HIPAA PASS
Privacy and Security Solutions

HIPAA Series: Updating your Breach Mitigation & Response Plans

Presented by Susan Clarke

Health Care Information Security and Privacy Practitioner

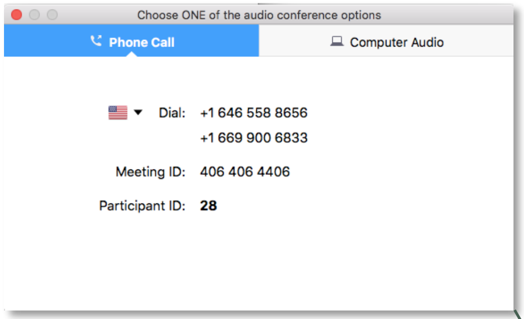
Thursday, June 17, 2021 | 11 AM – 12 PM

HCCN
Health Center Controlled Network

Mountain-Pacific
Quality Health

MPCA

Zoom tips and tricks!



Choose ONE of the audio conference options

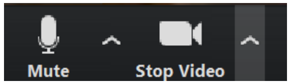
Dial: +1 646 558 8656
+1 669 900 6833

Meeting ID: 406 406 4406

Participant ID: 28

AUDIO: You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click “Join Audio,” this “Choose one…” box will pop up. If you dial in, just make sure you include your audio code.

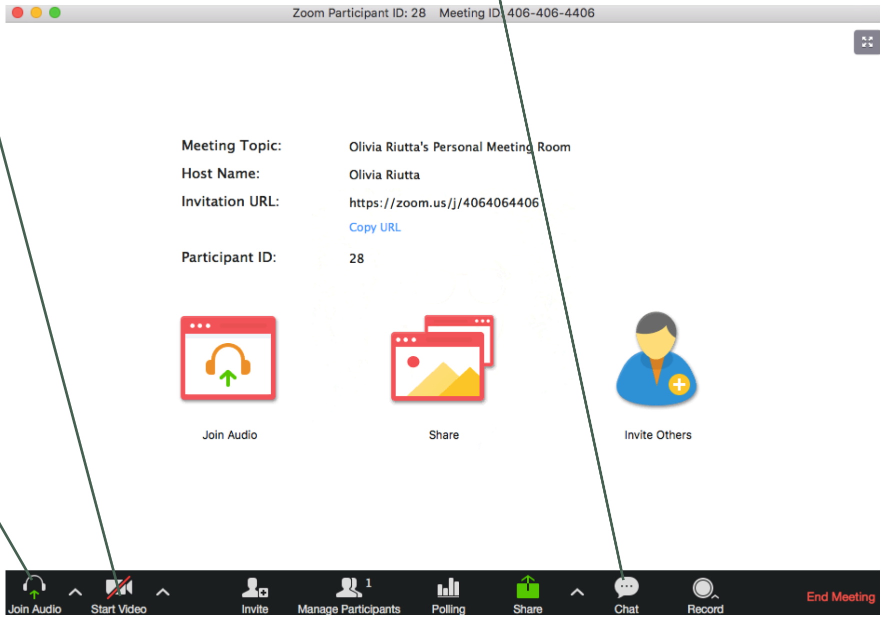
MUTE/UNMUTE: *6 or click the mic on the bottom left of your screen.



VIDEO: We want to see you! If your camera isn’t on, start your video by clicking here.

CHAT: Please jump in if you have something to share, but we also have this nifty chat function.

ATTENDANCE: If there are multiple attendees together on the call, please list the names and your location in the chat box



Zoom Participant ID: 28 Meeting ID: 406-406-4406

Meeting Topic: Olivia Riutta's Personal Meeting Room

Host Name: Olivia Riutta

Invitation URL: https://zoom.us/j/4064064406

Copy URL

Participant ID: 28

Susan Clarke, HISPP

$(ISC)^2$ Healthcare Information Security and Privacy Practitioner and Computer Scientist at Mountain-Pacific Quality Health.

Conducts privacy and security risk analysis in addition to HIPAA and 42 CRF, Part 2 training.

20 years' experience in health care operations.

10 years' design and coding EHR software including HL7 Healthcare application development.

Served on IT security, disaster recovery and joint commission steering committee at Mayo Clinic-affiliated health care system.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter's opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar and related materials (including but not limited to recordings, handouts and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar and webinar materials should not in any manner rely upon or construe the information as legal or other professional advice. Users should seek the services of a competent legal or other professional before acting or failing to act, based upon the information contained in the webinar to ascertain what may be best for the users' needs.

