HIPAA for LTC: New Rules Signal a Need to Review (or create) Compliance Policies

DeWitt Ross & Stevens S.C. Law Firm

About the Presenter

Brian R. Purtell
DeWitt Ross & Stevens S.C.
2 East Mifflin St., Ste. 600
Madison, WI 53703
(608) 252-9366
(608) 252-9243 (facsimile)
brp@dewittross.com

DeWitt Ross & Stevens S.C.

Today's Goals

- Appreciation of HIPAA Coverage and Applicability
- Basic Framework for compliance
- Interrelation/State laws
- Recent changes

DeWitt Ross & Stevens S.C.

Covered Topics

- Legal framework and timetables
- HIPAA terminology
- State Confidentiality laws
- Privacy Rule Provider Obligations and Patient Rights
- Security Rule Safeguards and Structure
- Business Associate Agreements
- HITECH and Breach Notifications

DeWitt Ross & Stevens

HIPAA Overview

- Transaction and Code Sets Rule - October 16, 2002 (H.R. 3323 allowed for a 1 year extension)
- Privacy Rule - April 14, 2003
- Security Rule - April 21, 2005
- National Employer Identifier - July 30, 2004
- National Provider Identifier - May 23, 2007
- HITECH 2010
- HITECH/Omnibus Rule 2012 (effective 2013)

DeWitt Ross & Stevens

HIPAA Overview

- Electronic transaction: How to electronically "speak"
- The Privacy Rule directs what to do, not how to do it.
- The Security Rule tells us what to do, with flexibility on how to do it.
- HITECH-new rules on BAA, breach notification.
- Penalties

DeWitt Ross & Stevens

Legal Framework

- The law
- The rules
- The penalties
- Preemption

DeWitt Ross & Stevens

State Law

- Statutes
  - Ch. 146, 50
  - Professional obligations
- Admin. Code
- *See also*, Regulation by Contract

DeWitt Ross & Stevens

When State Laws Not Preempted

- Non-conflicting State privacy provisions
- Conflicting State privacy provisions more stringent than HIPAA
  - Greater rights to individual than HIPAA
  - More restrictive use or disclosure than HIPAA
- State regulatory areas
  - Reporting disease, injury, vital statistics
  - Involving public health
  - Facility or professional licensure or certification
  - Health plan audits or evaluations
  - Parent/minor relationships

DeWitt Ross & Stevens

When State Law is Preempted

- Conflicting State privacy provision less stringent than HIPAA
- State provision making HIPAA compliance impossible
- State provision "obstacle to the accomplishment and execution" of HIPAA

DeWitt Ross & Stevens

HIPAA Privacy Rules Terminology

- Covered Entity
- Permitted use and disclosure
- Permission for use and disclosure
- Minimum necessary
- Individual rights
- Administrative requirements

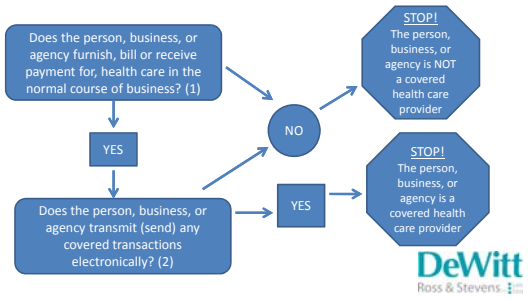
DeWitt Ross & Stevens

HIPAA Privacy Rules Terminology

- "Covered Entity"
  - Who is covered
  - What is covered
  - Special arrangements
  - Important, even if you are not a CE by definition

DeWitt Ross & Stevens

Covered Entities: Is a person, business, or agency a covered health care provider?



