HIPAA COW Mission

- Assist HIPAA Covered Entities, Business Associates, and other interested parties in implementing HIPAA's Privacy, Security and EDI Standard Transaction provisions, as amended over time.
- Foster public education about HIPAA.
- Facilitate and streamline HIPAA implementation through identification of best practices.
- Reduce duplicate efforts among entities obligated to comply with HIPAA.
- Offer opportunities for partnering and collaborating between entities implementing HIPAA.
- Identify and evaluate new or difficult HIPAA interpretation issues.

HIPAA 101/102, the basics

How do I investigate and resolve a potential privacy incident?
7/28/2020

hipaacow.org®

Today’s Webinar is Sponsored by:

Gold

Quarles & Brady LLP

HALL RENDER
KILLIAN HEATH & LYMAN

WIPFLi LLP
CPAs and Consultants

NUTANIX

Silver

GODFREY KAHN S.C.

core

HUSCH BLACKWELL

hipaacow.org®

Disclaimer

HIPAA Collaborative of Wisconsin (“HIPAA COW”) holds the Copyright © to this Security 101/102 Webinar (“Document”). HIPAA COW retains full copyright ownership, rights and protection in all material contained in this Document. Any HIPAA COW copyrighted document may be downloaded from the web, printed, and distributed in its entirety as long as: (i) the reproduced document contains the original HIPAA COW copyright and disclaimer and (ii) the document is provided free of charge. Any entity who wishes to adopt part or all of a document for its own internal compliance may do so without the copyright as long as the document is adopted solely for internal purposes and HIPAA COW is referenced as a source. Any other use of copyrighted material is prohibited without the express written permission of HIPAA COW. This Document is provided “as is” without any express or implied warranty. This Document is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney. Unless otherwise noted, HIPAA COW has not addressed all state pre-emption issues related to this Document. Therefore, this Document may need to be modified in order to comply with Wisconsin/State law.

LEGAL NOTICE: HIPAA Collaborative of Wisconsin Content and Liability Disclaimer

The HIPAA Collaborative of Wisconsin (HIPAA COW) shall not be responsible for any errors or omissions contained in materials provided by HIPAA COW. All information is provided on an "AS IS" basis.

HIPAA COW MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED (INCLUDING ANY WARRANTIES OF TITLE, NON-INFRINGEMENT AND IMPLIED WARRANTIES OF MERCHANT-ABILITY OR FITNESS FOR A PARTICULAR PURPOSE) REGARDING ANY INFORMATION CONTAINED IN ITS MATERIALS. THE USER OF THE MATERIALS SHALL ASSUME TOTAL RESPONSIBILITY AND RISK FOR THE USE OF THE MATERIALS. IN NO EVENT SHALL HIPAA COW BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO ANY INFORMATION CONTAINED IN THE MATERIALS PROVIDED BY HIPAA COW, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW OR OTHERWISE.

The content of the materials provided by HIPAA COW is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that HIPAA COW is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Presented by:

Holly Schlenvogt

Privacy & Security Consultant / Owner

HRT Consulting, LLC

(262) 468-4291 (Office)

hschlenv@hrt-consulting.com | http://hrt-consulting.com

HRT

Consulting, LLC

Your trusted compliance partner

Disclaimer

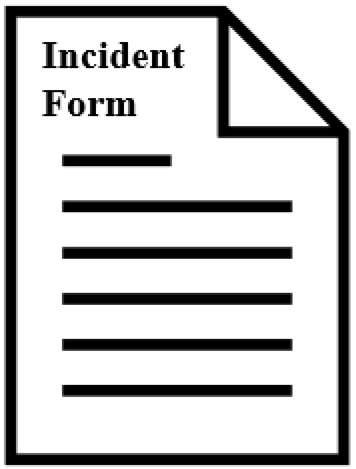
- I am not an attorney and am, therefore, not providing legal advice.

Objectives

You have been asked to look into a potential privacy incident. Now what???

- Explore basic steps to take to:
  - Make sure potential and known privacy incidents are identified and reported
  - Investigate it and determine whether it is a:
    - Privacy and / or security incident
    - Breach of unsecured protected health information that requires notifications
  - Resolve it

hipaacow.org®



Identify & Report It

- How likely will it be reported if your workforce and vendors do not know how to identify an issue and that they are required to report it?

