BUSINESS ASSOCIATES UNDER HIPAA

Sheba Vine, Esq., CIPP/US
First Healthcare Compliance

HIPAA

1st Healthcare® Compliance

Objectives

- HIPAA Overview
- Business Associate Standard
- Business Associate Agreements
- Enforcement Landscape
- Minimize BA Liability
- Responding to BA Violation

HIPAA Overview

Health Insurance Portability and Accountability Act of 1996

- Administrative simplification provisions focus on improving efficiency of healthcare delivery through standards and electronic transmission of health information

Health Information Technology for Economic and Clinical Health Act

- Enacted as part of the American Recovery and Reinvestment Act of 2009
- Strengthened privacy and security rules, enforcement, breach notification, direct liability for BAs

2013 Omnibus Final Rule

Privacy Rule	Security Rule	Enforcement Rule	Breach Notification Rule
Standards for using and disclosing PHI	Safeguards to protect ePHI confidentiality, integrity, and availability	Procedures for enforcement hearings and penalties	How/when to notify individuals HHS, and media of breach

Protected Health Information (PHI)

Created/received by covered entity that relates to:

- Individual's past, present or future health or condition
- Provision of healthcare to an individual; or
- Past, present, or future payment for the provision of healthcare to an individual

Includes data that can potentially identify the patient

Name	Address	Telephone No.	Fax No.	SSN	Email
License No.	Healthplan beneficiary No.	Device/ vehicle serial no.	DOB/ Death	Full-face photos	Biometric identifiers
	Acct no.	IP Address/ URLs	Admission /discharge date	Other unique identifiers	

Covered Entities

Healthcare Providers

- Provides, bills or is paid for health services if it transmits health information in electronic form
- Ex: doctors, hospitals, long-term care facilities, home health agencies

Health Plan

- Individual or group plan that pays for treatment or care
- Ex: health insurance companies, HMOs, employer sponsored group health plans

Healthcare Clearinghouse

- Translates healthcare transactions from non-standard to standard format and vice versa
- Ex: billing services, re-pricing companies, community health management information systems

Business Associate

Assists CE in performing functions that involve creating, receiving, maintaining or transmitting PHI

- Not a member of CE's workforce
- Includes subcontractors: if a BA subcontracts part of its functions to another organization
- BA functions and services:

Claims processing or administration	Data analysis, processing or administration	Legal
Utilization review	Quality assurance	Consulting
Billing	Repricing	Accounting
Benefit management	Practice management	Accreditation
Data aggregation	Actuarial	Management
Administrative	Financial	

BA Examples

- Data storage and disposal companies
- Data processing or management companies
- EHR vendors
- E-prescribing gateways
- IT support vendor
- Vendors of equipment that access PHI
- Answering services
- Transcription services
- Interpreters that provide services on behalf of CE
- Collection agencies
- Cloud Service Providers that access PHI

CE Responsibilities

Identify	• Identify and perform due diligence on vendors that qualify as BA
BAA	• Obtain satisfactory assurance that BA will appropriately safeguard information
Minimum Necessary	• Disclose only the minimum necessary amount of PHI
Cure Violations	• If CE aware that BA violated a material term of the BAA, take steps to end violation or terminate BAA
Report Breach	• Comply with Breach Notification Rule in reporting BA breach that impacts PHI

BA Responsibilities

Safeguard	• Implement administrative, technical, physical safeguards and comply with Security Rule
Individual Rights	• Obligation to provide individuals with their rights to access, amend, and receive an accounting of certain disclosures of PHI
BAA	• Enter into a BAA with CE and similar contracts with any subcontractors
Minimum Necessary	• Limit use/disclosure of PHI to the minimum necessary
Breach Notice	• Provide breach notification to CE
Cure Violations	• If aware that subcontractor violated a material term of the BAA, it must terminate the contract or take steps to end violation

May 2019, HHS OCR issued fact sheet on business associate liability https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html#footnote10_k06ryxr