DeWitt Ross & Stevens

"Covered Entity" Providers

- Covered: health care providers who transmit health information electronically in connection with "standard transaction"
- Not covered: Provider who never transmits health information electronically in connection with "standard transaction"

DeWitt Ross & Stevens

Other "Covered Entities"

- Payers, *i.e.*, health insurance issuers, HMOs, ERISA and non-ERISA group health plans, Medicare, Medicaid, other government health plans that furnish or pay for health care
  - Payers not covered: "accepted benefits" issuers, *i.e.*, workers compensation, disability income, liability, others where any payment for health care is "incidental" or "secondary" to other health insurance benefits; employers, unions, other group health plan sponsors; self-administered group health plans with less than 50 participants

DeWitt Ross & Stevens

Other "Covered Entities": Health Care Clearinghouse

- Processes, or facilitates processing, transactions received from one entity into or out of "standard transaction" for transmission to another
  - *e.g.*, billing service, repricing company, community health management or information management system, value added network or switch

DeWitt Ross & Stevens

"Health Information"

- Information, oral or recorded in any medium, that
  - Relates to individuals' past, present or future physical or mental health or condition, or provision of or payment for health care through an individual; and
  - Created or received by health care provider, health plans, public health authority, employer, life insurance, school, university, or clearinghouse

DeWitt Ross & Stevens

"Individually Identifiable Health Information"

- "Health information," *including* demographic data collected from an individual
  - Created or received by a health care provider, health plan, employer, or clearinghouse; and
  - Permits identification of the individual, or could reasonably be used to identify the individual
- Demographic information—name, address, SSN, phone numbers, similar identifiers

DeWitt Ross & Stevens

"Protected Health Information"

- "Individually identifiable health information"
- Transmitted or maintained electronically, on paper, orally or in any other medium or form

DeWitt Ross & Stevens

"De-Identified Health Information"

- Health information that cannot reasonably be associated with an individual
- 18 specified identifiers removed and cannot associate individual with remainder; or
- Statistical experts' documented finding "very small" risk could identify individual
- De-identified health information not subject to HIPAA restriction

DeWitt Ross & Stevens

Permitted Use and Disclosures

- Treatment, payment, health care operations (TPO)
- Research
- Public need

DeWitt Ross & Stevens

Treatment, Payment, Health Care Operations

- Covered entity may use or disclosure protected health information to:
  - Carry out treatment
  - To obtain payment for treatment
  - To carry out its own health care operations

DeWitt Ross & Stevens

Treatment

- One or more health care providers' provision, coordination, consultant, referral or management of health care and related services
- No minimum necessary limitation on treatment activities

DeWitt Ross & Stevens

Payment: Providers

- Providers' activities to obtain or provide reimbursement for health care to an individual
- Payment permits disclosure to any entity as needed to effect activity
  - *e.g.*, workers' compensation insurer, financial institution
- Minimum necessary limitation applies to payment activities

DeWitt Ross & Stevens

Providers' Payment Activities

- Eligibility, coverage determination
- Precertification, preauthorization
- Billing, claims management, collection, data processing
- Medical necessity, charge justification
- Utilization, concurrent, retrospect or review

DeWitt Ross & Stevens

Health Care Operations: Providers

- Activities related to furnishing health care that involved:
  - Quality assurance activities;
  - Business activities;
  - Marketing activities; or
  - Fundraising activities
- Health care operation permits disclosure to any entity as needed to effect activity
- Minimum necessary limitation applies to health care operations

DeWitt Ross & Stevens

Health Care Operations: Quality Assurance Activities

- Quality assessment and improvement activities
- Case management, coordination
- Medical review, audits, legal services, fraud and abuse detection, compliance
- Provider qualifications, performance evaluation
- Professional training, certification, licensure, credentialing

DeWitt Ross & Stevens

Health Care Operations: Business Functions

- Business planning and development, cost management, formulary development
- Management and administration, customer service, internal grievances
- Due diligence for asset sale or transfer, if potential successor is or will be covered entity

DeWitt Ross & Stevens

Health Care Operations: Marketing

- Health-related product or service communication if
  - Identifies covered entity making it;
  - Reveals a remuneration covered entity got or gets; and
  - Permits opt-out
- Face-to-face communication
- Product or service of nominal value