How to Make Sure Incidents are Reported: Policies and Procedures (P&Ps)

- Have written and implemented P&Ps:
  - That require reporting
    - By workforce
    - By vendors
  - Required to cooperate with the investigation and provide factual information
  - To not subject any individual to intimidation, threats, coercion, harassment, discrimination against, or any other retaliatory action as a consequence for reporting

How to Make Sure Incidents are Reported: Open Culture

- Make it an open, safe culture to report
- Guilty until proven innocent is not the right approach (but, this is not always easy to do)
- Remain calm (this also is not always easy to do either)

Incident Form

How to Make Sure Incidents are Reported: Training

- Training…training…training
  - Workforce
    - All workforce (employees, volunteers, interns, Board of directors, etc.)
    - Leadership – their responsibility to:
      - Make sure privacy and security P&Ps are followed, non-compliance and issues are reported
      - Monitor for issues and violations
    - Information technology / system administrators – specific to their support roles
  - Other users (e.g. vendors, Business Associates, other organizations, etc.)
- What to train all workforce, you may ask?

How to Make Sure Incidents are Reported: Training

- Report right away / as soon as possible
- Definition and examples of a:
  - Privacy incident
  - Security incident
  - Breach of protected health information (PHI)
- To whom to report potential and known incidents
- How to investigate potential and known incidents
- How to prevent incidents from happening

hipaacow.org®

Incident Form

How to Make Sure Incidents are Reported: Training

training training training training
training training training training

- **Privacy Incident**:
  - A violation of the HIPAA Privacy Rule and/or the organization’s privacy P&Ps and practices
- A few examples:
  - Unauthorized access, use, disclosure or request of PHI
    - This includes mistakes, looking up information out of curiosity or concern, and intentional breaches
  - A patient right was not granted, such as:
    - Requested access was not provided to medical and/or billing records (designated record set)
    - Notice of Privacy Practices was not provided

hipaacow.org®

How to Make Sure Incidents are Reported: Training

- **<u>Privacy Incident</u>**:
- A couple more examples:
  - PHI was shared with a vendor but a Business Associate Agreement was not in place
  - Unauthorized change or deletion of PHI

How to Make Sure Incidents are Reported: Training

- **<u>Security Incident</u>**
  - The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system
  - A violation or imminent threat of violation of information security P&Ps, acceptable use P&Ps, or security practices

How to Make Sure Incidents are Reported: Training

Security incident a few examples:

- Theft/lost laptop, smart phone, USB drive, etc.
- Virus
- Hacker
- Ransomware
- Alerts/pop-ups
- Password was breached
- Systems down/unavailable or are going slow

How to Make Sure Incidents are Reported: Training

- A privacy incident may also be a security incident
- A security incident may also be a privacy incident
- While this session focuses on privacy incidents, it is important to point this out