Abbreviations and Acronyms

- BA: Business Associate
- BAA: Business Associate Agreement
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare & Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis

Learning Objectives

HIPAA Enforcement

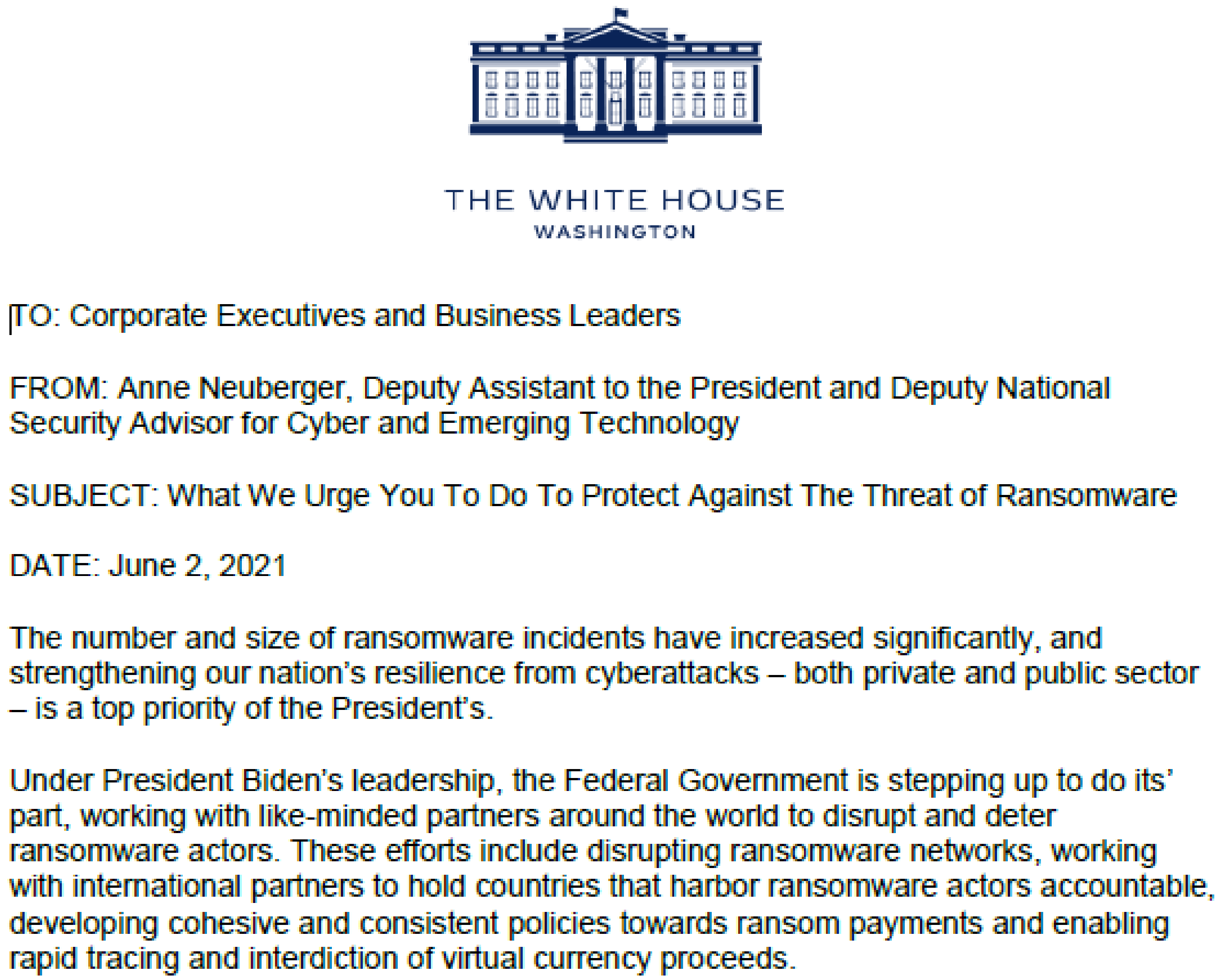
Breach Notification Rule

Breach Investigation Process

Conducting Risk Assessment

Incident Response Plan

Ransomware Updates



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

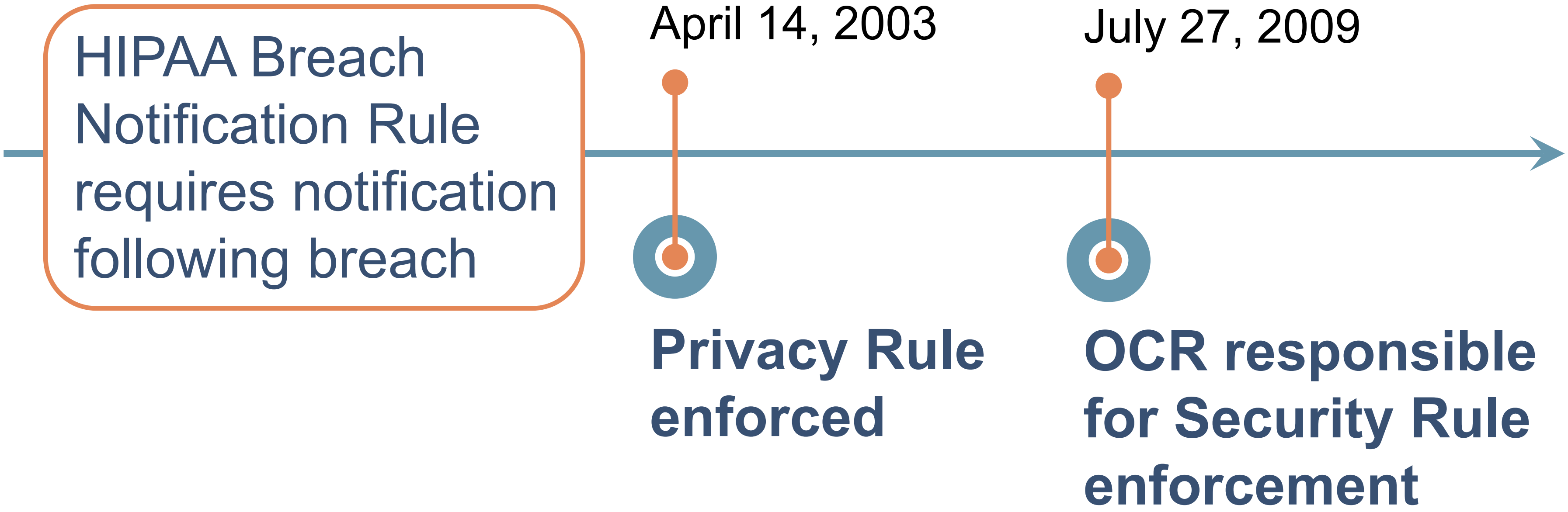
The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

Source: https://image.connect.hhs.gov/lib/fe3915707564047b761078/m/1/8eeab615-15a3-4bc8-8054-81bc23a181a4.pdf

HIPAA Enforcement

HHS Office for Civil Rights is responsible for enforcing HIPAA Privacy and Security Rules.



HIPAA Breach Notification Rule requires notification following breach

April 14, 2003

Privacy Rule enforced

July 27, 2009

OCR responsible for Security Rule enforcement

HIPAA Breach Notification Rule

Covered entity (community health centers [CHCs]) must notify affected patients, HHS and maybe media

BA must notify covered entity (CHC)

Notification must be provided no later than 60 days

Annual reporting for smaller breaches, less than 500

Top 5 Issues in Investigated Cases Closed with Corrective Action

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2020	Impermissible uses and disclosures	Safeguards	Access	Administrative safeguards	Technical safeguards
2019	Impermissible uses and disclosures	Safeguards	Access	Administrative safeguards	Minimum necessary
2018	Impermissible uses and disclosures	Safeguards	Administrative safeguards	Access	Technical safeguards
2017	Impermissible uses and disclosures	Safeguards	Administrative safeguards	Access	Technical safeguards

