The HIPAA Omnibus Rule

Addressing New Requirements

Agenda

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

Overview

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

I. Introduction

- Omnibus Rule – Overview
- Regulatory Development
- Upcoming Deadlines

Omnibus Rule - Overview

Enforcement Rule

- Civil Monetary Penalties
- Affirmative Defenses
- Standard of Culpability

Security Rule

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

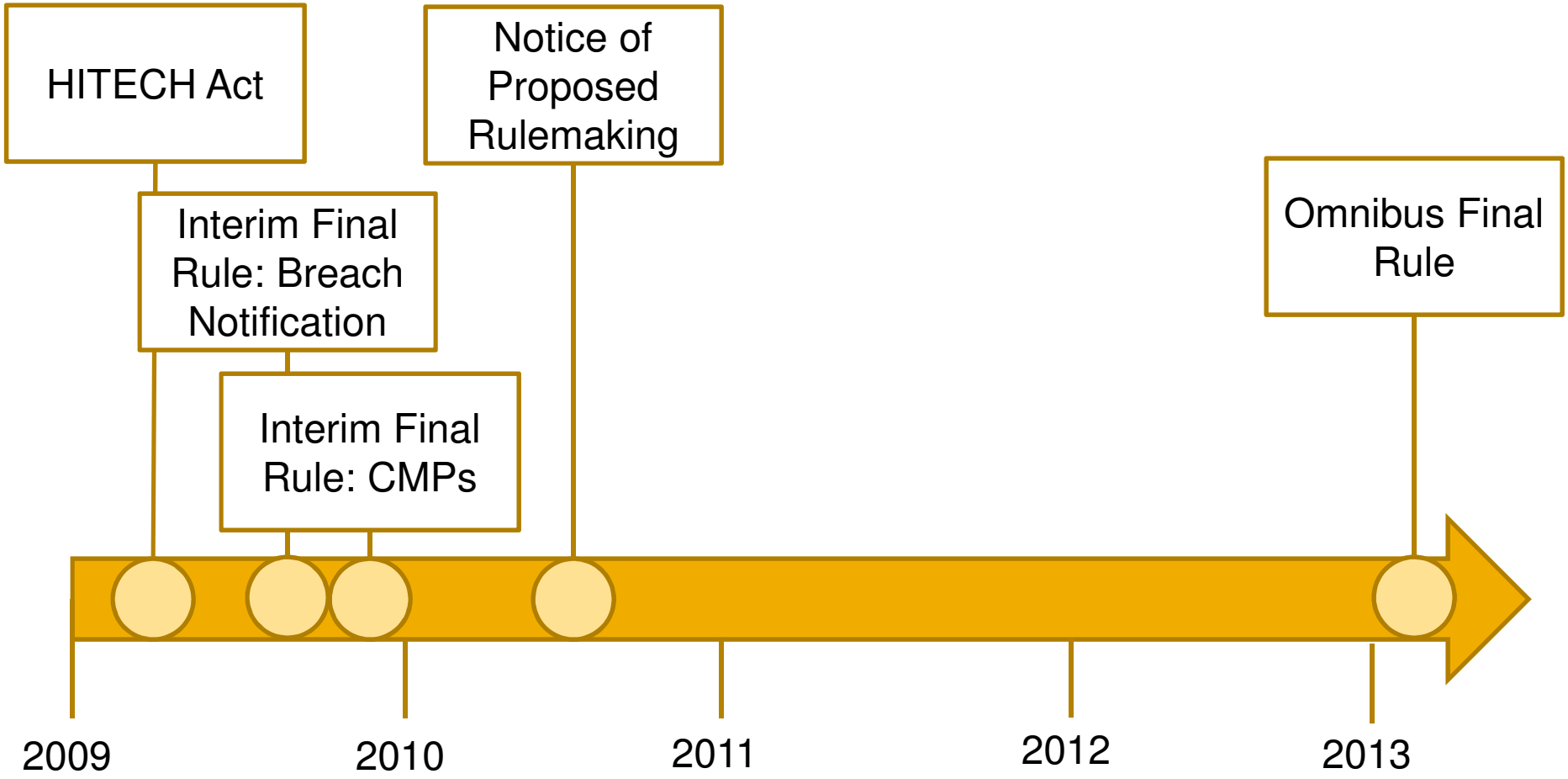
Privacy Rule

- Marketing
- Notice of Privacy Practices
- Research

Breach Notification

- Notification Standard
- Risk Assessment
- Notice Obligations

Regulatory Development



Key Implementation Dates

March 26, 2013	• Omnibus Rule Effective Date • Enforcement Rule changes in effect
September 23, 2013	• Compliance for Covered Entities & Business Associates • Deadline for Notice of Privacy Practices (NPP) revisions • New and renewal Business Associate Agreements executed after this date must comply with documentation and contract requirements
September 23, 2014	• Deadline for revisions to all BAAs executed prior to January 25, 2013 and not renewed or modified between March 26, 2013 and September 23, 2013 • Update required upon earlier of renewal date or September 23, 2014

Agenda

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

II. Covered Entities

- Notice of Privacy Practices
- Marketing
- Fundraising
- Access to PHI in Electronic Form
- Accounting of Disclosures
- Hybrid Entities

Notice of Privacy Practices

Opt-in	Describes uses and disclosures that require individual authorization
	States other uses and disclosures not described in the NPP requiring individual authorization.
Opt-out	Explanation of fundraising communications and right to opt out of such communications
	Providers: Limited right to restrict PHI disclosures Health Plans: No disclosure of genetic information
Data Breach	States that covered entities will notify individuals following a breach of their unsecured PHI

