ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

PREPARING FOR THE INEVITABLE

Best Practices for Preventing, Investigating and Responding to HIPAA Security Incidents and Breaches

B&F

Beth Anne Jackson
bjackson@bf-law.com
(806) 345-6346

Allison D. Shelton
ashelton@bf-law.com
(806) 345-6338

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

THIS WEBINAR HAS BEEN PRE-RECORDED FOR QUALITY PURPOSES

Please send all questions to customerservice@achcu.com

TOPICS

- Why is this Topic Relevant?
- Key Definitions
- General Rules under HIPAA
- Breaches
  - Identify a Breach
  - Reporting a Breach
- Tips

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

WHY IS THIS TOPIC RELEVANT?

OCR's settlement with Sentara Hospitals and enforcement action involving Jackson Health System

SENTARA HOSPITALS SETTLES FOR $2.175 MILLION

- November 27, 2019
- OCR alleged Sentara Hospitals violated the HIPAA Breach Notification and Privacy Rules
  - Sentara Hospitals failed to notify OCR of a breach of unsecured PHI
  - Sentara Hospitals failed to have a business associate agreement with its parent company that created, received, maintained, and transmitted PHI on behalf of Sentara Hospitals
- Sentara Hospitals agreed to pay $2.175 million to settle the potential violations

OCR FINES JACKSON HEALTH SYSTEM (JHS) $2.154 MILLION

- October 15, 2019
- OCR alleged JHS violated the HIPAA Security and Breach Notification Rules between 2013 and 2016
  - JHS failed to timely provide breach notification
  - JHS failed to conduct an enterprise-wide risk analysis and manage identified risks
  - Routinely review information system activity records
  - Restrict employees' authorization to the minimum necessary for assigned job
- OCR imposed a civil monetary penalty of $2,154,000 against JHS

OCR FINES PRACTICE $100,000/CORRECTIVE ACTIVE PLAN WITH TWO YEARS' MONITORING

- March 3, 2020
- Gastroenterology practice saw 3,000 patients per year
- OCR alleged the Practice violated the HIPAA Security Rule after breach report
  - No risk assessment ever performed
  - Practice failed to implement adequate security measures during and after investigation
- Civil monetary penalty of $100,000
- Corrective action plan with two years' monitoring

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

KEY DEFINITIONS

Protected Health Information (PHI) and Business Associate

HIPAA - PROTECTED HEALTH INFORMATION

- PHI is information, including demographic data, that relates to:
  - The individual's past, present, or future physical or mental health or condition,
  - The provision of health care to the individual, or
  - The past, present, or future payment for the provision of health care to the individual
  - And identifies or could reasonably be used to identify the individual
  - ePHI

IS IT PHI?

- Intake paperwork that includes patient's first and last name, treating physician, and primary diagnosis. Paperwork does not include patient's date of birth, insurance information, or social security number.
- Email from intake personnel that says: "We received Robert Jackson's medical records from the Hospital."
- Text from intake personnel that says: "We received RJ's medical records from the Hospital."
- Email sent from provider to BerlindaMahoney@hotmail.com. Email states: "Our agency will have a booth at the health fair on Saturday. We hope you can stop by to see us!"
- Email sent from provider to BerlindaM@hotmail.com. Email states: "Dear Ms. Mahoney: We received a new order for you from Dr. Smith."

HIPAA – BUSINESS ASSOCIATE

- A Business Associate is:
  - A person or organization that performs certain functions or activities on behalf of a Covered Entity that involve the use or disclosure of PHI
    - Business Associate functions include claims processing, data analysis, utilization review, and billing
    - Business Associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services
- A Business Associate does not include:
  - A person or organization who performs functions or services that do not involve the use or disclosure of PHI and where any access to PHI by such person would be incidental, if at all

Is it a Business Associate?