Business Associate Agreement

Contract that provides satisfactory assurances that BA will safeguard PHI

Must be signed on or before BA commences services

- **Establish Uses:** BA's use/disclosure of PHI is limited to permitted and required uses or as required by law
  - Based on services BA provides; may permit use for management and administration of the BA, data aggregation services on behalf of CE, or de-identify PHI
- **Safeguards**: Implement appropriate safeguards to comply with Security Rule
- **Report to CE**: Report use/disclosure of PHI not provided for by BAA and breaches of unsecured PHI
- **Subcontractor**: Execute BAAs with subcontractors

BAA *Cont.*

- **Individual Rights**: Make PHI available for purposes of individual request for access, amendment, and provide accounting of disclosures
- **Delegation**: If BA performs any HIPAA obligations for CE, BA must comply with the requirements that apply to CE
- **Audit**: Provide internal records for HHS investigation
- **Return/Destroy PHI**: Return/destroy PHI upon contract termination (if not feasible, continue to safeguard/limit further use)
- **Termination**: Allow termination if CE determines that BA has violated a material term of the contract
- *Additional Terms- Who is responsible for issuing notice to individuals and cost, information that needs to be reported to CE, cooperation, insurance coverage*

Exceptions

- Disclosure to healthcare providers for treatment purposes or to health plans for payment purposes
- Disclosures to public benefits program, such as Medicare, or the Social Security Administration
- Disclosures to entities that participate in an organized health care arrangement
- For services that do not involve PHI and where any access would be incidental (janitorial services)
- Disclosers to financial institutions for payment processing activities (providing normal banking services to its customers; not performing activity on behalf of CE)

Conduit Exception

To an entity that provides mere courier/transmission services for PHI

- Access to PHI is transient in nature (random or infrequent basis) vs. persistent access
- Examples: U.S. Postal Service and private couriers, Internet Service Providers
- Does not apply to cloud service providers that maintains/ stores ePHI (even if it cant view PHI because all data is encrypted and it does not hold the keys to unlock the encryption)

Cloud Service Providers

- A cloud service provider offers a cloud-based platform, infrastructure, application, or storage services.
- If CSP used to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI) it is a BA
- No restriction on storing ePHI on servers outside of US. Take into account in risk analysis:
  - Risks depending on geographic location- Is ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks?
  - May be difficult to pursue enforcement action- HIPAA is not extra-territorial in scope
- Have policy on approved vendors and prohibit use of personal accounts for storing PHI

- *Email*
- *Messaging platform*
- *Data storage*
- *Data Backup*
- *Servers*
- *Clinical applications*
- *Data analytics*
- *Financial, operational, back office applications*

Microsoft Office 365

Online Services Terms includes BAA by default to CE/BA customers that purchase through volume licensing program (can opt-out)

If Customer is a “covered entity” or a “business associate” and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of Customer’s volume licensing agreement includes execution of the HIPAA Business Associate Agreement (“BAA”), the full text of which identifies the Online Services to which it applies and is available at http://aka.ms/BAA. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer’s volume licensing agreement)…

Microsoft Online Services Terms, November 1, 2019

Google G Suite

- Google G Suite (Gmail, Google Calendar, Google Drive, Hangouts Meet)
  - Need to opt-in to BAA
- Ascension's partnership with Google gives access to PHI for:
  - Moving infrastructure to Google cloud platform
  - G Suite tools
  - Developing software that leverages its AI and machine learning technology to deliver targeted care to patients

WSJ NEWS EXCLUSIVE | TECH

Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans

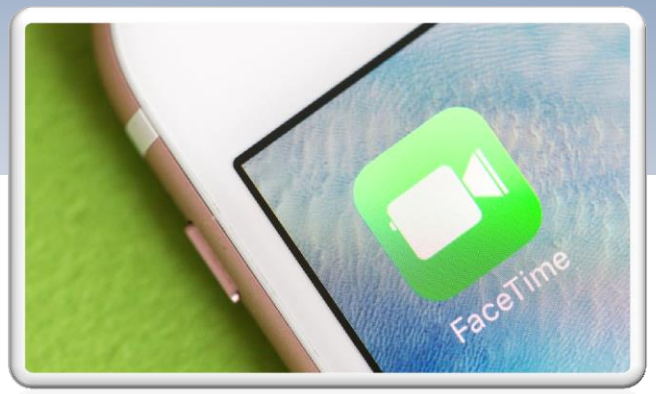
Search giant is amassing health records from Ascension facilities in 21 states; patients not yet informed