Marketing

	Authorization Required	Applicable Exceptions to Authorization
No Remuneration	Any communication about a third party's product or service that encourage an individual to purchase or use the product or service if an applicable exception does not apply.	• Communications made for Treatment Purposes • Communications made for Health Care Operations Purposes
Remuneration	Communications for the above purpose, including: • Communications made for Treatment Purposes • Communications made for Health Care Operations Purposes if an applicable exception does not apply.	• Face-to-Face Communications • Refill Reminders for current drugs or biologics: limited to reasonable remuneration • Promotional gifts of nominal value

Marketing

HHS Clarified the Definition of Remuneration in the Context of its Significant Modification to its Approach to Marketing

Remuneration	Not Remuneration
• Direct or indirect payment from or on behalf of a third party whose product or service is being described • Indirect payment occurs when a party makes a payment on behalf of the third party	• Non-Financial Benefits • Direct or indirect payment for treatment of the individual • Payments for purposes other than a marketing communication • Permitted uses or disclosures of PHI in exchange for the payment of the reasonable cost of providing the PHI

Fundraising

Required Content

- Opportunity to opt out must be “clear and conspicuous”
- Opt-out method must not impose an undue burden on the individual
- Must clearly inform individuals regarding the scope of any opt-out
- Opt-out must be treated as a revocation of an authorization by the individual

Fundraising

Covered Entities May Use Additional Demographic Information To Target Fundraising Communications

Previously Allowed	Additional Categories

• Demographic Information
  • Age
  • Gender
• Dates of Service
	• Department where individual received care
	• Treating physician
	• Ability to screen out individuals with "suboptimal outcomes"