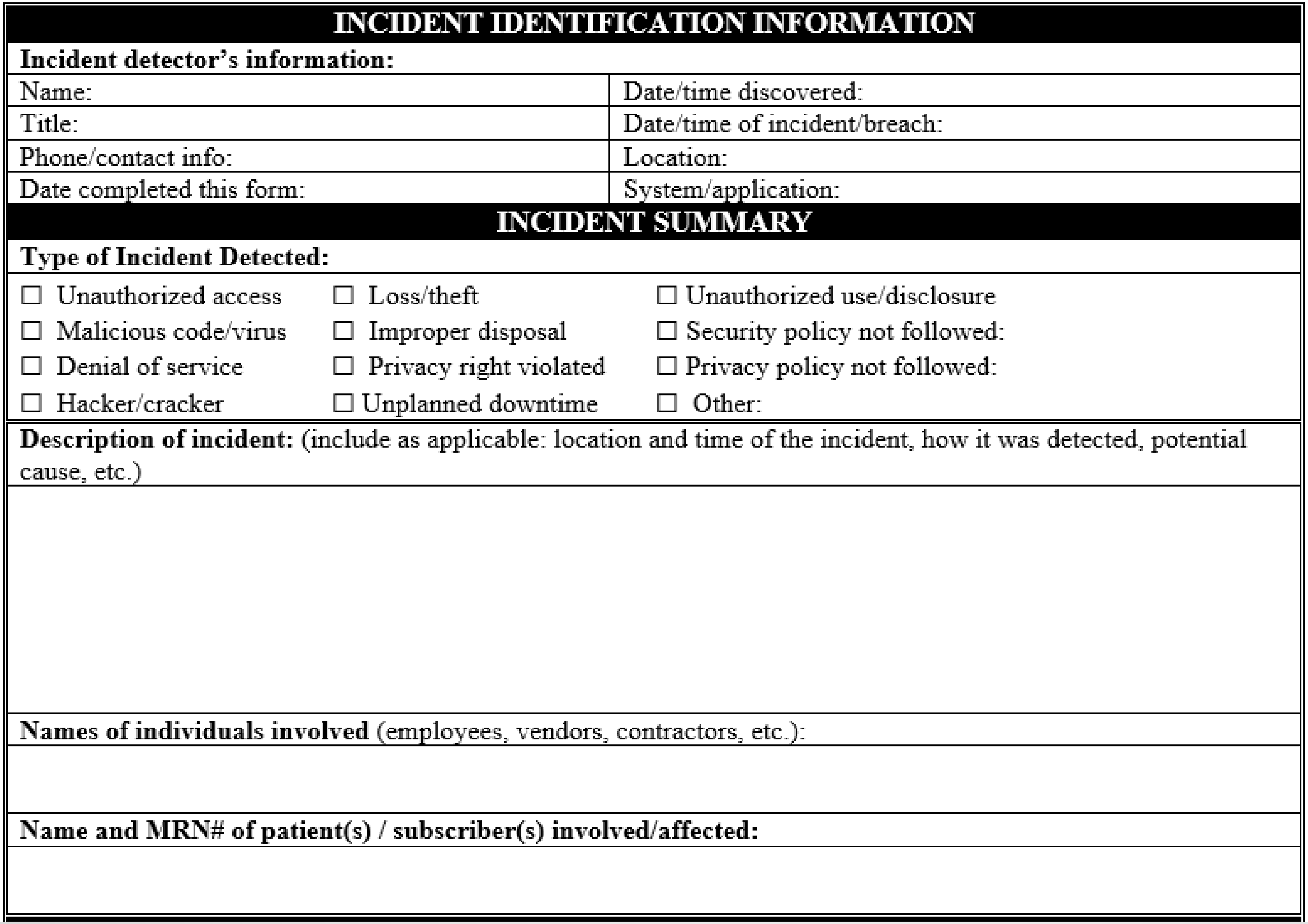
hipaacow.org®

Incident Form

How to Make Sure Incidents are Reported: Training

- To whom to report potential and known incidents as well as complaints
  - Privacy Officer?
    - HIM leadership role?
    - Business office leadership role?
  - Security Officer?
    - IT / help desk?
    - Contracted IT vendor?
  - Any Leader?
- Request details be provided and a form be completed

Incident Form



INCIDENT IDENTIFICATION INFORMATION

Incident detector's information:

Name:	Date/time discovered:
Title:	Date/time of incident/breach:
Phone/contact info:	Location:
Date completed this form:	System/application:

INCIDENT SUMMARY

Type of Incident Detected:

- ☐ Unauthorized access
- ☐ Malicious code/virus
- ☐ Denial of service
- ☐ Hacker/cracker
- ☐ Loss/theft
- ☐ Improper disposal
- ☐ Privacy right violated
- ☐ Unplanned downtime
- ☐ Unauthorized use/disclosure
- ☐ Security policy not followed:
- ☐ Privacy policy not followed:
- ☐ Other:

Description of incident: (include as applicable: location and time of the incident, how it was detected, potential cause, etc.)

Names of individuals involved (employees, vendors, contractors, etc.):

Name and MRN# of patient(s) / subscriber(s) involved/affected:

hipaacow.org®

Incident Form

How to Make Sure Incidents are Reported: Training

- How to investigate potential and known incidents
  - Who investigates what?
  - Who to involve and when
    - Executive team
    - Board of directors
    - Attorney (internal and / or external)?
    - Human Resources?
    - Insurance / cybersecurity / breach insurance plan?
    - Forensics?
    - Law enforcement?
  - Steps to take

How to Make Sure Incidents are Reported: Training

- How to prevent incidents from happening
  - Provide real life examples of incidents
    - Internal
    - In the news
  - Train privacy and security*:
    - Safeguarding requirements and tips (administrative, physical, and technical)
    - Privacy and security P&Ps and standards

*A key here is to train what they need to know to carry out their job responsibilities and prevent violations and incidents from happening

How to Make Sure Incidents are Reported: Training

- Train in the news / safeguarding tip examples:
  - How to respond to access to PHI requests
    - Timeliness
    - Allowable fees to provide copies (more on this from the Office for Civil Rights (OCR) today)
    - OCR Settles First Case in HIPAA Right of Access Initiative, 9/9/19
      - Bayfront Health St. Petersburg, FL: $85,000 and corrective action plan
      - Failed to provide a mother timely access to records about her unborn child

