HUNTON
ANDREWS KURTH

HIP, HIP-AA, Hooray! A Plan Sponsor's Guide to HIPAA Privacy and Security Compliance

Presentation for:
Employee Benefits Academy
May 2, 2024

Presentation by:
Lisa Sotto, Partner, Hunton Andrews Kurth
Michelle Lewis, Partner, Hunton Andrews Kurth
Elizabeth Breen, Counsel, Hunton Andrews Kurth

Housekeeping: Questions

HUNTON
ANDREWS KURTH

- Questions during this presentation
  - We encourage questions (even though your audio lines are muted)
  - To submit a question, simply type the question in the blank field on the right-hand side of the menu bar and press return
  - If time permits, your questions will be answered at the end of this presentation.

Housekeeping: Recording, CE Credits and Disclaimer

HUNTON ANDREWS KURTH

- Recording
  - This presentation is being recorded for internal purposes only
- Continuing education credits
  - A purpose of the webinar series is to provide FREE CE credits
  - To that end, each presentation is intended to provide 1 credit hour in the following areas:
    - CLE: 1 credit hour (CA, FL, GA, NC, NY, TX and VA)
    - CPE: 1 credit hour (Texas)
    - HRCI: This activity has been approved for 1 (HR (General)) recertification credit hours toward California, GPHR, PHRi, SPHRI, PHR, and SPHR recertification through the HR Certification Institute
    - SHRM: This program is valid for 1 PDC for the SHRM-CPSM or SHRM-SCPSM
  - If you have any questions relating to CE credits, please contact Anna Carpenter at acarpenter2@huntonak.com.
- Disclaimer
  - This presentation is intended for informational and educational purposes only, and cannot be relied upon as legal advice
  - Any assumptions used in this presentation are for illustrative purposes only
  - No attorney-client relationship is created due to your attending this presentation or due to your receipt of program materials

Lisa Sotto

HUNTON
ANDREWS KURTH

Partner
Email: lsotto@HuntonAK.com
Phone: 212-309-1223

200 Park Avenue
New York, NY 10166

Lisa Sotto is a partner and chair of Hunton's Global Privacy and Cybersecurity practice. Well-known in the field as a "legend" and "market leader," Lisa was rated the "No. 1 privacy expert" in all surveys by *Computerworld* magazine, is ranked as a "Star Individual" for privacy and data security by Chambers and Partners, and is recognized in the Hall of Fame for cyber law, privacy and data protection by *The Legal 500 United States*. Appointed by Secretaries Mayorkas, Nielson, Johnson, Napolitano, Lisa serves as Chair of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Elizabeth Breen

HUNTON
ANDREWS KURTH

Counsel
Email: ebreen@HuntonAK.com
Phone: 804-787-8920

951 East Byrd Street
Richmond, VA 23219

Elizabeth's practice focuses on representing integrated health systems, academic medical centers, hospitals and other health care providers, and on representing health care technology and services companies.

Elizabeth routinely advises on health care transactional and operational matters, addressing federal and state health care regulatory compliance issues, including "Stark" and anti-kickback law compliance, health privacy and security, certificate of public need and licensure issues.

Michelle Lewis

HUNTON
ANDREWS KURTH

Partner
Email: mlewis@HuntonAK.com
Phone: 202-955-1859

2200 Pennsylvania Avenue NW
Washington, DC 20037

Michelle concentrates her practice in the areas of health and welfare plans, qualified retirement plans, and executive deferred compensation plans.

She delivers insightful and practical advice to clients in addressing a broad spectrum of employee benefit issues, including drafting plan documents, preparing IRS submissions, resolving ERISA and Internal Revenue Code compliance issues, advising on benefit claims and appeals, addressing various litigation issues, and negotiating employee benefit vendor contracts and HIPAA business associate agreements.

Overview

HUNTON ANDREWS KURTH

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Federal law that sets forth permissible uses and disclosures of "protected health information" (PHI)
  - Provides individuals with certain rights
  - Sets forth specific information security safeguards for "electronic" PHI (ePHI)
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
  - The first federal law for private-sector data breach notification
  - Imposed direct liability on Business Associates

HIPAA Regulations: The Privacy Rule

What is Protected Health Information?