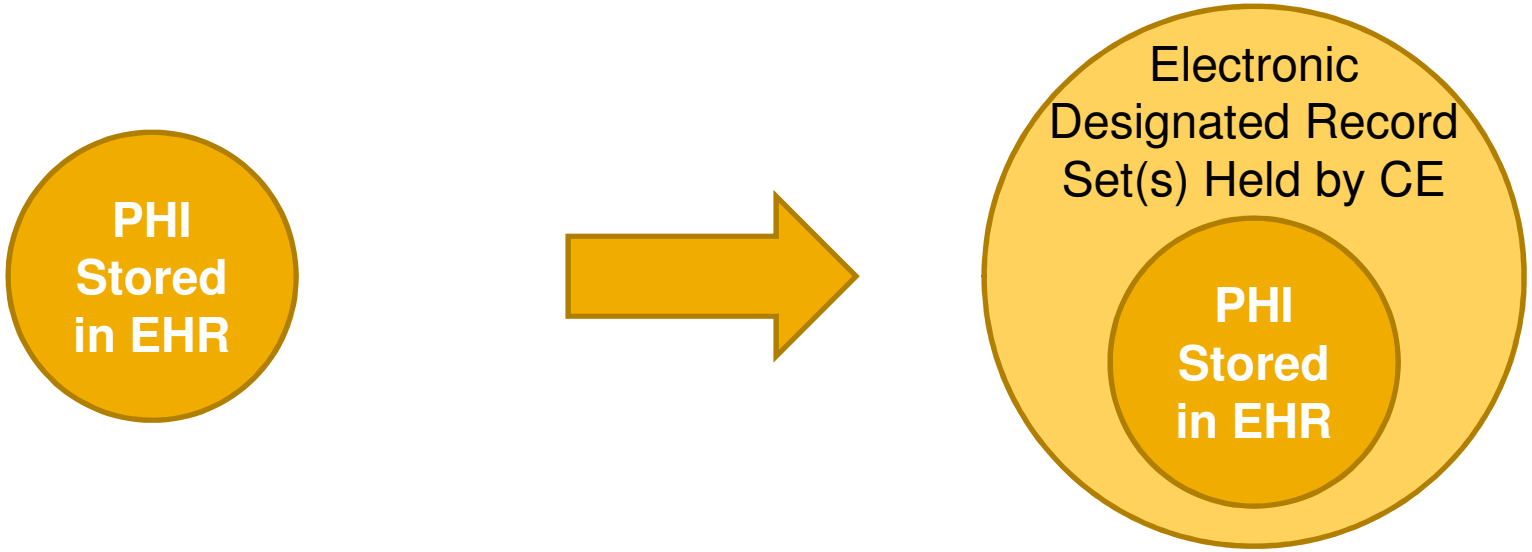
Access to PHI in Electronic Form

Covered Entities Must Provide Individuals with Access to PHI Maintained in Designated Record Sets in Electronic Form

- Covered entities:
  - Must provide PHI in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed upon.
  - Are not required to purchase new software to accommodate an request for a specific form that is not readily producible.
  - May charge individuals a reasonable, cost-based fee for copy of PHI.
  - Must approve or deny, and if approved, provide access to or a copy of the PHI, within 30 days of an individual's request. Timeframe applies to PHI maintained in both paper and electronic form.

Access to PHI in Electronic Form

Expands Upon Current Right of Access, which Requires Access only to PHI Maintained in an Electronic Health Record



HITECH/NPRM: Covered entities are required to provide an individual with an electronic copy of their PHI when it is used or maintained in an Electronic Health Record ("EHR")

Omnibus Final Rule: Covered entities must provide an individual with access to their PHI that is maintained electronically in one or more designated record sets in an agreed-on form and format.

Accounting of Disclosures

Requirements that Covered Entities Provide an Accounting of Disclosures Upon Request Remains Unchanged for Now

- Covered Entity:
  - Must provide a requesting individual with an accounting of disclosures without charge in any 12-month period.
  - May impose a reasonable, cost-based fee for each subsequent request for an accounting of disclosures during that 12-month period.
- This requirement is the subject of a separate proposed rule published on May 31, 2011 and will be the subject of a future rulemaking.

Hybrid Entities

Hybrid Entities Will Be Required To Move BA Functions Into the Health Care Component

