Enjoy the music while we await the beginning of our webinar today!

June 28, 2013
HIPAA PRIVACY RULE AFTER THE OMNIBUS FINAL RULE- The Details

June 28, 2013

OCR Representative: Iliana Peters
WEDI Representatives: Doreen Espinoza and Lesley Berkeyheiser

WEDI SNIP Privacy & Security Workgroup
Omnibus Components

- **HITECH Privacy & Security**
  - Business associates (BA)
  - Marketing & Fundraising
  - Sale of protected health information (PHI)
  - Right to request restrictions
  - Electronic access

- **HITECH Breach Notification**

- **HITECH Enforcement**

- **GINA Privacy**

- **Other Modifications**
  - Research
  - Notice of privacy practices (NPP)
  - Decedents
  - Student immunizations
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
Section 164.502
Uses and Disclosures; General Rules

- Prohibited Disclosures
  - Genetic Information for Underwriting Purposes
  - Sale
Genetic Information

- The Rule expressly provides that genetic information is PHI.
- The Rule prohibits the use or disclosure of genetic information for underwriting purposes by all health plans, except long-term care plans.
- Terms and definitions in the Rule track regulations prohibiting discrimination in health coverage based on genetic information.
Sale of PHI

• Even where disclosure is permitted, covered entity 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
  – Providing access or accounting to individual
  – Public health
  – Research, if remuneration limited to cost to prepare and transmit PHI
  – Any other permitted disclosure where only receive reasonable, cost-based fee to prepare and transmit PHI
Section 164.508
Authorization Required

- Marketing
- Research
Marketing

• Communications about health-related products and services by covered entity (or business associate) to individuals now marketing and 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
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
Section 164.512: Authorization/Opportunity to Object Not Required

- Student Immunizations
- Decedents
Student Immunizations

- 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
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
Section 164.514
Other Requirements

• Fundraising
Fundraising

• Covered entity 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

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

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

• Flexibility provided in scope of opt out and method to opt back in permitted
Section 164.520
Notice of Privacy Practices

• New Required Inclusions
• New Distribution Requirements
Notice of Privacy Practices

• Content must now include:
  – Statements regarding sale of PHI, marketing, and other purposes that require authorization
  – For covered entities engaging in fundraising, statement that individual can opt out of fundraising communications
  – For providers, statement that covered entity 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
Notice of Privacy Practices

- Health plans may distribute materially revised NPPs:
  - By posting on web site by effective date of change and including in next annual mailing to individuals; or
  - Mailing to individuals within 60 days of material revision
Section 164.522
Right to Request Restrictions

• New Required Restriction
Right to Request Restrictions

- Covered entity 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 the covered entity in full out of pocket
  - Disclosure is not required by other law
Right to Request Restrictions

- Preamble provides guidance on scope of restriction & other issues
  - Scope of restriction extends to health care item or service paid for out of pocket
  - Restriction on follow-up care – individual must pay out of pocket and request restriction for follow-up care
  - Restriction on downstream providers – individual has obligation to request restriction from downstream providers but providers encouraged to assist individual in notifying downstream providers of individual’s desire to restrict
Right to Request Restrictions

- Preamble provides guidance on scope of restriction & other issues
  - 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
Section 164.524
Access

- Electronic Access
- Designated 3\textsuperscript{rd} Parties
Electronic Access

- If individual requests e-copy of PHI maintained electronically in designated record set, covered entity must provide access in electronic form/format requested, if readily producible, otherwise in readable electronic form/format as agreed to by covered entity and individual
  - Must be able to produce some form of e-copy
  - Can provide hard copy if individual declines to accept any of the electronic formats of the covered entity
Electronic Access

• Covered entity 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

• Covered entity has 30 days (with one 30-day extension) to act on request for access
  – Provision allowing initial 60 days for off-site PHI removed
Designated Person

• If requested, covered entity 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
HIPAA Privacy Rule after the Omnibus Final Rule: 
The Details
– “Practically Speaking”