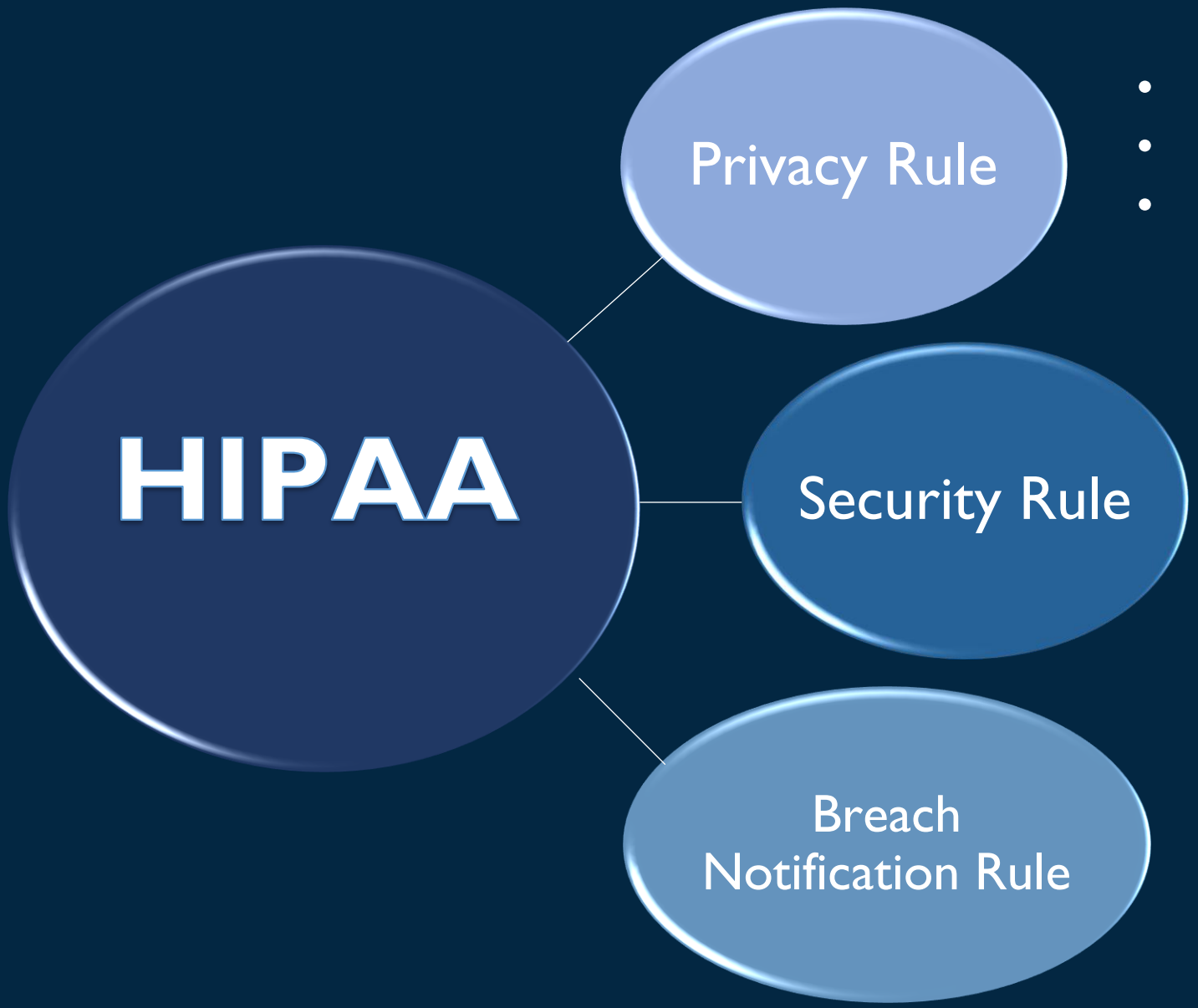
- USPS, UPS, FedEx, and other delivery services employees?
- Software vendors?
- Janitors?
- Plumbers, electricians or photocopy machine repairperson who provide repair services in a covered entity's office?
- Shredding service?

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

GENERAL RULES UNDER HIPAA

Privacy Rule, Security Rule, and Breach Notification Rule



- Permitted uses and disclosures of PHI
- Notice of Privacy Practices
- Right to access, amend, restrict, and receive accounting of disclosures

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Policies and documentation

- Breach
- Reporting requirements

HIPAA PRIVACY RULE

- Authorization
  - In general, the HIPAA Privacy Rule requires an individual's authorization to use and disclose PHI unless the use or disclosure is expressly permitted in the HIPAA Privacy Rule
- Third-Party Directive (HITECH)
- Treatment, Payment, and Health Care Operations
  - Covered entities (and business associates on behalf of CEs) may use and disclose PHI for treatment, payment and health care operations of the covered entities

IS AN AUTHORIZATION REQUIRED?