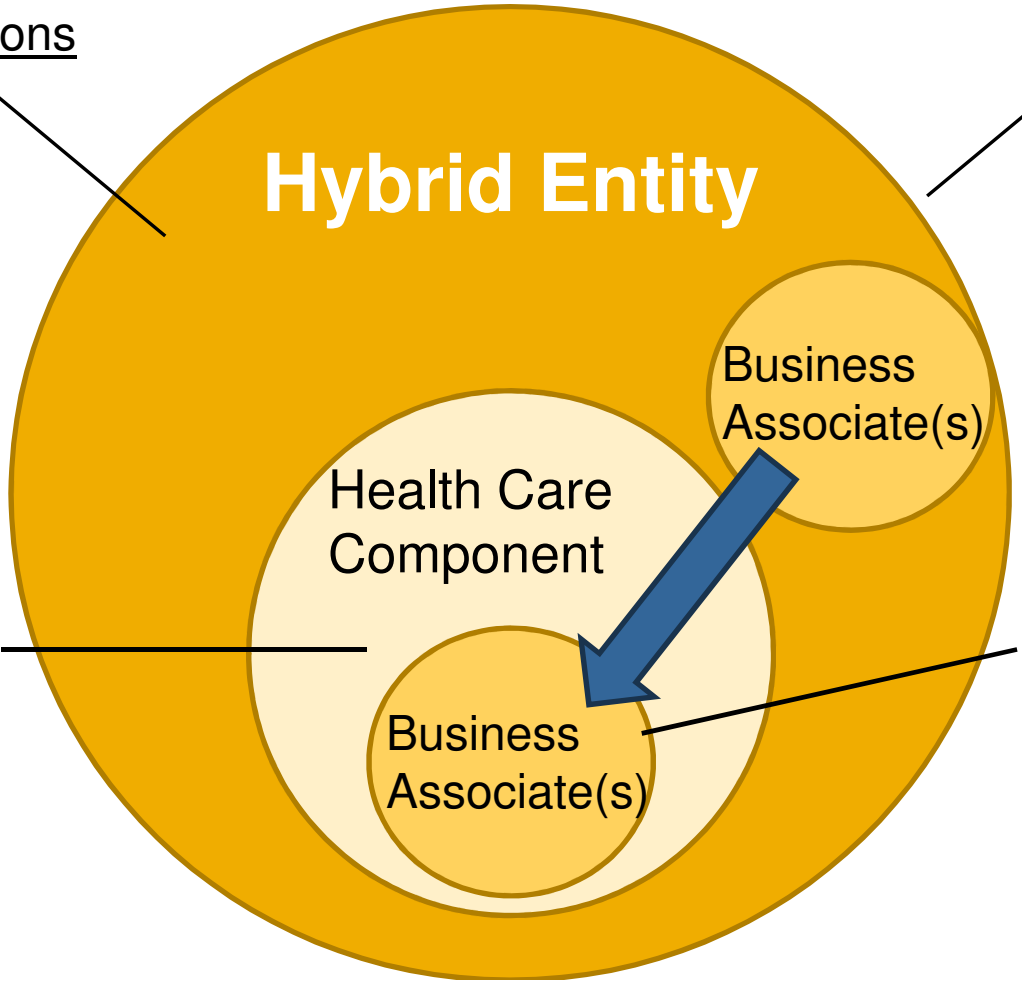
Non-Covered Functions

May Include:

- Employer
- Academic Functions
- Administrative

Covered Functions

Activities that would qualify the component as a CE, if the component were a separate legal entity



Pre-HITECH

Hybrid had discretion to include any BA functions in health care component.

Omnibus Rule

Hybrid MUST include BA functions within health care component

Agenda

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

III. Business Associates

- Modifications to Definition of Business Associate
- Direct Liability for Non-Compliance
- Subcontractors Subject to HIPAA

Modifications to Definition of BA

HHS Provided Additional Clarification Regarding the Types of Entities It Considers Business Associates

Business Associates

- Health Information Organizations (HIOs)
- Data Storage Organizations that "Maintain" PHI
- Personal Health Record (PHR) Vendors that receive PHI from Covered Entities
- Accreditation Organizations (AOs)
- Patient Safety Organizations (PSOs)
- e-Prescribing Gateways

Not Business Associates

- "Mere Conduits" Without Authority to Access PHI
  - Ex.: Internet Service Providers (ISPs)
- External Institutional Review Boards (IRBs)
- PHR Vendors that do not receive PHI from Covered Entities

Direct Liability for Non-Compliance

Business Associates and Subcontractors Will Be Subject to HHS Enforcement for HIPAA Violations

