Strafford

Presenting a live 90-minute webinar with interactive Q&A

HIPAA Compliance for Business Associates

Overcoming Complex Challenges With Data De-Identification, Security Breaches, Indemnification and More

WEDNESDAY, JULY 12, 2017

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Nathan A. Kottkamp, **McGuireWoods**, Richmond, Va.

Isaac M. Willett, Partner, **Faegre Baker Daniels**, Indianapolis

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-258-2056** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 35.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

HIPAA Compliance 2.0 for Business Associates Under the New Rule

Isaac M. Willett

FAEGRE BAKER DANIELS

Nathan A. Kottkamp

McGUIREWOODS

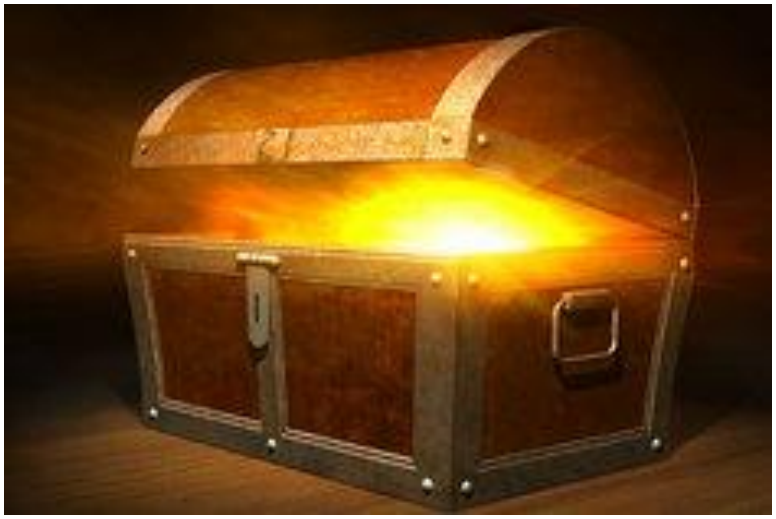
McGUIREWOODS
Relationships That Drive Results

Business Associate Agreements Now

Nathan A. Kottkamp

Business Associates after HITECH

- Under the Omnibus Final Rule, the definition of Business Associate ("BA") changed
  - Expanded to give OCR direct oversight authority over business associates and subcontractors (who are also "business associates")



Business Associates- 2-Part Definition

- Part 1: Providers of Certain Covered Functions
  - A person who, for or on behalf of a covered entity ("CE"), creates, receives, maintains, or transmits protected health information ("PHI") for a healthcare-related function or activity regulated by HIPAA
    - Examples of healthcare-related functions or activities include claims processing, data analysis, utilization review, quality assurance, billing, practice or benefit management
- Part 2: Providers of Professional Services
  - A person who provides professional services to a CE (or other BA) where the provision of the service involves the disclosure of PHI
    - Examples of professional services include legal, actuarial, accounting, consulting, data aggregation, accreditation, or financial services