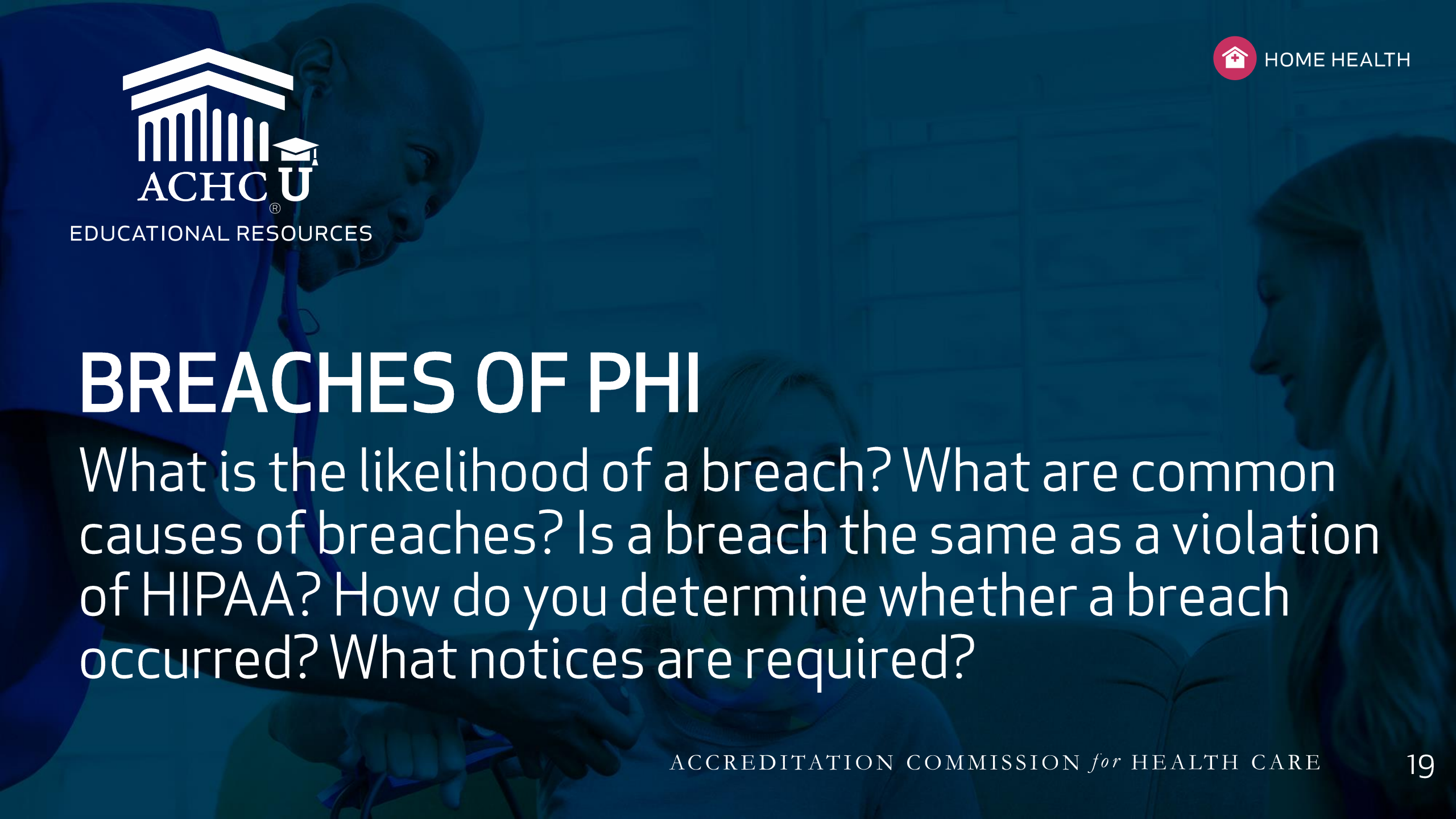
- A provider's website designer suggests that the provider include patient testimonials on the website. The testimonials will include a quote from the patient and a picture of the patient.
- A provider believes it is being underpaid by BCBS. The provider contacts BCBS's contract manager on behalf of our client. The contract manager requests a list of the claims in dispute. The contract manager wants the list to include each patient's name, date of service, diagnosis, and service provided.
- A home health agency sends a request for a patient's hospital records relating to a condition that is the basis for the patient's home health services.