DeWitt Ross & Stevens

Uses and Disclosure of Protected Health Information: General Rule

- A covered entity may not use or disclose protected health information, except as permitted by HIPAA or State law

DeWitt Ross & Stevens

Consent

- Revised Final Privacy Rule no longer requires a consent, however, Wisconsin law does require obtaining informed consent

DeWitt Ross & Stevens

Uses and Disclosure When Consent, Authorization or Opportunity to Object not Required

- Public health, FDA, national security, health care oversight, judicial and administrative proceedings, law enforcement
- Lawful reporting of disease, injury, vital statistics, child abuse, adult abuse, neglect, domestic violence
- State oversight
  - Management and financial audits, program monitoring and evaluation, licensure, certification

DeWitt Ross & Stevens

Uses and Disclosure When Consent, Authorization or Opportunity to Object not Required (*cont'd*)

- Coroners, medical examiners, funeral directors or decedents
- Medical emergencies, imminent and serious health or safety threats
- Organ donation
- Government functions
  - Military, national security, correctional institutions

DeWitt Ross & Stevens

Authorization

- Covered entity must obtain written authorization for any use or disclosure not permitted or required by the privacy rules
- Must not condition treatment on granting authorization

DeWitt Ross & Stevens

Authorization: Content Requirements

- Describe information to be used or disclosed
- Identify who authorized to use, disclose or receive
- Revocable at any time
- State expiration date or events
- Signed and dated

DeWitt Ross & Stevens

Minimum Necessary

- Limitations
- Exceptions
- Implementation

DeWitt Ross & Stevens

Minimum Necessary Limitation

- Reasonable effort to limit use, disclose, or request for protected health information to a minimum necessary to accomplish intended purpose

DeWitt Ross & Stevens

Minimum Necessary Exceptions

- No minimum necessary limitation for:
  - Disclosure to or request by provider for treatment
  - Use by or disclosure to information's subject
  - Use or disclosure authorized by information's subject
  - Disclosure to HHS
  - Use or disclosure required by law

DeWitt Ross & Stevens

Minimum Necessary Implementation

- Making or requesting disclosure
- Responding to request for disclosure
- Use

DeWitt Ross & Stevens

Minimum Necessary Implementation: Medical Records

- Requests for entire medical record must be specifically justifiable as reasonably necessary to accomplish purpose
- May develop policies and procedures describing circumstances justifying routine requests for entire medical record

DeWitt Ross & Stevens

Business Associates

- Who is a business associate
- Who is not a business associate
- Satisfactory assurance
- Required contract terms
- Compliance monitoring

DeWitt Ross & Stevens

Individuals' Rights

- Access
- Amendments
- Disclosure accounting
- Restriction requests
- Confidential communications

DeWitt Ross & Stevens

Administrative Requirements

- Notice of privacy practices
- Policies and procedures
- Data safeguards
- Workforce management
- Complaint procedures

DeWitt Ross & Stevens

The Security Rule

- ePHI
- Three broad categories of Safeguards:
  1. Administrative Safeguards
  2. Physical Safeguards
  3. Technical Safeguards

DeWitt Ross & Stevens

The Security Rule

- Implementation Specifications ("IS")
- Either Required or Addressable
  - Addressable still needs to be "addressed"
- Review of Systems and Procedures: not a one time compliance effort

DeWitt Ross & Stevens

The Security Rule- Admin Safeguards

- **Security Management Process**- policies to prevent, detect, respond and correct. (4 IS)
- **Assigned Security Responsibility**- "security officer"
- **Workforce Security**-employee policies (3 IS)
- **Information Access Management**-formal policy as to how ePHI is accessed (2 IS)

DeWitt Ross & Stevens

The Security Rule- Admin Safeguards

- **Security Awareness and Training**- for all workforce.
- **Security Incident Procedures**
- **Contingency Plan**
- **Evaluations**
- **Business Associate Contracts**

DeWitt Ross & Stevens

The Security Rule- Physical Safeguards

- **Facility Access Controls**- designed to limit physical access to EPHI systems (4 IS)
- **Workstation Use-** e.g., logoff process
- **Workstation Security-**
- **Device and Media Controls-** new wrinkles with smartphone, cloud, etc.

