



This Employer Webinar Series program  
is presented by Spencer Fane Britt & Browne LLP  
in conjunction with United Benefit Advisors

**SPENCER FANE**  
BRITT & BROWNE LLP

*Attorneys & Counselors at Law*

[www.spencerfane.com](http://www.spencerfane.com)

**UBA**® *United  
Benefit  
Advisors*

[www.UBAbenefits.com](http://www.UBAbenefits.com)



# SPENCER FANE

BRITT & BROWNE LLP

*attorneys and counselors at law*

## HIPAA/HITECH Refresher

*Chadron J. Patton*

*Julia M. Vander Weele*

# Presenters



Chadron J. Patton, JD  
Associate

[cpatton@spencerfane.com](mailto:cpatton@spencerfane.com)  
913-327-5137



Julia M. Vander Weele, JD  
Partner

[jvanderweele@spencerfane.com](mailto:jvanderweele@spencerfane.com)  
816-292-8182

# Evolution of HIPAA Privacy and Security Rules

- ▶ Mandated by HIPAA (1996)
- ▶ Privacy Rule: April 14, 2003
  - Applicable to all “protected health information”
- ▶ Security Rule: April 20, 2005
  - Specific to electronic PHI
- ▶ HITECH Act: February 17, 2010
  - Extended Privacy Rule and Security Rule to business associates
  - Increased penalties (effective immediately)
- ▶ Proposed Revisions to Privacy and Security Rule: July 14, 2010

# Civil Monetary Penalties

- ▶ Interim final regulations issued 10/09
- ▶ Penalty for violations where covered entity did not know and would not have known through exercise of reasonable diligence is at least \$100 per violation (maximum of \$50,000)
- ▶ Penalty for violations due to “reasonable cause” has increased from \$100 per violation to \$1,000 per violation (maximum of \$50,000)
- ▶ Violations due to willful neglect are subject to penalty of \$10,000 per violation (if corrected) and \$50,000 per violation (if not corrected)

# Civil Monetary Penalties

- ▶ Total penalty for multiple violations of an identical requirement during a calendar year is \$1.5 million
- ▶ Affirmative defense for violations that are timely corrected (except those due to willful neglect)
- ▶ Willful neglect = conscious, intentional failure or reckless indifference to the obligation to comply

# Enforcement

- ▶ August 2009 - Enforcement of Security Rule switched from CMS to HHS Office of Civil Rights (to consolidate with enforcement of Privacy Rule)
- ▶ Secretary of HHS required to conduct full investigation if preliminary investigation of complaint indicates possible willful neglect
- ▶ State attorneys general can sue on behalf of individuals (injunction or damages of up to \$25,000)
  - HHS began training program in 2011
- ▶ Future regulations will allow aggrieved individuals to share in penalties

# Enforcement

- ▶ From April 2003 to April 2011, HHS had received 60,550 privacy complaints ( $\approx 800/\text{mo.}$ ); of those, it had resolved more than 55,000 (91%)
- ▶ During this eight year period since the HIPAA Privacy Rule went into effect, HHS had not imposed a single civil monetary penalty for HIPAA violations, until . . .

# Enforcement

- ▶ February 22, 2011, HHS imposed a \$4.3M penalty against Cignet Health of Prince George's County, Maryland
  - Cignet failed to respond to patients' requests for access to medical records
  - Cignet failed/refused to cooperate in HHS's investigation

# Enforcement

- ▶ Two days later, Massachusetts General Hospital entered into \$1M settlement with HHS
  - Employee left paper records containing the PHI of 192 patients, including patients with HIV/AIDS, on the subway
  - Hospital did not admit liability and did not pay a penalty

# Enforcement

- ▶ The significant increase in available penalties as a result of the HITECH Act provides HHS with substantial leverage in settlement negotiations
- ▶ HITECH also gives HHS substantial discretion in deciding what constitutes a single violation

So.....