HUNTON ANDREWS KURTH

- Protected Health Information (PHI)
  - Individually identifiable health information created or received by a Covered Entity (e.g., most health care providers, health plans, and health care clearinghouses)
  - Relates to an individual's physical or mental health, provision of health care to an individual, or payment for provision of health care to an individual

What is not PHI?: De-Identified Information

HUNTON ANDREWS KURTH

- PHI can be de-identified, in which case it no longer is covered by HIPAA. This can be accomplished in two ways:
  - *Expert Determination* – A qualified professional determines that the risk is very small that the information could be used to re-identify an individual
  - *Safe Harbor* – Along with no actual knowledge that the information could be used to identify the individual, 18 identifiers must be removed:

1. Names
2. Certain geographic information (e.g., ZIP code, street address, city)
3. Certain dates and ages (e.g., admission dates, ages over 89)
4. Telephone numbers
5. Vehicle IDs and serial numbers
6. Fax numbers
7. Device IDs and serial numbers
8. Email addresses
9. URLs
10. SSNs
11. IP addresses
12. Medical record numbers
13. Biometric identifiers
14. Health plan beneficiary numbers
15. Full-face photographs
16. Account numbers
17. Certain unique ID numbers and codes
18. Certificate/license numbers

What is not PHI?: Other Exceptions

HUNTON ANDREWS KURTH

- PHI excludes health information found in certain records, such as:
  - Certain education records
  - Employment records held by a Covered Entity in its role as employer, including FMLA records and information related to workers' compensation and life insurance
  - Records regarding a person who has been deceased for more than 50 years

Privacy Rule: Key Definitions

HUNTON ANDREWS KURTH

- Covered Entity
  - Health care providers who transmit health information in electronic form in connection with a standard transaction
  - Health plans
    - Includes health insurers and employer group health plans
    - Does not include disability, worker's compensation or non-medical insurance
  - Health care clearinghouses – an entity that transmits claims and billing information between other players in the health care system
    - Example: a hospital sends the bill for a patient's treatment to a health care clearinghouse that will reformat and submit the information to an insurance company
- An employer's health plan is a Covered Entity

Privacy Rule: Key Definitions

HUNTON ANDREWS KURTH

- Business Associate
- An entity that, on behalf of a Covered Entity:
  - Creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA Privacy Rule, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management and repricing; or
  - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity, where the provision of the service involves the disclosure of PHI from the Covered Entity to the entity

Relationship between Covered Entities and Business Associates

HUNTON ANDREWS KURTH

- Governed by a contract known as a Business Associate Agreement (BAA)
- A BAA is typically an addendum or exhibit to an underlying services agreement
- A BAA must contain certain content. For example:
  - A Business Associate may not use or further disclose PHI other than as permitted or required by the BAA or as required by law
  - A Business Associate must ensure that any subcontractors agree to the same restrictions on the use or disclosure of PHI
  - A Business Associate must notify the Covered Entity of a breach of unsecured PHI

Use and Disclosure

HUNTON ANDREWS KURTH

- Generally, PHI cannot be used or disclosed without the individual's "Authorization"
- An authorization must:
  - Be written and signed
  - Describe the PHI, recipient and purposes of the use/disclosure
  - Provide an expiration date or event
  - Allow the individual to revoke the authorization

Use and Disclosure Exceptions

HUNTON
ANDREWS KURTH

- Exceptions to Authorization Requirement:
  - Payment, treatment or healthcare operations
  - If required for certain public health or safety reasons
  - If made to the individual (or, in certain limited cases, to a family member or close friend – see below)
  - If required by law
  - Disclosures to Business Associates under a BAA

Use and Disclosure Exceptions

HUNTON ANDREWS KURTH

- Exception for payment, treatment and plan operations
  - Payment includes the payment for health care, and the provision of health care benefits (e.g., eligibility determinations, health claim adjudication/subrogation, billings claims management, review of medical necessity and justification of charges and utilization review)
  - Treatment includes the provision, coordination and management of health care by health care providers (e.g., consultations between health care providers and referrals)
  - Operations include quality assessment, case management, treatment alternatives, medical review and audit, and general administration of the healthcare plan

Use and Disclosure Exceptions

HUNTON
ANDREWS KURTH

- Healthcare plan operations *exclude* the use of genetic information
- Genetic information may not be used for underwriting purposes
  - Eligibility determinations
  - Premium computations
  - Preexisting condition exclusions
- Genetic information includes genetic test results of the individual or family members, any disease or disorder of the individual or family members, and a request for or receipt of genetic services

Use and Disclosure Exceptions

HUNTON ANDREWS KURTH

- Disclosure may be made to family and friends without an authorization if:
  - The individual is given the opportunity to agree/object (can be oral); or
  - The individual is either incapacitated or not present, so long as:
    - The family member/friend is involved in the individual's health care or payment for health care; and
    - Disclosure is in the best interest of the individual, as determined by the covered entity in the exercise of professional judgment
    - The PHI disclosed is limited to PHI that is directly relevant to the family/member friend's involvement