DeWitt Ross & Stevens

The Security Rule-Technical Safeguards

- **Access Controls-**
- **Audit Controls**
- **Integrity**
- **Person or Entity Authentication**
- **Transmission Security**

DeWitt Ross & Stevens

HITECH Rules

DeWitt Ross & Stevens

What is HITECH?

- HITECH stands for "Health Information Technology for Economic and Clinical Health"
- Contained in American Recovery and Reinvestment Act of 2009
- Fundamental shifts in HIPAA's existing regulations in several key areas.
- Effective February 17, 2010, with delayed implementation of many of the changes.

DeWitt Ross & Stevens

HITECH → New HIPAA

- BAs / subcontractors / e-service vendors must comply **directly** with most Security and Privacy provisions
- Breach notification scope for CE and BA is broader
- "Clarified" minimum necessary standards
- Expanded individuals' rights to e-health records and families' rights to deceased individuals' records
- Increased enforcement and civil / criminal penalties
- Prohibited sale of PHI, marketing and fundraising restrictions enhanced.

DeWitt Ross & Stevens

Business Associates

BAs now covered directly by many of Privacy **and Security** rules. No longer only obligated by BAA:

- Must have policies and address the same safeguards that CEs must meet under Security Rule.
- Subject to enforcement directly from OCR; BA non-compliance previously a contractual issue for CE.
- Must follow the breach notification rules
- Expected to monitor CEs (two-way street now)
- Subject to $$ penalties for noncompliance

DeWitt Ross & Stevens

BA Definition Expanded:

- Subcontractors of BAs
- E-prescribing gateways and other services that provide data transmission of PHI
- Patient Safety Organizations
- Health Information Exchanges (eg WISHIN Direct)
- Vendors of "personal health records"

Related impact: MCOs deemed to be CEs

- Assisted Living Providers are BAs of MCO's by contract

DeWitt Ross & Stevens

Breach

Definition of Breach Expanded:

- An acquisition, access, use or disclosure of unsecured PHI
- "Unsecured" PHI = PHI not secured by a method specified by HHS that renders it unusable, unreadable, or indecipherable to unauthorized persons
- Two ways to "Secure" PHI
  - Encryption
  - Destruction

DeWitt Ross & Stevens

Secure PHI by Encryption

Encryption

- Using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key
- The confidential key or process must not have been breached
- Decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt

DeWitt Ross & Stevens

Secure PHI by Destruction

Destruction

- Shredding or destruction of paper, film, or hard copies such that PHI cannot be read or otherwise reconstructed
- Clearing, purging, or destroying of electronic media, *consistent* with certain standards
- Special Care!
  - Copier
  - Fax machine
  - Record Retention

DeWitt Ross & Stevens

Notification of Breach

- New, expansive "Presumption of Breach" applies to any and all access to or disclosures of Unsecured PHI
- Exceptions to Presumption:
  - Unintentional access by workforce member or agent
  - Inadvertent disclosure amongst authorized persons
  - Inability to retain the information
  - Low Probability of compromise based on risk assessment

DeWitt Ross & Stevens

New Breach Standard

Old standard for reportable breach = "Harm Standard": unauthorized use or disclosure of PHI that posed a significant risk of financial, reputational, or other harm.

New Standard: All unauthorized use or disclosure are presumed to be reportable unless, following a risk assessment, there is a low probability that the PHI has been compromised.

