

# Navigating Privacy and Security Issues Under HITECH

**Brent R. Eller**

**Partner**

brenteller@dwt.com

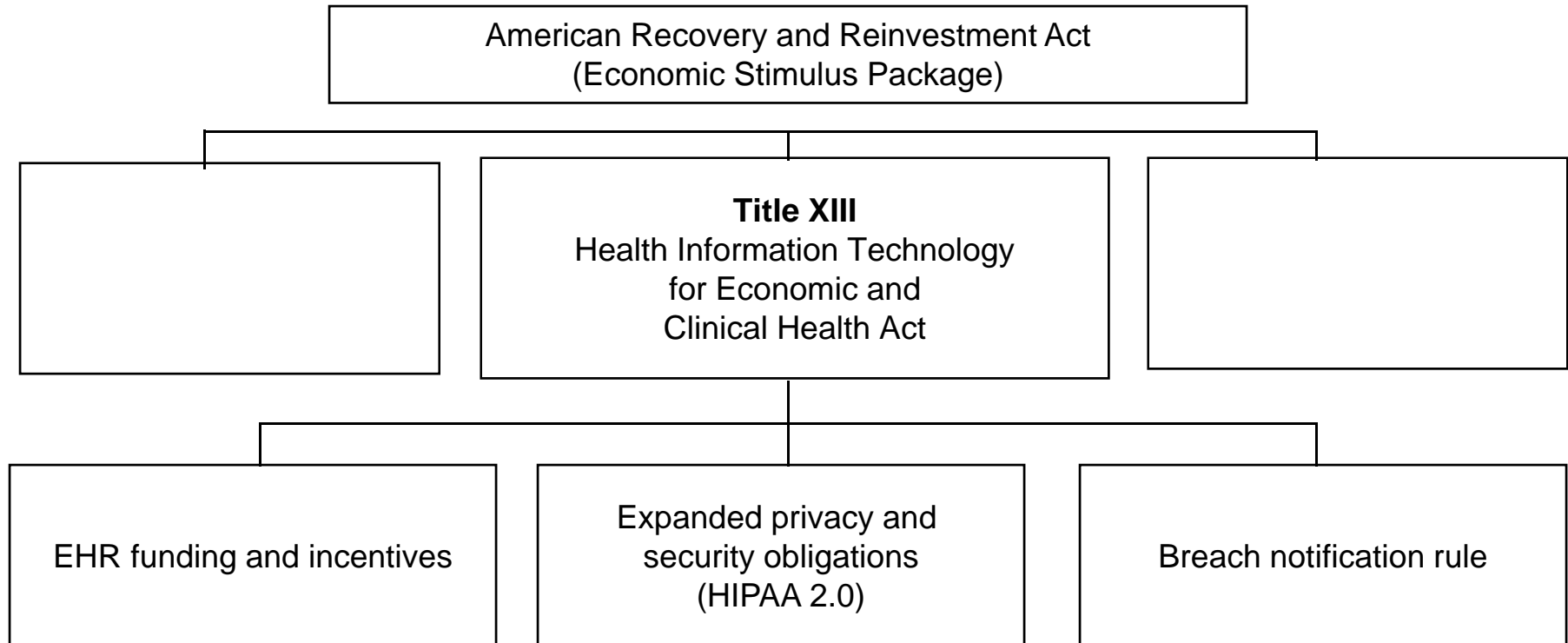
**Rebecca L. Williams, RN, JD**

**Partner and Co-chair of HIT/HIPAA Practice**

beckywilliams@dwt.com



# HIPAA 2.0



# Data Breach Notification



- **Prior Law:**
  - No HIPAA data breach notification requirement, but may have been part of mitigation
  - Most states have notification requirements
- **HITECH: First federal law mandating breach notification**
  - Affects covered entities, business associates, vendors of personal health records, and PHR service providers
  - **FTC: Final regulations**
  - **HHS: Interim final regulations**

# Data Breach Notification

- Upon the **discovery** of a
- **Breach** of
- **Unsecured PHI**
- **Covered entities or business associates must make required notifications**



# Data Breach Notification



- “Breach”
  - Unauthorized acquisition, access, use, disclosure of PHI
  - In a manner not permitted by the HIPAA Privacy Rule
  - That compromises the security or privacy of such PHI
    - Poses a significant risk of financial, reputational, or other harm to the individual
    - De-identified information does not pose risk of harm
    - Fact specific analysis
- Exceptions
  - Unauthorized person would not reasonably have been able to retain the PHI
  - Certain good faith or inadvertent access by or disclosures to workforce in same organization