HIPAA Security Rule

- Three categories of standards: Administrative, Technical, and Physical Safeguards
- 18 Standards
- 12 Standards have Implementation Specifications
  - "Required"
  - "Addressable"
- Policies and Procedures

HIPAA BREACH NOTIFICATION RULE

- Breach
  - "acquisition, access, use or disclosure of protected health information in a manner not permitted under" the Privacy Rule "which compromises the security or privacy of protected health information"
- Notification
  - Individual
  - Office for Civil Rights (OCR)
  - Media



ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

BREACHES OF PHI

What is the likelihood of a breach? What are common causes of breaches? Is a breach the same as a violation of HIPAA? How do you determine whether a breach occurred? What notices are required?

WHAT'S THE LIKELIHOOD OF A BREACH?

- OCR 2017 Desk Audits

94% of organizations had inadequate risk management plans

83% of organizations had preformed inadequate risk analysis

89% of organizations were inadequate on patient's right to access

- 90% of healthcare organizations experience at least one data breach within a two-year period. Half of those organizations experience more than five data breaches within a two-year period.

COMMON CAUSES OF BREACHES

- Third Parties
  - 41% of breaches experienced by covered entities
- Unintentional Employee Actions
  - 36% of breaches experienced by covered entities
  - 55% of breaches experienced by business associates

IS BREACH A FOUR-LETTER WORD?

- Not necessarily – A breach is NOT equivalent to a HIPAA violation that can result in significant fines and penalties
- Failing to report a breach and/or failing to take steps to prevent breaches will likely result in serious consequences for covered entities and business associates

CIVIL PENALTIES FOR HIPAA VIOLATIONS

Tier 1
- Did not know and could not have reasonably known of violation
- $100 - $50,000 per violation; maximum of $25,000 per year

Tier 2
- Reasonable cause to believe knew/should have known of violation
- $1,000 - $50,000 per violation; maximum of $100,000 per year

Tier 3
- Violation due to willful neglect but corrected within 30 days
- $10,000 - $50,000 per violation; maximum of $250,000 per year

Tier 4
- Violation due to willful neglect and not corrected within 30 days
- $50,000 per violation; maximum of $1.5 million per year

ACHC U®
EDUCATIONAL RESOURCES

IDENTIFY A BREACH

IDENTIFY A BREACH

- What is a breach?
  - The unauthorized "acquisition, access, use, or disclosure of protected health information in a manner not permitted under (the HIPAA Privacy Rule) which compromises the security or privacy of the protected health information"
- Four Key Questions:
  - Was there an unauthorized acquisition of, access to, or use or disclosure of PHI?
  - Was the PHI unsecure?
  - Does an exception to the definition of breach apply?
  - Can the entity demonstrate a low probability that the PHI has been compromised?

IDENTIFY A BREACH

- Question 1: Was there an unauthorized acquisition of, access to, or use or disclosure of PHI?
- To answer this question, it is necessary to understand a few terms:
  - Protected Health Information
  - Unauthorized
  - Acquisition / Access / Use / Disclosure

IDENTIFY A BREACH

- Question 2: Was the PHI unsecure when it
- was acquired/accessed/used/disclosed?
- PHI is secure if it is either:
  - Appropriately encrypted (i.e. converted into encoded or unreadable text that requires a confidential process or key to assign meaning), or
  - Properly destroyed
  - OCR has cautioned about the limits of full disk encryption
    - Laptop with full disk encryption – security of PHI depends on if the laptop was powered on and in use or was powered off