DeWitt Ross & Stevens

Notification Risk Assessment

- 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
- Extent to which the risk to the PHI has been mitigated

DeWitt Ross & Stevens

Notice Requirements

- Notify each individual whose PHI *may* have been breached
- Notify Department of Health and Human Services
- If breach involves 500 or more individuals, tell the media

DeWitt Ross & Stevens

Notice to Individuals

- Notice must be sent to the impacted individual:
  - Without unreasonable delay
  - Within 60 days of when breach was discovered or should have been discovered
  - By First class mail, Email or Telephone
- Delay if requested by law enforcement
- Minor or incompetent individual, notice to Parent or Personal representative
- Deceased individuals, notice to next of kin or personal representative

DeWitt Ross & Stevens

Notice to Individuals cont.

- If the CE /facility no longer has an individuals' contact information:
  - Less than 10 individuals = Use alternate form of written communication reasonably calculated to reach the individual
  - 10 or more individuals =
    - Conspicuous notice posted on CE's website for 90 days
    - Notice in "major" print or broadcast media
    - Include toll-free number, and keep it active for 90 days

DeWitt Ross & Stevens

Content of Notice -Individuals

- Description of the breach
- Description of the type of unsecured PHI involved
- Steps individuals should take to protect themselves
- Description of what the CE is doing to investigate, mitigate losses, and prevent future breaches
- CE's contact information, to ask questions and get more information

DeWitt Ross & Stevens

Notification to HHS / OCR

- Requirements vary by the number of individuals:
  - 500 or more individuals:
    - Same time as individual notice
  - Less than 500 individuals
    - Annually
    - Within 60 days of the end of the calendar year
- Report is made and retained on HHS website http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

DeWitt Ross & Stevens

Notifying the Media

If Breach involves 500 or more individuals, the CE must also notify "prominent" media outlets

- Timing = Within same timeframe as notices to individuals (60 days)
- Contents = Same elements as notice to individuals

DeWitt Ross & Stevens

Business Associates and Breach

BAs must provide Notice to the CE as agreed in the BAA, but not less than:

- Within 60 days of when breach was discovered or should have been discovered (subtracts from CE's time to notify individuals)
- Identifying each impacted individual, including all information needed for CE to notify the individual, and
- In the manner and to the CE's privacy officer or other individual as set forth in the BAA

DeWitt Ross & Stevens

Expansion of Individual Rights

While much of HITECH addresses CE and BA obligations, the rights granted individuals found primarily in Privacy Rule have expanded or have been altered.

- Impact:
  - Need to review and revised policies regarding respecting individual's rights
  - Update Notice of Privacy Practices
  - Forms review

DeWitt Ross & Stevens

Individual Rights to PHI - EHR

If the CE maintains an electronic health record ("EHR"), then the individual has the right to:

- receive an electronic copy of his or her PHI
- Have the PHI transmitted directly to a third party
- Must be encrypted unless individual directs otherwise; but only a writing - no authorization needed
- CE may charge a reasonable, cost-based fee

DeWitt Ross & Stevens

Expanded Rights to Accounting

- When providing an Accounting, facilities maintaining an EHR must include uses and disclosures related to treatment, payment, and health care operations
- Implementation deadline:
  - EHR acquired as of January 1, 2009 = January 1, 2014
  - EHR acquired after January 1, 2009 = the date on which the facility acquires EHR

DeWitt Ross & Stevens

Individual Right to Restrict Access

- CEs must comply with an individuals' request to prohibit disclosures to a health care plan for payment or health care operations
- Solely for a service for which the CE has been paid in full "out of pocket"

DeWitt Ross & Stevens

Right to Decedent Information

Limits on applicability

- Limits HIPAA protections and restrictions on disclosures to 50 years following death

Disclosures Permitted:

- Old: CE could disclose PHI to family, friend or other person involved in care or payment, but not after death unless personal representative
- New: CE may continue to communicate with involved family and friends, unless contrary to the individual's express wishes

DeWitt Ross & Stevens

Sale of PHI Prohibited

Authorization required:

- Disclosure of PHI where CE *or BA* directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI
- Must expressly allow the PHI to be exchanged for remuneration

DeWitt Ross & Stevens

Sale of PHI Exceptions

Exceptions to Authorization Requirement:

- Remuneration paid to a BA related to the BA's services as to the exchange of PHI
- Transfers for treatment, subject to any applicable regulation by HHS
- Transfers for public health activities already defined by HIPAA Transfers for purposes of a sale, transfer, or merger
- Providing an individual a copy of the individual's PHI
- Transfers for research purposes, if the price paid reflects only the costs of preparation and transmittal of the data

DeWitt Ross & Stevens

Marketing

- Expands the definition of marketing = more instances require individuals' authorization if any "financial remuneration" is received for making the communication
  - Example:
    - Old: mailer printed by device manufacturer and send by treatment center regarding a new treatment would not require an authorization
    - New: If a manufacturer funds the mailer, authorization is required
  - Exception: Communications about a Rx, if the Rx is already prescribed for the individual

DeWitt Ross & Stevens

Fundraising

Previously: CEs could only disclose demographic info and dates of services for fundraising.

Now:

- Use of PHI for fundraising is expanded to include physician, outcome information, hospital department where treated, and insurance.
- To balance the increased disclosure, individual have greater opportunity to "opt out".

DeWitt Ross & Stevens

Fundraising Opt Out

- No undue burden or more than nominal cost
- Treat individuals who have opted out as having revoked authorization
- Treatment may not be conditioned on receipt of fundraising communications

DeWitt Ross & Stevens

Genetic information

- May not be used by health plans for underwriting purposes, except for plans issuing long term care insurance

DeWitt Ross & Stevens

Enforcement and Penalties

State Attorney General

- May bring private actions on behalf of their affected residents
- Injunctive relief and damages available
- $100 per violation, not to exceed $25,000 per year for an identical violation
- Attorneys' fees and costs recoverable
- Audit program

DeWitt Ross & Stevens

Enforcement: Willful Neglect

- Willful Neglect means "Conscious, intentional failure or reckless indifference to the obligation to comply"
- HHS *must:*
  - investigate a complaint (that anyone can file) if a preliminary investigation indicates a possible (not "probable") violation due to willful neglect (no discretion remains);
  - Require a compliance review; and
  - Mandate civil monetary penalties if willful neglect is found

DeWitt Ross & Stevens

Agency Liability

- CEs and BAs with subcontractors (Principals) may be liable to HHS for the acts of BAs found to be agents, as determined under the federal common law of agency:
  - Whether the agent's conduct is subject to the principal's control
  - Whether the agent was doing something typically done by such an agent
  - Whether the principal reasonably expected the agent to engage in the questioned conduct

DeWitt Ross & Stevens

Enforcement and Penalties

Violation Category	Each Violation	Total CMP for Violations of an Identical Provision in a Calendar Year
Unknowing	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	At least $50,000	$1,500,000 –

DeWitt Ross & Stevens

Enforcement and Penalties

Tiered structure based on level of culpability:

- Unknowing -The CE/BA did not know and reasonably should not have known of the violation.
- Reasonable Cause - The CE/BA knew or by exercising reasonable diligence would have known, that the act or omission was a violation, but did not act with willful neglect.
- Willful Neglect – Corrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA; however, the CE/BA corrected the violation within 30 days of discovery.
- Willful Neglect – Uncorrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the CE/BA did not correct the violation within 30 days of discovery.

DeWitt Ross & Stevens

Enforcement and Penalties

HHS must consider the following in determining the $$s:

- The nature and extent of the violation, including the number of individuals affected and the time period during which the violation occurred;
- The nature and extent of the harms resulting from the violation, including whether the violation caused physical harm, whether the violation resulted in financial harm, whether there was harm to an individual's reputation and whether the violation hindered an individual's ability to obtain healthcare;
- The history of prior compliance, including previous violations; and
- The financial condition of the covered entity or business associate, including whether financial difficulties affected the ability to comply and whether the imposition of the CMP would jeopardize the ability of the covered entity to continue to provide or pay for healthcare.

DeWitt Ross & Stevens

Questions

?

DeWitt
Ross & Stevens