Do You Know What Your Business Associates' Subcontractors & Vendors Are Doing With Your PHI & ePHI?

Web Hull

Privacy, Data Protection, & Compliance Advisor

Web.Hull@icloud.com

HCCA 2017 Compliance Institute

This presentation and discussion is for Educational Purposes only

Should you desire advice on your specific situation, please seek the counsel of an advisor of your own choosing

The Challenge

- This is an evolving area
- There is no "Play Book" – only emerging, ad hoc approaches
- It takes time, resources, money, and management attention
- The numbers are daunting

Goal

- Begin to Develop a Subcontractor / 4th Party Program That Is
  - Effective
  - Implementable
  - Thoughtful, Respectful, & Sensitive
  - Appropriate to Your Size & Risk
  - Affordable
  - Doesn't "Boil the Ocean"

Key Tools for Meeting the Challenge

1. Your Contract with Your Business Associate
2. Your Business Associate / Third Party Risk Management Program

This Presentation

- Interactive
- Sharing Insights & Experiences
- Questions at Anytime
- A Few Exercises
- Discussion
- Some Handout Tools

Themes

- Having Something is Better Than Having Nothing
- Get Started Now
- Make Progress Everyday
- Document, Document, Document
- It's a Team Effort
  - BA / Third Party Risk Management
  - Security – Info, Physical
  - Privacy
  - Legal Contracts
  - …

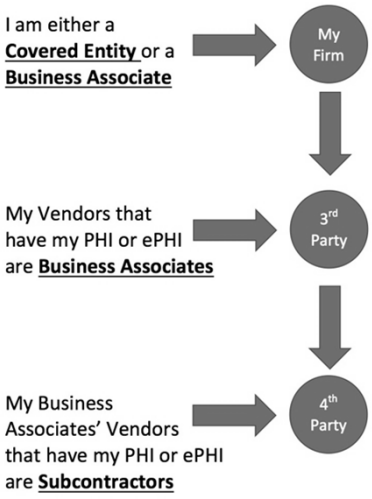
Definitions

- Business Associate
  - (A) "person (with respect to a covered entity) who: … other than in the capacity of a member of the workforce of such covered entity … **creates, receives, maintains, or transmits protected health information** … "or …
  - (p)rovides, other than in the capacity of a member of the workforce of (a) covered entity, **legal, actuarial, accounting, consulting, data aggregation … management, administrative, accreditation, or financial services** to or for such covered entity, … where the provision of the service involves the disclosure of protected health information"

Definitions

- Subcontractor
  - A person or entity that "**creates, receives, maintains, or transmits protected health information on behalf of (a) business associate**."
  - A Subcontractor is also a Business Associate & subject to all the requirements of a Business Associate
- 3rd Party = Your Business Associate
- 4th Party = Your Business Associate's Subcontractor

Definitions



Subcontractor / 4th Party Data Breach

- Multiple Choice Question - If Your Subcontractor / 4th Party Breaches Your PHI or ePHI, Who's Got the Problem?
  a) You
  b) Your BA / 3rd party
  c) Your Subcontractor / 4th party
  d) All of the above
- Discussion Question - What's the Nature / Implication / Consequences of the Problem?

Why I Should Care What A 4th Party Does with My PHI & ePHI

- I Am Ultimately Responsible for My PHI & ePHI
- Breach Notification
- Confidentiality, Availability, & Integrity of Data
- My Reputation
- Costs to Me - $, Time, Regulators, …
- Others?

BA & Subcontractor Requirements

- Business Associates ("BAs") and Subcontractors are required to comply with appropriate HIPAA / HITECH Rules
  - Security
  - Privacy
  - Breach
  - Have a Business Associate Agreement ("BAA") – OCR Template - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
  - Perform Risk Analysis
- Certain State Laws, Rules, & Regulations also apply

BA & Subcontractor Requirements

- Your requirements in regard to your BAs
  - Included in "Risk Analysis"?
  - Have a BAA
- Your Requirements in regard to your Subcontractors
  - Included in "Risk Analysis"?
- Your BA's Subcontractor Requirements
  - Included in "Risk Analysis"?
  - Have a BAA between the BA and the Subcontractor
  - Flow your Business Associate Agreement requirements down to every Subcontractor

