Am I a Business Associate? Now What?
agenda

» Overview of HIPAA / HITECH
» Business Associate (“BA”) Basics
» What Do BAs Have to Do to Comply?
» When Is a Covered Entity (“CE”) on the Hook for Actions of the BA?
» When Do BAs Have to Comply?
» The To-Do List
» Suspected Breaches: There’s More!
Overview of HIPAA and HITECH
data privacy & security

» HIPAA – Health Insurance Portability and Accountability Act of 1996
  – Covered entities: health care providers that engage in standard electronic transactions, health plans, health care clearinghouses

» ARRA – American Recovery and Investment Act of 2009
  – Includes the Health Information Technology for Economic and Clinical Health Act (HITECH Act)
  – HITECH amended HIPAA and applied requirements directly to covered entities’ business associates

» State law protections
HITECH Act

- Privacy and Security Rules apply directly to BAs
- Impose breach notification requirements on CE and BA
- Limit some uses and disclosures of protected health information
- Expand individual rights
- Increase penalties for HIPAA violations – expanded efforts to include proactive audits & State Attorney General enforcement
Omnibus Rule

» Compliance deadline is September 23, 2013 (with some limited exceptions)
» Implemented the HITECH Act
» Changed definition of BA and other requirements under the Privacy, Security, and other HIPAA Rules
» Expanded who is a BA and imposed additional requirements on BAs
» This presentation focuses on the Omnibus Rule and relevant parts of HIPAA and HITECH for BAs
Business Associate Basics
what does it mean to be a BA?

- CEs can share protected health information with BAs in order for BAs to perform services
- The BA must provide “satisfactory assurance” that it will safeguard the information – this is in the form of a Business Associate Agreement (“BAA”)
- BAs are directly required to comply with HIPAA and HITECH
who are **BAs**?

**With respect to a CE, a BA is a person who:**

> Creates, receives, maintains, or transmits protected health information

> For a function regulated by HIPAA

> CEs can also be BAs of other CEs

> A person or entity can be a BA even if they did not sign a BAA with the CE
examples of BAs

» Billing companies or Billing and Coding Consultant
» Data Storage Companies *(digital or physical)*
» Patient Safety Organizations *(PSOs)*
» Entities that offer Personal Health Records *(sometimes)*
» Health Information Organizations
» Sales and Marketing vendors *(sometimes)*
» Subcontractors that create, receive, maintain or transmit PHI on behalf of another BA
not a BA

- Employee
- Health insurance plan receiving PHI from provider
- Provider treating the patient
- Government agencies (such as public health department)
- External or independent Institutional Review Boards
- Banks/financial institutions with respect to payment activities
- Professional liability insurers/risk management companies where the relationship relates to insurance benefits
The “conduit exception” from the BA definition is limited to transmission services (digital or physical) including any temporary storage of transmitted data incident to such transmission.

An entity that stores or maintains PHI on behalf of a CE is not a conduit – even if it does not actually view the PHI – so that entity would still be a BA.

Difference is transience (occasional, random) versus persistent nature of the opportunity to access the PHI.

Examples that do not meet the conduit exception:

- **Data storage company** that has access to PHI is a BA even if it does not access the PHI.

- **Health information organizations** are BAs in that they require access to PHI to manage the exchange of PHI on behalf of the CE (e.g., through the use of a record locator service).
Data storage companies

» Data Storage Companies maintain PHI on behalf of CE – the opportunity to access data is constant, unlike a conduit

» Data Storage Companies are BAs “even if the entity does not actually view the protected health information”

» True whether digital or hard copy

» Definition of BA now amended to include a person who “creates, receives, maintains or transmits” PHI on behalf of a CE
personal health record vendors

» PHR vendors are BAs when they are functioning on behalf of a CE

» If they maintain PHI on behalf of the CE, and offer the PHR to the patient, they are going to be a BA whether or not they actually exercise the opportunity to access the PHI