NOTE: "Business Associate" does *not* include members of the CE's workforce

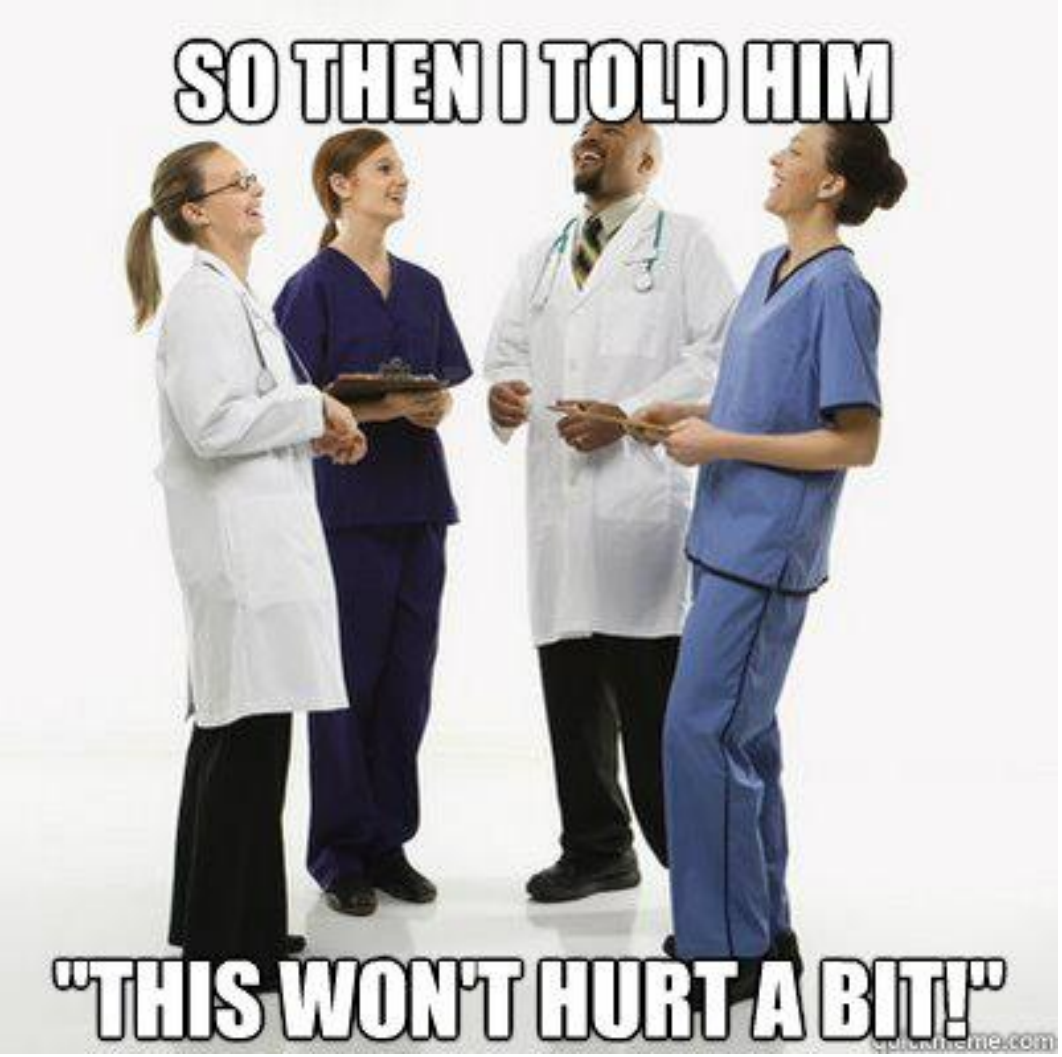
OCR Guidance (2016): Cloud Service Providers are Business Associates

- OCR confirmed cloud service providers (CSPs) are business associates under HIPAA
  - This applies even if the CSP does not have an encryption key and cannot actually view the ePHI stored on the cloud
  - The "conduit" exception does not apply to CSPs, as it is only available for PHI that is "transient" in nature
- Duties of CSPs:
  - CSPs must meet HIPAA requirements
  - CSPs likely have an affirmative duty to inquire about the nature of data stored on their systems or clearly warn users that they may not store ePHI within the CSP's systems
- Obligations of cloud users:
  - Users must have business associate agreements in place if storing PHI on a cloud service and include the use of cloud service in risk assessment
  - Users are not required to audit CSPs, but must obtain "satisfactory assurances" of compliance
  - Using a CSP that stores ePHI on services outside of the United States is not prohibited, but OCR urges caution

Business Associate Agreements

- Business Associate Agreement ("BAA") is required between:
  - CE and each BA
  - BA and each of its subcontractors or agents (also BAs)
- BA liability exists *even without* a BAA
  - "A person or an entity is a business associate if the person or entity meets the definition of ''business associate,'' even if a covered entity, or business associate with respect to a subcontractor, fails to enter into the required business associate contract with the person or entity." 78 FR 5566, 5575 (Jan. 25, 2013)

Little White Lie in Medicine



Little White Lie in HIPAA

Per the Omnibus Final Rule Impact Analysis:

- "[W]e estimate that each new or significantly modified contract between a business associate and its subcontractors will require, at most, one hour of a lawyer's time at a cost of $84.32." 78 FR 5678 (Jan. 25, 2013)

What is Required of a BA?