Privacy Rule

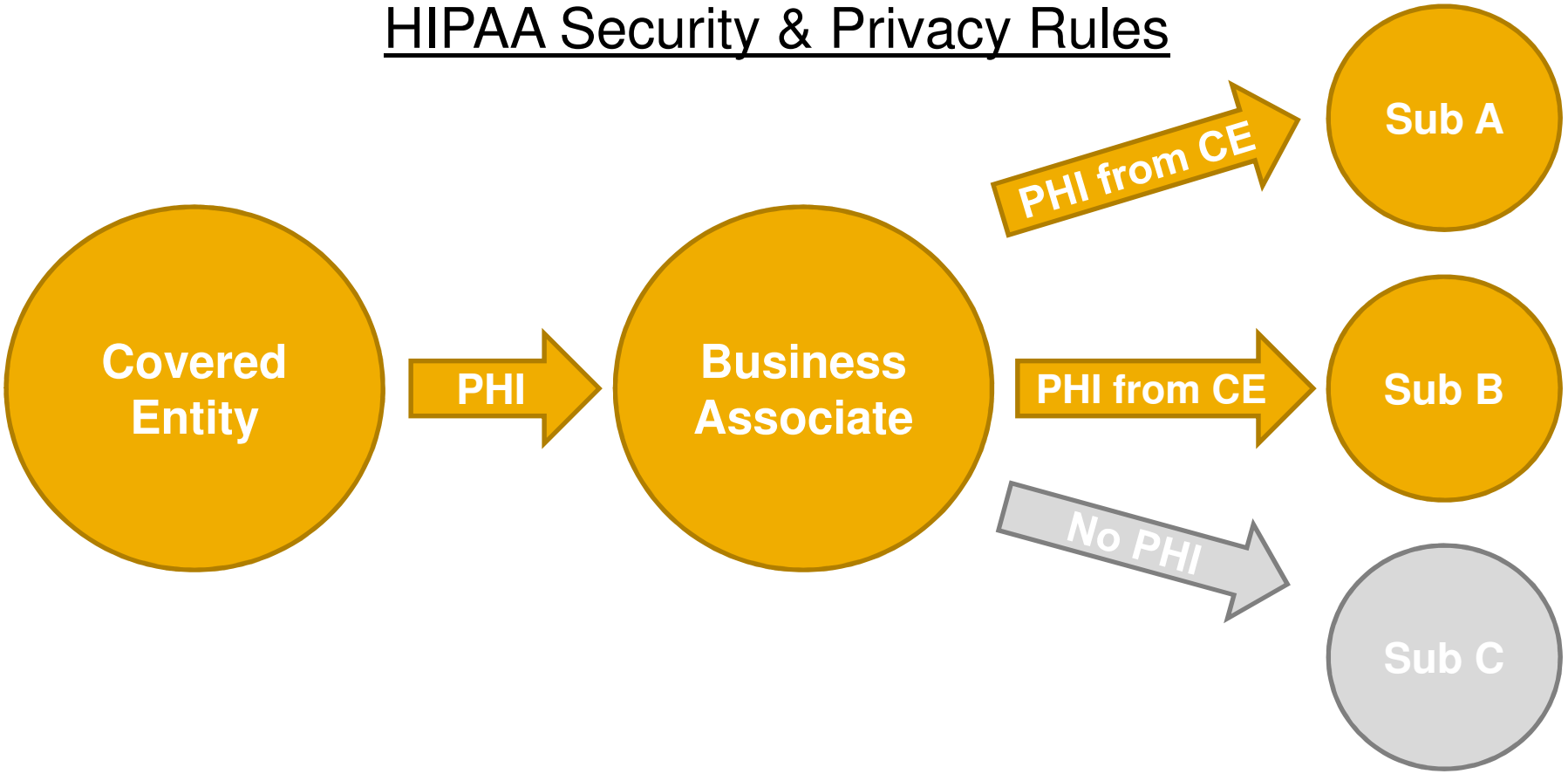
- Impermissible Uses and Disclosures
- Failure to Provide:
  - Breach Notification
  - Access to ePHI
  - Accounting of Disclosures
- Failure to Disclose When Required by the Privacy Rule
- Failure to Comply with the Security Rule

Security Rule

- Failure to Implement:
  - Administrative
  - Physical, and
  - Technical Safeguards
- Failure to Create and Maintain Policies and Procedures for the Protection of PHI
- Failure to Comply with the Security Rule's Documentation Requirements