Step 1 – My Business Associates

- How Many Business Associates Do I have?
  - If I am a Covered Entity, I might already know this number because OCR asked for it in its Audit Request
  - The OCR also requested Contact Names & Addresses
  - If you don't already have this inventory, now's a good time to start it
  - OCR Template Link
    - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html

Tool #1 – Contract with Business Associate

- Consult / Coordinate with Legal Contracts
- If it is not in a contract, it is very difficult to have the other party do it

Tool #1 – Contract with Business Associate

- Elements to consider
  - Business Associate Agreement
  - Other Agreements
    - Security
    - Data Protection
    - Privacy
    - Breach
  - Subcontractor Requirements
  - Flow Down Requirements

Tool #2 – BA / 3rd Party Risk Assessment Program

- Key Elements of a BA / 3rd Party Risk Assessment & Management Program?
  - Executive Management Support & Reporting
  - Policies & Procedures
  - Adequate Resources – People, Budget, Tools, …
  - Assessment / Reassessment – Questionnaire, Certifications (ISO 27001, AUP, SOC2, …), Evidence, Artifacts, Data Maps, Data Inventory, Subcontractors, …
  - Auditing & Monitoring – On-site & Desk
  - Exceptions & Remediation
  - Others

OCC Third Party Risk Bulletins

- Below are links to 2 OCC documents regarding 3rd and 4th Party Risk Management. The OCC is a major bank regulator & examiner
- These bulletins are relevant in that they address many issues that Healthcare professionals face in managing Business Associates & Subcontractors.
  - OCC Bulletin 2013-29 – "Third Party Relationships: Risk Management Guidance" - https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
  - OCC Bulletin 2017-7 – "Third Party Relationships: Supplemental Examination Procedures" - https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html

Elements to Consider in Contracts, Amendments, & BA / 3rd Party Risk Management Program

- This list is suggestive, not exhaustive

➢ Staff	➢ Transition Plan	➢ Amendment
➢ Funding	➢ Changes	➢ Pricing
➢ Cloud	➢ Agent	➢ Resources
➢ Security Rule	➢ Shared Assessments	➢ Translations
➢ Privacy Rule	➢ Medicare Part D	➢ Who Pays
➢ Omnibus Rule	➢ Assessment	➢ Record Keeping
➢ Denied Persons	➢ Reassessment	➢ Insurance
➢ OCC BULLETIN 2017-7	➢ Crown Jewels	➢ Liability
➢ Termination	➢ Data Minimization	➢ Prior Approval
➢ Mission Creep	➢ Minimum Necessary	➢ Contract
➢ SLA	➢ Monitoring	➢ Return Of Data

Elements to Consider in Contracts, Amendments, & BA / 3rd Party Risk Management Program

- This list is suggestive, not exhaustive

➢ Data Ownership	➢ AUP	➢ Availability
➢ Permitted Uses	➢ ISO27001	➢ Integrity
➢ Disclosure	➢ SOC2	➢ Resilience
➢ Encryption	➢ HIPAA	➢ Data Map
➢ Background Checks	➢ OCC Bulletin 2013-29	➢ Data Inventory
➢ Risk Rating	➢ Log Monitoring	➢ Disaster Recovery
➢ InfoSec	➢ Asset Management	➢ Business Continuity
➢ Physical Sec	➢ Security Incidents	➢ Certify
➢ Detection	➢ Pen Test	➢ Attestation
➢ NIST	➢ Hotline	➢ Certifications
➢ PCI	➢ Confidentiality	➢ Artifacts

Elements to Consider in Contracts, Amendments, & BA / 3rd Party Risk Management Program

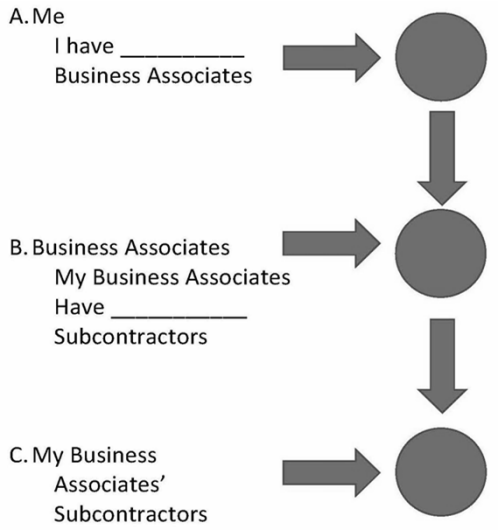
- This list is suggestive, not exhaustive

