HIPAA and How It Applies To You

Presented by Alessandra Swanson, Steve Flores, and Robert Newman

WINSTON & STRAWN LLP

Today’s eLunch Presenters

Alessandra Swanson

Associate, Privacy & Data Security Practice
Chicago

aswanson@winston.com

Steve Flores

Partner, Employee Benefits & Executive Compensation Practice
Chicago

saflores@winston.com

Rob Newman

Partner, Privacy & Data Security Practice
Chicago

rnewman@winston.com

Agenda

- Overview of HIPAA
- How HIPAA Affects Health Plans and Business Associates
- HIPAA Enforcement Landscape
- Best Practices for Creating HIPAA Compliance Infrastructure

Overview of HIPAA

WINSTON & STRAWN LLP

What Is HIPAA?

- HIPAA is the ***Health Insurance Portability and Accountability Act of 1996,*** as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act

- HIPAA imposes responsibilities on ***covered entities*** and, in some instances, ***business associates*** and ***subcontractors,*** related to the treatment of protected health information (PHI)

- ***Covered entities*** include health care clearinghouses, health plans, and health care providers

- ***Business Associates*** (BAs) are entities that create, receive, maintain, or transmit PHI on behalf of a covered entity. Business associates include subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate

- ***Subcontractors*** are entities to whom business associates delegate functions, activities, or services, other than in the capacity of a member of the workforce of such business associate

What Is The Purpose of HIPAA?

In the context of PHI, HIPAA has five principal functions:

- It imposes standards for the protection and security of PHI
- It governs how PHI may be used and disclosed
- When the security of PHI is compromised, it requires notification to affected individuals, the federal government, and in some cases, the media
- It gives individuals the right to access and control their PHI
- It requires entities to create compliance infrastructure

What Is Protected Health Information (PHI)?

- PHI is “individually identifiable health information” held or transmitted by a covered entity or its business associate

- This includes information about:
  - The past, present, or future physical or mental condition of an individual
  - The provision of health care to an individual
  - The past, present, or future payment for the provision of health care to the individual

- PHI maintained or transmitted in electronic form (*i.e.*, PHI that is saved in a Word document or sent via email) is referred to as ***electronic PHI*** or ***ePHI***

Examples of PHI

Exactly what constitutes PHI will vary based on an entity's business operations. However, the following are common examples of documents that may contain PHI:

- Medical records
- Any records related to an individual's involvement in a health, dental, vision, health flexible spending account, employee assistance program or health reimbursement account plan
- Lists of participants in a health, dental, vision, health flexible spending account, employee assistance program or health reimbursement account plan
- Medical claims and appeal data
- Explanation of Benefits documents
- Billing records
- Accounts receivable records
- Patient lists and patient data
- *(For business associates)* Any information designated as PHI by a covered entity client

The Privacy Rule's De-Identification Standard

Health information that is not ***individually identifiable*** is not PHI and is not protected under HIPAA. Information is not individually identifiable (or is "de-identified) if **all** of the following identifiers have been removed from the information:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code (with some exceptions)
- All elements of dates (except year) and ages directly related to an individual, including birth date, admission date, discharge date, date of death
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Overview of HIPAA Rules

HIPAA has three principal subparts:

- The Privacy Rule
- The Security Rule
- The Breach Notification Rule

The Privacy Rule (Subpart E)

The Privacy Rule regulates how PHI can be ***used*** and ***disclosed***

- A ***use*** of PHI is the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information

- A ***disclosure*** of PHI is the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information

The Privacy Rule (Subpart E)

The Privacy Rule regulates how PHI can be used and disclosed by:

- Specifying a limited set of uses and disclosures that can be made without obtaining an individual's prior written authorization (i.e., for treatment, payment, and health care operations purposes) or after giving the individual the opportunity to agree or object (i.e., for disclosures to those involved in the individual's treatment)

- Requiring a signed authorization from the subject individual for all other uses and disclosures

- Imposing requirements for the contents of a written authorization form to authorize the use or disclosure of PHI

The Privacy Rule (Subpart E)

The Privacy Rule also establishes certain rights an individual can exercise in relation to the individual's PHI. This includes:

- The right to get copies of PHI
- The right to amend PHI
- The right to request privacy protection for PHI (*i.e.*, by restricting the disclosure of PHI or receiving communications related to PHI in a confidential manner)
- The right to receive an accounting of disclosures of PHI

The Privacy Rule (Subpart E)

The Privacy Rule imposes a number of administrative requirements, including:

- Developing and implementing written policies and procedures
- Training workforce members who handle PHI and establishing sanctions for the misuse of PHI
- Establishing a complaint receipt process
- Designating a privacy officer
- Entering into agreements with business associates who handle PHI
- Providing notices of privacy practices to individuals

The Security Rule (Subpart C)

- Imposes administrative, technical, and physical safeguard requirements to ensure the confidentiality, integrity, and availability of all ***electronic PHI*** created, received, maintained, or transmitted by the covered entity or business associate

- ***Electronic PHI*** is PHI that is transmitted by electronic media or maintained in electronic media

The Security Rule – Administrative Safeguards

- Security Management Process
- Risk Analysis
- Risk Management
- Sanctions Policy
- Information System Activity Review
- Assigned Security Responsibility
- Workforce Security
- Authorization and/or Supervision (Addressable)
- Workforce Clearance Procedure (Addressable)
- Termination Procedures (Addressable)
- Information Access Management
- Isolating Health Care Clearinghouse Functions
- Access Authorization (Addressable)
- Access Establishment and Modification (Addressable)
- Security Awareness Training
- Security Reminders (Addressable)
- Protection from Malicious Software (Addressable)
- Log-in Monitoring (Addressable)
- Password Management (Addressable)
- Security Incident Procedures
- Response and Reporting
- Contingency Plan
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing and Revision Procedures (Addressable)
- Applications and Data Criticality Analysis (Addressable)
- Evaluation

The Security Rule – Physical Safeguards

- Facility Access Controls
- Contingency Operations (Addressable)
- Facility Security Plan (Addressable)
- Access Control and Validation Procedures (Addressable)
- Maintenance Records (Addressable)
- Workstation Use
- Workstation Security
- Device and Media Controls
- Disposal
- Media Re-use
- Accountability (Addressable)
- Data Backup and Storage (Addressable)

The Security Rule – Technical Safeguards

- Access Controls
- Unique Employee Identification
- Emergency Access Procedure
- Automatic Logoff (Addressable)
- Encryption and Decryption (Addressable)
- Audit Controls
- Integrity
- Mechanism to Authenticate ePHI
- Person or Entity Authentication
- Transmission Security
- Integrity Controls (Addressable)
- Encryption (Addressable)

The Security Rule – Administrative Requirements

The Security Rule also imposes administrative requirements, including:

- Entering into written agreements with business associates (and subcontractors) as appropriate
- Developing written policies and procedures to implement the safeguards

Required and Addressable Specifications

- ***Required*** specifications of the Security Rule must be implemented
- ***Addressable*** specifications are not required and are also not optional
  - An entity has three options related to addressable specifications:
    - Implement the addressable specification
    - Implement one or more alternative security measures to accomplish the same purpose
    - Decline to implement either an addressable implementation specification or an alternative
  - The covered entity's choice must be documented in writing
  - The standard is whether the specification is "reasonable and appropriate" for the entity in consideration of factors like entity's risk analysis, risk mitigation strategy, other safeguards that are already in place, and the cost of implementing the specification

The Breach Notification Rule (Subpart D)

- The Breach Notification Rule establishes what constitutes a breach of unsecured PHI and subsequent notification responsibilities
- A ***breach*** is the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the PHI
  - This excludes:
    - Any unintentional acquisition, access, or use of PHI made in good faith by a workforce member or person acting under the authority of a covered entity or BA
    - Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or BA to another person authorized to access PHI at the same covered entity or BA
    - A disclosure of PHI where a covered entity or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information
- What is unsecured PHI?
  - PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons (*i.e.*, it's not encrypted)

Breach Standards and Specifications

- A breach is *presumed* unless the entity can demonstrate through a risk assessment that there was a low probability that the PHI was compromised
- A risk assessment must evaluate the following:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated
- If a breach of unsecured PHI occurs:
  - Business associates must notify covered entities without unreasonable delay (and within 60 days)
  - Covered entities and/or BAs must then provide specific details in notifications to:
    - Secretary of Health and Human Services(through HHS-OCR)
    - Affected individuals
    - The media (if over 500 individuals in a jurisdiction were affected)

How HIPAA Affects Health Plans and Business Associates

WINSTON & STRAWN LLP

Health Plans Subject to HIPAA

- A covered entity includes a health plan
- A health plan includes an individual or group plan that provides, or pays the cost of, medical care, such as:
  - ERISA employee welfare benefit plans (insured or self-insured) that provide medical care, if the plan
    - has at least 50 participants, or
    - is administered by an entity other than plan sponsor

