule (IFR), with only minor changes/clarifications
  - E.g., clarifies that notification to Secretary of smaller breaches to occur within 60 days of end of calendar year in which breaches were discovered (versus occurred)

Enforcement

- Makes permanent the increased CMP amounts and tiered levels of culpability from 2009 IFR
- Clarifies “reasonable cause” tier
- Willful neglect cases do not require informal resolution
- Intentional wrongful disclosures may be subject to civil, rather than criminal, penalties
GINA

• Expressly provides that genetic information is PHI
• Prohibits the use or disclosure of genetic information for underwriting purposes by all health plans, except long-term care plans
• Terms and definitions track regulations prohibiting discrimination in health coverage based on genetic information

Research Authorizations

• Compound Authorizations
  – Single authorization form permitted for use/disclosure of PHI for conditioned & unconditioned research activities, with clear opt in for voluntary (unconditioned) component
  – Flexibility permitted on ways to differentiate components

• Future Use Authorizations
  – Permitted if authorization has adequate description such that it would be reasonable for the individual to expect his/her PHI could be used for the research

• Aligns with Common Rule informed consent requirements
Notice of Privacy Practices

- Content must now include:
  - Statements regarding sale of PHI, marketing, and other purposes that require authorization
  - Statement that individual can opt out of fundraising communications
  - Statement that CE must agree to restrict disclosure to health plan if individual pays out of pocket in full for health care service
  - Statement about individual’s right to receive breach notifications
  - For plans that underwrite, statement that genetic information may not be used for such purposes

OCR
Decedent Information & Student Immunizations

- **Decedent Information**
  - Decedent’s information is no longer PHI after 50-year period
  - CE may disclose decedent’s PHI to family members & others involved in care/payment for care of decedent prior to death, unless inconsistent with prior expressed preference

- **Student Immunizations**
  - CE may disclose proof of immunization of child to schools in States with school entry laws with oral or written agreement of parent

Guidance/Compliance Tools

- **De-identification Guidance**

- **Sample Business Associate Contract Language**
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

- **Risk Analysis Guidance**
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

- **Security for Mobile Devices (video/web)**
  http://www.healthit.gov/mobiledevices
### Guidance/Compliance Tools

**What’s in the Works**

- Fact Sheets/Q&A on New Provisions
- Breach Risk Assessment Tool
- Minimum Necessary Guidance
- Better Compliance Tools for Small Entities
- Adaptation of SAG Training for CEs
- Expanded Consumer Materials/Videos

### For More Information

www.hhs.gov/ocr/privacy/
The Data Breach Rule

- Interim Rule – since September 2009
- Omnibus Rule changes approach
- Choice of analysis until 9/23/13?
- Breach reporting will increase
- Burden of proof on Covered Entity
- Penalties are higher
Where To Start

• Omnibus Rule – New Analytical Framework
  – Harm standard removed
  – Presumption of required notification
• Security Risk Assessment in place
• Organizational perspective
• Satisfying a legal requirement
• Preparation
• Response

Security Risk Assessment

• Should already be in place
• Requires safeguards:
  – Administrative
  – Physical
  – Technical
• Required vs. Addressable “Specs”
• Assess security risks and gaps
• Adapt to your practice/entity
What You Can’t Control

• The human factor
• The IT factor & the human factor
• Can’t control the weather, but you can prepare for it
• Satisfying a legal requirement
• Cost of doing business – how can we minimize?

What You Can Control

• Knowledge
• Game plan
• Team
  – Internal
  – External
• Checklists – avoiding “mistakes”
• Practice/drill/audit
• Insurance
Knowledge - What Rules Apply

- HIPAA/HITECH is only one component
- State laws
- Other federal laws
- Contractual obligations
- Internal rules & regs

Knowledge – State Laws

- Does your state(s) have a data breach law?
- Key definitions
  - Personal information – SSN, financial, combo
  - Breach – electronic only?
  - Notice – timeframe, law enforcement, atty gen
  - Safe harbor? – HIPAA may help
- Consumer fraud
- Private cause of action?
NYS Information Security Breach & Notification Act

- NY State Entities/Persons/Businesses
  - Must disclose to NY resident when unencrypted computerized “private information” acquired w/o authorization

- Private Info = Personal information + one
  - SSN
  - Driver’s License/non-driver ID or Financial Account # with access code

NYS Information Security Breach & Notification Act

- Notice Methods
  - Written
  - Electronic (if previously consented to)
  - Telephone
    - Substitute (cost exceeds $250,000 or persons exceed 500,000 or insufficient contact info)

- Substitute Notice = email + website + media
NYS Information Security Breach & Notification Act

• Notify expediently & w/o unreasonable delay
• Delay if law enforcement requests
• Notify also:
  - State AG
  - Consumer Protection Board/Agencies
  - Office of NY Cyber Security & Critical Infrastructure Coordination

Knowledge – Other Mandates?

