Hogan Lovells

THE GEORGE WASHINGTON UNIVERSITY
SCHOOL OF PUBLIC HEALTH AND HEALTH SERVICES

# Exchanging Health Information: Key HIPAA Issues for AF4Q Alliances and CVEs

Melissa Bianchi, JD
Jane Hyatt Thorpe, JD
Lara Cartwright-Smith, JD, MPH

September 25, 2013

# Agenda

- Introductions
- Business Associates
- Compliance Deadlines
- Sale of PHI
- De-identified PHI
- Discussion
- Resources

# Business Associates and Business Associate Agreements

The HITECH Final Rule:

- Modifies definition of business associate (BA)
- Applies many HIPAA requirements directly to BAs
- Expands and revises the requirements for BA agreements (BAAs)
- Provides a Compliance Transition Period for entering into BAAs that satisfy the new requirements

# Who is a Business Associate?

- Business Associates
  - An entity that creates, receives, maintains or transmits PHI on behalf of a covered entity to perform a function or activity for that CE
    - E.g., claims processing, quality assurance, benefit management, data aggregation, administrative services
    - E.g., quality improvement activities sites perform for plans
  - BAs are BAs by virtue of their roles; liable even if don't enter into a business associate agreement

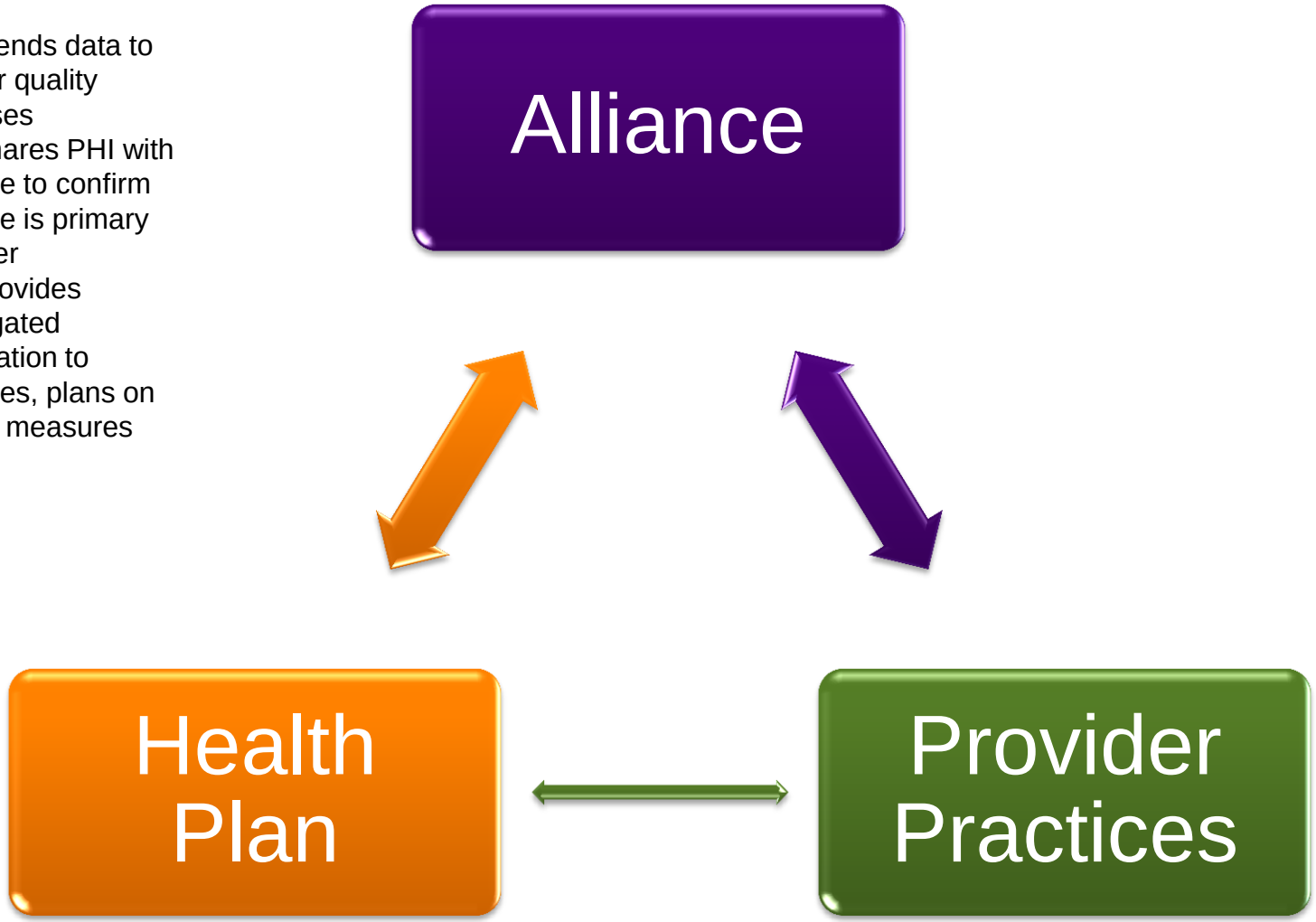
# Who is a BA Under the Final Rule?