# Data Breach Notification

- “Unsecured”
  - Not protected by “technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals”
  - Basically information that is not encrypted or destroyed (per National Institute of Standards and Technology standards)

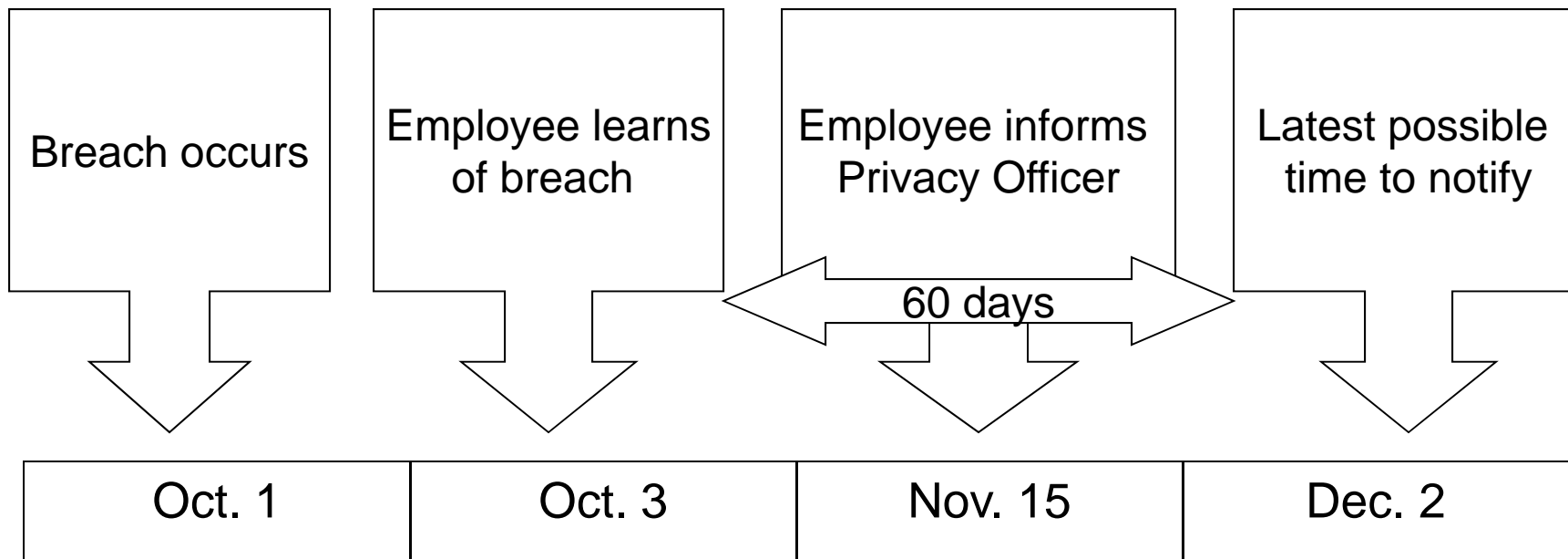
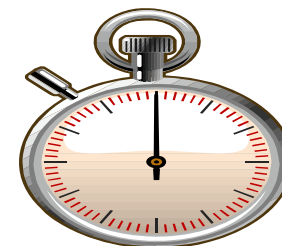


# Data Breach Notification



- Timing
  - Notification without unreasonable delay but not later than 60 days after “discovery”
  - Clock starts ticking on first day it is known – or using reasonable diligence would have been known – to any workforce member or agent (per federal common law of agency) (other than person committing the breach)
  - Subject to law enforcement delay

