4th Party Vendor Management: Managing Your Vendor's Vendor

SCCE 2018 CEI

Web Hull

Web.Hull@icloud.com

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

This Session

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

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
- How to "Scale" the Process

4th Party Management – Short Course

- Your 3rd Party Is Your Portal to Your 4th Parties
- You Want to Get It In Your Contract
- Review / Update / Revise Your 3rd Party Vendor Risk Program
  - Risk Ratings
  - Due Diligence / Audits
  - Resources - People, Tools, $, …
  - 4th Parties
  - Other?

Take-Away Goals

- Get up to date on current "reasonable practices"
- Learn privacy, data protection, security, and compliance requirements regarding 4th parties, and how to identify the 4th parties that your vendors use
- Hear effective strategies for getting cooperation and compliance from your 3rd parties regarding their vendors

Take-Away Goals

- Tips, tools, & tactics for managing 4th parties
- Address the difficult topics:
  - ✓What do I do if I don't like my vendor's 4th parties?
  - ✓4th party breaches
  - ✓Cross border transfer of my data from my vendor to a 4th party; audits, monitoring, assessments, certifications, data breaches, and
  - ✓A whole lot more

Focus Frameworks

- Regulatory Requirements
  - Healthcare
  - Financial Services
  - GDPR
- Customer Requirements
  - B2B
- Your Own Requirements

Goal Today

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

1

Key Tools for Meeting the Challenge

1. Your 3rd Party Vendor Risk Management Program
2. Your Contract with Your 3rd Party
3. Your Relationship with
   - Your Internal Business Owner
   - Internal Team
   - The 3rd Party
4. Charm!
5. Others?

Themes

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

Definitions - Healthcare

- 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 - Healthcare

- 3rd Party = Your Business Associate
- 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
- 4th Party = Your Business Associate's Subcontractor

Definitions – Financial Services

- OCC Bulletin 2017 – 7
  - ""***Third-party relationship***" is defined as any business arrangement between a bank and another entity, by contract or otherwise. Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements in which the bank has an ongoing relationship or may have responsibility for the associated records. Third-party relationships generally do not include customer relationships."

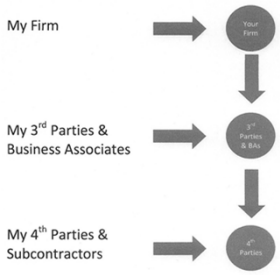
Definitions – Financial Services

- OCC Bulletin 2017 – 7
  - "The term "***subcontractor***" refers to any entity with which the third-party service provider itself has chosen to enter into a third-party relationship. Another term for ***subcontractor*** is "***fourth party***."

Definitions - GDPR

- GDPR
  - "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
  - Subcontractor of a Processor is also a Processor

Definitions



Why I Should Care What a 4th Party Does with My Personal Data, PII, & PHI?

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

Subcontractor / 4th Party Data Breach

- If Your 4th Party / Subcontractor Breaches Your Data, PII, PHI, or ePHI, Who Has the Problem?
  a) You
  b) Your 3rd Party / Business Associate / Processor
  c) Your 4th Party / Subcontractor
  d) a & b
  e) a & c
  f) b & c
  g) All of the above
  h) It depends

Subcontractor / 4th Party Data Breach

- Discussion Question
  - What is the Nature / Implication / Consequences of the 4th Party / Subcontractor Breach?

Healthcare 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

Healthcare 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

Financial Services Requirements

- OCC Bulletin 2017-7
  - "Obtain and review … (the) inventory or database of third-party relationships (and ***related subcontractors***) that indicates risk ranking (e.g., low, high, or critical) of each third-party relationship"
  - "Determine whether any third-party relationships involve the use of ***subcontractors***.
    - Review the bank's methodology for determining whether third parties use ***subcontractors***.
    - Determine if the bank maintains a database or inventory that can distinguish all third parties that use ***subcontractors***."

Financial Services Requirements

- OCC Bulletin 2017-7
  - "Determine if the bank has conducted adequate due diligence to verify whether third parties or their ***subcontractors*** have publicly known outstanding issues with regulatory entities or law enforcement agencies."
  - "Determine if the bank periodically reviews online activity, publicity, public reports, or social media for adverse events involving third parties and their ***subcontractors***. If so, assess to what extent bank management incorporates this information into its ongoing monitoring."