-Doreen Espinoza, UHIN/ WEDI P&S
Practically Speaking

- Uses and Disclosures
  - Internal:
    - Job Descriptions
    - Policies and Procedures
    - Risk Analysis and Risk Assessment
  - External Business:
    - Business Associate Agreements
  - Patient Facing:
    - Notice of Privacy Practices
Job Descriptions

• Make sure the job description matches the access allowed to your PHI
  – Do all members of your staff need full access to all PHI
    • Consider view only, add only, or control access by the roles that staff fulfill
Internal Documentation

• Policies and Procedures
  – Align your desk procedures with your company policies, you may have more than one procedure for a given policy
  – Help your staff know the consequence for non-compliance with a procedure

Example: Procedure for providing documents to a third party. What happens when the patient requests that the records are sent via e-mail to a third Party?
• Train all staff and when appropriate include your business associates

• Not all training must be formal
  • Once a year for the formal training
  • Reminders or updates when appropriate

• Keep track of:
  • Who attended
  • When training was provided
  • What you trained
Risk Assessment

• Follow the data
  – What type of data do you have
  – Where is it stored
  – See who has access
  – Are there procedures for access
  – Are there audit logs
  – Is it encrypted, if not why not
Business Associate Agreements

• Determine: who is your business associate
• Review what is currently in your agreements
  – Access
  – Disclosure
  – Security
• Decide what you want your business associate to handle or not handle
• Remember your deadline of 9/22/2014
The NPP now requires language to include:

- When an authorization is needed for use or disclosure of PHI
- Brief statement regarding the restriction of Psychotherapy Notes from being shared (when appropriate)
- If information is sent and the provider receives financial remuneration then the notice must tell the patient how to opt out (Marketing)
- Statement regarding the sale of PHI
- Statement when Other uses not described in the Notice and authorization is required
- Right to request a restriction (required for Providers only)
  - Not a guarantee to a restriction
- Breach notification
- Information on Genetic Information Nondiscrimination Act
Authorization

• When is an Authorization needed
  – Psychotherapy Notes
  – Research and Marketing
  – Disclosure of immunization information (does not need to be written)
  – For disclosure to a third party: attorney, a medical representative or a stand alone electronic patient health record

• Statement for “Other Uses”
• Other uses statement
  – Employer
  – Business associates that are not involved with Treatment Payment or Operations
Breach

• Notification
  – Describe how your organization will you handle breach
  – A breach does not need to be 500 or more

• Risk Assessment
  – After the fact
  – Not a risk analysis (before the fact)
Practically Speaking

Right of the patients (you and me)

- Right to access PHI by the patient
- Right to request restriction for those services paid for by the patient or a third party on behalf of the patient
- Right to authorize marketing communication

Right to participate with the use and disclosure of the medical record.
HIPAA Privacy Rule after the Omnibus Final Rule:  
- Back to the Basics

Lesley Berkeyheiser,  
N-Tegrity Solutions Group/ WEDI P&S
Determine How You Are Subject to HIPAA

Are you a covered entity?

- Provider - Hospitals and Doctors
- Insurers – HMOs; Payers and Group Health Plans
- Clearinghouse
- Medicare Part D Plan

How has your business changed in the past 10 years?

- Social media
- Smart phones
- Personal Health Records
- Email communications with members/patients
- National Provider Identifier (NPI)
Determine Your Starting Point

Do you electronically engage in any of the transactions?
- Eligibility
- Billing/invoices/remittance advice/payment
- Enrollment
- Other

Has your business changed?
- Subject to new transactions effective January 1, 2014 (e.g., EFT)?
- Business Associate now directly subject to Security Rule and much of Privacy?
Review Data and Documents

Know your data - PHI

- Additional sensitive information covered under state laws?
- Will you address PHI separately?
- Data flow may reveal complexity

