Getting into the Weeds with Business Associate Agreements

Blue Cross Blue Shield Association Legal Department Cooperative Teleconference

December 12, 2018

Tom Bixby
Thomas D. Bixby Law Office LLC
608.661.4310
tbixby@tbixbylaw.com

BlueCross BlueShield Association

AGENDA

1. Being Sure a BAA is Necessary
2. Strategic Considerations
3. Common Sticking Points
4. Situational Provisions
5. Questions

*With a few of **HIPAA Headscratchers** interspersed throughout the presentation . . . .*

BlueCross BlueShield

3

Being Sure a BAA is Necessary

BlueCross BlueShield

4

Is a BAA Necessary?

Common belief:

- No harm in requiring business associate agreement
- "I can't be blamed" if anything goes wrong

Business Associate Agreement

- *Does* impose safeguards on members' information
- *Should* be imposed when required

BlueCross BlueShield

5

Risks of engaging in unnecessary BAA

Unnecessary business associate agreement:

- **Blue Plan as Covered Entity: BAA unnecessarily imposes:**
  - Breach notice obligation (affected members, HHS, media)
  - Account and public relations difficulties
  - Regulatory oversight/Civil Money Penalties
- **Blue Plan as Business Associate: BAA unnecessarily:**
  - Limits ability to use/disclose PHI
  - Requires return or destruction of PHI

BlueCross BlueShield

6

When is a BAA *not* necessary?

HHS Guidance:

"Whether a disclosure is allowable for health care operations . . . is determined separately from whether a business associate contract is required.

"These provisions of the rule operate independently.

"Disclosures for health care operations may be made to an entity that is neither a covered entity nor a business associate of the covered entity."

- **Treatment, Payment, Health Care Operation Disclosures to third party**
  - **Recipient not always Business Associate**
  - **Disclosures to covered entity often permitted w/o BAA**
  - **Disclosures to other third parties also permitted w/o BAA**

BlueCross BlueShield

7

When is a third party a business associate?

- Two elements to be business associate:
  - Perform on behalf of covered entity function or activity
  - Involves use, disclosure, maintenance, or transmission of PHI
- Performs on behalf of Covered Entity
  - Covered Entity's Payment activities
  - Covered Entity's Health Care Operations
  - [*Health Care Provider's Treatment activities*]

December 12, 2018

BlueCross BlueShield

8

When is a BAA *not* necessary?

- Disclosures to Covered Entity w/o BAA
  - **Health care clearinghouse** (when plan is CE)
  - **Participating provider** (when plan is BA)
- When a disclosure is for *recipient's* TPO
- Disclosures to other third parties w/o BAA
  - **Pharmaceutical Manufacturer**
  - **Stop Loss Carrier**
  - **Health oversight agency (*e.g.*, FBI)**
  - **Bank (*i.e.*, check made out to member)**
- When recipient not performing on CE's behalf

December 12, 2018

BlueCross BlueShield

HIPAA Headscratcher

HIPAA and HITECH Act or 2013 "Omnibus Rule"

- Several statutes affect HIPAA Rules since HIPAA—not just HITECH Act
- "Omnibus Rule" amended HIPAA Rules (not a separate Rule)
- 27 Amendments—not one

BlueCross BlueShield

Strategic Considerations

BlueCross BlueShield

Strategic Considerations

Who is the Covered Entity?

- **Dictates different approach to:**
  - Permitted uses and disclosures
    - > Data aggregation, Limited Data Sets, de-identification
  - Reporting requirements (what gets reported, timing)
    - > Breaches, other Privacy Incidents, Security Incidents
  - Return or destruction
  - Indemnification
  - Audit rights
  - Compliance with all requirements

BlueCross BlueShield

Strategic Considerations

Aligning terms with actual practice

- Reporting requirements (what gets reported, timing)
  - > Breaches, other Privacy Incidents, Security Incidents
- Permitted uses and disclosures
  - > Data aggregation, Limited Data Sets, de-identification
- Return or destruction
- Security requirements

BlueCross BlueShield

13

Strategic Considerations

Sophistication of Business Associate

- **Determining what constitutes a "breach"**
- **Disclosure accounting**
  - > Maintain records for six years; or
  - > Report accountable disclosures when they happen
- **Detail of permitted/prohibited disclosures**
- **Detail of Security requirements**
- **Return or destruction requirements**

BlueCross BlueShield

14

Strategic Considerations

Is Business Associate an "Agent"

- Breach Notification: deemed discovery date
- AWS/Microsoft/Cloud Vendors
- Other vendors?

- **Federal Common Law of Agency**
  - Principal manifests assent to agent acting on behalf of principle
  - Agent's acts have legal consequences for principal
  - Agent consents to act on principal's behalf
  - Principal has right to control agent
  - Factors:
    - > Interaction with third parties
    - > Practice in industry
  - Facts and circumstances—simple statement not dispositive

BlueCross BlueShield

Strategic Considerations

- **Tracking Tool**
  - **Table of template provisions, including**
    - > Limits of terms to which Blue Plan can agree
    - > Compromises to which Blue Plan has agreed
  - **Documentation for consistency:**
    - > Among multiple individuals reviewing BAAs
    - > For new people taking over responsibilities

Template Provision	Common issues	Alternative Approach	Notes
5.1 Breach Notification reports	24-hour reporting requirement	Up to 5 days is acceptable	
5.2 Reporting other privacy incidents			
5.3 Reporting security incidents	Objection to reporting unsuccessful security incidents	BAA is deemed to be report of unsuccessful security incidents	See language in 6/11/2017 BAA with Vendor X.