Enforcement Results by State

The table below represents the enforcement resolutions pertaining to complaints received, for each state for the period from April 14, 2003 through December 31, 2020.

There were:

STATE	INVESTIGATED: NO VIOLATION	RESOLVED AFTER INTAKE AND REVIEW	INVESTIGATED: CORRECTIVE ACTION
MT	**8%**	**68%**	**24%**
ND	8%	66%	27%
SD	6%	67%	26%
UT	5%	67%	28%
WY	6%	66%	27%

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-state/index.html?language=es

Determining Breach

1 Impermissible use or disclosure of PHI?

2 Perform risk assessment. Determine and document at minimum:

- ❑ Nature and extent of PHI involved
- ❑ Who received/accessed PHI
- ❑ Potential PHI was acquired or viewed
- ❑ Extent data risk has been mitigated

3 Determine if incident falls under any exceptions to the definition of breach.

Risk Assessment

As soon as possible, the compliance officer will **complete a risk assessment** to determine probability that PHI has been compromised. The risk assessment shall **include, at minimum, four factors**.

Factor 1:
Nature and Extent of PHI

Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification:

A. Was PHI involved?

B. Type of PHI?

C. Does incident meet breach definition?

D. Likelihood of re-identification?

Factor 2:
To Whom Disclosure Was Made

A. Did recipient have obligation to protect PHI privacy and security?

B. Was acquisition, access or use of PHI by workforce member/authority of practice?

C. Was such acquisition, access or use made in good faith?

D. Does recipient have ability to re-identify PHI?

E. Was acquisition, access or use within recipient's scope of authority?

F. Did acquisition, access, use or disclosure result in further use or disclosure in a way **not** permitted by the Privacy Rule?