Minimum Necessary Requirement

HUNTON ANDREWS KURTH

- In general, covered entities and their business associates must take reasonable steps to limit PHI uses and disclosures to the minimum necessary to accomplish the intended purposes.
- Minimum necessary does not apply to:
  - Disclosures to or requests by a health care provider for treatment
  - Disclosures to the individual who is the subject of the PHI
  - Uses or disclosures pursuant to an authorization
  - Use or disclosures required for HIPAA Administrative Simplification Rules compliance.
  - Disclosures to HHA when required under the Privacy Rule for enforcement
  - Uses or disclosures required by law

Individual Rights

HUNTON ANDREWS KURTH

- Plan participants have a number of rights relating to their PHI:
  - Accessing PHI
  - Amending PHI
  - Receiving an accounting of disclosures of PHI
  - Requesting additional restrictions on the disclosure of PHI
  - Alternative communication methods
  - Receiving notices of breaches of unsecured PHI

Key Requirements for Covered Entities

HUNTON ANDREWS KURTH

- The Privacy Rule requires Covered Entities to:
  - Provide a Notice of Privacy Practices that contains certain elements (e.g., a description of individuals' rights under HIPAA)
  - Develop privacy policies and procedures that are consistent with the Privacy Rule
  - Designate a HIPAA Privacy Official responsible for overseeing compliance with HIPAA
  - Train relevant workforce members on HIPAA compliance
  - Execute BAAs with vendors that handle PHI on the Covered Entity's behalf

HIPAA Regulations: The Security Rule

Security Rule: Key Concepts

HUNTON ANDREWS KURTH

- Need to develop and implement administrative, physical and technical safeguards for ePHI
- Key definitions:
  - ePHI: PHI that is transmitted or maintained in electronic media
  - Electronic Media:
    - Electronic storage media: computer hard drives, digital memory cards
    - Transmission media used to exchange information already in electronic storage media

Security Rule: Standards and Implementation Specifications

HUNTON ANDREWS KURTH

- *Standards*: general security areas to be addressed
- *Implementation specifications*: safeguards adopted to address specific standards that are either:
  - Required – must be implemented
  - Addressable – presumed reasonable and appropriate for implementation but an alternative may be adopted
- Security measures must be reviewed and modified as needed to continue to provide reasonable protection of ePHI

Security Rule: Administrative Safeguards

HUNTON ANDREWS KURTH

- What are Administrative Safeguards?
  - Administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of the entity's workforce in relation to the protection of that information
- Examples of Administrative Safeguards include:
  - Risk analysis
  - Assigned security responsibility
  - Access authorization
  - Log-in monitoring
  - Breach response and reporting

Security Rule: Physical Safeguards

HUNTON ANDREWS KURTH

- What are Physical Safeguards?
  - Physical measures, policies, and procedures to protect an entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion
- Examples of Physical Safeguards include:
  - Contingency operations
  - Access control and validation procedures
  - Workstation security
  - Data disposal
  - Media re-use
  - Accountability

Security Rule: Technical Safeguards

HUNTON ANDREWS KURTH

- What are Technical Safeguards?
  - The technology (and the policies and procedures for its use) that protect and control access to ePHI
- Examples of Technical Safeguards include:
  - Unique user identification
  - Automatic logoff
  - Audit controls
  - Mechanism to authenticate ePHI
  - Encryption

HIPAA Regulations: The Breach Notification Rule

Breach Notification Rule: Definitions

HUNTON ANDREWS KURTH

- "Breach" is the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of PHI
- Notification is required only if the breach involves "unsecured" PHI
- Unsecured PHI
  - PHI not rendered unusable, unreadable, or indecipherable to unauthorized individuals
  - Only encryption and destruction render PHI "secured"

Breach Notification Rule: Risk Assessment

HUNTON ANDREWS KURTH

- Entities are not required to report breaches for which there is a "low probability of compromise" to PHI, which must be demonstrated through a documented risk assessment that considers at least the following four factors:

(1) nature and extent of the PHI
(2) the unauthorized person who used the PHI or to whom the disclosure was made
(3) whether the PHI was actually acquired or viewed
(4) the extent to which the risk to the PHI has been mitigated

Breach Notification Rule: Exclusions

HUNTON ANDREWS KURTH

- "Breach" excludes:
  - Unintentional good faith acquisition, access, or use of PHI by a workforce member
  - Inadvertent disclosure to another person authorized to access PHI
  - Disclosure to an unauthorized person who would not reasonably have been able to retain such information