Subcontractors Subject to HIPAA

Downstream Entities that Work at the Direction of/on Behalf of a Business Associate ***and*** Handle PHI Must Comply with HIPAA Security & Privacy Rules



Agenda

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

IV. Data Breaches

- Breach Notification Paradigm Shift
- Revised Definition of Breach
- Breach Notification Standard
- Expansion of Potential Breaches
- Risk Assessment
- Notification Timing
- Business Associate Agents

Breach Notification Paradigm Shift

NPRM:
Risk of
Individual Harm

Final Rule:
Presumption of
Breach

Revised Definition of Breach

- Under the Interim Breach Rule, the breach notification requirement is triggered when PHI is acquired, accessed, used or disclosed in a manner not permitted by the Privacy Rule that:
  - "…compromises the security or privacy of the protected health information and such unauthorized acquisition, access, use or disclosure…poses a significant risk of financial, reputational, or other harm to the individual."
- The Final Rule eliminates the harm standard and instead creates a presumption of a breach unless the covered entity or business associate can demonstrate through a risk assessment that:
  - "…there is a low probability that the PHI has been compromised based on a risk assessment."

Breach Notification Standard

- HHS made clear in the commentary that the former harm standard was overly subjective and believes that the new standard will be more objective
  - Will likely increase the number of incidents resulting in breach notifications
- HHS retained exceptions to the definition of breach for
  - (i) limited types of unintentional access by workforce members,
  - (ii) some forms of inadvertent disclosures, and
  - (iii) non-retainable disclosures.

Expansion of Potential Breaches

- Previous exception for Limited Data Set information eliminated; any compromise of Limited Data Set is a potential breach
  - Limited Data Set / Data Use Agreements should be revised to account for new breach notification requirements
- Violations of minimum necessary requirements now potential breaches
  - Requires much more careful tracking and treatment of minimum necessary
- Breaches can occur within an organization as a result of unauthorized use or access

Risk Assessment

- Covered Entities and Business Associates may undertake a risk assessment or simply notify affected individuals.
- If elect to undertake a risk assessment, must evaluate all of the following factors in determining whether a breach notification is required:
  - Nature and extent of the PHI involved
  - Type of unauthorized person in receipt of the PHI as a result of the breach
  - Whether the PHI was actually "acquired or viewed"
  - The extent to which the risk to the PHI has been mitigated
- Other factors may be considered

Notification Timing

- 60 day notification deadline should be considered the “outer limit”
- Notification period begins
  - At the time the Covered Entity knows or should have known of the breach
  - If breach by Business Associate, knowledge of Covered Entity depends upon whether Business Associate is considered an agent or independent contractor.
  - State data breach notification laws must also be considered

Business Associate Agents

Covered Entities and Business Associates Are Liable for the Acts of their Business Associate agents, in accordance with the Federal Common Law of Agency

Federal Common Law of Agency - Factors

Right of Authority to Control

Which Party Controls Performance of the Function?

Can the Covered Entity provide interim instructions or directions?

What Is the Time, Place, & Purpose of the Conduct?

Is the Conduct Onsite at the Covered Entity's location?

Which Party Usually Performs Function?

Is the Conduct Commonly Performed by a Business Associate?

Business Associate Agents

Important to Balance the Risk/Reward of Controls in Business Associate Agreements; Must Consider Whether Business Associate Is/Ought to Act as Agent of Covered Entity

Business Associate Is Covered Entity's Agent	Knowledge of a Data Breach will be imputed to the Covered Entity as of the date of discovery by the Business Associate
Business Associate Is Not Covered Entity's Agent	Knowledge of a Data Breach will be imputed to the Covered Entity as of the date of notification of the Covered Entity by its Business Associate

Business Associate Breaches

- Commentary also addresses the situation in which a breach by a Business Associate involves PHI of multiple Covered Entities:
  - If the Business Associate cannot readily determine to whom the breached PHI relates, the Business Associate may need to notify all potentially affected Covered Entities
  - Covered Entities and Business Associates should address the Business Associate's ability to maintain PHI of multiple Covered Entities in a segregable form