• State licensing laws?
  – Hospital
  – Ambulatory care facility
  – LTC
• State confidentiality laws
• Private accreditation
Knowledge – Federal Laws

• Do you operate in other realms?
  – Public company?
  – Personal Health Record vendor?
• FTC
  – Representations made/promises not kept
• Cybersecurity – Exec Order
• Pandemic & All-Hazards Preparedness Act

Knowledge – Contracts

• Commercial payor participation agreements?
• ACO agreements?
• Business Associate/Sub BA?
• Different definitions/timeframes
• Payment Card Industry – Data Security Standard
Knowledge – PCI - DSS

• Applies to entity that stores, processes or transmits credit card data
• Self-regulatory within industry
• Card association assess penalties for non-compliance
• Revoke right to process credit cards

Data Breach – What To Do

• Want to avoid needless alarm if no harm
• Want to satisfy a legal requirement
• Want to do what’s right
• Risk Factors to Consider
  – Was “no harm/no foul”
  – Now “low probability of compromised PHI”
Satisfying a Legal Requirement

- Impermissible use or disclosure of unsecured PHI
- Presumed to require notification
- Unless demonstrate low probability that PHI has been compromised
- Based on risk assessment applying at least four factors specified in the Rule

Data Breach – Four Factors

- Nature & extent of PHI involved
  - Types of identifiers
  - Likelihood of re-identification
- Who received or accessed the PHI
- Potential that the PHI was actually acquired or viewed
- Extent to which risk to the PHI has been mitigated
The Five W’s + How

• Ask & answer
  – Who?
  – What?
  – When?
  – Where?
  – Why?
  – How?
• In your security incident response plan
• In your response to a security incident

Data Breach – The 5 W’s

• What is it? (Factor 1 – Nature & Extent)
  – PHI?
  – Elements involved?
    • Financial? Identity theft at issue?
    • Clinical?
    • Sensitive? Mental health/STD/substance abuse
  – Secured or unsecured?
    • Electronic? Encrypted?
    • Paper? Destroyed?
Data Breach – The 5 W’s

• What is it?
  – Identifiers? Re-identification possible?
• What else is it?
• Do other laws apply?
  – Credit card information?
    • PCI-DSS
    • State Data Breach/Identity Theft Law
  – SSN?
    • State law

Data Breach – The 5 W’s

• Who is involved? (Factor 2 – who received or accessed)
  – Work force member?
  – Intruder?
  – Another Covered Entity?
  – Business Associate?
  – Patient?
  – Public?
  – Media?
Data Breach – The 5 W’s

• How did it happen?
  – Internal or external?
    • Minimum Necessary violation?
  – Negligent or intentional?
    • Theft?
    • Malicious?
  – Does an exception apply?
  – Retrievable?
  – Subject to forensic assessment?

Data Breach – Exceptions

• Workforce Member –
  – Unintentionally acquires
  – Within Scope of Authority
• Authorized Person-
  – Inadvertently discloses
  – To another AP within entity
• Additional requirements
  – Made in Good Faith
  – No Further Use/Disclosure
Data Breach – Exceptions

• CE discloses PHI to an Unauthorized Recipient
  &
  CE has a good faith belief the recipient would not have been able to retain the PHI

Data Breach – The 5 W’s

• Where did it happen? (Factor 2 – unauthorized person; Factor 3 – acquired or viewed)
  – Physical location?
    • CE’s premises?
    • Doctor’s car?
      • Work force member home?
  – Internal system? External system?
  – Business associate’s office/system?
Data Breach – The 5 W’s

• What can we do about it? (Factor 4 – mitigation)
  – Stop the bleeding
    • But preserve the evidence
    • Get guidance
  – Retrieve if possible
  – Obtain confirmation from recipient
  – Law enforcement?
  – Credit reporting agencies?

Data Breach – The 5 W’s

• When did it happen?
  – Reported by?
    • Work force member?
    • Patient?
    • Business associate?
  – Verified?
  – Time lapse since “knowledge”?
  – Workforce member/agent knowledge?
  – Is it still happening?
Data Breach – The 5 W’s

• After you get the call, who do you call?
  – Team members/critical roles
  – Legal counsel
    • Investigative IT consultant
    • Attorney-client privilege
  – Law enforcement?
  – Insurance carrier?
  – Your boss

Data Breach – The 5 W’s

• What evidence and how to preserve?
  – Internal IT
  – External forensics
  – Shut down/lock up/back up
Decision Time

• Is there a low probability that PHI was compromised?
• If yes – document your reasoning & decision not to notify
• If no – document your reasoning & decision to notify

Data Breach Notice – To Whom?

• Every affected individual
  – Current patients
  – Former patients
• Or their representative if:
  – Deceased
  – Minor
  – Incompetent
• HHS/The Media (in some cases)
Data Breach Notice – When?

• Promptly/without unreasonable delay
• Not more than 60 days after Discovery
• Discovery = first day CE knows/should have known
  – Workforce & agents – knowledge imputed to CE
  – BA – knowledge imputed only if your agent

Data Breach Notice – When?