Health Plans Subject to HIPAA

- This means that the following types of plans can be covered entities:
  - Medical plans
  - Dental plans
  - Vision plans
  - Health flexible spending accounts
  - Health reimbursement arrangements
  - Employee assistance plans
  - Retiree health plans
  - Wellness plans

Distinction Between Employer and Health Plan

- Employers often perform administrative functions on behalf of the health plan
- Common examples include
  - Handling reimbursement requests
  - Deciding claims and appeals
  - Plan audits
- To receive PHI from a health plan, the employer must:
  - Agree to comply with certain HIPAA requirements and to amend its plans
  - Implement HIPAA policies and procedures
  - Distribute notice of privacy practices
  - Ensure business associate agreements are in place

Distinction Between Employer and Health Plan

- Employers who perform health plan functions and their health plans are distinct legal entities
- Distinction between employer information and health plan information can be confusing
  - The same information may or may not be PHI depending on the circumstances
  - Ask yourself:
    - What type of information is being transmitted?
    - What is the source of the information?
    - What is the information being used for?

Health Plans Subject to HIPAA

- The distinction between fully insured and self-insured health plans is important
  - "Hands off" approach where employer receives no PHI or only certain types of PHI is subject to more limited HIPAA requirements
  - Self-insured plans are subject to a full array of HIPAA requirements even if a third party administrator is used

When Do Business Associates Need to Worry About HIPAA?

- **Per the regulation:** When you create, receive, maintain, or transmit PHI on behalf of a covered entity. This may include providing services like claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management; or, when the services involve the disclosure of PHI, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services

- **In reality:** When a client hands you a business associate agreement and says, “Here. Sign this”

Business Associate Agreements

- Covered entities and business associates are required to enter into written business associate agreements with any entities that create, receive, maintain or transmit PHI on their behalf

- The Privacy Rule specifies certain terms that must be included in a business associate agreement, including:
  - Establishing permitted uses and disclosures of PHI
  - Requiring the business associate to comply with the Security Rule
  - Requiring the business associate to report breaches to the covered entity
  - Requiring the business associate to enter into agreements with subcontractors that contain terms at least as strict as the corresponding business associate agreements
  - Requiring the business associate to make PHI available for access, amendment, and accounting of disclosure purposes
  - Requiring the business associate to make its practices/books/records available to Secretary for evaluation of its HIPAA compliance
  - Requiring the business associate to return/destroy all PHI at termination of contract

The HIPAA Enforcement Process

WINSTON & STRAWN LLP

Who Enforces HIPAA

- Primary regulator is the ***U.S. Department of Health and Human Services, Office for Civil Rights (OCR)***
- OCR is comprised of Washington, D.C. office and eight regional offices
  - **New England Region** (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont)
  - **Eastern and Caribbean Region** (New Jersey, New York, Puerto Rico, Virgin Islands)
  - **Mid-Atlantic Region** (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia)
  - **Southeast Region** (Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee)
  - **Midwest Region** (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, Ohio, Wisconsin)
  - **Southwest Region** (Arkansas, Louisiana, New Mexico, Oklahoma, Texas)
  - **Rocky Mountain Region** (Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming)
  - **Pacific Region** (Alaska, American Samoa, Arizona, California, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Guam, Hawaii, Idaho, Marshall Islands, Nevada, Oregon, Republic of Palau, Washington)
- ***State Attorneys General*** also have the ability to bring actions on behalf of affected constituents
- No private right of action under HIPAA, but ***class action cases*** may be brought following breaches on various causes of action

What May Trigger OCR Inquiries

HIPAA Audit Program – Phase II

- Audits began in July 2016 and will be carried out in three waves, with approximately 200-250 audits in total
  - The first wave launched in the summer, and consists of desk audits of covered entities
    - As part of the audits, the covered entities have been asked to identify their business associates
  - The second wave, also in progress, consists of desk audits of business associates
    - OCR has indicated it would select the business associate auditees based in part on the business associates identified during the first wave
  - The third wave, scheduled to roll out in 2017, will involve a small number of comprehensive on-site audits
    - OCR noted it could opt to conduct an on-site audit for an entity that had already undergone the desk audit process

How OCR Enforces HIPAA

- No Investigation
- Technical Assistance Letter
- Disposition Based on Corrective Action Taken
- Enforcement Case

2016 HIPAA Enforcement Highlights

- OCR significantly ramped up formal enforcement actions for HIPAA violations with 13 enforcement actions (100% increase over 2015) and approximately $23.5M in settlements (400% increase over 2015)

- The perennial “most popular” violation is the failure to conduct accurate and thorough risk analyses.

