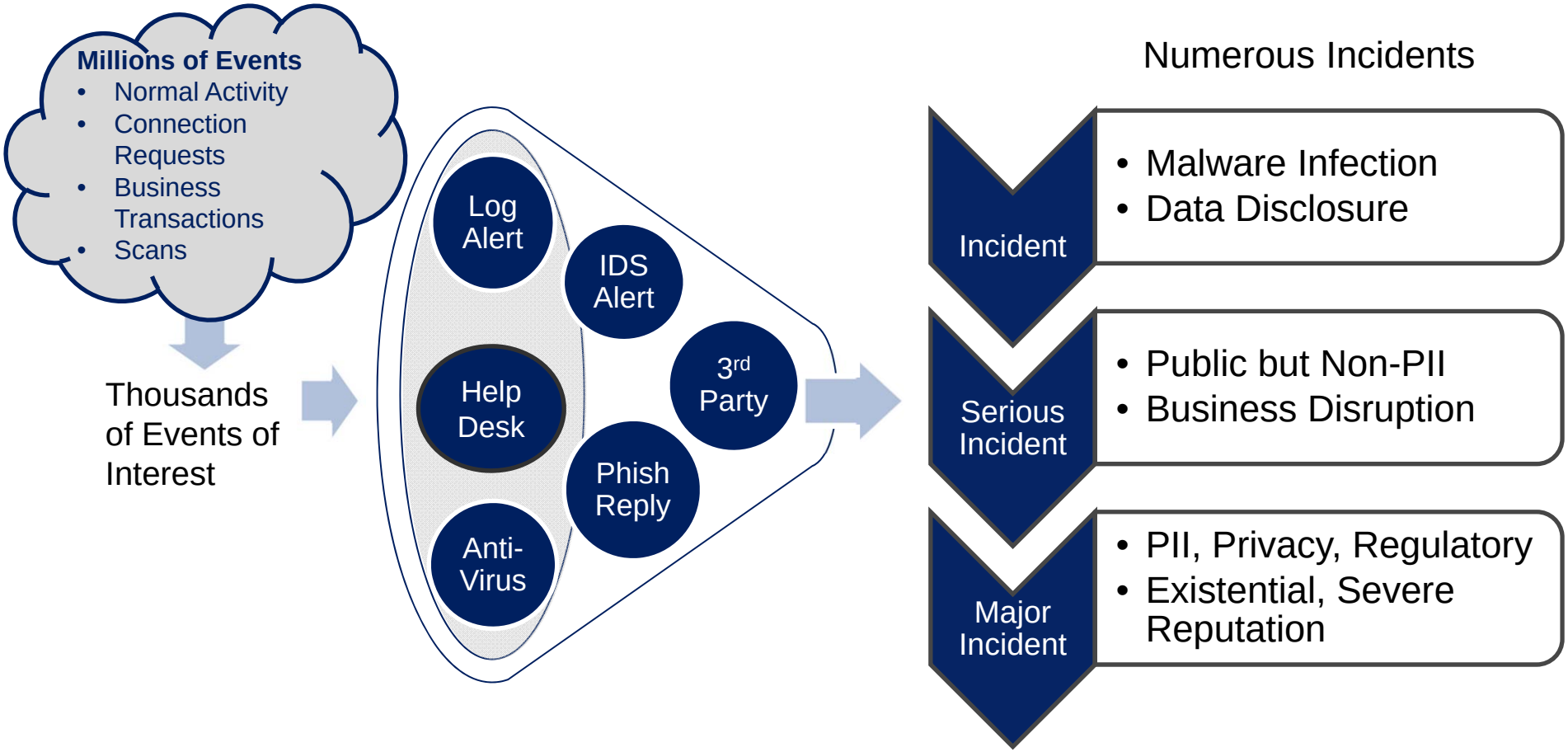
Incident Management & Response

Incident Handling and Data Breach Communications

The material contained herein represents the personal opinions of the presenter and are offered for educational purposes only. In all cases of suspected or actual data breach the advise of competent legal counsel should be sought. All attempts have been made to cite original sources.

Holland&Hart

Birth of a Major Incident



Event: Any observable occurrence in a system and/or a network
Incident: An adverse event in an system and/or network….or the threat of the occurrence of such an event

Incident Handling Lifecycle

Preparation

- Key Contact List, Test your plans (table top)
- Funding, Human Resources, Contracts in Place
- Toolkit, Written Procedures, Process, Roles & Resp.

Identification & Analysis

- Events of Interest
- Incident Type
- Vitals: system, location, owner, data, pivot, etc.

Communication & Containment

- Stop the bleeding, kill chains, run book
- Identify data lost, Isolate, track pivots
- Once contained, Immediately commence notification

Eradication & Notification

- Close access, remove accounts
- Address vulnerability
- Clean up

Recovery

- System restore
- Test

https://www.sans.org/score/incident-forms/

https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf

Incident Handling Lifecycle

Preparation

- Key Contact List, Test your plans (table top)
- Funding, Human Resources, Contracts in Place
- Toolkit, Written Procedures, Process, Roles & Resp.

Identification & Analysis

- Events of Interest
- Incident Type
- Vitals: system, location, owner, data, pivot, etc.

Communication & Containment

- Stop the bleeding, kill chains, run book
- Identify data lost, Isolate, track pivots
- Once contained, Immediately commence notification

Eradication & Notification

- Close access, remove accounts
- Address vulnerability
- Clean up

Recovery

- System restore
- Test

Preparation: Key Contact List

- Corporate Security Officer or CISO
- CIRT, CSIRT, Incident Handling Team (in house or contract)
- Corporate Legal Officer
- Outside Data Security or Privacy Counsel
- Insurance Agent
- Privacy Officer
- CIO or Systems Manager
- ISP Technical Contact
- Local FBI Field Office
- Local Law Enforcement Computer Crime
- Key Vendor Contacts (Software, Infrastructure, Data Center)
- Optional:
  - Local Computer Forensics Contractor (funded, contracted)
  - Malware Reverse Engineering Contractor (funded, contracted)

PREPARATION: KEY CONTACT LIST (CONT.)