- ▶ Now that we have scared you, let's refresh on the rules

# Covered Entities

- ▶ Health care providers (who conduct electronic transactions)
- ▶ Health plans
- ▶ Health care clearinghouses
- ▶ Not employers
- ▶ Not Business Associates, BUT under HITECH:
  - Indirect liability under Privacy Rule (for breach of business associate agreement)
  - Direct liability under Security Rule

# What's a Health Plan?

- ▶ Medical, Dental, Vision, Health Care Flexible Spending Accounts
- ▶ Maybe Employee Assistance Programs
- ▶ Not Workers' Compensation, Long-term Disability, Life Insurance, or On-site Medical Clinics
- ▶ Not employer functions such as FMLA, drug testing, sick leave, return to work physicals, ADA, OSHA, fitness for duty
  - However, employer may need authorization to obtain records from provider

# Protected Health Information

- ▶ Protected Health Information (“PHI”) = individually identifiable health information relating to past, present or future health *or payment* for health care
- ▶ Includes not only claims information, but name, address, premiums, coverage amounts, etc.
- ▶ Does not include employment records held in the capacity of employer

# Primary Privacy Standards

- ▶ Do not use or disclose PHI, unless an exception applies
- ▶ Disclose or request only the minimum required amount of information
- ▶ Establish safeguards to prevent and minimize incidental disclosures
- ▶ Obtain assurances from business associates of their compliance and assistance

# Permitted Uses and Disclosures

- ▶ To the Individual or Personal Representative
- ▶ To a Person Involved in the Individual's Care
- ▶ For Treatment, Payment or Health Care Operations
- ▶ For Public Responsibility purposes
- ▶ **Otherwise, need an Authorization**

# Required Disclosures

- ▶ To the Individual when part of right to access or an accounting
- ▶ To the Secretary of Health and Human Services for purposes of investigating compliance

# Personal Representatives

- ▶ Same rights as the Individual
- ▶ Adults = Guardian or Power of Attorney
- ▶ Minors = Parent or other guardian unless state law allows minor to make health care decisions
- ▶ Decedents = Administrator or Executor
- ▶ Do not have to treat person as PR if not in the best interest of Individual

# Persons Involved in Individual's Care

- ▶ Family member, close personal friend or other person identified by the Individual
- ▶ If present - must obtain consent (can be oral) or provide opportunity to object
- ▶ If Individual is incapacitated or not present, may exercise professional judgment to use or disclose information in Individual's best interests
- ▶ Disclosure must be limited to only the information directly relevant to Individual's care

# Treatment, Payment and Health Care Operations

- ▶ Treatment = health care providers, pharmacists, hospitals
- ▶ Payment = contributions, coverage, benefits, subrogation, billing, claims, reinsurance
- ▶ Health Care Operations = auditing, legal, fraud and abuse detection, business planning and administrative activities
- ▶ Must have authorization for psychotherapy notes

# Public Responsibility

- ▶ Required by law
- ▶ Judicial and administrative orders
- ▶ Other subpoenas and discovery requests (must either notify individual or obtain protective order)
- ▶ Abuse situations
- ▶ Threats to health and safety
- ▶ Workers' Compensation
- ▶ Disclosure must be limited to particular purpose

# Authorization

- ▶ Valid Authorization must contain certain elements
- ▶ May be revoked at any time, unless already relied upon
- ▶ Can be combined
- ▶ Must be maintained

# Disclosures to Employer

- ▶ Summary health information okay (for purposes of renewal)
- ▶ Enrollment information (for purposes of payroll deduction)
- ▶ To disclose any other PHI to employer, plan documents must contain specific privacy protections (firewalls)
- ▶ Employer may not use PHI to make employment-related decisions or for other benefit plans

# Minimum Necessary

- ▶ Uses, disclosures and requests for PHI must be limited to the minimum necessary to accomplish the purpose
- ▶ Applies to Payment and Health Care Operations
- ▶ Does not apply to disclosures to the Individual or pursuant to authorization
- ▶ May rely on representations from public officials, other covered entities, or business associates as to the minimum necessary
- ▶ Limited Data Set (excludes many common identifying elements of PHI) is the minimum necessary for now; more guidance to come

# Safeguards

- ▶ Must be reasonably designed to minimize incidental disclosures
- ▶ People
  - Access to PHI limited to those who have need for information in connection with job duties performed for benefit plans
  - Do not disclose PHI to other employees that do not have duties that require access to PHI
- ▶ Paper
  - Don't leave in plain view
  - Sealed envelopes
  - Promptly remove printed material from printers

# Safeguards

- ▶ Fax
  - Designated fax machines
  - Distribute promptly
  - Disclaimer
- ▶ Phone
  - Verify identity and authority
  - No speakerphones/low voices
- ▶ Storage
  - Lock, put away, or cover
- ▶ Destruction
  - Shred

