CIS 2018 Annual Conference

HIPAA Update

Walter W. Miller
Schwabe, Williamson & Wyatt, P.C.

Schwabe WILLIAMSON & WYATT

PURPOSE OF THE HIPAA PRIVACY RULE

- The HIPAA Privacy Rule first became effective in 2003
- Its purpose is to ensure that health plans and health care providers keep each individual's health information as confidential and as securely safeguarded as is reasonably possible
- It is enforced by the Department of Health and Human Services (the "HHS") Office of Civil Rights ("OCR")

Schwabe WILLIAMSON & WYATT

COVERED ENTITIES

- The HIPAA Privacy Rule pertains only to "covered entities"
- Covered entities are:
  - Health care providers
  - Health plans
- An employer, in its role as an employer, is not a covered entity, and therefore is not directly governed by the Privacy Rule

Schwabe WILLIAMSON & WYATT

COVERED ENTITIES

- CIS Trust is a health plan
  - Governed by HIPAA
- CIS members are not HIPAA-governed via CIS Trust
- May be governed by HIPAA via sponsorship of their own health plan (e.g., an HRA)

Schwabe WILLIAMSON & WYATT

COVERED ENTITIES

- Municipalities are HIPAA-covered entities via public health services (i.e., as a health care provider)
- Hybrid status
  - Part HIPAA health care; part not
- Must define and designate its health care components

Schwabe WILLIAMSON & WYATT

FIRE FIGHTERS

- Fire fighters, if not EMTs, do not provide medical services
- Ergo, typically not subject to the HIPAA Privacy Rule

Schwabe WILLIAMSON & WYATT

EMERGENCY MEDICAL SERVICES

- Generally, an EMT is a health care provider for purposes of HIPAA
- May freely disclose PHI for treatment purposes
  - E.g., calling ahead to hospital regarding injury

Schwabe WILLIAMSON & WYATT

EXAMPLES OF EMS PHI

- Call for Service Reports (CFS)
- Patient Care Report (PCR)
- Transport Care Report (ACR)
- EGG Strips
- Medical Release / Billing Information Form
- Photographs

Schwabe WILLIAMSON & WYATT

LAW ENFORCEMENT

- Police are not governed by HIPAA
- A covered entity may disclose PHI to police:
  - For court-ordered proceedings
  - In response to qualified subpoenas
  - To locate a suspect of missing person
  - When required by law (e.g., reporting of gunshot wound)

Schwabe WILLIAMSON & WYATT

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

Schwabe WILLIAMSON & WYATT

WHAT IS PHI?

- PHI is "individually identifiable" information that is created or received by a covered entity, and which relates either to:
  - The past, present, or future physical or mental health or condition of the person;
  - The provision of health care to the individual; or
  - The past, present or future payment for the provision of health care to the person.

Schwabe WILLIAMSON & WYATT

WHAT IS PHI?

- Health information is "individually identifiable" if it either:
  - Identifies the individual to whom it relates; or
  - Creates a reasonable basis on the part of the disclosing entity for believing that the information may be used to identify the individual (i.e., putting 2 and 2 together).

Schwabe WILLIAMSON & WYATT

WHAT IS PHI?

- To be PHI, information must be created or received by the covered entity
- Information created or received by an employer, in its role as employer, is not PHI
- Enrollment information becomes PHI once it is in the hands of the plan

Schwabe WILLIAMSON & WYATT

WHAT ISN'T PHI?

- Types of medical information commonly received by an employer in its role as an employer that is NOT PHI, include:
  - FMLA leave requests
  - Sick leave reports
  - Accident reports
  - Workers' compensation claims
  - Fitness for duty exams

Schwabe WILLIAMSON & WYATT

ADMINISTRATIVE REQUIREMENTS

- Designation of "Privacy Official"
- Written policy manuals addressing all aspects of the HIPAA Privacy and Security Rules
- HIPAA training
- Administrative and technical safeguards

Schwabe WILLIAMSON & WYATT

BUSINESS ASSOCIATES

- A Business Associate is an individual or entity that assists in a plan function or activity
- Business Associates include:
  - Claim Administrators (Regence)
  - Benefit consultants

Schwabe WILLIAMSON & WYATT

BUSINESS ASSOCIATES

A covered entity cannot allow a Business Associate to receive or use PHI, unless a proper Business Associate Agreement is in effect

Schwabe WILLIAMSON & WYATT

NOTICE OF PRIVACY PRACTICES

Schwabe WILLIAMSON & WYATT

NOTICE OF PRIVACY PRACTICES ("NOPP")

- Must provide notice of an individual's rights and plan's duties under HIPAA
- Must be provided to new employees upon enrollment in plan
- Must provide reminder of availability of Notice of Privacy Practices at least every 3 years
- Notice must be posted on covered entity's website (if any)