» Also covered under FTC rules
subcontractors

» The Final Rule applies the BA provisions of HIPAA to subcontractors (obligations, liability)

» The definition of BA thus includes a “subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate”

» A subcontractor is a person to whom a BA has delegated a function, activity or service that the BA has agreed to perform for the CE

» The CE is not required to have a direct contract with the subcontractor to establish the BA relationship
subcontractors

» A BA must have a written agreement with its subcontractor containing satisfactory assurances that the subcontractor will comply with applicable provisions of the Privacy and Security rules

» A BA aware of noncompliance by its subcontractor must respond in the same way a CE would respond to noncompliance by a BA

» Distinguish between subcontractor and workforce – may be a fine line

» Once a BA identifies its subcontractors, evaluate whether the relationship involves the creation, receipt, maintenance or transmission of PHI
What do Business Associates Have to Do to Comply?
BAs are on the hook!

» Direct Liability
  – Impermissible uses and disclosures (including more than the minimum necessary)
  – Comply with breach analysis & notification requirements
  – Provide access to copy of electronic PHI
  – Disclose PHI where required by HHS to investigate/determine compliance with HIPAA
  – Provide an accounting of disclosures
  – Comply with Security Rule
  – Comply with applicable Privacy Rule requirements

» Noncompliance could subject the BA to civil and criminal penalties

» Legal obligation to comply with applicable HIPAA provisions CANNOT be limited by refusing to sign a BAA
What do BAs (and Subcontractors) need to do to comply with the Security Rule?

» Identify Security Officer

» Conduct Risk Assessment to determine gaps in security measures

» Identify and implement what additional security measures need to be put in place to address gaps

» Draft policies and procedures to address standards and implementation specifications in the Security Rule
What do BAs (and Subcontractors) need to do to comply with the Privacy Rule?

- BAs may only use and disclose PHI as permitted in the BAA, 45 C.F.R. § 164.504(e) or as required by law.
- Technically, BAs are not required to comply with all requirements of the Privacy Rule — but in practice, most requirements will apply.
- Will need to train employees on policies and procedures.
- BAs may contractually agree to implement additional Privacy Rule requirements on behalf of the CE.
Minimum necessary standard modified to apply directly to BAs

BAs must use / disclose / request only the minimum amount of PHI necessary to accomplish the purpose intended

Applies to disclosures or requests to another BA, to a BA’s subcontractor, or to a CE
revise your BAAs!

Changes in **legal requirements** for BAAs:

- Statement that BAs are subject to the Security Rule and applicable provisions of the Privacy Rule
- Statement that BAs are subject to the Minimum Necessary Rule
- Requirement that BAs must enter into written agreements with Subcontractors that comply with the same restrictions and obligations that apply to BAs
- Requirement that BAs report breaches of unsecured PHI to CE
- Statement that to the extent BA carries out one or more CE’s obligations under the HIPAA Privacy Rule, BA shall comply with the requirements of HIPAA that apply to CE in the performance of such obligation(s)
other topics BAA may address

In that case, parties may negotiate matters such as:

- Breach Notification and mitigation – who responds, who pays, process for providing notice, etc.
- Responding to requests from individuals related to access of PHI, amendments, accountings, etc.
- Indemnification
- CE prohibiting BA from de-identification and aggregation services
- Minimum necessary language – BA will comply with CE policies
- CE conducting audits of BA
- CE prohibiting PHI from being transferred offshore/outside the United States
- CE may want to review BA subcontractor agreements
- Type of notification for unsuccessful security incidents

CEs may make additional requests of BAs that go beyond what is required by HIPAA
BAAs

Sample BAA from OCR:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
de-identification

» A BA may not de-identify PHI for its own use unless that is permitted by the terms of the BAA

» If de-identification is not permitted in the BAA between the CE and the BA, the BA may not permit a subcontractor to de-identify the data for its own use either