# Individual Rights

- ▶ Notice of Privacy Practices
- ▶ Request additional restrictions
- ▶ Receive information by alternative means or at alternative locations (“confidential communications”)
- ▶ Obtain access to information
- ▶ Correct erroneous information
- ▶ Obtain accounting of prior disclosures

# Notice of Privacy Practices

- ▶ Must be written in “plain language”
- ▶ Must contain specific information
- ▶ Must be provided upon enrollment and within 60 days of material change
- ▶ Must advise participants of the availability of notice once every three years

# Privacy Notice and GINA

- ▶ 10/09 – OCR proposed revisions to HIPAA Privacy Rule to strengthen protections for genetic information
- ▶ Genetic information is health information
- ▶ Prohibits use of genetic information for underwriting purposes
- ▶ May require revisions to privacy notice

# Potential Changes to Privacy Notice

- ▶ Proposed changes include:
  - Description of types of disclosure that require individual authorization
  - Specific statement that other disclosures not mentioned in notice will be made only with individual authorization
  - Revision to individual's right to request restrictions
- ▶ Request for comments on whether 60-day requirement for issuing new privacy notices should be extended or delayed
- ▶ Won't be effective until 180 days after effective date of final regulations

# Right to Request Restrictions

- ▶ Any Individual can request restriction on how PHI is used or to whom it is disclosed
- ▶ Need not agree, **EXCEPT (new under HITECH)**
  - Covered entity must comply with the requested restriction if the disclosure is to a health plan for a payment or health care operations purpose (but not for treatment purposes) if PHI relates to item or service for which individual paid in full out-of-pocket
- ▶ If agreed, must honor restriction
- ▶ Exception for emergencies
- ▶ Must be documented

# Right to Request Confidential Communications

- ▶ Alternative Location or Alternative Means (e.g. mail claims info to alternative address)
- ▶ Must accommodate reasonable requests if accompanied by statement of danger
- ▶ Flag the file
- ▶ Must be documented

# Right to Access

- ▶ Individual can inspect and copy his or her own PHI in a Designated Record Set
- ▶ Designated Record Set = enrollment, payment, claims, case and medical management, and other records used to make decisions re Individual
- ▶ Not applicable to psychotherapy notes or litigation
- ▶ Right of Review in certain instances
- ▶ 30 days to respond (60 days if off-site)
- ▶ May charge reasonable cost-based fee for copies and postage

# Right to Access - Electronic Health Records

- ▶ Right to request and receive information in an electronic format if it is maintained as an electronic health record (EHR)
- ▶ Electronic health record defined as “an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff”

# Right to Request Amendment

- ▶ Right to request amendment if Individual believes PHI maintained in designated record set is inaccurate or incomplete
- ▶ 60 days to respond (30 day extension)
- ▶ May be denied with right to appeal
- ▶ Must be documented

# Right to Request Accounting of Disclosures

- ▶ Must track certain disclosures made during the last six years and provide accounting (“list”) upon request from individual
- ▶ Applies to public responsibility disclosures and inadvertent errors
- ▶ Does not apply to payment or health care operations or authorized disclosures
- ▶ Must respond within 60 days (30 day extension)
- ▶ Accounting must include date, name and address of recipient, description, and purpose

# Right to Request Accounting - Electronic Health Records

- ▶ Right to an accounting of disclosures applies even to disclosures made for treatment, payment, or health care operations purposes
- ▶ Applies only for past three years (vs. six years for other requests for accounting)
- ▶ EHR accounting requirements effective 2011 or 2014

# Right to Request Accounting – Proposed Rules

- ▶ Creates distinction between “right to an accounting” and an “access report”
- ▶ Would reduce the accounting period from 6 to 3 years (for paper and electronic PHI)
- ▶ Access report would be limited to electronic access, but would include access for any purpose

# Administrative Requirements

- ▶ Privacy Officer
- ▶ Train workforce on privacy and security issues (new hires and periodic refreshers)
- ▶ Establish complaint process
  - With Department of Health and Human Services
  - No retaliation
- ▶ Apply sanctions for violations
- ▶ Mitigate harmful effects of violations
  - And potentially notify affected individuals if “breach” of “unsecured” PHI (see next slide)
- ▶ Document Retention (6 years)

# Security Rule

- ▶ Standards
  - Administrative
  - Physical
  - Technical
- ▶ Implementation Specifications
  - Required
  - Addressable