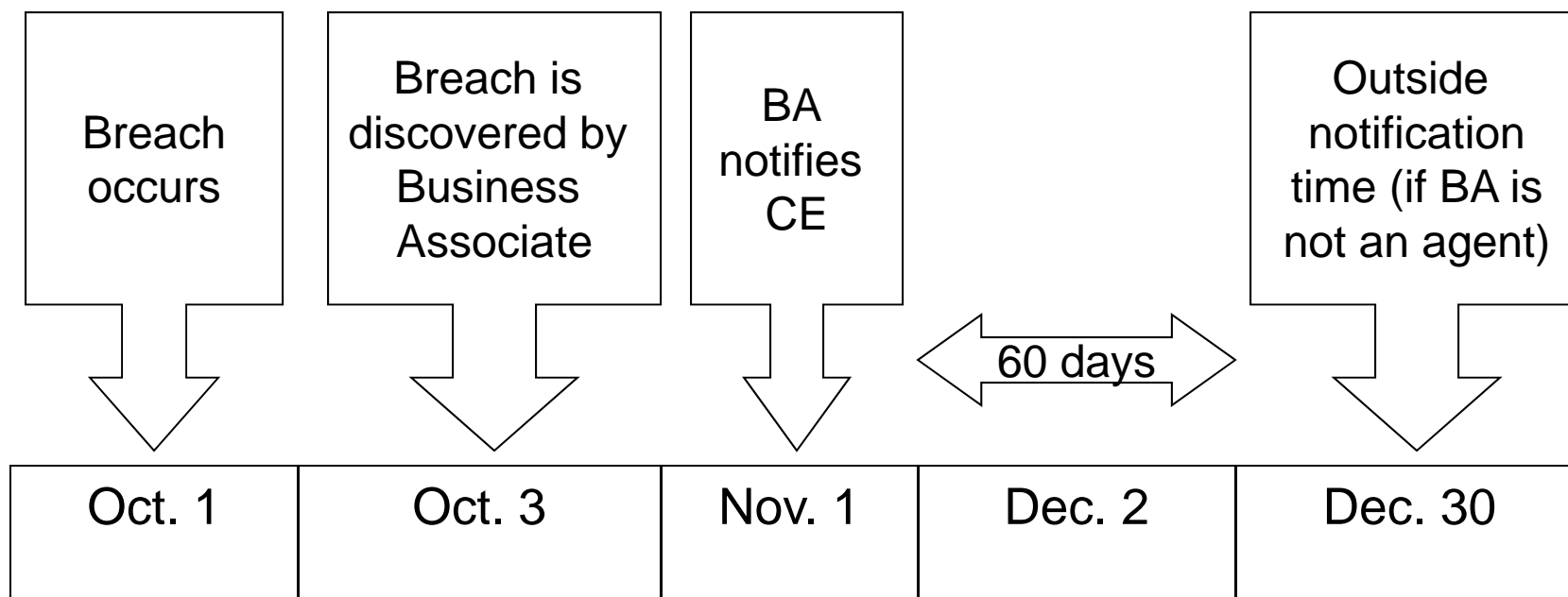
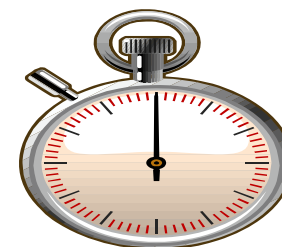
# Examples of Timing



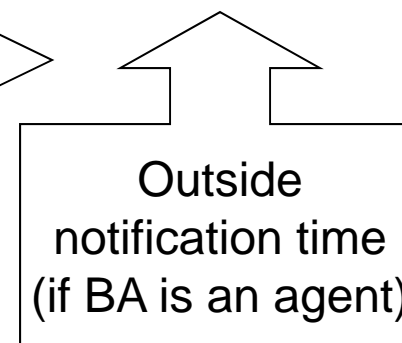
But remember without unreasonable delay

Beware: Clock starts when entity learns of – or using reasonable diligence should have learned of – the breach

# Examples of Timing



Business associate must notify without unreasonable delay, but in no event longer than 60 days



# Notification of Data Breach



- Notification to affected individuals
  - Written notice
  - Electronic notice if individual agrees
  - Next of kin/personal representative for deceased patients
- Substitute notice
  - Insufficient or out-of-date contact information
  - Reasonably calculated to reach individual
  - Not required for next-of-kin/personal representative
  - If fewer than 10 individuals have incomplete information
    - Alternative written, telephone, or other notice
  - If 10 or more individuals have incomplete information
    - Conspicuous posting on website for 90 days or
    - Conspicuous notice in major print or broadcast media and
    - Must include a toll-free number to get more information

# Notification of Data Breach

- Notification to HHS
  - If 500 or more residents in a state affected → notice contemporaneous with individual notice
  - If fewer than 500 individuals are affected → notice through log submitted annually
- Notification to the media
  - If more than 500 residents in a state or jurisdiction affected → notice to prominent media outlet
  - Also may be part of substitute notice

# Content of Notification



- What happened
- Types of unsecured PHI involved
- Steps individuals should take to protect themselves
- What the covered entity is doing to
  - Investigate the breach
  - Mitigate harm
  - Protect against further breaches
- Contact procedures for questions/information
- Business associates, as possible, should provide:
  - Identification of each individual affected
  - Other available information CE must provide

# Data Breach Notification

- Administrative Requirements
  - Policies and procedures
  - Training
- Burden on organization to prove compliance
- Need a plan to respond