Resource: https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html

How to Make Sure Incidents are Reported: Training

- Train in the news / safeguarding tip examples:
  - OCR Settles Second Case in HIPAA Right of Access Initiative, 12/12/19
    - Korunda Medical, LLC, FL: $85,000 and corrective action plan
    - Despite repeated requests, failed to forward a patient's medical records in electronic format to a third party and charged more than the reasonably cost-based fees as allowed under HIPAA
    - OCR provided technical assistance on how to correct this
    - Despite OCR's assistance, still did not provide the records

Resource: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/korunda/index.html

How to Make Sure Incidents are Reported: Training

training training training training
training training training training
training training training
training training training
training training training

- Train in the news / safeguarding tip examples:
  - OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System, Miami, FL, for HIPAA Violations, 10/23/19
    1. August 2013 submitted a breach report: Health Information Management Department lost paper records of 756 patients in January 2013
       - Also determined an additional three boxes of patient records were lost in December 2012; did not report increased number of patients affected to 1,436, until June 7, 2016
    2. July 2015: OCR investigated a media report that a reporter shared a photograph with a patient's medical information on social media; two employees accessed ePHI without a job-related purpose
    3. February 2016: submitted a breach report an employee sold PHI; inappropriate access of over 24,000 patient records

Resource: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jackson/index.html

How to Make Sure Incidents are Reported: Training

- Train in the news / safeguarding tip examples:
  - Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients’ Protected Health Information, 10/2/19 (and corrective action plan)
    - Elite Dental Associates, Dallas, TX: OCR received a patient complaint alleging Elite responded to a social media review by disclosing the patient’s last name and details of the patient’s health condition
    - OCR found Elite impermissibly disclosed the PHI of multiple patients in response to patient reviews on the Elite Yelp review page
    - Did not have:
      - P&Ps regarding disclosures of PHI to ensure that its social media interactions protect the PHI of its patients; or
      - A Notice of Privacy Practices that complied with HIPAA

Resource: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite/index.html

How to Make Sure Incidents are Reported: Training

- And remember…
  - Provide training on a regular basis
    - Once is not enough
    - Annually is a start, but still is not enough
  - Vary the training to continuously raise awareness
    - Standard PowerPoint
    - In meetings
    - Emails
    - Intranet
    - Phishing campaigns, etc.
    - Other?

How to Make Sure Incidents are Reported: Training Resources

- HIPAA Collaborative of Wisconsin
  http://hipaacow.org
- HHS / OCR HIPAA information
  http://www.hhs.gov/hipaa/for-professionals/index.html

- OCR YouTube Videos
  http://www.youtube.com/USGovHHSOCR
- Resolution Agreements
  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

How to Make Sure Incidents are Reported: Training Resources

- OCR Privacy and Security listservs: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html
- Medscape provider education http://www.medscape.org/
- HeatlhIT.gov resources
  - Privacy & Security Training Games: https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-training-games
  - Resources for Providers: https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

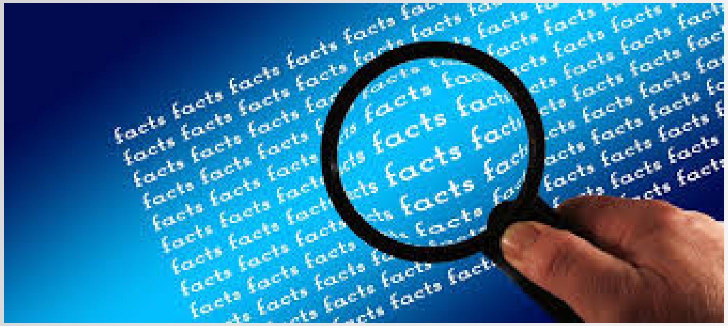
How to Make Sure Incidents are Reported: FTC Training Resources

- Federal Trade Commission
  - Scams: https://www.consumer.ftc.gov/features/scam-alerts
  - Consumer Information Blog: https://www.consumer.ftc.gov/blog
  - Able to sign up for email updates on the above links
  - Video and Media: https://www.consumer.ftc.gov/media
  - Privacy, Identity & Online Security: https://www.consumer.ftc.gov/topics/privacy-identity-online-security