# Administrative Safeguards

- ▶ Security Management Process
  - Risk Analysis (A)
  - Risk Management (R)
  - Sanctions (R)
  - Information System Activity Review (sign-on/sign-off activity; unsuccessful log-on attempts) (R)
- ▶ Security Officer (R)
- ▶ Workforce Security
  - Authorization and/or Supervision (A)
  - Workforce Clearance Procedures (background checks) (A)
  - Termination Procedures (disable user id and password) (A)
- ▶ Information Access Management
  - Access Authorization (controlled by user id and password) (A)
  - Access Establishment and Modification (A)

# Security Rule Safeguards

- ▶ Security Awareness and Training
  - Security Reminders (training) (A)
  - Protection from Malicious Software (anti-viral software/firewall) (A)
  - Log-in Monitoring (report suspicious activity) (A)
  - Password Management (change periodically?) (A)
- ▶ Security Incident Procedures (Response and Reporting) (R)
- ▶ Contingency Plans
  - Data Backup (nightly? weekly?) (R)
  - Disaster Recovery (R)
  - Emergency Mode Operation (R)
  - Testing and Revision Procedures (A)
  - Applications and Data Criticality Analysis (A)
- ▶ Evaluation

# Physical Safeguards

- ▶ Facility Access
  - Contingency Operations (A)
  - Facility Security Plan (badge readers, alarm system) (A)
  - Access Control and Validation Procedures (escort visitors) (A)
  - Maintenance Records (A)
- ▶ Workstation Use (automatic screensavers)
- ▶ Workstation Security (shut down procedures)
  - Also applies to remote workstations
- ▶ Device and Media Controls
  - Disposal (delete or purge PHI first) (R)
  - Media Re-use (delete or purge PHI first) (R)
  - Accountability (A)
  - Data Backup and Storage (A)

# Technical Safeguards

- ▶ Access Controls
  - Unique User Identification (do not share user id or passwords) (R)
  - Emergency Access Procedure (R)
  - Automatic Logoff (mandatory screensavers and shut down procedures) (A)
  - Encryption and decryption (alternative: passwords for Blackberrys and laptops) (A)
- ▶ Audit Controls
- ▶ Data Integrity
- ▶ Person or Entity Authentication
- ▶ Transmission Security
  - Integrity Controls (A)
  - Encryption and decryption (for e-mails or file transfers containing PHI) (A)

# Notification of Breach

- ▶ New requirement under HITECH (in addition to the existing obligation to mitigate)
- ▶ Applies to “unsecured” PHI that is “accessed, acquired, or disclosed” by or to an unauthorized person as a result of a “breach”
- ▶ Must notify “affected individuals” and the Department of HHS in the event of breach
  - Notify CMS immediately if breach affects 500 or more individuals; otherwise 60 days after end of calendar year
  - Online form available
  - “Group health plan” responsible for reporting breaches to CMS

# Notification of Breach

- ▶ “Breach” does not include certain unintentional acquisition by a member of the workforce or where unauthorized person would not reasonably have been able to retain the information
- ▶ “Breach” must compromise the security or privacy of the protected health information; regulations say that this means “poses a significant risk of financial, reputational, or other harm to the individual”

# Notification of Breach

- ▶ “Unsecured” means not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals
- ▶ Guidance issued by Secretary of Health and Human Services on approved technologies or methodologies to secure PHI
- ▶ Encryption or destruction are only approved methods
- ▶ Interim final regulations published August 24, 2009
- ▶ Effective September 23, 2009 (but enforcement discretion for breaches discovered before February 22, 2010)

# Notification of Breach

- ▶ Notice must include:
  - A brief description of the breach, including the date of breach and discovery
  - A description of the types of unsecured PHI disclosed or misappropriated during the breach
  - The steps individuals should take to protect themselves from potential harm
  - A description of the covered entity's actions to investigate the breach and mitigate harm now and in the future
  - Contact procedures (including a toll-free telephone number, e-mail address, website, or postal address) for affected individuals to find additional information

# Notification of Breach

- ▶ Notice must be provided “without unreasonable delay” and in no event later than 60 days after discovery of breach
- ▶ Notice must be provided to each individual, in writing, by first-class mail
- ▶ If more than 500 affected individuals in same state or geographic area, must also provide notice to prominent media outlets
- ▶ If 10 or more affected individuals cannot be located, must post notice in major print media or on home page of Company website

# Notification of Breach

- ▶ Burden of proof that notice requirements have been met rests with covered entity or business associate
- ▶ Breach will be treated as “discovered” on first day on which breach is known or should reasonably have been known through exercise of reasonable diligence