- 2016 settlements demonstrated an increased emphasis on business associate agreements and continued emphasis on policies and procedures requirements

- While earlier enforcement cases focused on entities that lacked HIPAA infrastructure, recent cases reveal that established compliance measures are now being closely scrutinized

Breach Reports – OCR Keeps Tabs!

- In 2016, OCR announced an initiative to investigate breaches affecting under 500 individuals

- In August, OCR settled with Advocate Health Care for $5,550,000 after OCR received three breach reports involving various Advocate entities in a four-month period

- In January, OCR settled with Presence Health for $475,000 for its failure to submit timely breach reports to HHS and affected individuals

Recent Enforcement Cases

- Children's Medical Center of Dallas – $3,217,000 *(February 1, 2017)*
- MAPFRE Life Insurance Company of Puerto Rico – $2,200,000 *(January 18, 2017)*
- Presence Health – $475,000 *(January 9, 2017)*
- University of Massachusetts Amherst – $650,000 *(November 22, 2016)*
- St. Joseph Health – $2,140,500 *(October 17, 2016)*
- Care New England Health System – $400,000 *(September 23, 2016)*
- Advocate Health Care Network – $5,550,000 *(August 4, 2016)*
- University of Mississippi Medical Center – $2,750,000 *(July 21, 2016)*

Best Practices for Creating HIPAA Compliance Infrastructure

WINSTON & STRAWN LLP

Translating Regulations Into Infrastructure

- OCR Website (the hub for all things HIPAA-related)
- Audit Protocol (describes standards of review used by OCR during the audit process)
- Security Rule Guidance Materials (provides insight on how to translate Security Rule specifications into safeguards)
- ONC Security Risk Assessment Tool (guides small- and medium-sized entities through the process of conducting a risk analysis)
- HIPAA FAQs for Professionals (provides information about how to interpret HIPAA specifications)
- NIST/OCR Security Rule Crosswalk (tags Security Rule standards to established NIST standards)
- OCR Enforcement Examples (contains press releases, resolution agreements, and corrective action plans for all of OCR's formal enforcement actions)

Initial Diligence

- Get the lay of the land – each entity's HIPAA compliance infrastructure will look different based on its status (covered entity v. business associate), workforce members, and business operations

- As appropriate, initial diligence may include:
  - Identifying who works with PHI
  - Understanding where PHI "lives" within the organization
  - Determining what workforce members are doing with PHI
  - Establishing ingress and egress points for PHI
  - Examining past policies and procedures and training documents

Additional Considerations

- Written policies and procedures are required
- Policies and procedures must include both “policies” and “procedures”
- Workforce members should be able to comply with the policies and procedures (red flag to regulators – and class action attorneys – if policies and procedures are ignored or not appropriately followed)
- A comprehensive and enterprise-wide risk analysis is the foundation of a Security Rule compliance program
- “Addressable” specifications of the Security Rule are not optional
- Everything is fair game if a regulator comes knocking on your door

Security Rule Implementation

- Look at what is going on in your organization – what works for another company may not work for you
  - This is especially true for business associates who may only have special projects or very limited circumstances where they interact with PHI
- Examine the IT policies and procedures already in place to harmonize implementation of HIPAA and other legal/industry security requirements
  - Do you already have password requirements?
  - Do you already have access termination procedures?
- Use available resources to better understand regulatory expectations
  - The Security Risk Assessment Tool and NIST crosswalk were created in collaboration with OCR to assist in Security Rule implementation

- It may be helpful to map out how ePHI flows into, through, and out of the organization, what happens to it along the way, and how it is protected (or not protected)
  - Where does it come from?
  - How is it received?
  - Who touches it?
  - Where is it stored?
  - How is it shared?
  - What is done with it?
  - Where is it sent?
  - How is it sent?
  - How is it protected throughout this journey?
  - What other safeguards should be in place to protect the ePHI?

Implementation Example – Maintenance Records

- Maintenance Records (Addressable) *("Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks")*
- OCR's audit criteria provides the following insights:

Does the entity have policies and procedures in place to document repairs and modifications to the physical components of a facility which are related to security?

Does the entity document repairs and modifications to the physical components of a facility which are related to security?

Obtain and review such policies and procedures related to maintaining maintenance records. Evaluate the content in relation to the specified performance criteria for documenting repairs and modifications to the physical components of a facility related to security.