Factor 3:
Was PHI Accessed

Must make determination whether PHI was actually acquired or viewed, or whether the opportunity to acquire or view existed, but was not acted upon.

A. Was PHI encrypted or destroyed by acceptable method?

B. Following forensic examination, did evidence establish information was not accessed?

Factor 4:
Risk Mitigation

Extent to which PHI risk has been mitigated

A. Satisfactory assurance received from recipient stating PHI has or will not be further used or disclosed

B. Efficiency of mitigation effectively limited availability to PHI

C. Does exception to notification requirement exist?

D. Do affected patients need to be notified?

Three Exceptions to “Breach”

1 **Unintentional** acquisition, access or use of PHI by workforce member or person acting under authority of covered entity or business associate, if such acquisition, access or use was **made in good faith** and **within scope of authority**

2 **Inadvertent disclosure** of PHI **by person authorized** to access PHI at covered entity or business associate **to another person authorized** to access PHI at covered entity or business associate, or organized health care arrangement in which covered entity participates

3 Covered entity or business associate has good faith belief **unauthorized person** to whom impermissible disclosure was made would be **unable to retain PHI**

HIPAA Safe Harbor Bill

Signed January 5, 2021

Amends HITECH Act ("recognized cybersecurity practices")

Lenient fines if basic safeguard requirements met

- HIPAA Security Rule
- Security risk analysis

Encryption and Safe Harbor

Covered entities and business associates must only provide required notifications if **breach involved unsecured PHI**.

Notification not required if one or more of the following:

1 Electronic PHI has been encrypted (safe harbor)

2 Media on which PHI is stored or recorded has been destroyed

https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

Notification Obligation Only Applies to "Unsecured PHI"

Unsecured PHI

=

Not rendered unusable, unreadable or indecipherable to unauthorized patients

Acceptable methods of securing PHI

=

Encryption and destruction

Loss or compromise of encrypted or properly destroyed PHI

≠

Duty to notify or report

Serious and Imminent Threat

HIPAA expressly defers to health professionals’ judgment in making determinations about nature and severity of threat to health or safety posed by patient.

https://www.hhs.gov/hipaa/for-professionals/faq/3002/what-constitutes-serious-imminent-threat-that-would-permit-health-care-provider-disclose-phi-to-prevent-harm-patient-public-without-patients-authorization-permission/index.html

Examples:
Unintentional Acquisition, Access or Use

1

Billing employee receives/opens email from a nurse about a patient

Billing employee alerts nurse and deletes email

NOT A BREACH

- Unintentional
- Done in good faith
- Within scope of authority

2

Clinician authorized to view patient records accesses neighbor's record

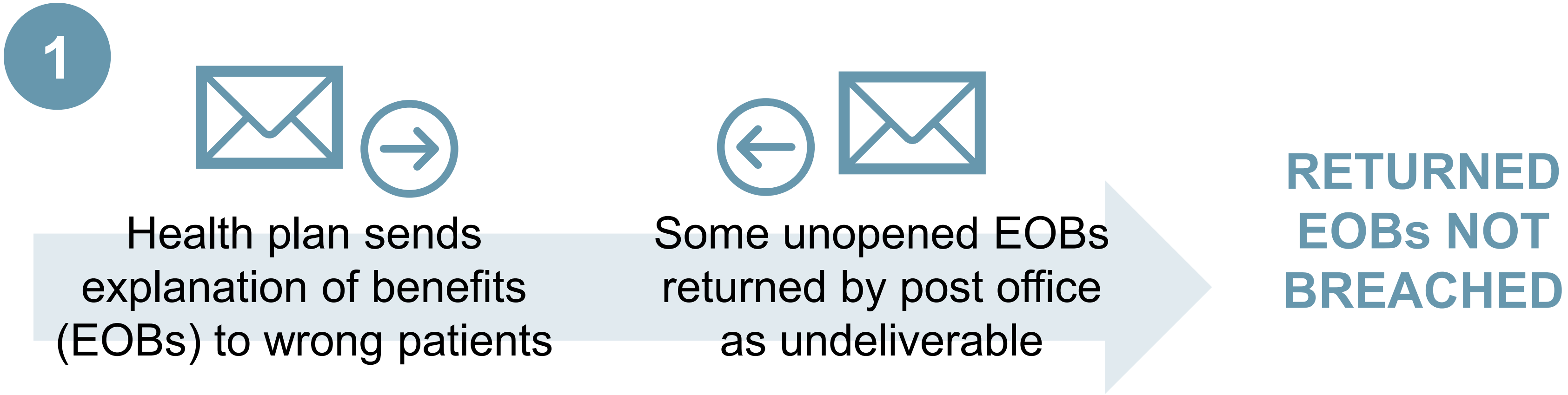
Neighbor is not the Clinician's patient

BREACH

- Intentional
- Not done in good faith
- Outside scope

Examples:

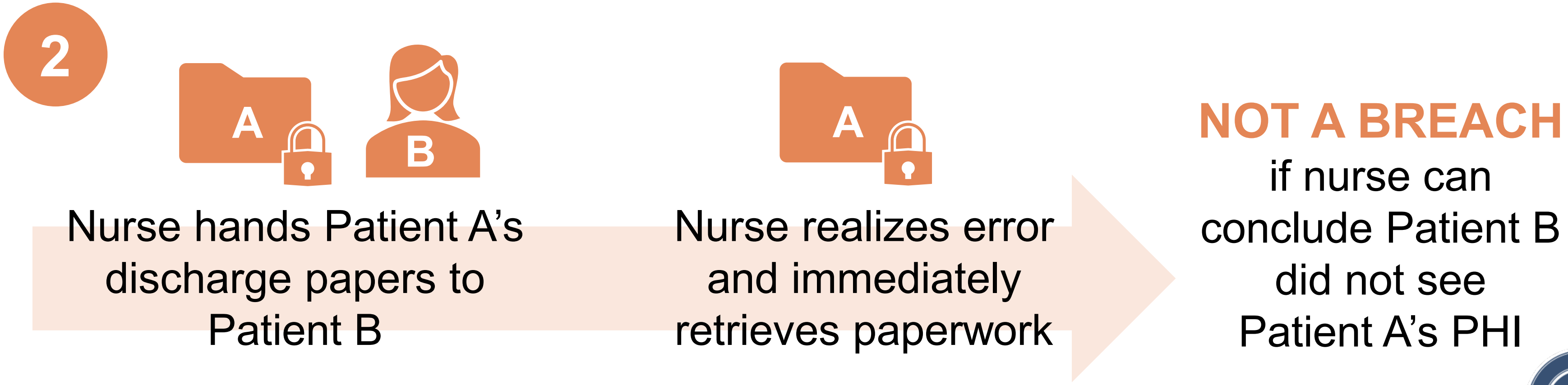
Good Faith Belief Information Was Not Retained



Health plan sends explanation of benefits (EOBs) to wrong patients

Some unopened EOBs returned by post office as undeliverable

RETURNED EOBs NOT BREACHED



Nurse hands Patient A’s discharge papers to Patient B

Nurse realizes error and immediately retrieves paperwork

NOT A BREACH if nurse can conclude Patient B did not see Patient A’s PHI

Notice to Patient(s)

Notice no later than 60 days contains:

- Brief description of breach, dates, if known
- Types of involved unsecured PHI
- Steps patient should take for protection
- Steps being taken to mitigate harm/prevent further breaches
- Your contact information

Urgent Notice

If you determine the potential for imminent misuse, you may **provide information regarding breach to patients by telephone or other means**, in addition to providing required written notice.

Notice to HHS

At same time as notice to patient(s):