# Business Associates

- ▶ Business Associate Defined:
  - Person or organization, other than a member of covered entity workforce; who
  - Performs functions/activities on behalf of, or provides services to, a covered entity; which
  - Involves creation, use or disclosure of individually identifiable health information

# Business Associate Agreement

- ▶ Covered entities (health care providers, group health plans) must include provisions to protect privacy and security of PHI in any agreement with a Business Associate
- ▶ Must impose specified written safeguards on any individually identifiable health information used or disclosed by the business associate

# B/A Agreement - Privacy

- ▶ Specifically, a contract with a business associate (B/A) must:
  - Establish permitted/required uses and disclosures of PHI by B/A
  - Prohibit other uses/disclosures of PHI by B/A
  - Prohibit illegal use/disclosure of PHI by B/A
  - Require appropriate safeguards to prevent non-permitted use/disclosure of PHI by B/A
  - Authorize termination of contract by covered entity for breach by B/A of any material term

# B/A Agreement - Privacy

- ▶ B/A agreement must also provide that:
  - B/A will report any misuse or unauthorized disclosure of PHI
  - B/A will mitigate harmful effects of misuse or unauthorized disclosure
  - B/A will require its agents (subcontractors) to adhere to the same rules re: PHI
  - B/A will provide access to PHI to allow covered entity to meet its obligations
  - B/A will return or destroy PHI upon termination of agreement

# B/A Agreement - Privacy

- ▶ If B/A breaches the agreement, the covered entity must:
  - Take steps to cure the breach or end the violation; and
  - If breach cannot be cured, the covered entity must terminate the agreement; or
  - If termination is not feasible, the covered entity must report the breach/violation to Health and Human Services (HHS)

# B/A Agreement - Security

- ▶ B/As must implement administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic PHI created, received, maintained or transmitted on behalf of the covered entity
- ▶ B/As must report any “security incident” that it becomes aware of

# Business Associates – Prior Law

- ▶ Liability of Business Associates prior to HITECH –
  - No direct application of HIPAA privacy or security rules – so no civil or criminal penalties could be assessed on B/As
  - Potential liability to covered entity (if B/A agreement included indemnification) but generally covered entity's only recourse is right to terminate agreement upon B/A's breach and failure to cure

# Business Associates – New Law

- ▶ Business Associates under HITECH:
  - Now directly subject to many of the HIPAA Security Rules in the same manner as covered entities
  - Now subject to civil and criminal penalties for violating those Security Rules in the same manner as covered entities
  - Also subject to civil and criminal penalties for failure to adhere to the Privacy provisions in the Business Associate agreement

# Business Associates – New Law

- ▶ Business Associates must now “monitor” the covered entity, and if covered entity is violating the privacy or security rules, the B/A must:
  - Ask covered entity to stop violation; and
  - Terminate agreement if violations are not stopped; or
  - Report violations to HHS if termination of the agreement is not feasible

# Business Associates – New Law

- ▶ General effective date was February 17, 2010 but enforcement delay announced in March 2010 for business associate provisions
- ▶ Under proposed regulations issued in 2010, requirements would extend to business associate's subcontractors
- ▶ Transition rule would apply to updating business associate agreements

# Business Associates – New Law

- ▶ May need to amend existing business associate agreements to:
  - Address new breach notification requirements that are effective September 23, 2009
  - Reflect direct application of security rules effective February 17, 2010
  - Reconsider remedies for breach and indemnification provisions (now that business associates are directly liable for violations of the security rule and breach of the privacy provisions in the agreement)
  - Provide for termination by B/A if covered entity violates privacy/security rules

# What Else?

- ▶ HHS required to annually evaluate suitable security protections, develop plans to improve compliance, and conduct periodic audits
- ▶ Plan sponsors should conduct periodic privacy and security reviews to keep up with HHS guidance
- ▶ Revise policies/procedures as technology improves and becomes more affordable



**Thank you for your participation  
in the Employer Webinar Series.  
To obtain a recording of this presentation,  
or to register for future presentations,  
contact your local UBA Member Firm.**

**SPENCER FANE**  
BRITT & BROWNE LLP

*Attorneys & Counselors at Law*

[www.spencerfane.com](http://www.spencerfane.com)

**UBA**® *United  
Benefit  
Advisors*

[www.UBAbenefits.com](http://www.UBAbenefits.com)