How to Make Sure Incidents are Reported: Current P&Ps

- Keep P&Ps current, based on regulatory changes, guidance, and cases
- Important Notice Regarding Individuals' Right of Access to Health Records, 1/28/2020
- 1/23/20 federal court ruling:
  - Vacated the "third-party directive" within the individual right of access "insofar as it expands the HITECH Act's third-party directive beyond requests for a copy of an electronic health record with respect to [PHI] of an individual . . . in an electronic format."
  - The fee limitation set forth at 45 C.F.R. § 164.524(c)(4) will apply only to an individual's request for access to their own records, and does not apply to an individual's request to transmit records to a third party

Resource: https://list.nih.gov/cgi-bin/wa.exe?A2=ind2001&L=OCR-PRIVACY-LIST&P=3632



Investigate It

- How likely will a potential incident be appropriately investigated if you do not know what actions to take?

Investigate It: P&Ps

- Have written and implemented P&Ps
  - Identify who investigates different types of potential and known privacy and security incidents
  - Determine whether it is a privacy incident and / or security incident
  - Complete a breach risk assessment
  - Steps to take, who does them, timeframes in which to complete them
  - Who to notify
  - Send breach notifications
  - Document the report and actions taken

Investigate It: P&Ps – HIPAA COW Resources

- Patient / Insured Privacy-Related Complaints P&P
  - Policy
  - Procedures
    - Filing a complaint
    - Investigation of complaint
    - Response to complaint
    - Documentation, etc.
  - Patient / insured privacy complaint form
- Privacy Breach – Privacy Officer's Response & Investigation Checklist

Investigate It: P&Ps – HIPAA COW Resource

- HIPAA COW Breach Notification – Protected Health Information for Covered Entities
  - Policy
  - Procedures
  - Examples of potential breaches of unsecured PHI
  - Breach penalties
  - Sample notification letter to patients
  - Sample media notification statement / release
  - Sample talking points
  - Examples of Violations and notification recommendations
  - Sample breach notification log
  - Risk Assessment Analysis Tool

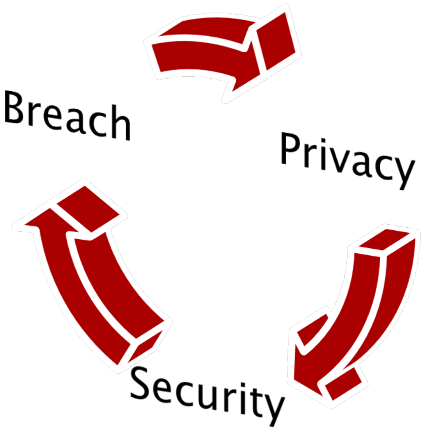
Investigate It: P&Ps – HIPAA COW Resource Security Incident Response P&P

- Policy
- Procedures
  - Preparation and identification / detection phase
  - Containment phase
  - Eradication phase
  - Follow up phase
  - Retention
- Security incidents response flow
- Sample information security incident report
- Chain of custody procedures
- SANS sample Incident handling forms (links)

Investigate It: Who?

- Who investigates different types of potential and known privacy and security incidents?
  - Privacy related:
    - Privacy Officer?
    - Health Information Management Director?
    - Business Office Manager if billing is involved?
    - Facilities Manager if physical security is involved?
    - HIPAA Team?
  - Security related:
    - Security Officer?
      - IT Director?
      - HIPAA Team?
  - Privacy and security related:
    - Same as the above?

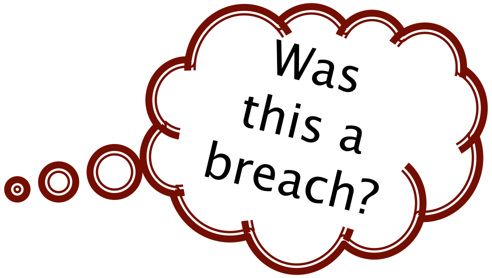
Investigate It: Is It an Incident and/or Breach?



- Is it a privacy incident?
  - Refer to definitions and examples on other slides
- Is it a security incident?
  - Refer to definitions and examples on other slides
- Is it a breach of unsecured PHI?
  - Did the incident involve the impermissible use/disclosure involve unsecured PHI? If yes:
    - Deem is a breach of unsecured PHI, or
    - Complete a breach risk assessment

hipaacow.org®

Investigate It:
Breach Risk Assessment



- Determine if it included **Unsecured PHI**
  - PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html)
- Examples:
  - Encrypted ePHI (at NIST standards)
  - Media is shredded / destroyed so PHI cannot be read or reconstructed

hipaacow.org®

Investigate It: Breach Risk Assessment

Was this a breach?