≥ 500

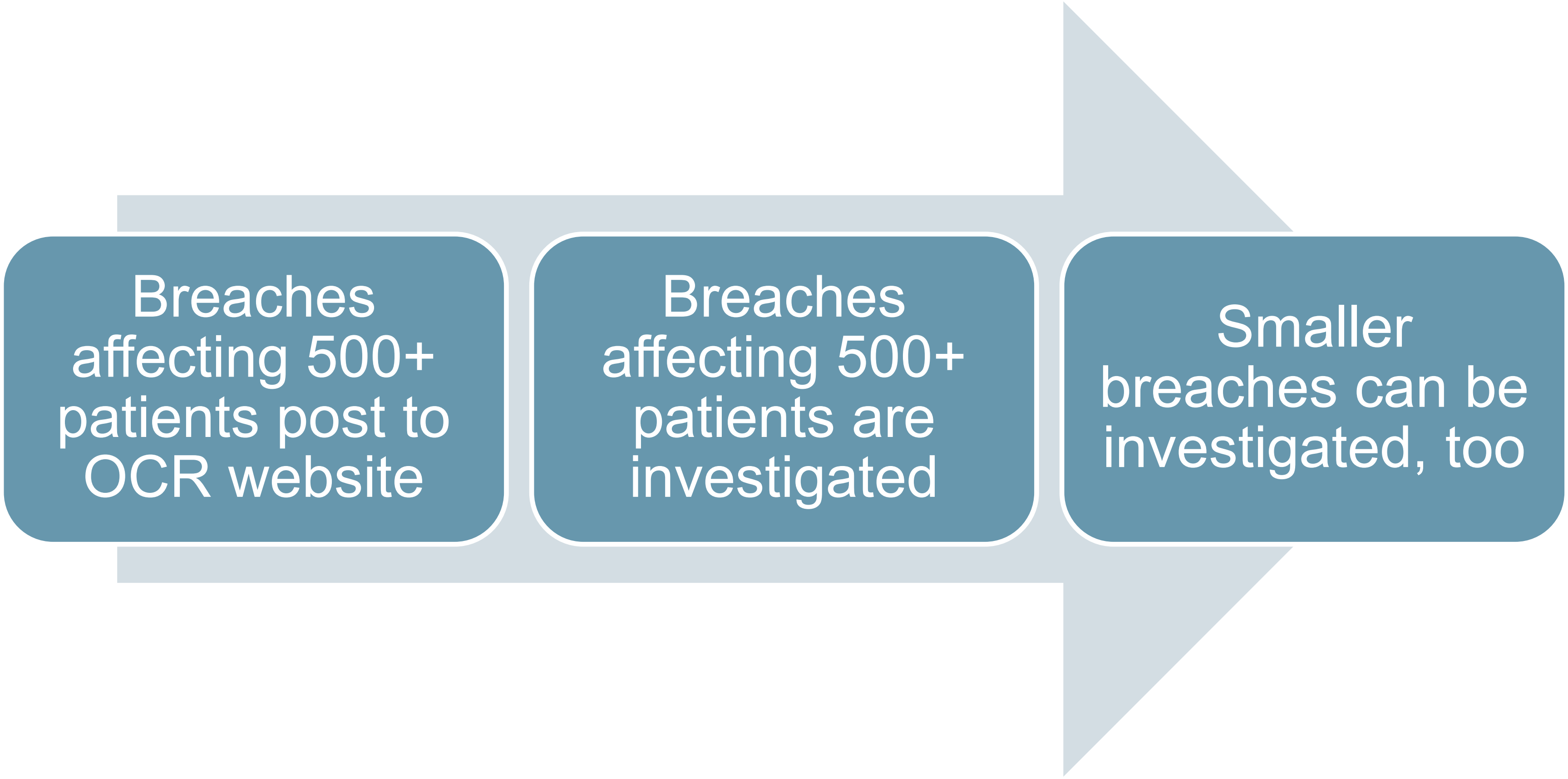
If breach affects 500 or more patients, must notify without unreasonable delay and **no later than 60 calendar days** from discovery.

< 500

If breach affects fewer than 500, must notify **within 60 days of end of calendar year** in which breach was discovered.

https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html?language=es

What Happens When HHS/OCR Receives a Breach Report?



Breaches affecting 500+ patients post to OCR website

Breaches affecting 500+ patients are investigated

Smaller breaches can be investigated, too

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Notice to Media

At same time as notice to patient(s) and HHS:

If breach affects more than 500 patients, must give notice to prominent media outlet

Likely as press release serving affected area; designate representative to talk to press

Media notification must be provided without unreasonable delay and never later than 60 days after discovery of breach