» Agreement between BA and subcontractor must be as stringent as the BA’s agreement with the CE
the BA relationship is not contingent on the BAA

Having a BAA does not make everything you do compliant and it does not authorize every disclosure or use

Not having a BAA does not excuse you from liability if a BA relationship exists

A BA relationship exists if the person performing the services meets the definition of “business associate”

This is true even if the parties fail to enter into a BAA – but then the failure to have an agreement is itself a HIPAA violation – for BOTH the CE and the BA
“Oh we hardly see any PHI”

» Seeing a little PHI (or having the opportunity) is like being a little bit pregnant

» The preamble to the Final Rule states that an entity is a BA even if the PHI it maintains is not diagnosis-specific and is not indicative of the health care services provided to the patient.

» Even if the only PHI that a BA receives is the fact that the patient received care or benefits from the CE, that information must be protected by the BA in accordance with HIPAA.
additional regulated activities

» Use and disclosures of PHI for marketing or fundraising purposes and sale of PHI are all highly regulated

» BA and CE involved will want to plan so they can comply with additional applicable HIPAA requirements, including obtaining patient authorization

» Each arrangement involving payments or other consideration and transfers or sharing of PHI should be evaluated for compliance with the Final Rule in order to avoid “accidentally” triggering the sale and marketing rules
when is a CE on the hook for the actions of the BA?

When the BA is an “Agent”

(So what does that mean??????)
why do CEs care if a BA is an agent?

Two Reasons:

1. The CE is deemed to have knowledge of a breach at the same time as a BA if the BA is an agent
   » CE has to provide notifications of a breach
   » BA knowledge imputed to CE if BA is an agent

2. The CE can be liable for BA HIPAA violations if the BA is an agent acting within scope of agency
when is a BA an agent?

Fact specific – analyzed under federal common law of agency

Depends overall on the right of the CE to control the BA’s conduct

Can the CE give instructions/directions or does the contract give the BA the power to control its activities for the CE?

This same analysis between the CE and BA also applies to the BA’s relationship between the BA and its own subcontractors who may be agents.
factors to consider for agency

- Time, place, purpose of the BA’s (bad) conduct
- Whether the BA’s (bad) course of conduct is under CE control
- Whether the BA’s (bad) conduct is commonly carried out by a BA for a CE
- Whether the CE reasonably expected that the BA would engage in the (bad) conduct
- Was the CE able to give interim instructions relating to the (bad) conduct?
- Contract may be relevant but labels (e.g. “independent contractor”) are not dispositive
When Do Business Associates Have to Comply?
Rule was effective March 26, 2013; compliance due within 180 days of effective date

- New BAAs = September 23, 2013

- Existing BAAs = For BAAs that were entered into prior to January 25, 2013 (and that complied with HIPAA regulations in effect at that time), and are not renewed or modified between March 26, 2013 and September 23, 2013, the BAAs shall be deemed compliant until the earlier of:
  - The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or
  - September 22, 2014
If a BAA automatically renews, without modification of terms, that won’t be considered a “renewal” for the purposes of the grandfathered status.

In other words, if you had a compliant BAA in place by January 25, and that BAA auto-renewed without modification of terms on April 1 (or really any date before September 22, 2014), you would still have until September 22, 2014 to comply with the new rules.
The TO DO LIST
what CEs are doing now

» Auditing their existing BA database – sound like fun?
» Updating BAAs
» Figuring out which BAAs must be revised by September 23, 2013 and which may qualify for the grace period
» Identifying relationships where there is NOT a BAA but should be
» Communicating expectations to their BAs – such as contracting with subcontractors
» Assessing obligations as a BA to other CEs and what needs to be done to document those or update the documents
» Revising policies and procedures to reflect BA changes (as well as the other regulatory changes)
» Re-training of staff
what BAs are doing now

» Evaluating relationships with CEs to determine if there is a business associate relationship