It included Unsecured PHI, now what?

- Complete a **breach risk assessment** to determine whether it resulted in a breach of unsecured PHI
- Breach definition: When PHI is involved, it is presumed a breach **unless** you are able to demonstrate there is a low probability that PHI has been compromised, based on these four factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the PHI or to the Disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated

hipaacow.org®

Investigate It: Breach Risk Assessment

Was this a breach?

- Start with an examination of the breach definition exemptions. Then look at the above four factors.
- Breach definition: a breach excludes:
  1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the organization or a Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or Disclosure in a manner not permitted under the Privacy Rule.

Investigate It: Breach Risk Assessment

Was this a breach?

- Breach definition: a breach excludes:
  2. Any inadvertent disclosure by a person who is authorized to Access PHI at the organization or BA to another person authorized to Access PHI at the organization or BA, or organized health care arrangement in which the organization participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule

Investigate It: Breach Risk Assessment

Was this a breach?

- Breach definition: a breach excludes:
  3. A disclosure of PHI where the organization or BA has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.
- Incorporate the three exclusions into the breach risk assessment

Investigate It:
Breach Risk Assessment

Was this a breach?

Federal Register January 25, 2013, p. 5642

"…if a covered entity misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, the covered entity may be able to determine after performing a risk assessment that there is a low risk that the protected health information has been compromised. Although this scenario doesn't fit any of the statutory or regulatory exceptions to breach, notification should not be required if the covered entity demonstrates a low probability that the data has been compromised."

hipaacow.org®

Investigate It: Breach Risk Assessment

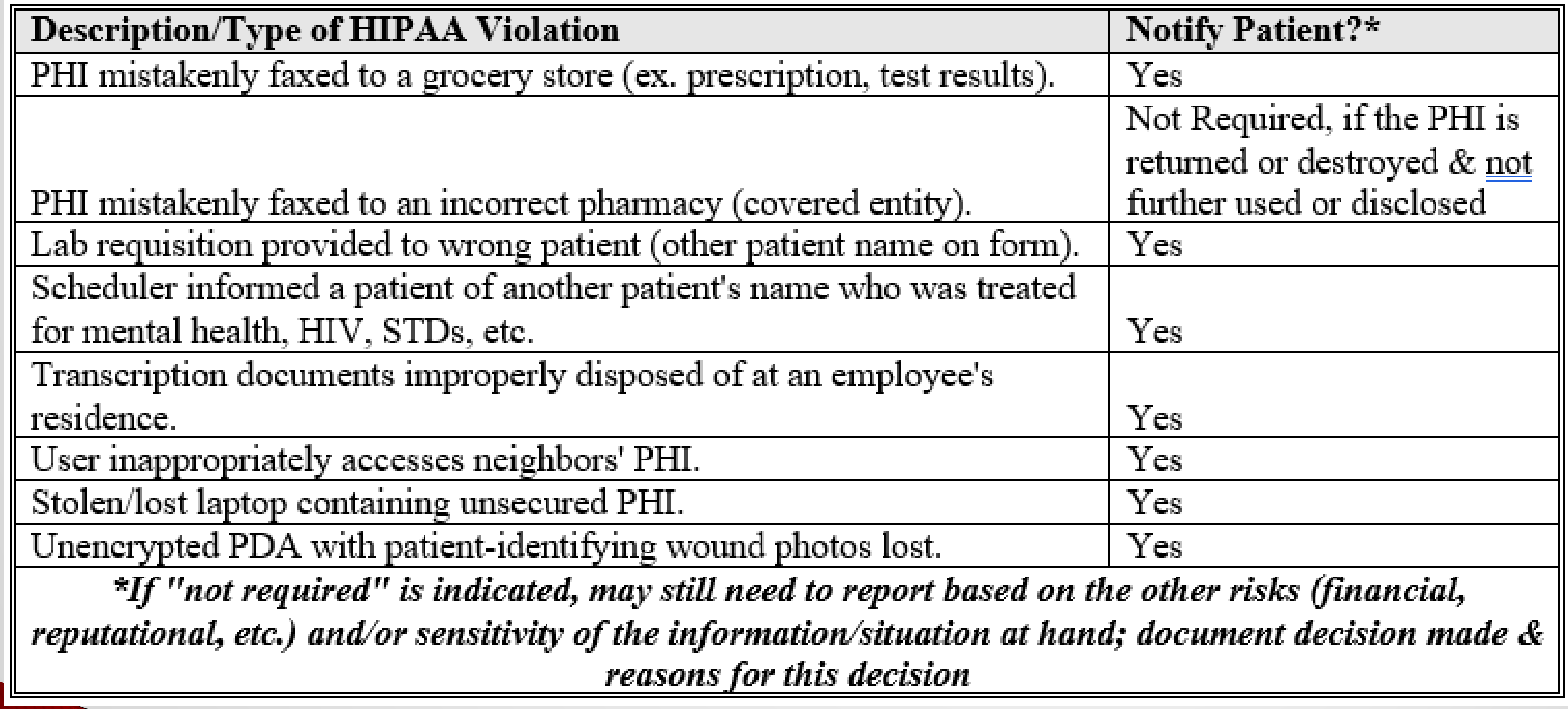
Was this a breach?