- **BAA Checklist**
  - https://tbixbylaw.com/resources.php

BlueCross BlueShield

HIPAA Headscratcher

PHI Definition

- **PHI means "PHI received from, or created or received by Business Associate on behalf of covered entity"**
- **Business Associate must return or destroy "PHI received from, or created or received by Business Associate on behalf of covered entity"**
- **Include limitation in some places, not in others . . .**

BlueCross BlueShield

17

Common Sticking Points

BlueCross BlueShield

18

Sticking Points

Whose Data is it?

Blue Plans as BA to ASO Accounts

- **Limits on Use of Account's Protected Health Information for:**
  - Data aggregation?
  - Limited Data Sets?
  - De-Identification?
- **Can Blue Plan segregate data for these purposes?**
- **Return or destroy PHI at termination of Agreement?**
  - Who decides whether to return or destroy?
- **Can Blue Plan (and is it willing to) return or destroy?**

BlueCross BlueShield

19

Sticking Points

Whose Data is it?

Blue Plans as BA to ASO Accounts

- **Argue: Account's information integral to services provided**
- **Retain PHI in accordance with record retention policies**
- **"Proper management and administration" provision**
  - During term of agreement
  - After termination?
- **Business risk:**
  - Contractual and regulatory risk for failure to comply with BAA?
  - Regulatory risk for non-compliant BAA?

BlueCross BlueShield

20

Sticking Points

Reporting Breaches and other incidents

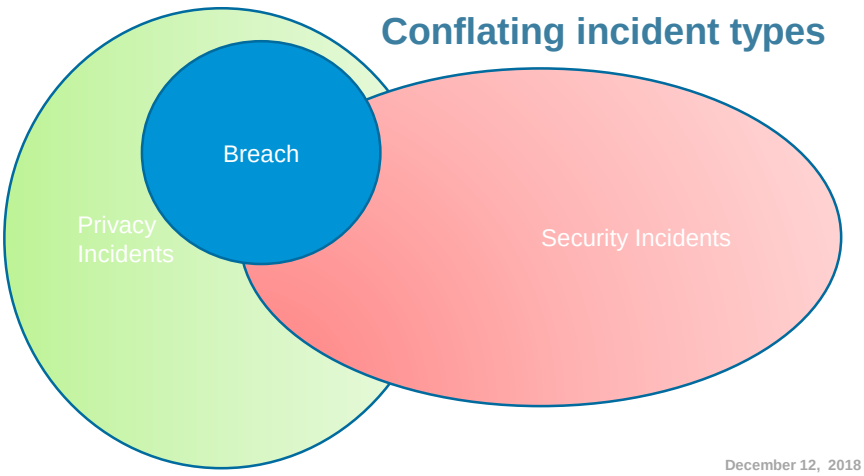
- **Who determines whether an incident is a breach?**
  - **Blue Plan? Its business associate? ASO group?**
  - **Who reports to HHS? Control of determination? Of message?**
  - **Establish terms in contract**
- **When are reports made?**
  - **Timeline too short? Initial notice now, report details later**
  - **Unsuccessful security incidents:**
    - **Report upon request;**
    - **Report annually;**
    - **Report significant change in volume or nature;**
    - **BAA provision serves as notice of unsuccessful security incidents.**
  - **Consider similar approach for non-breach privacy incidents**

BlueCross BlueShield

Sticking Points

Reporting Breaches and other incidents:

Conflating incident types



BlueCross BlueShield

Sticking Points

Indemnification

- **Who is indemnifying whom?**
  - Blue Plan as covered entity
  - Blue Plan as business associate
- **Underlying Agreement**
  - Conflict with indemnification provision in underlying agreement?
  - Argue: delete BAA provision due to provision in underlying agreement
  - Argue: price for services based on provision in underlying agreement
  - Argue: unlimited indemnification unacceptable
- **Don't forget limitation of liability provisions!**
  - Limit to (for example) one year of fees

BlueCross BlueShield

Sticking Points

Indemnification

- **Cyber liability coverage**
  - Cyber breaches primary source of risk
  - Tie to indemnification/limitation of liability
  - List as additional insured
- **Cause of action for breach of contract**
  - May be better than limited indemnity or low limitation on liability
- **Counter arguments**
  - Can we live with provision in underlying agreement?
  - Can we build comprehensive provision into underlying agreement?
  - Limit indemnification to amount of cyber insurance coverage

Business risk

- Indemnification limits built into pricing
- Limitations on liability

BlueCross BlueShield

Sticking Points

Compliance with State Privacy/Breach Laws

- **Difficulty tracking State laws (especially multiple States)**
  - **Compliance with laws identified in BAA (or in writing)**

BlueCross BlueShield

HIPAA Headscratcher

Post Omnibus Amendments Faux Pas

- "Subcontractor and agent"
- Report violation to Secretary
- "Electronic Health Records"
- "Required" agreement to restriction requests
- Use a Limited Data Set for minimum necessary compliance

BlueCross BlueShield

Situational Provisions

BlueCross BlueShield

Situational Provisions

Compliance with HIPAA Transactions Rule

- Conduct in accordance with applicable standards
- Conduct in accordance with CORE Operating Rules
- Cooperate with Plan to Certify Compliance in accordance with ACA

Substance Use Disorder Patient Records Rule Compliance

- Part 2 requires contract language in place by Feb 2, 2020

Auto Amendment

- Plan will send amendment
- BA has 30 days to object (negotiate acceptable change or terminate)
- Bound by terms of amendment

BlueCross BlueShield

Questions?