• Timeframes in Special Cases
• CE Can Choose Earlier Notice:
  – If Expect Imminent Misuse
  – Alternative warning can be used
• Law Enforcement Can Delay:
  – Criminal Investigation
  – National Security
Specified in state law
Data Breach Notice – What?

• In Plain Language:
  – Dates of breach & discovery
  – Brief description of breach
  – What information involved
  – How the person can protect him/herself
  – CE’s remedial actions
  – Contact info (phone/email/postal address and/or website)

Data Breach Notice – How?

• 1st Class Mail to Last Known Address or . . .
• Email if Patient has Consented (have they?)
• If lack contact information:
  – Fewer than 10 – Use Reasonable Substitute Notice
  – More than 10 – Post Notice for 90 days w/ toll-free #
    • CE’s Website or Media
Data Breach Notice – HHS

- More than 500 persons –
  - Within 60 days of discovery
- Fewer than 500 persons –
  - Annual Electronic Report
  - Within 60 days of calendar year end
- See HHS website for form & instructions: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Data Breach Notice – HHS

- Look at the HHS reporting form
- Instructive as to what you must report
- Including safeguards in place prior to breach and actions taken in response
  - “Please indicate what protective measures were in place prior to the breach”
  - “Please describe in detail action taken following the breach”
Data Breach Notice – Media

- Only if More than 500 persons
- Prominent media outlets
  - Electronic and/or print, serving affected area
- Without unreasonable delay but no later than 60 days after discovery
- Same content as individual notice
- Know who will do this, how they will do this, and what they will say

Data Breach – Business Associates

- Subject to Data Breach Rule
- Notice is given to the CE
- Within 60 days of discovery
- BA Agreement
  - BA should be your independent contractor
  - BA should be required to give early notice of any security incident
Data Breach – Administrative

• Post-mortem each security incident
  – What worked
  – What didn’t work & why
• Fix what broke/sanctions where required
• Revise policies & process as needed
• Re-train staff
• Work with Business Associates

Enforcement Lessons

• [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html)
  – Reported breaches/type/location
  – Corrective Action Plans
Guidance & Resources

• Guidance coming from OCR
  – What “compromised” means
  – Breach notification tool

• Risk assessment/breach notification tools
  – NIST
  – Privacy organizations
  – Industry groups
  – Insurer?

Data Breach – Administrative

• Try to fit within safe harbor
  – Encrypt/Destroy

• Policies & protocols in place

• Train staff

• Document to meet burden of proof

• Log security incidents/report breaches

• Work with Business Associates
Data Breach To Do List

• Knowledge
• Update & Implement Security
• Team (Internal & External)
• Plan/Train/Document

Questions

Should you have any questions, please feel free to contact me at DSanders@DrLaw.com or call us at 800-445-0954

Thank you
The Rules...Then and Now...and How

The Final Rules: Then and Now

Important to Remember
The Big 5-0

Money talks, but we can’t

Did you Notice?

Oops

I didn’t shoot the sheriff (but I gave him a flu shot)

Roger, Copy that!

---

50 Year Protection of PHI

Restriction of Disclosures to Health Plan

Material Changes to Notice of Privacy Practice

Breach Assessment Perspective

Immunization Disclosure to School

Right to Electronic Copy of PHI

---

Frank Ruelas: frank@hipaafinalrules.com
50 Year Protection of PHI

Frank Ruelas: frank@hipaafinalrules.com
Immunization Disclosure to School

Then:
Traditional authorization of release process

Now:
Flexible approach

Frank Ruelas: frank@hipaafinalrules.com

Immunization Info Disclosure to School

Effective date “opportunity”

Frank Ruelas: frank@hipaafinalrules.com
Material Changes to Notice of Privacy Practice

Material changes trigger subsequent tasks

Frank Ruelas: frank@hipaafinalrules.com

Material Changes to Notice of Privacy Practice

May be first time NoPP Revised

Understand “next steps”

Redistribution ...or not

Frank Ruelas: frank@hipaafinalrules.com
Breach Assessment Perspective

Then:
Assessment determines if a breach

Now:
Assessment determines if not a breach

Low
High

Frank Ruelas: frank@hipaafinalrules.com

*B Your exclamation may vary...
Right to Electronic Copy of PHI

Then: E.H.R.  
Now: D.R.S.

Frank Ruelas: frank@hipaafinalrules.com

Right to Electronic Copy of PHI

Date Request Fulfilled

Not the date of the request

Frank Ruelas: frank@hipaafinalrules.com
Restriction of Disclosures to Health Plan

Then:
Right to Request Restriction

Now:
Right to Request Restrict

Frank Ruelas: frank@hipaafinalrules.com

Restriction of Disclosures to Health Plan

Don’t get tripped up by “auto pilot” errors

Frank Ruelas: frank@hipaafinalrules.com