Agenda

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

V. Research

- Evolution of Research Regulations
- Compound Authorizations
- Use of PHI in Future Research
- Sale of PHI & Research Exception
- Definition of a Business Associate
- Access to Decedents' PHI
- Next Steps

Evolution of Research Regulations

- Final Rule is a “win” for research community – simplifies requirements and increases flexibility
- Changes driven by comments and recommendations over past ten years, including:
  - 2002 - National Human Research Protections Advisory Committee (NHRPAC)
  - 2004 and 2010 - HHS Secretary’s Advisory Committee on Human Research Protections (SACHRP)
  - 2009 - Institute of Medicine (IOM)
- Addresses many concerns of national research community and facilities research efforts

Compound Authorizations

Before Final Rule

- Privacy Rule generally prohibited compound authorizations
  - Research exception: research authorizations could be combined with informed consents for *same research study*, subject to limitations for conditioned authorizations and authorizations for use/disclosure of psychotherapy notes
- Privacy Rule generally prohibited conditioning the provision of treatment on the provision of an authorization
  - Research exception: provision of research-related treatment could be conditioned on provision of an authorization for the use/disclosure of PHI for research purposes

Compound Authorizations

Before Final Rule

- Limitation to research exceptions – could not combine, even for purposes of the same study:
  - A ‘‘conditioned authorization’’ – participation in research-related treatment **is conditioned** on authorizing use/disclosure of PHI *with*
  - An “unconditioned authorization” – participation in research-related treatment is **not conditioned** on authorizing use/disclosure of PHI
- Permitted combinations
  - informed consent with multiple conditioned authorizations for one study
  - informed consent with multiple unconditioned authorizations for one study

Compound Authorizations

Before Final Rule

- Prohibited combinations
  - informed consent with conditioned and unconditioned authorizations
  - informed consent with authorizations for multiple studies
  - authorizations for use/disclosure of psychotherapy notes with any other authorization
- Result was that multiple forms were required for collection in research repositories of PHI and identified bio-specimens generated during trial

Compound Authorizations

After Final Rule

- 42 C.F.R.§ 164.508 now allows combining research authorizations "with any other type of written permission for the same **or another** research study"
- **Specifically permits compound authorizations when one of the authorizations is for the creation or maintenance of a research database or repository (unconditioned), and the other is for participation in a clinical trial (conditioned)**
- When conditioned authorizations are combined with unconditioned authorizations, the form must:
  - (1) Clearly differentiate between the conditioned vs the unconditioned components, and
  - (2) Allow individual opportunity to "opt in" to unconditioned authorization
- Excludes authorizations for use or disclosure of psychotherapy notes, which still may only be combined with other psychotherapy note authorizations

Compound Authorizations

HHS clarified acceptable methods for differentiating conditioned and unconditioned components

Combined informed consent / research authorization form with:

- (1) a check-box for the individual to ‘‘opt in’’ to the banking component, and one signature for the clinical trial and banking component
- (2) one signature for the clinical trial and another signature to indicate the individual agrees to the banking component; and
- (3) a check box for the individual to “opt in” to the banking component, and one signature for the clinical trial and banking component, but with detailed information about the banking component in a separate information sheet that is referenced in the form

Use of PHI for Future Research

Before Final Rule

- Required element of valid authorization is a "description of each purpose of the requested use or disclosure"
  - In 2002, HHS interpreted the "purpose" to be study-specific, with the result that research participants could not authorize future, unspecified research
  - This further complicated research using PHI from data repositories
- More restrictive than Common Rule, which generally had been interpreted to allow subjects to consent to future uses of their data, if subjects had a reasonable understanding of the scope of future research

Use of PHI for Future Research

After Final Rule

- **HHS has revised its original 2002 interpretation to allow authorizations for future studies, if purpose is "adequately described"**
  - Must be "reasonable" for subject to expect that PHI will be used for future study
  - Researchers and IRBs have some flexibility in determining what adequately describes a future research purpose depending on the circumstances
- Researchers have flexibility in satisfying authorization elements for future research
  - Specific PHI to be disclosed, recipients of PHI
- New interpretation facilitates secondary research based on PHI in databanks and tissue repositories