Apple iCloud

- iCloud, Apple's online storage service cannot be used to store PHI

> If you are a covered entity, business associate or representative of a covered entity or business associate (as those terms are defined at 45 C.F.R § 160.103), You agree that you will not use any component, function or other facility of iCloud to create, receive, maintain or transmit any "protected health information" (as such term is defined at 45 C.F.R § 160.103) or use iCloud in any manner that would make Apple (or any Apple Subsidiary) Your or any third party's business associate.
>
> *iCloud Agreement, updated September 1, 2019*

Apple FaceTime



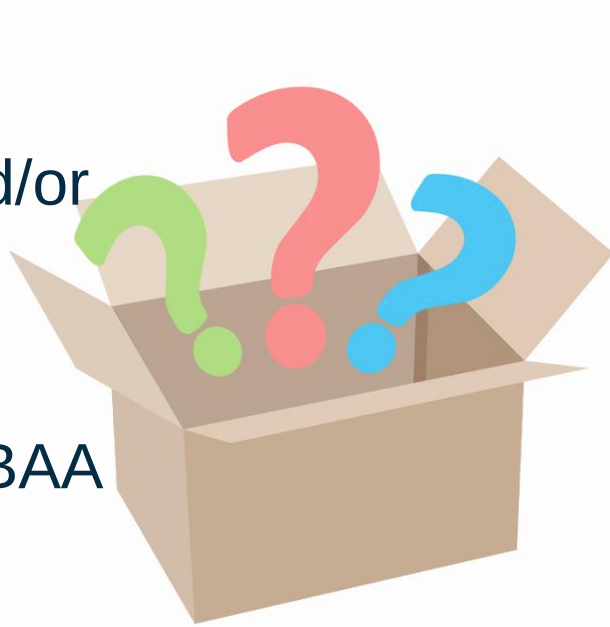
- Does not offer BAA
- Conduit exception applicable?
  iMessage and FaceTime & Privacy, Sept.19, 2019:
  - End-to-end encryption
  - Does not store the content of FaceTime calls
  - Apple may record and store some information related to your use to operate and improve Apple's products and services:
    - May store information about your use of the services in a way that doesn't identify you.
    - May record and store information about FaceTime calls, such as who was invited to a call, and your device's network configurations, and store this information for up to 30 days. Apple doesn't log whether your call was answered, and can't access the content of your calls.

Apple FaceTime Cont.

- Apps on device (including FaceTime) may communicate with Apple's servers to determine if other people can be reached by FaceTime. Apple may store these phone numbers and email addresses associated with your account, for up to 30 days.
- Jan 2019 FaceTime bug discovered that allowed caller to hear audio and video before recipient's phone accepted or declined the call

CE Liability

- Breaches at the BA level can impact CE
  - Cost to investigate, mitigate, provide notice to affected individuals
  - State breach notification laws
  - Prompt investigation by HHS and/or State AGs
  - Individual/Class action lawsuits
  - Fines for invalid, untimely or no BAA



Untimely BAA

$31K Settlement– Center for Children's Digestive Health, April 2017

- Arose out of $100k settlement with is business associate FileFax, a medical records storage/disposal vendor for leaving medical records in unlocked truck in parking lot
- OCR initiated a compliance review of CCDH- BAA with FileFax only signed on Oct 12, 2015 but PHI disclosed since 2003.