*Definition of "business associate" revised to include*:

- Subcontractors (acting on behalf of another BA)
- Entities performing patient safety activities listed at 42 CFR 3.20 (Patient Safety Act)
- Health Information Organization, E-prescribing gateway, or other provider of data transmission services requiring PHI access on a routine basis
- Entities that maintain PHI on behalf of a CE
- Entities providing Personal Health Records on behalf of CE

# Example of Data Exchange

- Plan sends data to Site for quality purposes
- Site shares PHI with practice to confirm practice is primary provider
- Site provides aggregated information to practices, plans on quality measures



# What Requirements Will Apply to BAs?

- Enforcement, Security, Privacy Rules will apply to varying extents (Breach Rule already applies).
  - Security Rule: bootstraps virtually entire rule and imposes it on BAs directly.
  - Privacy Rule: provisions restricting uses and disclosures of PHI and the BAA requirements, among others, apply directly.

# What Requirements Will Apply to BAs?

*Privacy Rule*: *Uses and Disclosures include:*

- BA may not use or disclose PHI except as permitted or required by the Privacy Rule or Enforcement Rule .
- BA may use and disclose PHI only as permitted or required by its BAA.
- BA may not use or disclose PHI if would violate Privacy Rule if done by CE.
- BA may use/disclose for data aggregation services related to CE's health care operations as defined in the Privacy Rule.
- De-identify or create a limited data set, only with express permission.

# Direct business associate requirements include:

- Compliance with Security Rule
- Privacy Rule provisions, including:
  - Use/disclose only the minimum necessary amount of PHI required for the task
  - Enter into subcontractor BAAs with vendors
  - Report breaches of unsecured PHI to CE
  - Provide an accounting of disclosures
  - Respond to CE or individual when receive a request for electronic access

# Timeframe for BA-Related Compliance

September 23, 2013

- BAs are required to comply with Security Rule and all BA obligations under the Privacy Rule, *whether or not they have entered into a BAA with the CE or other BA*
- CEs are required to comply with new Privacy and Security Rule requirements except for the requirements for new BAA provisions for BAAs that qualify for a transition period *(see next page)*
- BAs and CEs are required to comply with requirements for new BAA provisions for any BAAs

  (i) executed on or after January 25, 2013, or

  (ii) executed prior to January 25, 2013, and either (x) not in compliance with pre-HITECH rules, or (y) renewed or modified between March 26, 2013 and September 23, 2013

*Note: CEs and BAs already required to comply with Breach Rule, and Enforcement Rule compliance required March 26, 2013*

# Compliance Date for BAAs that Qualify for Transition Period

- Date of BAA renewal or modification:
  - BAAs renewed or modified between September 23, 2013 and September 22, 2014
- September 22, 2014:
  - BAAs executed prior to January 25, 2013 that (i) comply with pre-HITECH rules, and (ii) are not renewed or modified between March 26, 2013 and September 22, 2014
- *It is not considered a renewal or modification when "evergreen" contracts automatically roll over*

# Business Associate Resources

- Fast Facts: Are You a Business Associate Under the HIPAA Privacy and Security Rules? www.healthinfolaw.org/article/ff-hipaa-BA
- Myth Buster: A business associate's scope of liability is determined by the terms of its business associate agreement www.healthinfolaw.org/article/mb-ba-liability
- Decision Support Tool: Are You a Business Associate? Flowchart www.healthinfolaw.org/article/flowchart-ba
- Fast Facts: HIPAA Final Rule Compliance – September 23, 2013 www.healthinfolaw.org/article/ff-hipaa-compliance-09-23-2013
- Fast Facts: What are HIOs and PHRs? www.healthinfolaw.org/article/ff-hio-phr

# No Sale of PHI Without Authorization

Sale of PHI is prohibited without an individual's prior authorization (2013 Omnibus Final Rule).

Sale of PHI =

- Disclosure by a covered entity (CE) or business associate (BA) of PHI in exchange for direct or indirect remuneration from or on behalf of the recipient of the PHI;
  - "sale" is not limited to transfer of ownership; includes disclosures in exchange for remuneration that are the result of agreements to access, license, or lease the PHI

Remuneration =

- Direct remuneration (payment from the 3rd party that receives the PHI)
- Indirect remuneration (payment from another party on behalf of the 3rd party receiving the PHI)
- In-kind remuneration and non-financial benefits (e.g., computers in exchange for disclosing PHI)

# Re-disclosure for remuneration

A CE or BA may re-disclose PHI (that is, share or release health information that was received from another source) for remuneration only:

- If authorized by the patient in the original or an additional patient authorization; or
- If the re-disclosure meets an exception to the definition of sale of PHI.

# Exceptions

Transactions that fall under one of these exceptions will not be considered “sale” of PHI:

- Public health activities (such as reporting of communicable diseases)
- Research purposes, as long as the price charged reflects the cost of preparation and transmittal of the information for research purposes
- Treatment and payment activities (such as processing insurance claims);
- Sale, transfer, merger, or consolidation of all or part of a CE or BA
- Providing access or an accounting of disclosures to an individual
- Disclosures required by law (such as federal program requirements, like Medicare audits to identify fraud)
- For business associate activities
- As otherwise allowed under HIPAA, where a reasonable cost-based fee is paid.