# Business Associates

- Pre-HITECH: Business associates have not been directly regulated by HIPAA
  - Instead Covered Entities were required to enter into business associate contracts with their business associates
  - Way to backdoor some of the HIPAA requirements



# Business Associate: HITECH

- Clarification of business associate status
  - HIEs
  - RHIOs
  - e-Prescribing Gateway
  - PHR vendors that provide PHRs to covered entities
- No change to definition of business associate in HITECH Act

# Business Associate: Proposed Regs

- “Business Associate” includes:
  - Patient Safety Organizations (under PSQIA)
  - RHIOs, HIEs, e-Prescribing Gateways, and PHR vendors acting for covered entities
  - Subcontractors of business associates (except they must have business associate agreements with the business associate they contract with, not the covered entity)
- BAs are subject to “minimum necessary” standard
- BAs are directly subject to Security Rule, but not Privacy Rule

# Business Associate: Proposed Regs

- BAs may only use or disclose PHI as permitted or required by agreement with covered entity or as required by law
- BA may not use or disclose PHI in a way that would violate the Privacy Rule if the covered entity did it
- BA must disclose PHI to the Secretary of HHS, when required, and to respond to individual's request for an electronic copy of PHI

# Business Associate: Proposed Regs

- Subcontractors of BAs are considered BAs
  - Proposed rule would require written business associate contracts between BAs and their subcontractors
  - No requirement for CEs to have direct contracts with subcontractors of their BAs
  - BA has to respond to subcontractor's breaches the same way the CE would respond to breaches by BA—take reasonable steps to cure breach or terminate the contract, if feasible
  - Triggered by becoming aware of pattern or practice of activity of subcontractor that constituted a material breach or violation of the subcontractor's BA contract
  - Would eliminate requirement to report to Secretary if termination is not feasible (for CEs and BAs).

# Business Associate: Proposed Regs

- New requirements for BA contracts:
  - BA must “use appropriate safeguards and comply, where applicable, with [the Security Rule], with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract”
  - BA must report breaches of unsecured PHI as required by the data-breach reporting rule (in addition to current requirement to report security incidents)
  - BA must comply with the requirements of the Privacy Rule to the extent that the BA is to carry out a CE’s obligation under the Privacy Rule (e.g., providing individuals access to PHI)

# Business Associate: Proposed Regs

- Transition Period:
  - CEs and BAs can continue operating under current contracts for up to 1 year and 240 days after the final regulations are published
  - Unless the agreement is renewed or modified sooner
  - Renewals within 60 days of the publication date don't affect the grace period
  - Extension of “evergreen” contracts isn't considered a renewal
  - To qualify, contracts must be compliant with current requirements on the date the final rule is published

# Business Associate: Proposed Regs

- Now subject to civil and criminal enforcement and penalties under HIPAA
  - Criminal enforcement – previously a possibility
  - Civil enforcement and audits – new liability exposure
- Triggered by violating Security Rule or required provisions of business associate contracts
- Business associates have CMP liability for acts of their agents
- Would delete current exception for covered entities for acts of agents that are business associates where the BA contract requirements have been met, the CE didn't know of pattern or practice that violated the contract, and didn't fail to act as required by Privacy or Security Rule

# Expanded Accountings of Disclosures



- Existing Law: Individuals have right to receive accounting of disclosures of their PHI, but no TPO in accounting
- HITECH: If CE uses/maintains an EHR
  - Right to accounting of TPO through EHR
  - For previous 3 years (as opposed to 6)
- Compliance Date:
  - January 1, 2011
  - Reprieve for existing EHRs (as of 1/1/09):  
January 1, 2014

# Access to PHI

- Existing Law: Individual has a right to access/receive a copy of medical record
- HITECH: If CE uses/maintains an EHR
  - Right to electronic copy of records
  - Right to direct CE to transmit electronic copy to another entity or person
- Fees = no more than labor costs
- Proposed regs: Extend to all electronic health information, whether or not in EHR; can charge for electronic media if applicable

# Individually Requested Privacy Restrictions

- Existing Law: Individual has right to request privacy restrictions but binding on CE only if CE agrees
- HITECH: No disclosure to health plans for self-pay services if so requested by individual



# Minimum Necessary

- Preference for
  - De-Identified Information
  - Limited Data Sets
- Clarifications to follow



# Marketing



- Existing Law: Exceptions to “marketing” (treatment, care coordination, part of plan of benefits, etc.)
- HITECH: Marketing exceptions do not apply if CE receives direct or indirect payment for a communication unless the communication:
  - Regards a drug currently prescribed for the recipient and payment is “reasonable in amount”
  - Is made by the CE pursuant to a valid authorization in accordance with HIPAA
  - Is made by a BA, on behalf of a CE, and is consistent with its business associate contract