Media notification must include same information required for patient notice

State Law MT.gov

Data Breaches for Businesses

Reporting Requirements for Businesses

Montana Department of Justice

https://dojmt.gov/consumer/data-breaches-businesses/

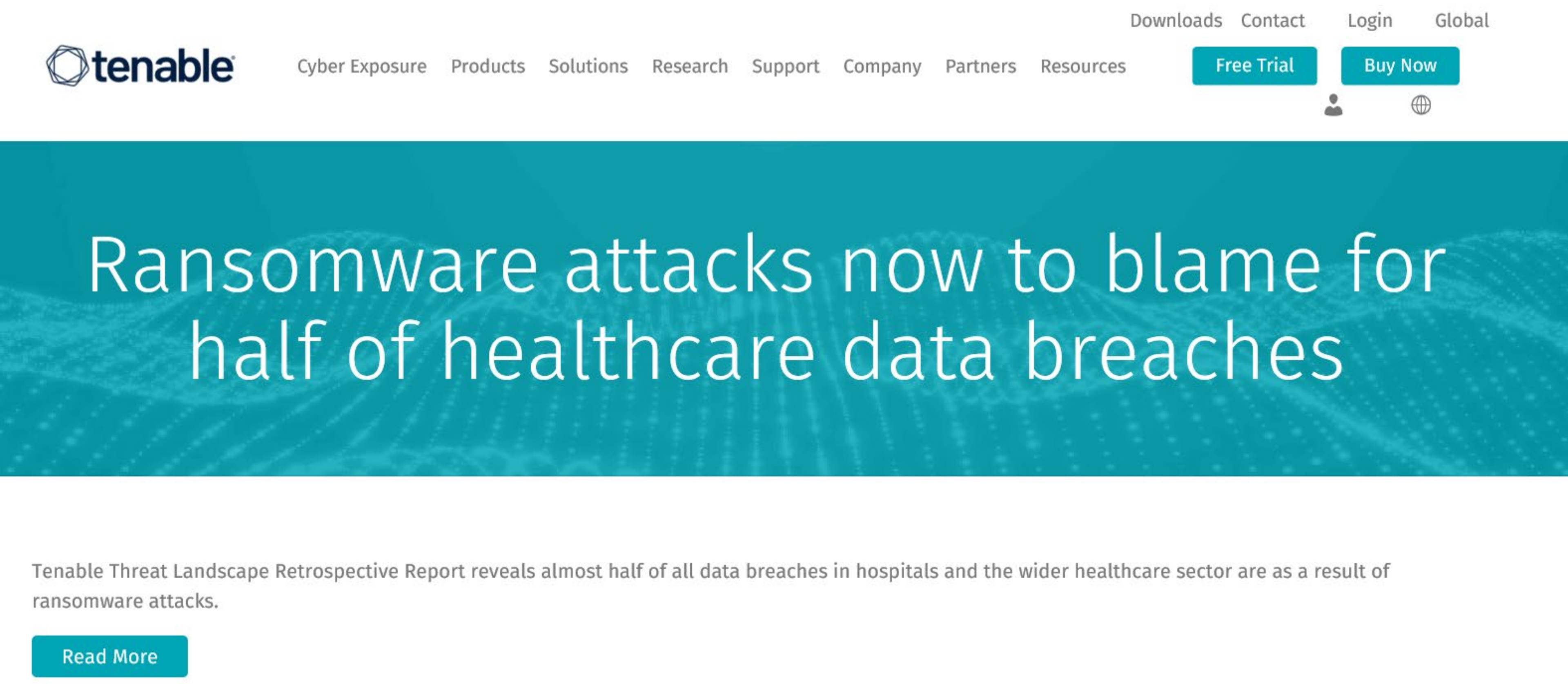
What’s the Risk of Reporting?

Legal Implications

Financial Damage

Reputational Impact

PREPARE
& PRACTICE
YOUR PLAN



Ransomware attacks now to blame for half of healthcare data breaches

Tenable Threat Landscape Retrospective Report reveals almost half of all data breaches in hospitals and the wider healthcare sector are as a result of ransomware attacks.

Source: https://www.tenable.com/in-the-news/ransomware-attacks-now-to-blame-for-half-of-healthcare-data-breaches

Why is ransomware so painful?

Encrypts files and holds for ransom

More and more cases of file exfiltration

Impact → panic, helplessness, embarrassment

Forces tough deliberations

Goes beyond technical

Ransomware Examples

Colonial Pipeline

- Darkside ransomware
- Both encryption and data exfiltrated
- Paid $4.4M ransom
- Decipher inefficient; backups required
- Millions estimated for incident response

Hollywood Presbyterian Medical Center

- Requested $3.6M ransom; paid $17K
- Malware-encrypted files
- Impacted patient care
- Lost access to patient records

NIST Risk Matrix

Level of Impact to Health Center

Likelihood of Occurrence

	Little	Some	Moderate	Serious	Critical
Very Likely	Very Low	Low	Moderate	High	Very High
Likely	Very Low	Low	Moderate	High	Very High
Moderately Likely	Very Low	Low	Moderate	Moderate	High
Unlikely	Very Low	Low	Low	Low	Moderate
Very Unlikely	Very Low	Very Low	Very Low	Low	Low