- Focus on risk of PHI, not the risk of harm to the individual
- Required to document the breach risk assessment if you decide it was not a breach of unsecured PHI and do not send breach notifications

Investigate It:
Breach Risk Assessment

Was this a breach?

- Examples of violations and notification recommendations



Description/Type of HIPAA Violation	Notify Patient?*
PHI mistakenly faxed to a grocery store (ex. prescription, test results).	Yes
PHI mistakenly faxed to an incorrect pharmacy (covered entity).	Not Required, if the PHI is returned or destroyed & not further used or disclosed
Lab requisition provided to wrong patient (other patient name on form).	Yes
Scheduler informed a patient of another patient's name who was treated for mental health, HIV, STDs, etc.	Yes
Transcription documents improperly disposed of at an employee's residence.	Yes
User inappropriately accesses neighbors' PHI.	Yes
Stolen/lost laptop containing unsecured PHI.	Yes
Unencrypted PDA with patient-identifying wound photos lost.	Yes

If "not required" is indicated, may still need to report based on the other risks (financial, reputational, etc.) and/or sensitivity of the information/situation at hand; document decision made & reasons for this decision

Extracted from the 7/7/13 HIPAA COW Breach Notification – Protected Health Information for Covered Entities document

Investigate It: Breach Risk Assessment

Was this a breach?

- Potential consequence if incidents and breaches are not correctly investigated and reported:
  - OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information, 9/27/19 (and corrective action plan)
  - Sentara Hospitals, NC and VA: OCR received a complaint they sent a bill to an individual containing another patient's PHI.
  - OCR determined had mailed 577 patients' PHI to wrong addresses
  - Sentara reported only 8 breaches, as they incorrectly concluded that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred

Resource: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sentara/index.html

hipaacow.org®

Investigate It: Steps? Who? Timeframes?

- After receiving a report of potential and known incidents what steps are taken to investigate and resolve it?
  - Do you request return and/or destruction of PHI
    - Do you request certification that copies are not kept and PHI will not be shared?
  - Do you have detailed steps and the right personnel to take for security incidents to:
    - Contain it
    - Eradicate it (remove the cause)
    - Recover (restore back to operations)
  - Who is responsible for each step?

Investigate It: Steps? Who? Timeframes?

- Who may speak with the media?
  - How much may be shared with the media?
- How do you document actions taken to investigate and resolve it?
- How quickly do you close incidents?
- How quickly to you respond to a patient / subscriber that submitted a complaint?

Investigate It: Who to Notify?

- When do you notify and how frequently do you provide updates to the following?:
  - Executive leadership
  - Board of Directors
  - Business liability / cybersecurity insurance carrier
  - Legal counsel
  - HIPAA team
  - External partners, vendors, clients, etc.
- Who provides these notifications?

Investigate It: Breach Notifications

- Business Associates to Covered Entities
  - To individuals
  - To the media
  - To OCR

Link to report breaches to OCR:
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

U.S. Department of Health and Human Services
Office for Civil Rights

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Investigate It: Breach Notifications

- Write and implement P&Ps including:
  - Notification timeframe requirements to:
    - Individuals
    - Secretary of HHS (Office for Civil Rights)
    - The Media
  - Whether to provide credit monitoring services for any types of breaches
  - Content of the notices
  - Methods of notification

Investigate It: Breach Notifications

- Prepare for an OCR investigation
  - Automatic for breaches of 500+ individuals
  - May also be done for breaches under 500 individuals
- Organize all notes, actions taken, etc.
- Provide to OCR what they request

Investigate It:
Document the report and actions taken

- Document:
  - What happened, when it happened, who was involved, and what caused the incident
  - All actions taken, with dates, times, and people interviewed and involved
  - On an incident response form or in a database
- Refer to additional information to document in the Resolve It section

Resolve It

- How likely will a potential incident be resolved appropriately if you do not know how to appropriately resolve it?