Lack of BAA

$750,000 Settlement – Raleigh Orthopedic Clinic, April 2016

- ROC orally arranged for an entity to harvest the silver from x-rays for more than 17,000 patients in exchange for converting the film to electronic media; No BAA
- ROC was scammed and never received electronic files for the x-rays. Entity sold x-ray films to a recycling company
- Breach reported and HHS investigation resulted in settlement and 2 yr. CAP

Lack of BAA with Cloud Service Provider

$2.7M Settlement– Oregon Health & Science University, July 2016

- OHSU reported multiple breaches to HHS in 2013
  - Unencrypted laptop containing ePHI stolen surgeon's Hawaiian vacation rental home
  - Physicians-in-training maintained spreadsheets using Gmail and Google Drive to track patients admitted to the hospital. No BAA with Google.
    - OHSU became aware in May 2013, Google only started offering BAAs for select apps in Sept. 2013
- HHS investigation found HIPAA violations- lack of security policies, encryption, and BAA; Settlement and 3 yr CAP

Impact of BA Breach

- Billing collections vendor American Medical Collection Agency victim of an 8 month cyberattack affecting over 24.5 million patients
  - Discovered by security firm on dark web
  - 21 healthcare entities affected, including Quest Diagnostics and LabCorp
- Class-action lawsuits filed against Quest, AMCA, and LabCorp
- Substantial costs for providing notice to individuals, cybersecurity forensics analysis, IT costs to prevent further attacks, litigation costs, and loss of business resulted in AMCA's parent company filed for bankruptcy
- Currently under investigation by multiple State AGs' offices

Impact of BA Breach

- Jan. 2016, Virtua Medical Group's business associate Best Medical Transcription caused a breach of 1,654 patient files
- Password protection removed during software update on FTP server that stored transcribed documents. Issue was corrected but files were indexed by Google and accessible on the web
- Virtua became aware of breach from a patient stating portions of her medical records were discovered on online
- NJ AG investigation led to $200,000 fine against defunct BA and banned owner of BA from doing business in NJ
- Virtua fined $418,000- failed to conduct risk analysis of ePHI transmitted, didn't implement necessary security measures to reduce risk, failed to create a security training program, that led to delays in identifying and responding to the breach.

"Although it was a third-party vendor that caused this data breach, VMG is being held accountable because it was their patient data and it was their responsibility to protect it," Sharon Joyce, NJ acting director of the division of consumer affairs

Minimize Liability

- Have an effective HIPAA Compliance program- *Best defense is a good offense*
- Process to identify BA- will entity create, receive, maintain or transmit PHI on CE's behalf? Does an exception apply?
- Evaluate the BA before you do business and sign BAA- confirm security program in place, are there physical, technical, administrative safeguards for PHI
- Monitor contracts/BAAs-
  - Older BAAs should be updated to comply with Omnibus Final Rule
  - Have services of third party changed to include handling of PHI?
- Be judicious with PHI- minimum necessary
- Document all actions

Responding to BA Violation

Promptly address any violation of the BA that CE learns of

- Do not ignore! Affirmative obligation to cure BA violations
- Breach notification rule requires breach to be reported within 60 calendar days from discovery
- Failure to take action may constitute willful neglect resulting in mandatory penalties
- CE may avoid HIPAA penalties if no willful neglect and corrected within 30 days
- Notify insurance carriers

Responding to BA Violation *Cont.*

- Get the facts:
  - Description of violation
  - Dates of violation and its discovery
  - Types of PHI involved, affected individuals
  - BA's actions to investigate
  - Measures to mitigate and protect against future violations
- CE's measures to mitigate and protect against future violations
- Review BAA to determine responsibilities in of the parties

Responding to BA Violation *Cont.*

- Does the violation constitute a reportable breach of unsecured PHI?