GDPR Requirements

- GDPR – http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en
- GDPR Article 28 - Processor
  - "2. The processor shall not engage another processor ***without prior specific or general written authorisation of the controller***.
  - In the case of general written authorisation, the ***processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes."***

GDPR Requirements

- GDPR Article 28 - Processor
  - "4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, ***the same data protection obligations*** as set out in the contract or other legal act between the controller and the processor … ***shall be imposed on that other processor by way of a contract*** or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation."

Tool #1
3rd Party Risk Assessment Program

- Key Elements of a 3rd Party Risk Assessment & Management Program?
  - Risk Assessment / Tiering
  - 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

Tool #2 – Contract with 3rd Party

- Consult / Coordinate with Legal Contracts
- If it is not in a contract, it is very difficult to have the other party do it
- GDPR is an opportunity to leverage changes
- Contract Resources
  - GDPR Articles 28 & 29
  - UK ICO GDPR Guidance
  - OCC Bulletin 2013 - 29

Tool #2 – Contract with 3rd Party

- Resources to consider
  - Business Associate Agreement / UK ICO Guidance / OCC Bulletins
  - Other Agreements

Security	**Breach**
Privacy	**Data Protection**

  - Customer Requirements Regarding Subcontractors
  - Flow Down Requirements

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 / GDPR professionals also face in managing Business Associates, Processors & 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

3rd / 4th Party Management Tools - VRMMM

Maturity Level	VRMMM High Level Program Categories							
	Program Governance (1)	Policies, Standards, Procedures (2)	Contracts (3)	Vendor Risk Identification and Analysis (4)	Skills and Expertise (5)	Communication and Information Sharing (6)	Tools, Measurement, and Analysis (7)	Monitoring and Review (8)
0 – Non Existent	No formalized third party governance program	No formalized third party related policies, standards, and procedures	No formalized third party contract processes	No formalized vendor risk identification and analysis process	No formalized requirements for third party related skills and expertise	No formalized third party related communication and information sharing processes	No formal tools, measurement, and analysis processes present	No formalized program monitoring and review processes
1 – Initial Visioning	Need for third party program has been established, governance not yet fully defined	Policies, standards and procedures are not yet fully defined	Third party contract policies, procedures are not yet fully defined	Vendor risk identification and analysis is ad-hoc and processes are not yet fully defined	Some third party skills and expertise may be recognized but no formal placement program exists	Internal and external communications are ad-hoc, program needs have been identified but are not yet fully defined.	Third party related measurement and analysis is ad-hoc and metrics are not yet fully defined	Monitoring and Review activities are ad-hoc and processes are not yet fully defined
2 – Determining Roadmap to Achieve Success	Program governance is defined and approved but is not fully in place	Policies, standards and procedures are defined and approved	Third party related contract provisions are defined and approved	Third party related risk identification and analytic criteria are established and approved	Current staff's third party skills and expertise have are being identified and slotted to positions	Internal and external communications are still ad-hoc, but formal communications and information sharing programs are identified and approved	Tools, measurement and analytic needs are identified and approved but are not yet fully implemented	Internal and external third party monitoring and review needs are identified and approved
3 – Fully Determined and Established	Approved governance program is established but is not fully operational	Approved policies, programs and procedures are established but not all fully operational	All contract provisions have been approved, but not all are fully operational	Approved third party analytic and risk identification processes are in place, but not all are fully operational	Skill sets and expertise are being appropriately deployed, any skill gaps have been identified	Formal internal and external communications and information sharing programs are established but are not yet fully mature	Third party related tools and analytics are established but are not fully operational; not all applicable metrics are measured	Monitoring and review programs are defined and established but are not yet fully operational; enforcement is lacking
4 – Fully Implemented and Operational	Program governance is completely established and operational across the organization	Policies, standards and procedures are consistently applied across the enterprise and are externally benchmarked	Contract provisions are consistently deployed across the enterprise and are externally benchmarked	Risk identification and analysis is fully operational across the enterprise and is externally benchmarked	Required skill sets and expertise are optimally deployed	Communications and information sharing processes are fully functional, external outreach is present for benchmarking and other purposes	Third party related tools and analytics are optimally deployed	All program related monitoring and compliance measures are in place and enforced
5 – Continuous Improvement	Program governance represents best practice, and is regularly tested, measured and enhanced as needed	Policies, standards and procedures represent best practice and are regularly measured, tested and enhanced as needed	Contract process is best practice and is regularly evaluated and enhanced as needed	Vendor risk identification and analytics are best practice and are regularly evaluated and enhanced as needed	Skills and expertise are best in class and enhanced as needed, new processes are routinely evaluated	Communications and information sharing processes are continuously evaluated and routinely enhanced; there is organizational visibility in industry associations; the organization actively promotes external outreach.	Tools, measurement and analytics are automated and represent best practice. They are regularly evaluated and enhanced as needed	Monitoring and review processes are best practice, and are regularly evaluated and enhanced as needed

