



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*

Kansas City • Omaha • Overland Park  
St. Louis • Jefferson City  
[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 Privacy and Security Update**

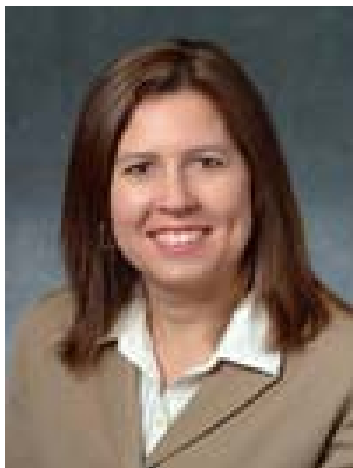
**Robert A. Browning**  
**Julia M. Vander Weele**

# Presenters



Robert A. Browning, JD  
Partner

[rbrowning@spencerfane.com](mailto:rbrowning@spencerfane.com)  
913-327-5192



Julia M. Vander Weele, JD  
Partner

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

# Overview

---

- ▶ HITECH – Health Information Technology for Economic and Clinical Health Act
- ▶ Enacted as part of economic stimulus bill on February 17, 2009
- ▶ Federal funding for health information technology initiatives to improve administrative efficiencies

# Summary of Changes

- ▶ Notification of breach
- ▶ Expanded right to request restrictions
- ▶ Special rules for electronic health records
- ▶ Prohibition on sale of PHI
- ▶ Increased civil monetary penalties and enforcement
- ▶ Direct application of security rule to business associates

# Notification of Breach

---

- ▶ New requirement (in addition to the existing obligation to mitigate)
- ▶ Similar to state data breach notification laws
- ▶ 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

# 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 April 17 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 HHS will use its enforcement discretion to not impose sanctions for breaches that are discovered before 180 days from the publication of regulations

# 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

# Requests for Restrictions

- ▶ Under HIPAA, individuals have the right to request restrictions on disclosure of PHI
- ▶ 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

# 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”

# 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)

# Prohibition on Sale of PHI

- ▶ Neither covered entity nor business associate can directly *or indirectly* receive remuneration in exchange for PHI without authorization
- ▶ Exception if purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a BAA
- ▶ Regulations due within 18 months; rule effective 6 months after final regs

# Civil Monetary Penalties

- ▶ Penalty for violations due to reasonable cause has increased from \$100 per violation to \$1,000 per violation
- ▶ Violations due to willful neglect are subject to penalty of \$10,000 per violation (if corrected) and \$50,000 per violation (if not corrected)
- ▶ Willful neglect to be defined by regulation within 18 months

# Enforcement

- ▶ 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)
- ▶ Future regulations (within 36 months) will allow aggrieved individuals to share in penalties

# 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 Associates

- ▶ Business associate “functions or activities” include, but are not limited to:
  - Claims processing
  - Data analysis
  - Utilization review
  - Billing

# Business Associates

- ▶ Business Associate “services” are limited to:
  - Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services
- ▶ Functions or services must involve use or disclosure of PHI (other than incidental or accidental use)

# 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

- ▶ 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

- ▶ Security Provisions Now Applicable:
  - Administrative Safeguards – 9 standards, 23 implementation specifications
  - Physical Safeguards – 4 standards, 10 implementation specifications
  - Technical Safeguards – 5 standards, 9 implementation specifications
  - Policies and Procedures/Documentation – 3 implementation specifications

# Business Associates – New Law

- ▶ Security Provisions Now Applicable:
  - Appoint a security official
  - Train workforce in the Security Rule
  - Perform a risk assessment
  - Develop specific Security policies and procedures
  - Adopt physical safeguards
  - Adopt technical safeguards
  - Notify covered entity of security breach

# 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

- ▶ Still not directly subject to Privacy Rule, but now subject to civil and criminal penalties for failure to comply with privacy provisions in Business Associate agreements
- ▶ New requirement to provide individuals with accounting of disclosures (in last 3 years) of information in “electronic health record”

# 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

# Other Changes

- ▶ Companies that provide data transmission of PHI to covered entities or business associates, such as:
  - Health information exchange organizations; and
  - Vendors of personal health records
- ▶ Will be subject to the same requirements as business associates

# Effective Dates

---

- ▶ Increase in civil penalties effective immediately
- ▶ Notification of breach provisions effective September 23, 2009
- ▶ General effective date for most other provisions (including business associate requirements) is February 17, 2010
- ▶ EHR accounting requirements effective 2011 or 2014

# Next Steps

---

- ▶ Review and update notice of privacy practices
- ▶ Review and update privacy and security policies and procedures
- ▶ Review plan document
- ▶ Amend business associate agreements
- ▶ Provide updated training to workforce



Thank you for your participation in the Employer Webinar Series.

To obtain a recording of this presentation and qualify for HRCI credits, or to register for future presentations, contact your local UBA Member Firm.

**SPENCER FANE**  
BRITT & BROWNE LLP  
*Attorneys & Counselors at Law*

Kansas City • Omaha • Overland Park  
St. Louis • Jefferson City  
[www.spencerfane.com](http://www.spencerfane.com)

**UBA** *United  
Benefit  
Advisors*

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