» Evaluating relationships with subcontractors to determine who should be subject to a sub-BAA

» Updating any existing BAA to reflect the new requirements

» Establishing or updating required policies

» Conducting workforce training as needed

» Implementing security fixes, such as password protect mobile devices, as needed

» Complying with the BAA and any investigation or notice obligations in the event of a breach

» Appointing a security/privacy officer
Suspected Breaches: There’s More!
security breach investigation steps

1. Determine whether there has been an impermissible acquisition, access, use or disclosure of PHI in violation of the Privacy Rule

2. Determine if the PHI is unsecured

3. Evaluate whether the incident falls under one of the exceptions to the notification obligations

4. Conduct a risk assessment to determine whether the impermissible use or disclosure poses a low probability of compromise to the PHI

5. Resist the urge to automatically assume notification is required
risk assessment

Old “subjective” standard:
Notification required if significant risk of financial, reputational, or other harm to the individual.

New “objective” standard:
Notification required unless a low probability that the PHI has been compromised. Also, presumption that impermissible use or disclosure is a breach.

Focus is now on the risk the PHI was compromised, instead of the risk of harm to the individual.
four factors

1. Nature and extent of the PHI, including types of identifiers and likelihood of re-identification

2. Unauthorized person who used the PHI or to whom the PHI was disclosed

3. Whether PHI actually acquired or viewed

4. Extent the risk to the PHI has been mitigated
complete risk assessment

» **Analyze** four factors, plus any other relevant factors

» **Evaluate** overall probability that PHI has been compromised

» Risk assessment **must be thorough**, completed in good faith, and conclusions must be reasonable

» Must be **documented in writing**

» **Notification required if risk assessment fails to show low probability that PHI has been compromised**
complete risk assessment (cont’d)

» If notice is provided, no risk assessment is necessary

» OCR says it will issue guidance on performing risk assessments for frequently occurring scenarios
burden of proof

CE or BA has burden of proof for showing why breach notification was not required!
BA notification requirement

» BAs must notify CEs without unreasonable delay and in no case later than 60 days after BA discovers breach (no delay for investigation)

» Time period for notification from BA to CE might be shorter in the BAA

» Considered to have been discovered when workforce member (other than the person who committed the breach) or other agent finds out

» If BA is an agent of CE, the 60-day clock starts running the day the BA “discovers” the breach

» Agency relationship determined by principles of federal common law
other considerations

» Payment Card Industry (PCI) Data Security Standards

» International Breach Laws

» State Law

» FTC Rules
tips to prevent breaches

» Conduct periodic risk analyses/assessments

» Implement strong security protections for PHI
  - Implement encryption technology and password protection mechanisms
  - Evaluate your mobile devices, data destruction, and data transmission practices
  - Generally review your security policies and procedures — the first step in avoiding a trap is knowing of its existence

» Train your employees
tips to prevent breaches (cont’d)

» Evaluate and limit the type of information your organization receives, uses, discloses, and retains to only the minimum necessary amount of information that is needed
  – The less PHI your organization has, the lower risk of a security breach
  – Proactively Develop a Security Incident Response Plan
  – Assemble a breach team
  – Review your breach notification policies and procedures to help guide your organization through handling breaches
HIPAA breaches

**Wellpoint** – Settled HIPAA breach for $1.7 million; noncompliance included failure to perform an adequate technical evaluation in response to a software upgrade.

**Cedars Sinai Hospital** – Fired 6 staff for snooping in 14 patient medical records; coincidentally, this was during the time period that Kim Kardashian had her baby at the facility.

**Prime Healthcare Services hospital system** – Fined $275,000 for its staff disclosing information without authorization from patient medical records to media and an internal email to 700 employees while defending the facility against an overbilling allegation; noncompliance included failure to follow its own policies because the hospital did not sanction its employees for the violations.
to get more info and discuss your Business Associate needs

contact:

BA@vendormate.com