- Compliance with:
  - 45 CFR § 160.304 – Cooperation and Assistance
  - 45 CFR § 160.306 – Subject to Complaints/Investigations
  - 45 CFR § 160.308 – Subject to HHS Compliance Reviews
  - 45 CFR § 160.310 – Provides the following to HHS:
    - Records and Compliance Reports
    - Cooperation with Investigations and Compliance Reviews
    - Access to Information

What is Required of a BA?

- Compliance with:
  - 45 CFR § 160.312 – Subject to HHS Action, including but not limited to:
    - Corrective Action Plans or Agreements
    - Civil Money Penalties
  - 45 CFR § 160.314 – Subject to HHS Investigations and HHS Subpoena Authority
  - 45 CFR § 160.316 – Refrain from Intimidation or Retaliation

What is Required of a BA?

- Compliance with:
  - 45 CFR §§ 164.302 – 164.312 –Security Rule Requirements, including:
    - Risk Assessment
    - Administrative, Technical, and Physical Safeguards
    - Security Officer
    - Documentation
    - Execution of BAAs

What is Required of a BA?

- Compliance with:
  - 45 CFR §§ 164.402, 164.410, 164.412, and 164.414 – Breach Notification Rule
  - 45 CFR § 164.502 – Comply with General Rules for Uses and Disclosures of PHI, including Minimum Necessary rule
  - 45 CFR § 164.504 – Execute BAAs with sub-BAs
  - 45 CFR § 164.508 – Comply with Authorization Requirements for Certain Disclosures

The Omnibus Final Rule: Changes Requiring Action

- Definition of Business Associate Now Includes Subcontractors
  - Subcontractor agreements must be in writing and must contain the same privacy and security restrictions and conditions that apply to the BA
  - 45 CFR § 164.504(e)(5)
- Agency Rule
  - BAA must include additional language regarding Privacy Rule Compliance when a BA will serve as the CE's agent (under Federal Common Law)
  - 45 CFR § 164.504(e)(2)(ii)(H)

The Omnibus Final Rule: Changes Permitting Action

- Parties no longer obligated to report to Secretary of HHS if a breach of a BAA cannot be cured and termination of BAA is infeasible

Do I Need a New BAA?

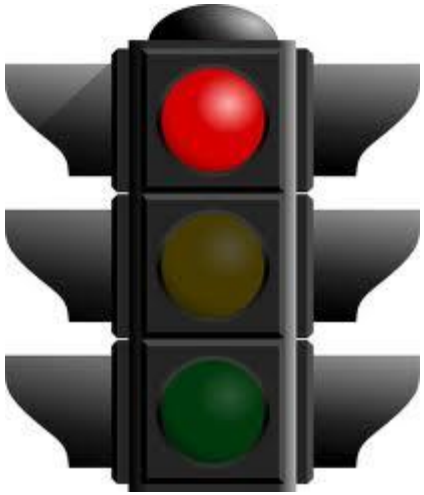
- An existing BAA may continue to operate beyond the compliance deadline (September 23, 2013) if:

  (i) the agreement is effective PRIOR to Jan. 25, 2013, and it contains all the elements required by the regulations as of that date; and

  (ii) the agreement was *not* modified or renewed from March 26, 2013 (the Final Rule effective date) until Sept. 23, 2013 (the Final Rule compliance date)
- If both elements above are satisfied, the existing BAA is deemed compliant until the earlier of:
  - Date of modification or renewal (after Sept. 23, 2013), or
  - Sept. 22, 2014

Key Prohibition

- The BAA may not authorize the BA to use or further disclose PHI in a manner that would violate the requirements of HIPAA, if done by the CE
  - 45 CFR § 164.504(e)(2)(i)



Required Provisions:

- Establish the permitted and required uses and disclosures of PHI by the BA
  - 45 CFR § 164.504(e)(2)(i)
- Prohibit BA from using or further disclosing PHI other than as permitted or required by the BAA or as required by law
  - 45 CFR § 164.504(e)(2)(ii)(A)
- Require BA to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by BAA
  - 45 CFR § 164.504(e)(2)(ii)(B)

Required Provisions:

- Require BA to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the CE
  - 45 CFR § 164.504(e)(2)(ii)(B), *see also* 45 CFR §§ 164.308, 310, and 312
- Require BA to ensure that any agent, including a subcontractor, to whom it provides PHI agrees to implement reasonable and appropriate safeguards to protect it
  - 45 CFR § 164.504(e)(2)(ii)(B), *see also* 45 CFR § 164.314(a)(2)(i)(B)

Required Provisions:

- Require BA to Report to CE (or higher level BA):
  - Any security incident of which it becomes aware
  - Any use or disclosure of the information not provided for by the BAA of which it becomes aware
  - Any breach of unsecured PHI, including, to the extent possible, identity of each individual involved and other information to allow CE to provide notice within 60 days
  - 45 CFR § 164.504(e)(2)(ii)(C)
- Require BA to obtain written assurances that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of the CE agrees to the same restrictions and conditions that apply to the BA with respect to such information
  - 45 CFR § 164.504(e)(2)(ii)(D)

Required Provisions:

- Require BA to make an individual's PHI available to them upon request and in accordance with 45 CFR § 164.524
  - 45 CFR § 164.504(e)(2)(ii)(E)
- Require BA to make available PHI for amendment and incorporate amendments to PHI in accordance with 45 CFR § 164.526
  - 45 CFR § 164.504(e)(2)(ii)(F)
- Require BA to make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528
  - 45 CFR § 164.504(e)(2)(ii)(G)

Required Provisions:

- To the extent that the BA is to carry out CE's obligations under the Privacy Rule (as an agent), require BA to comply with the requirements of the Privacy Rule
  - 45 CFR § 164.504(e)(2)(ii)(H)
- Require BA to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of the CE available to the Secretary of HHS for purposes of determining the CE's compliance with this subpart
  - 45 CFR § 164.504(e)(2)(ii)(I)

Required Provisions:

- At termination of the BAA, require BA, if feasible, to return or destroy all PHI received from or created or received by the BA, and retain no copies of such PHI
  - If return or destruction is *infeasible*, require BA to extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction infeasible
  - 45 CFR § 164.504(e)(2)(ii)(J)
- Authorize termination if BA has violated a material term of the BAA
  - 45 CFR § 164.504(e)(2)(iii)

Permitted Provisions:

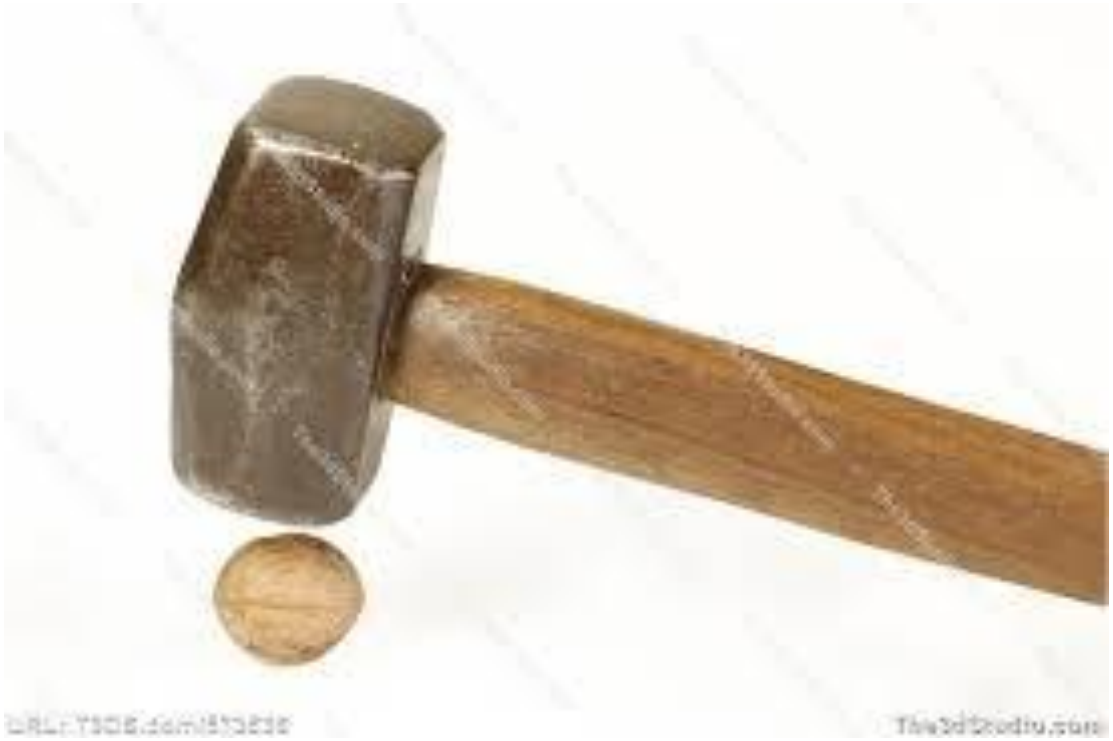
- Use PHI if necessary for its proper management and administration or to carry out BA's legal responsibilities
  - 45 CFR § 164.504(e)(4)
- Disclose PHI:
  - If the disclosure is required by law, or
  - If necessary for its proper management and administration or to carry out BA's legal responsibilities, so long as the BA
    - Obtains reasonable assurances that the disclosed PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed, and
    - The person to whom the PHI was disclosed agrees to notify the BA of any breach
  - 45 CFR § 164.504(e)(4)
- Provide data aggregation services relating to the health care operations of the CE
  - 45 CFR § 164.504(e)(2)(i)(B)

Negotiating BAAs

- Sometimes…..

Negotiating BAAs

- Other times…..



Hot Topics

- Overly Expansive Definitions
- Timing for Breach Notification
- Breach Notification & Mitigation Responsibility
- Breach Notification & Mitigation Payment
- Indemnity/Limitations on Liability
- Insurance
- Audit Rights
- Right to Cure Before Termination
- Right to Determine if Return/Destruction is Infeasible
- Timing for Access, Amendment, and Accounting
- Use of the “Cloud”

Hot Topics

- Right to Approve Subcontractors
- State Law Requirements
- Encryption
- Equitable Relief
- International Subcontractors
- Notice Regarding Subpoenas/Legal Action
- Right to Control Litigation
- Unilateral Amendment
- Ownership of PHI
- Specific IT Requirements
- Notification to Secretary

Hot Topics

- Survival Clauses
- Termination of Other Contracts Between the Parties
- Compliance with CE's Policies/Procedures/Training
- Minimum Necessary—for CE
- 42 CFR Part 2
- Gramm-Leach-Bliley Act
- Red Flag Rules
- Shenanigans

Penalties for HIPAA Violations

Civil Penalties	$100-$50,000 per violation <u>Tiered Penalties Based on Culpability</u> • Unknowing ($100 per violation/ $25K max) • Reasonable Cause ($1K per violation /$100 K max) • Willful neglect ($10K per violation/$250K max) • Uncorrected willful neglect ($50K per violation/$1.5M max)
Criminal Penalties	up to $250,000
Imprisonment	up to 10 years

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS): OCR Takes Actions Against a Business Associate (June 2016)

- CHCS entered a settlement of $650,000 as a BA to six SNFs where CCHS provided management and information technology services.
- There was a breach involving 412 patients due to the theft of an unencrypted, non-password protected, employee iPhone.
- CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident.
- OCR also determined that CHCS had no risk analysis or risk management plan