➢ Evidence	➢ PII	➢ Patching
➢ Training	➢ Trade Secrets	➢ Data Destruction
➢ Laws	➢ ITAR	➢ Procedures
➢ Regulations	➢ M&A	➢ Risk Ratings
➢ Supplier Code	➢ Access To	➢ Risk Management
➢ Fifth Parties	➢ Access Controls	➢ Policies
➢ Flow Down	➢ Records Retention	➢ Periodic Reviews
➢ Policies	➢ Backup	➢ Software Escrow
➢ Vendor Program	➢ BAA	➢ Data Escrow
➢ Offshore	➢ Security Addendum	➢ Audit Rights
➢ PHI	➢ Privacy Addendum	➢ Breach

4th Parties

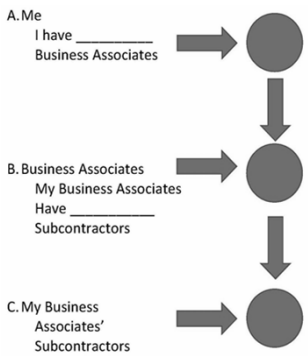
- Do I already Assess & Audit My BA's
  - What is the Cost, Effort, & Success?
- Should I
  - Preapprove My Subcontractors?
  - Assess / Reassess My Subcontractors?
  - Audit My Subcontractors?

How Many 4th Parties Do I Have?



How Many 4th Parties Do I Have?

- Answer = A x B = Total Number of Subcontractors
  _____ x _____ = _____
- If I have 10 Business Associates and each BA has 10 4th parties, I will have 100 4th parties - (10 x 10 = 100)
- If I have 100 Business Associates and each BA has 100 4th parties, I will have 10,000 4th parties - (100 x 100 = 10,000)

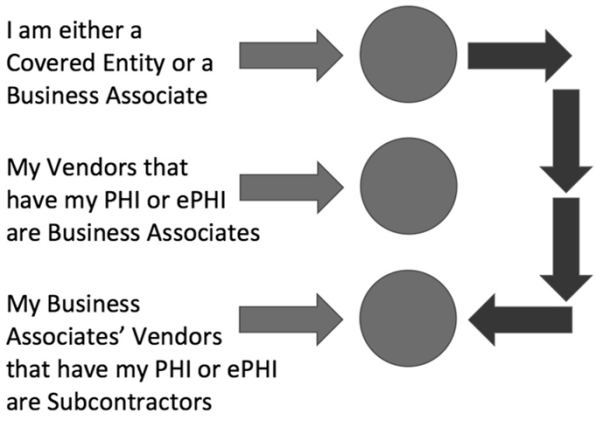


Subcontractor Challenges

- Preapprove / Reapprove Subcontractors
  - How Many Will You Have to Approve?
  - What About the Legacy Subcontractors?
  - What Criteria Will You Use to Approve / Disapprove?
  - What Will Your Turn Around Time Be?
  - What if you Approve a Subcontractor & Something Goes Wrong?
  - What if You Disapprove?
  - Others?

The 4th Party's Challenge

Some people recommend having the right to bypass the 3rd party and directly Assess and Audit the 4th party



The 4th Party's Challenge

- Often the 4th Party's Customer has many Customers of its own. For example:
  - The 4th Party's Customer is a Software As a Service (SAaS) Vendor
  - The SAaS provider has 4,000 customers.
- What If the 4th Party Has 100 Customers & Each Customer Has 100 Customers?
  - 100 x 100 = 10,000 Assessment & Audit Requests

Your 4th Party Challenge

- How reasonable is it for you to Directly Assess / Reassess & Audit your Subcontractors?
  - Large Number of Subcontractors
  - Large Effort & Cost
  - No Direct Relation with Subcontractor – Confidentiality, etc.
  - Subcontractor Push Back
- Your Key Building Blocks Are Already in Place
  - Contract with BA
  - BA / 3rd Party Risk Management Program