IDENTIFY A BREACH

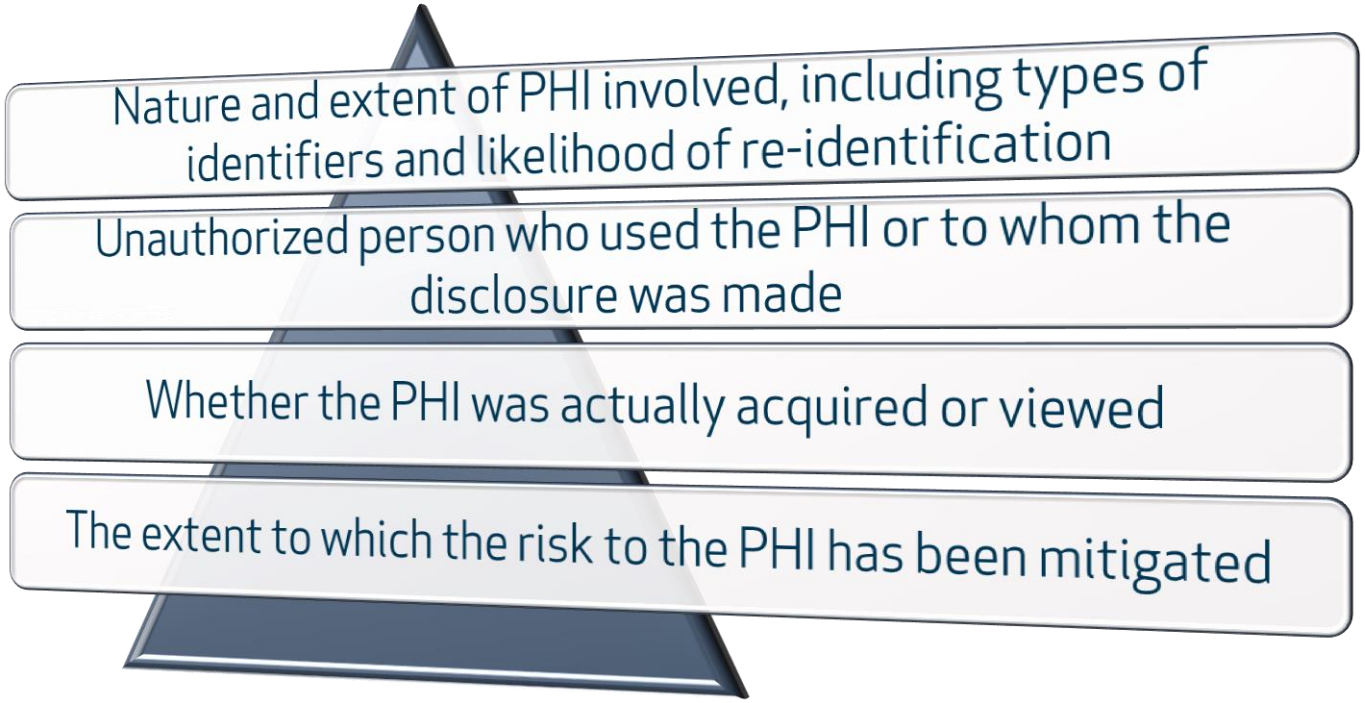
- Question 3: Does an exception to the definition of breach apply?
- There are three exceptions under the Breach Notification Rule:
  - Unintentional acquisition, access, or use of PHI by a workforce member made in good faith, was within the scope of authority, and does not result in further inappropriate use or disclosure
  - Inadvertent disclosure of PHI by an authorized person to another person authorized to access PHI at the same covered entity or organized health care organization and does not result in further inappropriate use or disclosure
  - Disclosure of PHI where the entity has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information

IDENTIFY A BREACH

- Question 4: Can the entity demonstrate a low probability that the PHI has been compromised?
  - Presumption
    - If there was an unauthorized acquisition, access, use, or disclosure of PHI and no exception applies, then the incident is presumed to be a breach unless the entity can demonstrate that there is a low probability that the PHI has been compromised

IDENTIFY A BREACH

- Question 4: Can the entity demonstrate a low probability that the PHI has been compromised? (cont'd)
  - How to rebut the presumption?