Schwabe WILLIAMSON & WYATT

NOTICE OF PRIVACY PRACTICES

- ACA §1557 requires notice of nondiscrimination on the basis of race, sex, etc.
- Applies to health care providers that received federal financial assistance (e.g., Medicaid)
- Notice must include language taglines informing non-English reading individuals of language assistance

Schwabe WILLIAMSON & WYATT

NOTICE OF PRIVACY PRACTICES

- §1557 notice and language tagline must be included in any "significant" communication
- HHS confirms that NOPP is a significant communication
- HHS also declared the change is not material, so NOPP need not be redistributed just for §1557

Schwabe WILLIAMSON & WYATT

GENETIC INFORMATION NONDISCRIMINATION ACT ("GINA")

Schwabe WILLIAMSON & WYATT

GINA

- Prohibits health plans from collecting genetic information prior to or in connection with enrollment
- Cannot ask enrollees about medical history of family members

Schwabe WILLIAMSON & WYATT

EEOC WELLNESS RULES

Schwabe WILLIAMSON & WYATT

EEOC WELLNESS RULES

- Programs that solicit health information (e.g., health risk assessments or biometric screenings) must provide notice of use and confidentiality
- If spouses receive an incentive for participation (e.g., a premium reduction), written consent of spouse is required

Schwabe WILLIAMSON & WYATT

HIPAA ePHI SECURITY RULE

Schwabe WILLIAMSON & WYATT

HIPAA ePHI SECURITY RULE

- Electronic Protected Health Information ("ePHI") means PHI that is:
  - Transmitted by electronic media; or
  - Maintained in electronic media

Schwabe WILLIAMSON & WYATT

SECURITY RULE GOALS

- Ensure confidentiality and integrity of ePHI
- Protect against any "reasonably anticipated" threats to the security
- Protect against any "reasonably anticipated" unauthorized disclosures of ePHI
- Ensure compliance by workforce members

Schwabe WILLIAMSON & WYATT

HIPAA ePHI SECURITY RULE

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Security Policy Manual
- Documentation Requirements
- Risk Analysis

Schwabe WILLIAMSON & WYATT

REQUIRED RISK ANALYSIS

- Must conduct an accurate and thorough assessment of the potential risks to the confidentiality and integrity of ePHI
- Must implement security measures sufficient to reduce risks and vulnerabilities

Schwabe WILLIAMSON & WYATT

WORKFORCE SECURITY

- Appointment of Security Official
- A security awareness and training program for all workforce members
- Policies and procedures to prevent non-authorized disclosure accessing ePHI
- Procedures for terminating access to ePHI upon termination of employment or need for access

Schwabe WILLIAMSON & WYATT

PHYSICAL AND TECHNICAL SAFEGUARDS

- Must implement
  - Mechanisms to encrypt ePHI, unless inappropriate
  - Technical security measures to guard against unauthorized access of ePHI
  - Procedures and policies for final disposition of ePHI

Schwabe WILLIAMSON & WYATT

BREACH NOTIFICATION REQUIREMENTS

Schwabe WILLIAMSON & WYATT

NOTICE OBLIGATIONS

- Covered entities must provide notification to affected individuals and to HHS following the discovery of a breach of unsecured PHI
- Business Associates must notify the covered entity of a breach that it discovers. The covered entity will then notify the affected individuals and the HHS

Schwabe WILLIAMSON & WYATT

WHAT IS A "BREACH"?

- A "breach" is an unauthorized acquisition, access, use, or disclosure of unsecured PHI that "compromises" the security or privacy of such information
- "Unsecured PHI" is PHI that is not secured through encryption or proper destruction
- "Compromised" is not the same as harmed

Schwabe WILLIAMSON & WYATT

WHAT IS A "BREACH"?

- An impermissible disclosure is presumed to be a breach unless
  - A risk analysis is performed; and
  - The analysis demonstrates a low probability that the PHI has been compromised
- Failure to perform the risk analysis means a breach occurred

Schwabe WILLIAMSON & WYATT

RISK ANALYSIS FACTORS

- Sensitivity of the PHI
- Likelihood of identification of individuals
- Person to whom the PHI was improperly disclosed
- Whether the PHI was actually viewed
- Extent to which risk was mitigated

Schwabe WILLIAMSON & WYATT

NOTIFICATION BY A BUSINESS ASSOCIATE

- A Business Associate that discovers a breach must notify the covered entity so that the plan can notify the affected individuals
- Notice must be without unreasonable delay (and in all events, within 60 days)
- Obligation should be in BAA

Schwabe WILLIAMSON & WYATT

NOTIFICATION TO INDIVIDUALS

- A covered entity must notify each individual whose information has been acquired as a result of the breach
- Notice must be sent without unreasonable delay, and in all cases within 60 calendar days after the date the breach was "discovered"