Building / Designing a 4th Party Program That's Right for You

- 4th Party Worksheet

Action	Effectiveness	Cost	Ease of Implementation
	High	Low	Easy
	Medium	Medium	Difficult
	Low	High	Very Difficult

Building / Designing a 4th Party Program That's Right for You

- 4th Party Worksheet

Action	Effectiveness	Cost	Ease of Implementation
	High	Low	Easy
	Medium	Medium	Difficult
	Low	High	Very Difficult

  - Use it to define the building blocks that work for you
  - In light of limited resources, the goal is to get all Greens
  - Go for the "Low Hanging Fruit"
  - Do a lot of "Actions" – and then pick the winners

Building / Designing a 4th Party Program That's Right for You

- Example #1 - 4th Party Worksheet

Action	Effectiveness	Cost	Ease of Implementation
Assess Every 4th Party	High	Low	Easy
	Medium	Medium	Difficult
	Low	High	Very Difficult

Building / Designing a 4th Party Program That's Right for You

- Example #2 - 4th Party Worksheet

Action	Effectiveness	Cost	Ease of Implementation
Encryption	High	Low	Easy
	Medium	Medium	Difficult
	Low	High	Very Difficult

Building / Designing a 4th Party Program That's Right for You

- My top "Building Blocks" – Yours might be different
  1. Have Flow Downs to every 4th Party in the 3rd Party Contract
     - Consider having a 4th and Downstream Parties section in the 3rd Party contract
     - This is a "One and Done" activity. Draft them once. Include them in each 3rd Party Contract
     - Make sure that you can have access to all the documents, evidence, artifacts, people, facilities, and the like that you will need to do a complete job
     - Remember – If it is not in the contract, you most likely will not be able to do it

Building / Designing a 4th Party Program That's Right for You

Items to consider in the Flow Downs to every 4th Party

- BAA
- Data Protection Agreement
- Security & Breach Notification Requirements
- Right for you to Assess / Reassess & Audit 4th Party
- Process for Amendment
- Confidentiality, Availability, Integrity, & Return of Data
- Termination
- …

Building / Designing a 4th Party Program That's Right for You

- My top "Building Blocks" – Yours might be different

2. Get evidence in your 3rd Party Risk Assessment that the 3rd Party has a mature & robust 3rd Party Risk Management Program that it uses on all of its 3rd parties (your 4th Parties)
   - This is a "One & Done" update to your assessment tool

Building / Designing a 4th Party Program That's Right for You

Areas to consider in updating your 3rd Party Risk Assessment tool regarding your 3rd Party's Risk Management Program that it uses on its 3rd parties (your 4th Parties)

- Policies & Procedures
- Resources – Staff, Budget, …
- Risk Assessments
- Supplier Code of Conduct

Building / Designing a 4th Party Program That's Right for You

Areas to consider in updating your 3rd Party Risk Assessment tool regarding your 3rd Party's Risk Management Program that it uses on its 3rd parties (your 4th Parties)

- Control & Process Assessments and Reassessments – Questionnaires, Evidence, Artifacts, 3rd Party Assessments & Certifications, …
- Monitoring
- Auditing
- Exceptions
- …

Building / Designing a 4th Party Program That's Right for You

- My top "Building Blocks" – Yours might be different
  3. When Auditing the 3rd Party – either on site or a desk audit
     - Assess the 3rd Party's 3rd Party Risk Management Program
     - Review BA Inventory / List
     - Sample Contracts for Flow Downs
     - Sample Assessments / Reassessments
     - Review "Exceptions"
     - Sample Their Audits of Their 3rd Parties
     - Evaluate Staff
     - …

Building / Designing a 4th Party Program That's Right for You

- My top "Building Blocks" – Yours might be different
  4. Encryption!!!

Thank You!

Questions & Discussion

Web Hull
Privacy, Data Protection, & Compliance Advisor
eMail: Web.Hull@icloud.com
Linkedin: https://www.linkedin.com/in/webhull
Twitter: @WebHull