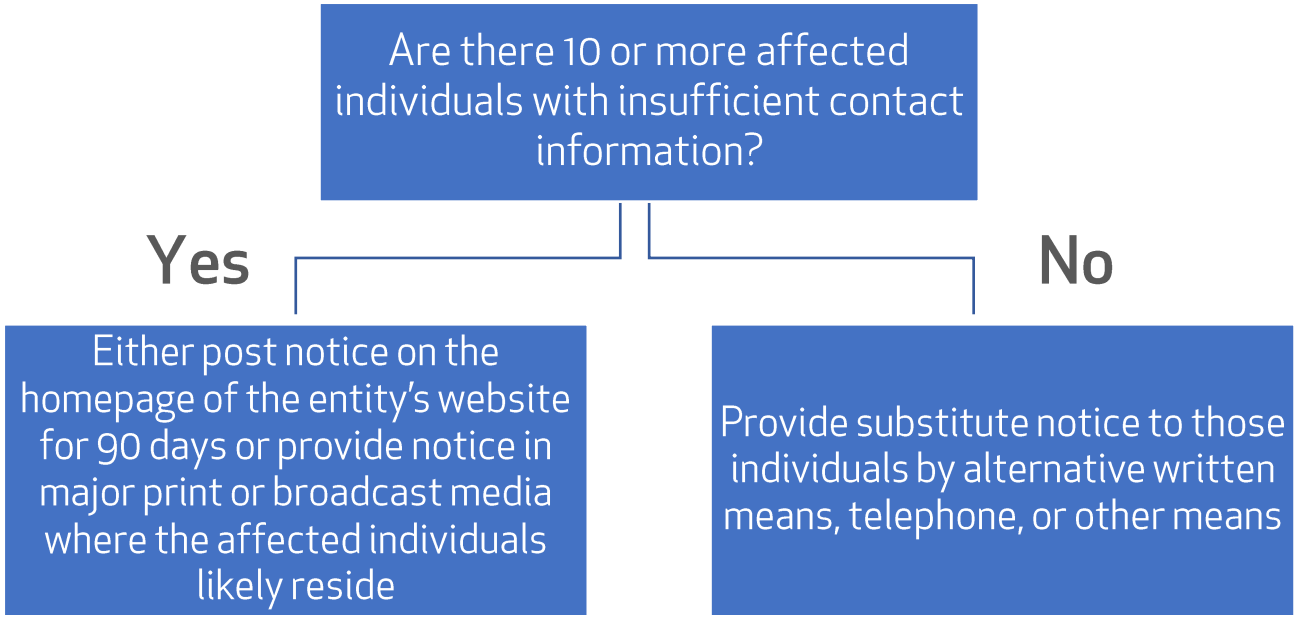
ACHC U®
EDUCATIONAL RESOURCES

REPORTING A BREACH

- Federal Requirements for Reporting a Breach
  - Individual notice
  - Notice to OCR
  - Notice to media
  - State Law Requirements

REPORTING A BREACH

- Individual Notice
  - General Notice Requirement
    - Written notice sent by first-class mail or by email if the affected individual has agreed to electronic notice
    - Without unreasonable delay but in no case more than 60 days after discovery of the breach
  - Substitute Notice