Elements to review but are not limited to:
• Workforce members' roles and responsibilities in repairs and modification to the physical components
• Record-keeping process of repairs and modification to the physical components
• Specification of when repairs or modification of physical security components are required
• Authorization process of repairs or modification of physical security components

Obtain and review documentation demonstrating records of repairs and modifications to physical security components. Evaluate and determine if records of repairs and modifications are being tracked and reviewed on periodic basis by authorized personnel.

Has the entity chosen to implement an alternative measure?
If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead.
Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.

Implementation Example – Maintenance Records

- ***Remember:*** Addressable specifications should be implemented if it is reasonable and appropriate to do so, and an organization must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative
- In practical terms, this involves assessing whether it is "reasonable and appropriate" to implement this safeguard
  - Does the organization have control over repairs made to the facility?
  - Would repairs made to the facility impact the security of ePHI under the organization's purview?
    - If not – why?
  - Does the organization have compensating controls in place?
- Decision should be documented in writing

Privacy Rule Implementation

It may be helpful to break the compliance program into digestible chunks:

- *(For health plans)* Making sure plan documents are updated
- What to know before using and disclosing PHI
  - *Including what constitutes PHI, verification procedures, minimum necessary standard, authorization requirements, etc.*
- How PHI may be used or disclosed
  - *Helping workforce members understand when they can use and disclose PHI for things like treatment, payment and health care operations purposes*
- How PHI should be safeguarded
  - *Including guidelines on how to safeguard paper PHI and best practices when discussing PHI*
- How to respond to individual requests
  - *Including what to do when a workforce member receives a request for an amendment or access to PHI*
- How to implement administrative requirements
  - *Including how to vet/contract with business associates, appointing a privacy official, implementing investigation and sanctions procedures*

Implementation Example – Verification

- 45 C.F.R. 164.514(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:
- (i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and
- (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.
- (2) *Implementation specifications: Verification*—(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.
- (A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.
- (B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).
- (ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
- (A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- (B) If the request is in writing, the request is on the appropriate government letterhead; or
- (C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- (iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
- (A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
- (B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.
- (iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

Implementation Example – Verification

It may be helpful to consider:

- Who generally requests disclosures of PHI?
  - Members of the health plan? Business associates? Subcontractors? Government officials?
- Under what circumstances might a workforce member need to verify someone's identity or authority?
  - In person? Over the phone? After receiving a letter or email?
- Who might receive such a request?
  - HR Director? General Counsel? Privacy Officer?
- Should the workforce member complete the verification, or should someone else in the organization handle it?
  - Should the General Counsel or Privacy Officer handle all such requests, or only out of the ordinary requests, like requests from public officials?
- When might documentation need to be collected in connection with the request? Who should ultimately receive this documentation and where should it be stored?
- What are the current verification procedures, and are they sufficient given the most recent analysis?

Implementation Example – Verification

- Depending on business operations, the analysis may be distilled down into a policy and procedure that covers:
  - Who should receive disclosure requests
  - Who should be responsible for verifying identity and authority of individual requesting PHI
  - How identity and authority should be verified in the different scenarios that may occur (over the telephone, in person, etc.)
  - Who should be responsible for collecting any relevant paperwork
  - Where relevant paperwork should be stored

- As always, there is a balance between creating accurate procedures and ensuring that it is reasonable for workforce members to follow such procedures

Breach Notification Rule Implementation

- It may be helpful to take a holistic look at all of the issues that may impact your organization's ability to fulfill its breach notification responsibilities, including:
  - The Security Rule's Security Incident Procedures, Response and Reporting, Security Awareness Training, and Security Reminder specifications
  - The Privacy Rule's training requirements
  - How employees are using and disclosing PHI (*i.e.*, how they transmit paper-based PHI and ePHI)
  - The types of security incidents that are "popular" or have previously occurred
  - What general security incident procedures are already in place

Breach Notification Rule Implementation

- Depending on business operations, Breach Notification Rule infrastructure may incorporate:
  - Enabling workforce members to recognize a potential or actual breach or security incident, through training, email reminders, and incorporating examples into policies and procedures
  - Providing instructions to inform workforce members how to respond and who to contact in case of a potential or actual breach or security incident
  - Coordinating HIPAA risk assessment and notification requirements with existing incident procedures to avoid gaps in reporting, investigating and providing notification of breaches

Thank You.

Alessandra Swanson

Associate, Privacy & Data Security Practice
Chicago

aswanson@winston.com

Steve Flores

Partner, Employee Benefits & Executive Compensation Practice
Chicago

saflores@winston.com

Rob Newman

Partner, Privacy & Data Security Practice
Chicago

rnewman@winston.com