2016: The Need for BAAs gets Real

- The Center for Children's Digestive Health (CCDH) entered a settlement for $31,000 for failure to maintain a BAA with FileFax, Inc. in October 2016.
  - CCDH first began sharing PHI with FileFax in 2003, but the parties could not provide a signed BAA prior to October 12, 2015.
- Care New England Health System ("CNE") entered a $400,000 settlement and CAP for acting as a BAA to its various entities under common ownership and control in September 2016.
  - CNE provided centralized support for various entities such as finance, HR, IT, insurance, and compliance.
  - One such entity, Woman & Infants Hospital of Rhode Island reported loss of unencrypted back up takes containing ultrasounds for 14,000 patients.
  - BAA between entity and CNE was effective March 15, 2005 but not updated until August 28, 2015 as a result of the OCR investigation and therefore failed to incorporate revisions under HIPAA Omnibus Final Rule.

Questions?

Nathan A. Kottkamp

804.775.1092
nkottkamp@mcguirewoods.com

www.mcguirewoods.com

Privacy & Security Challenges

Isaac M. Willett

FAEGRE BAKER DANIELS

Harnessing Health Data

- Electronic format makes analysis easy
- Promote population health
- Improve outcomes
- Better allocate resources
- Predict trends and prevent illness/outbreaks
- Increase sales

Examples

- Optum Labs – joint venture of UnitedHealth and Mayo Clinic
  - Links 5 million Mayo records + 100 million UH claim records
  - Examine outcomes and cost
- CMS Basic Stand Alone Claims Public Use Files (de-identified) and Limited Data Sets (partially de-identified)

Examples

- Professional society data registries
  - NCDR – American College of Cardiology
- FDA post-market surveillance registries
- IMS Health – vendor of physician prescribing data
- Business associates of all varieties

Related HIPAA Issues

- Data aggregation
- De-identification and limited data sets

Data Aggregation

- Combining of PHI of one covered entity with that of another
- Can be done only by business associate
- Must further health care operations of the respective covered entities
- Must be authorized by BAA

Data Aggregation Challenges

- BA wants to aggregate data and CE refuses
- CE wants benefit of data aggregation but says its PHI cannot be used for other CEs
- CE wants to be able to remove its data
- BA wants to use aggregated data for purpose other than health care operations of CEs

De-Identification

- De-identified data is not PHI and can be used and disclosed for any purpose
- De-identification standards are strict
- Person with appropriate knowledge applies statistical principles, determines risk is very small that information could be used to identify the individual & documents that
- 18 specific identifiers removed (safe harbor)

De-Identification Challenges

- BAA does not address de-identification
- CE and BA do not agree on whether/when permitted
- Parties misunderstand de-identification standard – common to think removal of limited direct identifiers is sufficient
- CE and BA do not agree on use of de-identified data

Limited Data Sets

- Partially de-identified data that removes direct identifiers
- Can retain dates, zip codes
- Must have data use agreement
- Use only for health care operations of CE, research, public health purposes

LDS Challenges

- BAA does not provide for creation/use of LDS
- BA wants to use LDS for purposes other than those permitted
- Confusion over use of LDS to meet minimum necessary requirements and use of LDS for public health, research, HCO
- Failure to recognize this is still PHI

Best Practices

- Think through data aggregation, de-identification, LDS on front end
- Be sure underlying agreement/BAA address these issues
- Educate clients on requirement/limitations of each

Security Breaches

- BAs must give notice of breaches of unsecured PHI
- BA must give notice to CE of a breach
- Subcontractor BAs must give notice to primary BA
- BAA must address security breaches

Security Breach Challenges

- Requests that BA provides notice directly to individuals rather than CE
  - Works in some cases (TPA of health plan), but not in others
- Unrealistic time frames for breach reporting
- Downstream BAAs that are not as restrictive as primary BAA

Security Breach Challenges

- Content of notice involving BA
  - Allocation of responsibility, use of name/trademarks
- Managing foreign subcontractors
- Liquidated damages clauses for violations
- State law notification obligations
- Implementation

Contact Information

Isaac M. Willett | isaac.willett@faegrebd.com | 317-569-4640

FAEGRE BAKER DANIELS