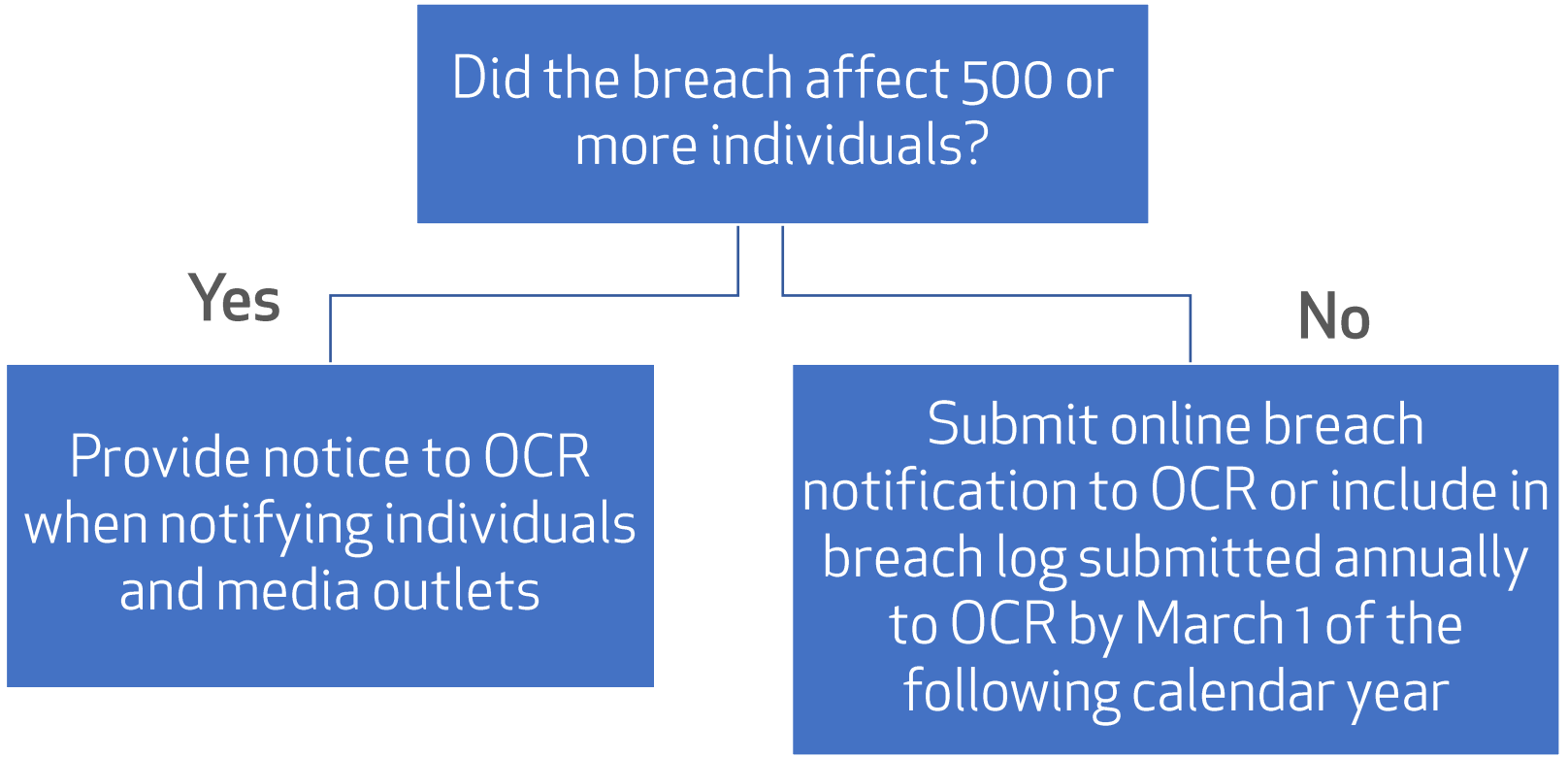
ACHC U®
EDUCATIONAL RESOURCES

REPORTING A BREACH

- Content of Individual Notice
  - Description of incident
  - Description of PHI involved
  - Steps that can be taken to protect against potential harm
  - Description of investigation undertaken
  - Steps taken to mitigate harm and protect against future breaches
  - Contact information

REPORTING A BREACH

- Notice to OCR and Others



ACHC U®
EDUCATIONAL RESOURCES

REPORTING A BREACH

- Notice to Media

REPORTING A BREACH

- State Law Breach Reporting
  - All states have laws governing patient privacy and require reporting of certain breaches
  - Such laws may be stricter than HIPAA and should be reviewed in the event of a breach to ensure compliance

ACHC U®
EDUCATIONAL RESOURCES

TIPS

- Tips for responding to breaches

ACHC U®
EDUCATIONAL RESOURCES

RESPONDING TO A BREACH

- Assemble a Team
  - The team should include high level personnel and others as necessary
  - It may be necessary to involve an attorney to keep the investigation privileged
  - If the breach involves electronic data or systems, a computer forensic consultant may be necessary
  - If the breach is large, a public relations company may be useful to minimize negative press for the company

RESPONDING TO A BREACH

- Investigate, Analyze, and Take Action
  - Gather information and interview employees
  - Take steps to maintain confidentiality and preserve evidence
  - Mitigate harm
  - Develop and implement a corrective action plan (including an update to the entity's risk analysis and management plan)
  - Involve law enforcement?
  - Notify insurance carriers?
  - Determine what kind of breach reporting will be required
  - Document the company's investigations and actions

FINAL TIPS


Conduct & update
Conduct and update security risk assessments
Prepare & implement
Prepare and implement risk management plans
Invest in
Invest in (and use) encryption technology
Train
Train employees
Investigate
Investigate business associates and strengthen rights with business associates
Know
Know who your business associates are and ensure you have current agreements in place
Have policies
Have policies and safeguards in place to ensure PHI is only disclosed when required or permitted under the law

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

QUESTIONS?

Please email us at customerservice@achcu.com

ACHC U®
EDUCATIONAL RESOURCES

HOME HEALTH

THANK YOU!

Beth Anne Jackson, J.D.
Brown & Fortunato, P.C.
905 S. Fillmore, Ste. 400
Amarillo, TX 79101
bjackson@bf-law.com | 806-345-6346

Allison D. Shelton, J.D.
Brown & Fortunato, P.C.
905 S. Fillmore, Ste. 400
Amarillo, TX 79101
ashelton@bf-law.com | 806-345-6338

B&F