*Limited data set not exempted*

# Business Associate Exception

Not a Sale of PHI if:

- To or by a business associate for activities performed on behalf of the covered entity
- To or by subcontractor BA for activities performed on behalf of the BA
- Provided the only remuneration is from the BA to the CE, or the BA to the sub-BA for performing such activities

- Note that the exchange of PHI through a health information exchange paid for through fees assessed on participant. May also fit within BA exception, but not a Sale of PHI regardless

# Sale of PHI – Public Health and Research Exceptions

- Public health exception:
  - Disclosures to public health authorities authorized by law to receive the information (reporting of disease, public health surveillance, etc.)
  - No cost limitation
- Research exception:
  - Reasonable cost-based fee to cover the cost to prepare and transmit data
    - Labor, materials supplies necessary to generate, store, retrieve, transmit PHI and to ensure it is disclosed in a permissible manner; capital and overhead costs.
    - Profit not allowed.

# Sale of PHI – Exception for Grants

- Exceptions – Not a Sale of PHI
  - Grants, contracts, or other arrangements to perform programs or activities, such as a research study
    - Any provision of PHI to the payer of the grant, etc. is a byproduct of the service being provided
    - Example: Grant or other funding from government, even if as a condition of funding, CE is required to report PHI for program oversight or other purposes
    - Example: payment by research sponsor to CE to conduct research study, even if research results that include PHI are disclosed to the research sponsor

# Examples

- A physician sells a list of patients suffering from a certain condition or taking certain types of medications to a pharmaceutical company, which will send coupons directly to the patients. This activity constitutes a sale of PHI. Patient authorization is required before the physician may provide the list.

- A physician gives a patient their medical records upon request but charges a reasonable fee for copying the records. This activity is not a sale.

- A hospital pays fees to participate in the regional Health Information Exchange (HIE) and shares PHI with the HIE. This activity is not a sale.

# Sale of PHI Resources

- Fast Facts: Can You Sell Protected Health Information Under HIPAA? www.healthinfolaw.org/article/ff-sale-phi
- Myth Buster: A health care provider cannot sell an individual's protected health information www.healthinfolaw.org/article/mb-sell-phi
- Fast Facts: HIPAA Final Rule Compliance – September 23, 2013 www.healthinfolaw.org/article/ff-hipaa-compliance-09-23-2013

# Looking at De-Identification

There are two methods of de-identifying PHI in accordance with the HIPAA Privacy Rule

## 1. Statistician Certification

- A statistician must determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information.
- The statistician must document the methods and results of the analysis that justify the determination.
- A similar determination by a non-statistician would not satisfy the HIPAA standard. *See* 45 C.F.R. § 164.514(b)(1)

# HIPAA De-Identification Requirements

**2.** **<u>Safe Harbor</u>**: (a) The following 18 identifiers of the individual or of relatives, employers, or household members of the individual must be removed:

| | | |
|---|---|---|
| 1. Name | 7. Social security number | 13. URLs |
| 2. Geographic subdivisions smaller than a state | 8. Health plan beneficiary number | 14. Device identifiers/serial number |
| 3. All elements of dates (except year) for dates directly related to an individual (e.g., DOB, admission date) | 9. Medical record number | 15. Biometric identifiers including finger and voice prints |
| 4. Telephone number | 10. Account numbers | 16. Full face photo and comparable image |
| 5. Fax number | 11. Certificate/license numbers | 17. IP address numbers |
| 6. E-mail | 12. Vehicle identifiers/serial numbers | 18. Unique identifying number, characteristic or code |

(b) and the covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

# De-Identification Resources

- Fast Facts: What is Protected Health Information? www.healthinfolaw.org/article/ff-what-PHI
- New Guidance from HHS Office for Civil Rights on De-Identifying Patient Information www.healthinfolaw.org/article/hhs-ocr-de-identifying-patient-information
- More resources on de-identification coming to www.healthinfolaw.org in late October

# www.HealthInfoLaw.org

- Health system transformation (especially quality improvement and delivery system reform) depends on use and exchange of health information
- Valuable resource covering:
  - All federal and state laws relating to the use and exchange of health information (e.g., HIPAA - http://www.healthinfolaw.org/federal-law/HIPAA)
  - Analyses of emerging issues in state and federal law affecting the transformation of the health care system
  - Content: brief summaries of state and federal laws, fast facts and myth busters, comparative analyses, and longer, in-depth analyses, presented in multiple formats for a variety of audiences

# Legal Barriers Project

- Scope: research and analysis re: actual and perceived legal barriers to health system transformation
- Funded by RJWF since 2006
- Key Staff:
  - Sara Rosenbaum, JD
  - Jane Hyatt Thorpe, JD
  - Lara Cartwright-Smith, JD, MPH
  - Taylor Burke, JD, LLM
  - Devi Mehta, JD, MPH
  - Elizabeth Gray, JD