Schwabe WILLIAMSON & WYATT

NOTIFICATION TO HHS

- A covered entity must notify HHS of each breach
  - Breaches involving 500 or more individuals: Notify HHS immediately (i.e., within 60 days of breach)
  - Breaches involving less than 500 individuals: Maintain a log of such breaches and annually submit the log to HHS

Schwabe WILLIAMSON & WYATT

NOTIFICATION TO THE MEDIA

- For a breach involving more than 500 residents of a state, notice must be sent to prominent media outlets
- The notice must be sent without unreasonable delay
- HHS expects that most plans will provide this notice in the form of a press release

Schwabe WILLIAMSON & WYATT

HIPAA PENALTIES

Schwabe WILLIAMSON & WYATT

HIPAA VIOLATION PENALTIES

- The penalties for violating the HIPAA can be draconian
- For an innocent mistake, a covered entity can be subject to a civil penalty of $100 for each HIPAA violation, up to a maximum of $25,000 per calendar year

Schwabe WILLIAMSON & WYATT

HIPAA VIOLATION PENALTIES

- The penalties for less-than-innocent mistakes are:
  - $1,000 per violation due to reasonable cause but not willful neglect, up to a maximum of $100,000 per calendar year for violation of the same requirement
  - $10,000 for each violation due to willful neglect that is timely corrected, up to a maximum of $250,000 per calendar year for violation of the same requirement
  - $50,000 for each violation due to willful neglect if not timely corrected, up to a maximum of $1,500,000 per calendar year for violation of the same requirement

Schwabe WILLIAMSON & WYATT

SAMPLE PENALTIES

OHSU	$2,700,000	Inadequate e-PHI security risk analysis.
BlueCross BlueShield of Tennessee	$1,500,000	57 unencrypted hard drives stolen.
Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates	$1,500,000	Unencrypted laptop stolen, poor risk analysis, policies.
Affinity Health Plan	$1,215,780	Returned photocopiers without erasing the hard drives.
St. Joseph Hospital	$2,140,000	E-PHI accessible through internet search engines.
Raleigh Orthopaedic Clinic	$750,000	No Business Associate Agreement.

Schwabe WILLIAMSON & WYATT

HIPAA ENFORCEMENT

Schwabe WILLIAMSON & WYATT

WHO MAY BRING ACTION

- HHS
- Affected individuals may recover a percentage of civil monetary penalties or settlements collected by HHS
- Although HIPAA is a federal law, states may also bring a civil action and obtain damages

Schwabe WILLIAMSON & WYATT

OCR COMPLIANCE AUDITS

- HHS must conduct periodic audits to ensure HIPAA compliance
- OCR will review the following:
  - Policies and procedures
  - Documentation
  - Training
  - Business associate agreements and contracts
  - Risk analysis and management

Schwabe WILLIAMSON & WYATT

OCR COMPLIANCE AUDITS

- A compliance review may also include:
  - Implementation of minimum necessary standard
  - Providing of Notice of Privacy Practices
  - Physical security of facilities and mobile devices
  - Technical safeguards in place to protect ePHI
  - Monitoring of access to ePHI

Schwabe WILLIAMSON & WYATT

OCR COMPLIANCE AUDITS

- A compliance review may also include:
  - Off-site access and use of ePHI form remote locations
  - Storage of ePHI on portable devices and media
  - Disposal of equipment containing ePHI
  - Data encryption
  - Virus protection

Schwabe WILLIAMSON & WYATT

SKAGIT COUNTY CASE STUDY

Schwabe WILLIAMSON & WYATT

SKAGIT COUNTY CASE STUDY

- On 9/14/11, the County uploaded files containing ePHI on to a public web server
- Gave web browsers public access to ePHI about infectious disease testing and treatment
- Discovered and corrected (9/28/11)
- 7 files were actually accessed

Schwabe WILLIAMSON & WYATT

SKAGIT COUNTY CASE STUDY

- On 12/9/11, the County notified OCR of the 7 breaches
- The County did not notify the affected individuals
- On 5/25/12, OCR commenced an investigation
- OCR discovered that 1,581 files were accessible during 2 week period

Schwabe WILLIAMSON & WYATT

SKAGIT COUNTY CASE STUDY

- Charges
  - Improper disclosure of 1,581 files
  - Failure to provide required breach notification to affected individuals
  - Failure to implement sufficient security procedures
  - Failure to maintain written policies to comply with Security Rule

Schwabe WILLIAMSON & WYATT

SKAGIT COUNTY CASE STUDY

- Remediation
  - $215,000 penalty
  - Provide belated breach notification to affected individuals
  - Prepare and submit security policies to OCR

Schwabe WILLIAMSON & WYATT

SKAGIT COUNTY CASE STUDY

- Remediation
  - Conduct a thorough security risk analysis
  - Train all workforce members having access to ePHI
  - Annual reporting for three years

Schwabe WILLIAMSON & WYATT

QUESTIONS

Schwabe WILLIAMSON & WYATT