Under 500 patients

Over 500 patients--Ransomware

Develop Incident Response for Ransomware

No clear answer on whether to pay ransom

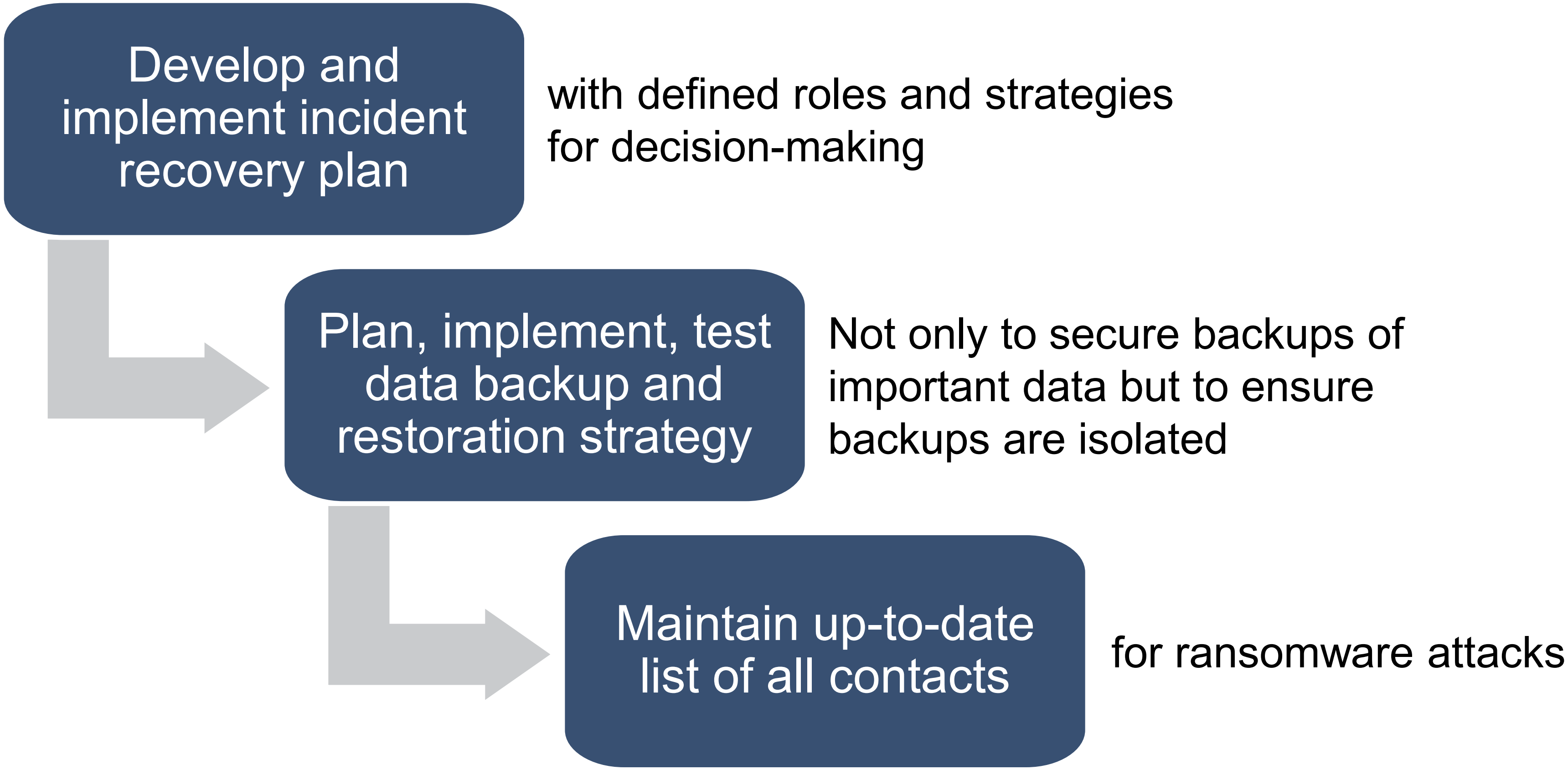
If you do pay, should you pay the entire amount?

Identify when to disable and segment networks

Evaluate your backups

Develop your incident response in advance

NIST recommends these steps:



Develop and implement incident recovery plan

with defined roles and strategies for decision-making

Plan, implement, test data backup and restoration strategy

Not only to secure backups of important data but to ensure backups are isolated

Maintain up-to-date list of all contacts

for ransomware attacks

Ransomware Resources

- CISA Ransomware Guidance and Resources
- CISA Ransomware Guide
- DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
- FBI Ransomware Webpage
- FBI IC3 Webpage for Ransomware
- NIST Tips and Tactics for Dealing with Ransomware
- HHS HC3 Homepage
- 405(d) Ransomware Threat Flyer
- 405(d) Spotlight Webinar- Ransomware
- 405(d) Ransomware Cyber Awareness Flyer
- Ransomware Task Force: Combatting Ransomware Report
- Software Engineering Institute Resources for Preparing and Responding to Ransomware

Breach Resources

- Breach notification requirements at HHS.gov
  https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- Breach reporting at HHS.gov
  https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
- OCR breach portal – Notice to HHS Secretary
  https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
- Guidance to secure PHI
  https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
- OCR list of breaches affecting ≥ 500
  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Please let me know how I can help.

For assistance, please contact:

Susan Clarke

sclarke@mpqhf.org | (307) 248-8179

THANKS FOR YOUR VALUABLE TIME TODAY!

Questions