Locate initial compliance documents

- Were all forms of PHI analyzed? (spoken, hard copy, electronic)
- Balance between Security and Privacy
- All departments in sync? (IT-systems, Legal-policies)
Know the Rules - Privacy & Security

- Stay up to date - Omnibus changed built upon basic Privacy and Security
- Privacy covers 4 main types of requirements: Administrative; Uses and Disclosures; Individual Rights and General Safeguards. There are probably 50 or so topic areas that often say: “If this applies to your organization you must have a policy and procedure…”
- Security Safeguards cover 3 main areas of requirements: Administrative, Physical and Technical – 20 or so topic areas; some cross over into Privacy

Double Check All Policies and Procedures
Assess adequacy of your Risk Analysis

Is your Risk Analysis current?

- Conduct initial and then ongoing (routine) Risk Analysis
- Ensure Risk Analysis goes beyond just systems (to include hard copy or spoken PHI)

Does your Risk Analysis include PHI documentation?

- Document PHI flow (how information is created, received, maintained and transmitted)
- Consider technology evolution (social media, cloud, smart phones, etc.)
- Refer to ONC fact sheets for guidance
Evaluate Compliance with Minimum Necessary

Ensure workforce obtains and uses only minimum necessary

- Workforce member = anyone under your direct control (paid or unpaid)
- Which workforce ember use data internally vs. disclosure externally?
- Ensure policies define “routine and reoccurring disclosures” versus disclosures under special circumstances
Is your NPP compliant & current?

Does your Notice of Privacy Practices contain standard components and examples?

- Standard heading
- Who must abide by the NPP
- How your organization uses and discloses PHI for treatment, payment and operations (with examples)
- Information about individual’s rights
- Statement about organization’s right to change the NPP and contact information

Does the Notice reflect your type of organization

- Omnibus language changes apply to your organization when you use PHI to do those things (e.g., fundraising)
- Reinforce your entity type by using applicable examples
Use PHI documentation to determine DRS

- Individual Rights apply to information stored in designated record sets
- DRS contain PHI of the individual you serve
- DRS used to make decision about the individuals whose PHI it contains

Document what constitutes your DRS

- Different organizations include different items in DRS
- Not free-form text fields
What is the standard way used to validate identity?

- Standard method (e.g., series of questions) should be determined
- Develop workforce policy and procedures, including script
- Train workforce
- Be able to demonstrate good faith attempt to validate
Specific Changes with Individual Rights - Access

Does Omnibus require encryption?

- Encrypt in order to “safe harbor” themselves from having to report a breach and or to decrease their risk that a breach will occur.
- Unencrypted email to individuals permitted if individuals advised of risk, and individual prefers use of unencrypted email.
- Resist temptation to move to unencrypted email / Yet it is specifically stated in the pre-amble.

Removal of 60-day response requirement

- Revise policies and make sure workforce members are retrained.
Specific Changes with Individual Rights - Restrictions

Changes to Restriction

● Providers will need to determine what the changes are and how they will implement them
  – Documentation regarding collecting payment up front
  – Identifying and “tagging” data elements to keep safeguarded from Health Plan per individual’s request

● Understanding which mandatory claim submission provisions under Medicare, Medicaid or state law will “over-rule” the individual’s request.

● This issue still has yet to “play out” across the industry.
Today’s Hand-outs

1. ONC’s Mobile Health Information

2. Summer Series Quick Reference Sheet
Join a WEDI workgroup!

- Have a special interest in a particular area?
- Rules always changing
- More changes expected soon (Accounting for Disclosures)
Questions / Answers
Future Webinars

- **July 17 – Breach and Enforcement**
  - Changes to the Breach rule
  - Changes to the Enforcement Landscape

- **July 26 – Business Associates**
  - Modified definition
  - BA liability
  - Privacy and Security rule provisions applicable to BA

- **August/September – Drill Downs…. Details TBD**
• Thank You for participating in today’s webinar.