# Marketing



## Proposed regulations:

- Payment for communications regarding currently prescribed drugs must be reasonably related to the covered entity's cost in making the communication
- Attempt to distinguish more clearly between treatment-related communications (tailored to individual; no authorization required) and communications for health care operations (population-based communications; authorization required)
- Treatment-related communications that are subsidized by a third party must be disclosed in the Notice of Privacy Practices, and patient must be given the opportunity to opt out

# No Sale of PHI



- Existing Law: No prohibition on a CE being paid for PHI as long as the disclosure is otherwise permitted
- HITECH: Prohibits a covered entity or business associate from directly or indirectly receiving payment in exchange for any PHI without a valid authorization from the individual (that includes a specification of whether the PHI is subject to sale for re-disclosure)

# No Sale of PHI



- Exceptions:
  - Public health activities
  - Research – with price reflecting costs for preparation and transmittal
  - Treatment of the individual, subject to any regulation
  - Sale, transfer, merger, or consolidation
  - Payment to business associate for its BA services
  - Provision to an individual with a copy of his/her record
  - As otherwise determined by HHS

# No Sale of PHI



- Proposed regulations:
  - Authorization for sale of PHI must disclose that the CE is receiving remuneration for the disclosure
  - Treatment exception would be extended to include disclosures for payment
  - Permitted charges for an accounting of disclosures aren't a sale of PHI
  - Payment allowed for disclosures required by law
  - Reasonable, cost-based fee may be charged to prepare and transmit health information for any purpose for which disclosure is permitted

# Fundraising

- HITECH Act:
  - Requires regulations to provide that any written fundraising communication must provide for an opt out from further communications; CE must make reasonable efforts to ensure individuals who opt out are not sent further communications
- Proposed regulations:
  - Flat prohibition on sending communications to person who opts out
  - Opt out right must be stated in Notice of Privacy Practices
  - Opt-out mechanism must not require undue burden or more than nominal cost (email/toll-free call OK; writing a letter is not)
  - Treatment can't be conditioned on agreement to receive fundraising communications

# Decedents

- Privacy Rule:
  - Protects PHI of decedents as it does for the living
  - Information may be disclosed to personal representative, but not other family members or friends
- Proposed regulations:
  - Allow disclosure to family members, or to friends involved in care or payment for care, unless inconsistent with a prior expressed preference of the individual
  - Remove all protection for records of persons deceased more than 50 years

# Research Authorization

- Privacy Rule:
  - OK to condition participation in clinical trial on authorization
  - Research authorizations can be combined with other research-related consents
  - Research authorization can't be combined with other authorizations that can't be conditioned (e.g., authorization for tissue banking)
- Proposed regulations:
  - Allow combined authorizations, if
    - Conditioned and unconditioned research components are clearly differentiated in the authorization
    - Individual must clearly be given the option to opt in to the unconditioned research activities

# Notice of Privacy Practices

- Proposed regulations:
  - Must disclose intent to send subsidized treatment communications, if any, and provide right to opt out
  - Must notify individual of the right to opt out of fundraising solicitations, if the CE intends to send them
  - Must describe the need for an authorization for:
    - Use of psychotherapy notes
    - Marketing
    - Sale of PHI for which an authorization is required
  - Must inform the individual that the CE may not refuse a request to withhold information from a health plan where the individual pays in full for the service

# Penalties



- Tier A (if offender did not know, and by exercising reasonable diligence would not have known, that he or she violated the law): \$100 for each violation, up to \$25,000 for identical violations
- Tier B (if the violation was due to reasonable cause and not willful neglect): \$1,000 for each violation, up to \$100,000 for identical violations
- Tier C (if the violation was due to willful neglect but was corrected): \$10,000 for each violation, up to \$250,000 per year
- Tier D (if the violation was due to willful neglect and was not corrected): \$50,000, up to \$1,500,000 per year

# New Enforcement Approaches

- Clarifies/expands liability for criminal violations
- Increases civil penalties
- Harmed individuals to receive percentage of CMP
- State Attorneys General may bring civil actions
- Continuation of OCR corrective action plans
- Audits
- Proposed regs:
  - Secretary must conduct formal investigation of a complaint if preliminary investigation indicates willful neglect
  - Must conduct compliance review if preliminary review of facts indicates a possible violation due to willful neglect (no complaint required)
  - May conduct compliance reviews in any case