Elements to Consider in Contracts, Amendments, & 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, & 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, & 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

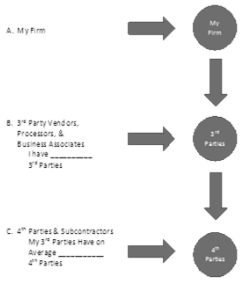
My 3rd Parties

- How Many 3rd Parties, Processors, & 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

4th Parties

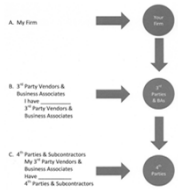
- Do I already Assess & Audit My 3rd Parties?
  - ➢ What is the Cost, Effort, & Success?
- Should I
  - ➢ Preapprove My 4th Parties / Subcontractors?
  - ➢ Assess / Reassess My 4th Parties / Subcontractors?
  - ➢ Monitor & Audit My 4th Parties / Subcontractors?

How Many 4th Parties Do I Have?



How Many 4th Parties Do I Have?

- Answer: B x C = Total Number of 4th Parties
  _____ x _____ = _____
- If I have 10 3rd Parties and each 3rd Party has an average of 10 4th parties, I will have 100 4th Parties - (10 x 10 = 100)
- If I have 100 3rd Parties and each 3rd Party has an average of 100 4th Parties, I will have 10,000 4th Parties - (100 x 100 = 10,000)



Managing 4th Parties – Daunting Numbers

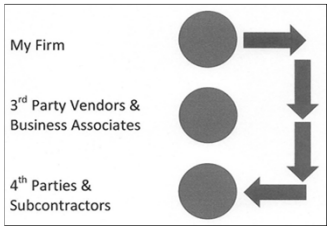
- Use Your 3rd Party Risk Tiering
  - Focus on the High Risk 3rd Parties
- Use Your 4th Party's Risk Tiering
  - Focus on Their High Risk 3rd Parties

4th Party Challenges

- Preapprove / Reapprove 4th Parties
  - How Many Will You Have to Approve?
  - What About the Legacy 4th Parties?
  - What Criteria Will You Use to Approve / Disapprove?
  - What Will Your Turn Around Time Be?
  - What if you Approve a 4th Party & 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 Average 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 / Processor / 3rd Party
  - 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. Auditing the 3rd Party – either on site or a desk audit
   - Assess the 3rd Party's 3rd Party Risk Management Program
   - Review 4th Party 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!!!

4th Party Management – Short Course

- Your 3rd Party Is Your Portal to Your 4th Parties
- You Want to Get It In Your Contract
- Review / Update / Revise Your 3rd Party Vendor Risk Program
  - Risk Ratings
  - Due Diligence / Audits
  - Resources - $, People, Tools
  - 4th Parties
  - Other?

Take-Away Goals

- Get up to date on current "reasonable practices"
- Learn privacy, data protection, security, and compliance requirements regarding 4th parties, and how to identify 4th parties that your vendors use
- Hear effective strategies for getting cooperation and compliance from your third parties regarding their vendors

Take-Away Goals

- Tips, tools, and tactics for managing 4th parties
- Address the difficult topics:
  - What do I do if I don't like my vendor's 4th parties?
  - 4th party breaches
  - Cross border transfer of my data from my vendor to a 4th party; Audits, monitoring, assessments, certifications, data breaches, and
  - A whole lot more

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

Thank You!

Questions & Discussion

Web Hull

eMail: Web.Hull@icloud.com
Linkedin: https://www.linkedin.com/in/webhull
Twitter: @WebHull