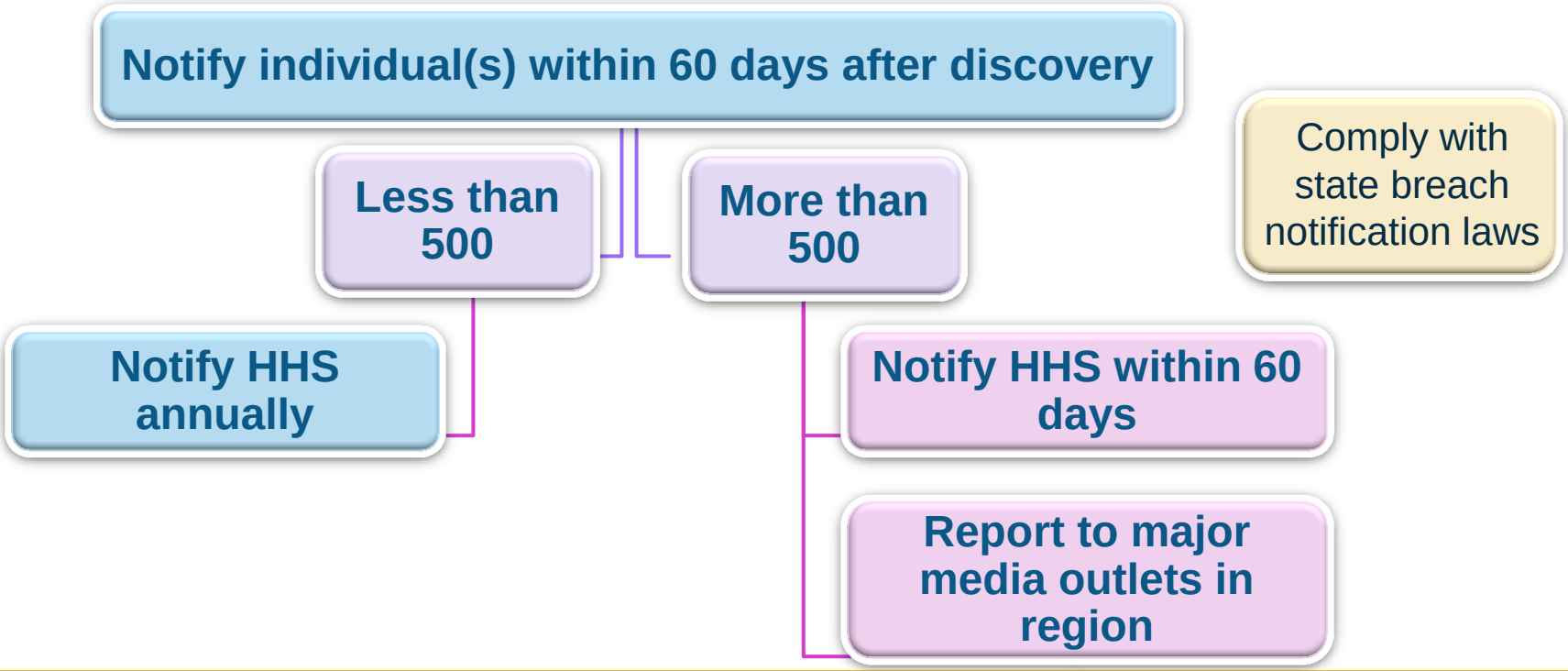
Breach	Unsecured PHI
Impermissible use/disclosure under the Privacy Rule that compromises the security or privacy of PHI	Has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology / methodology

Exceptions
Good faith unintentional access by workforce member, within scope of authority
Inadvertent disclosure between authorized persons; or
Good faith belief that unauthorized person would not retain PHI

Responding to BA Violation *Cont.*

Does risk assessment demonstrate low probability of PHI compromise?

1. Nature/extent of PHI involved, types of identifiers and likelihood of re-identification
2. Unauthorized person who used/viewed PHI
3. Whether PHI was actually acquired or viewed; and
4. Extent of risk to PHI has been mitigated



Responding to BA Violation *Cont.*

- Determine if relationship with BA should be terminated- Was BA cooperative, should BAA be amended?
- Document all actions and decisions

Sheba Vine, Esq., CIPP/US

Vice President, General Counsel

First Healthcare Compliance, LLC

shebavine@1sthcc.com