Breach Notification Rule: Content and Timing

HUNTON ANDREWS KURTH

- **Notification Content Requirements**
  - What happened, date of breach, date of discovery
  - Types of unsecured PHI involved
  - How individuals can protect themselves
  - Investigation and mitigation efforts
  - Contact information
- **Timing of Notification**
  - *Covered Entities*
    - Must notify affected individuals within 60 days of discovery
    - Must notify HHS within 60 days if >500 individuals are affected or within 60 days of the end of the calendar year if <500 individuals are affected
    - Must notify the media within 60 days of discovery if >500 individuals are affected
  - *Business Associates*
    - Must notify Covered Entities within 60 days of discovery
    - May be fewer days as specified contractually in BAAs

HIPAA Enforcement: Violations and Penalties

HIPAA Penalty Scheme

HUNTON ANDREWS KURTH

- Penalties are based on the level of knowledge by the entity that violated the HIPAA Rules
  - Did not know: entity did not know it violated HIPAA Rules and, even if it exercised reasonable diligence, would not have known it violated HIPAA Rules
  - Reasonable cause: entity knew, or by exercising reasonable diligence would have known, it violated HIPAA Rules, but did not act with willful neglect
  - Willful neglect, corrected within 30 days: entity willfully neglected HIPAA Rules but corrected its violation within 30 days
  - Willful neglect, not corrected within 30 days: entity willfully neglected HIPAA Rules and did not correct its violation within 30 days

Violations and Penalties

HUNTON ANDREWS KURTH

Violation Category	Penalty per Violation (2024)	Maximum Yearly Penalty for All Violations (2024)
Did Not Know	$137 to $68,928	$2,067,813
Reasonable Cause	$1,379 to $68,928	$2,067,813
Willful Neglect (corrected in 30 days)	$13,785 to $68,928	$2,067,813
Willful Neglect (not corrected in 30 days)	$68,928	$2,067,813

- Some violations are tolled on a daily basis (e.g., number of days without a compliant risk analysis), while others may be tolled per occurrence (e.g., number of individuals' records disclosed during a breach)

A Health Plan's Obligations as a Covered Entity

Privacy Rule Obligations

HUNTON
ANDREWS KURTH

- Provide a Notice of Privacy Practices that contains specified elements
- Develop privacy policies and procedures that are consistent with the Privacy Rule
- Take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose
- Designate a HIPAA Privacy Official responsible for overseeing HIPAA compliance
- Train employees who have access to PHI on HIPAA compliance

Privacy Rule Obligations

HUNTON ANDREWS KURTH

- Business Associate Agreements
  - Contracts with vendors (Business Associates) that handle PHI
  - BAA must contain certain content, such as:
    - A limitation that the Business Associate may use or disclose the PHI only as permitted by the agreement or as required by law
    - A requirement that the Business Associate report any "security incident" (as defined by the Security Rule) to the health plan
    - An authorization for the BAA to be terminated if the health plan determines that a material term of the BAA has been violated
  - Can contain other standard (but not required) contractual provisions (e.g., breach reimbursement, indemnity, anti-assignment clause)

Privacy Rule Obligations

HUNTON ANDREWS KURTH

- Prohibition on sale of PHI without an individual's authorization
- Authorizations must contain certain elements, and exceptions to the requirement include disclosures that are required by law or that are requested for judicial or administrative proceedings
- Limits on use of PHI for marketing and fundraising

Security Rule Obligations

HUNTON ANDREWS KURTH

- Implement administrative, physical and technical safeguards to protect ePHI
  - For example, a health plan must have written HIPAA policies and procedures in place to comply with the Security Rule
- Ensure that Business Associates agree to protect ePHI (i.e., via a BAA)

Breach Notification Rule Obligations

HUNTON ANDREWS KURTH

- First, perform a risk assessment to determine if a "breach" of unsecured PHI has occurred
  - Is there a "low probability" that PHI was compromised?
  - Document results of risk assessment
- Second, report a "breach" of unsecured PHI to affected individuals, HHS, and the media, as applicable
  - Must notify affected individuals within 60 days of discovery
  - Must notify HHS within 60 days if >500 individuals are affected or within 60 days of the end of the calendar year if <500 individuals are affected
  - Must notify the media within 60 days of discovery if >500 individuals are affected

Upcoming Webinars

HUNTON ANDREWS KURTH

Executive Compensation Academy

- Title: Comparing and Contrasting Equity Awards: A Life Cycle Approach
- When: May 9, 2024
- Time: 10:00 am – 11:00 am CT
  11:00 am – 12:00 pm ET