Sale of PHI

- Final Rule codifies HITECH's general prohibition on the sale of PHI without prior authorization
- HHS defined "sale of PHI": Disclosure of PHI where the covered entity directly or indirectly receives remuneration from the recipient of the PHI in exchange for the PHI
- Research Clarifications
  - Transfer of PHI to study sponsors or funders - NOT "sale of PHI":
    - Although the terms of the grant or contract may require reporting of PHI to the research sponsor or funding agency, the disclosure is simply a byproduct of the service being provided
  - Transfer of PHI from covered entity to researcher with remuneration – IS "sale of PHI"
    - When a covered entity is providing PHI to a researcher for some remuneration, and its only service is the collection and transmission of data, arrangement
  - Sale of de-identified data – is NOT sale of PHI

Sale of PHI

- Research Exception
  - Only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit PHI
  - Also applies to limited data sets
- Transition provision - existing data use agreements for limited data sets, if accompanied by remuneration exceeding reasonable cost, valid until the earlier of:
  - Renewal/modification after September 23, 2013, or
  - September 22, 2014

Sale of PHI – Reasonable Costs

Reasonable	Unresolved	Not Reasonable
• Direct and indirect costs, including labor, materials and supplies for generating, storing and transmitting PHI • Labor and supplies to ensure PHI is disclosed in a permissible manner • Related capital and overhead costs	• Treatment of certain in kind benefits – for example, data collaborations → contribution of PHI to database in exchange for right to access database	• Profit margin

Definition of a Business Associate

Final Rule Clarifies What Research Functions Give Rise to Business Associate Relationship

Institutional Review Boards	Researchers
• Research review, approval and oversight for covered entity by external IRBs and "central IRBs" – are NOT business associate functions	• Performing research activities – are NOT business associate functions • Performing health care operations or creating a de-identified or limited data set – ARE business associate functions

Access to Decedents' PHI

Before Final Rule

- General Rule: PHI of decedents subject to same Privacy Rule protections as PHI of living individuals
- Research Exception: use allowed with documented assurances –
  - (1) individual is actually deceased (2) sole purpose of use/disclosure is for research on deceased individual and (3) PHI is necessary for the research
  - Exception limited to "research" – "systematic investigation … designed to develop or contribute to generalizable knowledge" – does not cover many studies undertaken by historians, archivists, biographers
- Authorization: use allowed with authorization from personal representative (executor, administrator)
- Difficulty in collecting necessary assurances and authorizations over time impeded historical studies and other studies not classifiable as "research"

Access to Decedents' PHI

After Final Rule

- HHS limited protection of decedents' PHI to 50 years after death
- Strikes a balance between rights of individuals with a relationship to the decedent and the challenge of obtaining assurances or authorizations over time
- Expands access to PHI in covered entities' documentary collections, when their PHI contents meet the 50 year standard
- Facilitates library management within covered entities and expedites research and studies involving decedents' PHI

Next Steps – Transition Provisions

- Compound Authorizations
  - A new option – no revision required for ongoing studies
- Future Research
  - Covered entities may rely on IRB-approved consents obtained prior to March 26, 2013 that reasonably informed individuals of future research, if consent was combined with a HIPAA authorization (even if the authorization was specific to the original study or to the creation and maintenance of a repository)
- Sale of PHI
  - Covered Entities may rely on:
    - (1) research authorizations obtained prior to September 23, 2013, even if remuneration is involved but not disclosed, and
    - (2) waiver of authorization from an IRB or Privacy Board obtained prior to September 23, 2013, even if the covered entity receives remuneration in the form of more than a reasonable, cost based fee

Agenda

I. Introduction

II. Covered Entities

III. Business Associates

IV. Data Breaches

V. Research

VI. Recommended Approaches

VI. Recommended Approaches

- Revision and Negotiation of New Business Associate Agreements
- Revision of Notice of Privacy Practices
- Implementation of Security and Privacy Rule Requirements for Business Associates and subcontractors
- Re-analysis of Relationship to State Privacy Laws
- Implementation of New Procedures for Data Breach Risk Analysis and Notification