Resolve It: Mitigate Harm

- Have written and implemented P&Ps to mitigate to the extent practicable, any harmful effect

hipaacow.org®

CASE CLOSED

Resolve It: Sanctions

- Provide fair, impartial, and consistent levels of sanctions
  - In a timely manner
  - Based on:
    - The type and magnitude of harm
    - Prior performance reviews and non-compliance
    - Previous education provided
    - Whether it was intentional or a mistake
    - Relevant laws
  - Provide to workforce
  - Follow up with vendors / Business Associates to make sure they provided sanctions. Or do you terminate the contract?

Resolve It: Prevent Recurrence

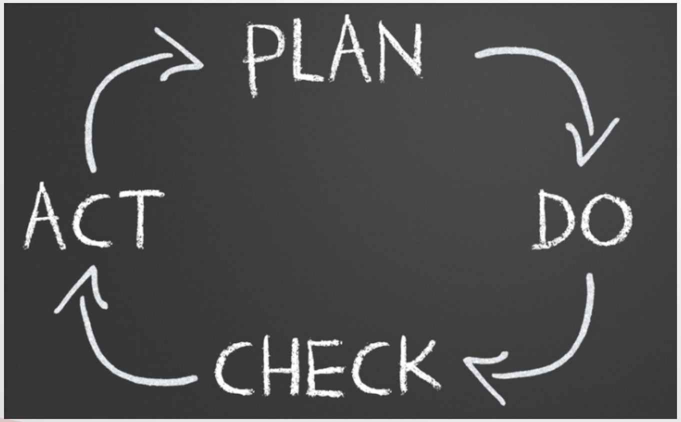
- Take appropriate steps to prevent recurrence (when possible and feasible)
- Document key lessons learned and take actions on them
- Some examples:
  - Review and perhaps update P&Ps
  - Provide training to workforce members and system users
  - Change/reduce access levels to PHI
  - Requiring the return or destruction of PHI
  - Improve privacy and security controls

hipaacow.org®

CASE CLOSED

Resolve It: Continuous Monitoring

- Continuous monitoring, specific to the incident
- Monitor the privacy and security compliance P&Ps and practices
  - Review and update on a regularly scheduled basis
  - Keep current with laws, best practices, trends, etc.
- Conduct risk analyses / compliance assessments on a regular basis
  - Mitigate identified risks



Resolve It: Documentation Requirements

- Document all investigation actions taken, breach risk assessment and notifications made, decisions made, actions taken to prevent recurrence, and lessons learned
- Document breaches of unsecured PHI on an accounting of disclosure log
- Include dates, times, and people interviewed and involved
- Maintain documentation for six years after the incident was “closed”
- Refer to additional details to document in the “Investigate It” section of this session

CASE CLOSED

Resolve It: Documentation Requirements

- Example template forms to have on hand and use (or consider using electronic systems):
  - Privacy and Security Incident Response Form
  - Breach risk assessment tool
  - Talking points to respond to breach of unsecured PHI inquiries
  - Sample notification letter to patients / subscribers
  - Sample media notification
  - Breach Notification log
  - Privacy and security violations, breach notification recommendations, and disciplinary actions taken

CASE CLOSED

Recap

You have been asked to look into a potential privacy incident. Now what???

- Make sure potential and known privacy incidents are identified and reported
- Investigate it and determine whether it is a:
  - Privacy and / or security incident
  - Breach of unsecured protected health information that requires notifications
- Resolve it

hipaacow.org®

Thank you!

Holly Schlenvogt
Privacy & Security Consultant / Owner
HRT Consulting, LLC
(262) 468-4291 (Office)
hschlenv@hrt-consulting.com | http://hrt-consulting.com

HRT
Consulting, LLC
Your trusted compliance partner

Thank You!

Thank you for viewing this webinar. If you have any comments or feedback, please feel free to email us at admin2@hipaacow.org.

Visit our website at hipaacow.org!!

hipaacow.org®

“Like Us” on facebook

“Follow Us” on LinkedIn