- Regulators
- Bulk print and mail facility
- Crisis management firm, or public relations consultant
- List of third-parties who must be notified of any breach due to contractual requirements
- Pre-selected credit monitoring service provider

Preparation: Tabletop Testing

Advantages

- Low cost
- Real scenarios in non-disruptive format
- Educational for participants

Variants

- Simulations
- Blind study – some participants not in the know
- Real Simulation: Red Team vs. Blue Team

Disadvantages

- Difficult to simulate real-time pressure and stress
- Actual technical readiness difficult to ascertain

Preparation: Data Breach Response Toolkit

Incident Response Plan

Response Team Roster, Contact Info

Key Contact List

Draft Notification Templates

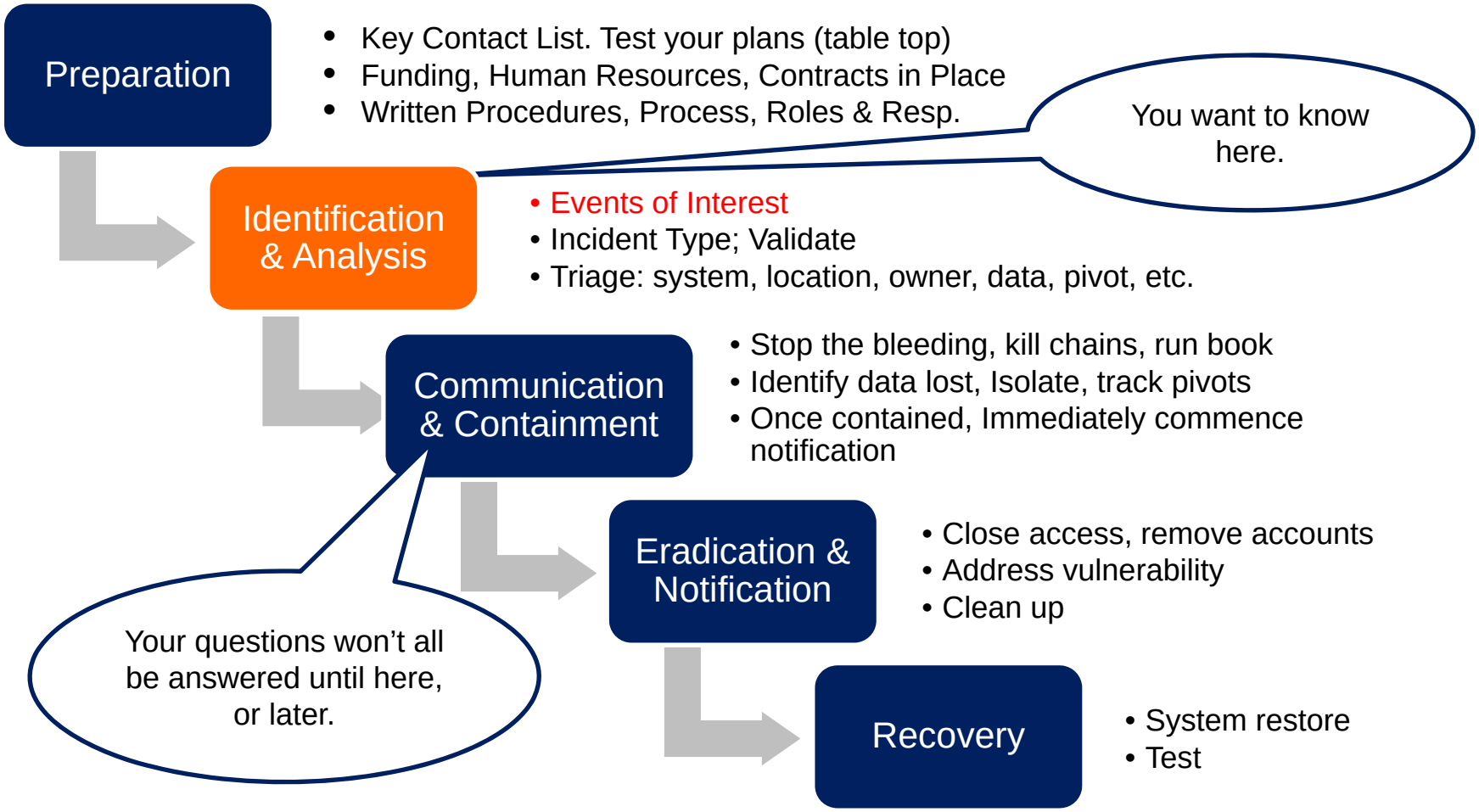
- Notification letters to regulators, credit reporting bureaus, victims
- Security incident notification for employees

Depending on Size of Breach

- Draft letters to Experion, Equifax, Transunion
- Draft letters to State AG or other government authorities as required

Review and update templates frequently as state laws are constantly changing

Incident Handling Lifecycle



Identification: Events of Interest

- Remote Access Trojan (RAT) or Command and Control (C+C), Hosts talking to known bad IPs
- Public data dumps of credentials containing your organization's email addresses
- Encrypted communications discovered
- Email filtering, reported phishing attempts, social engineering reports
- Host based IDS/ IPS alert of unexpected system call, data access, port open
- Direct external notification (Law Enforcement, Business Partner)
- Indirect external notification (Open Source Intelligence of behavior, search in your environment)

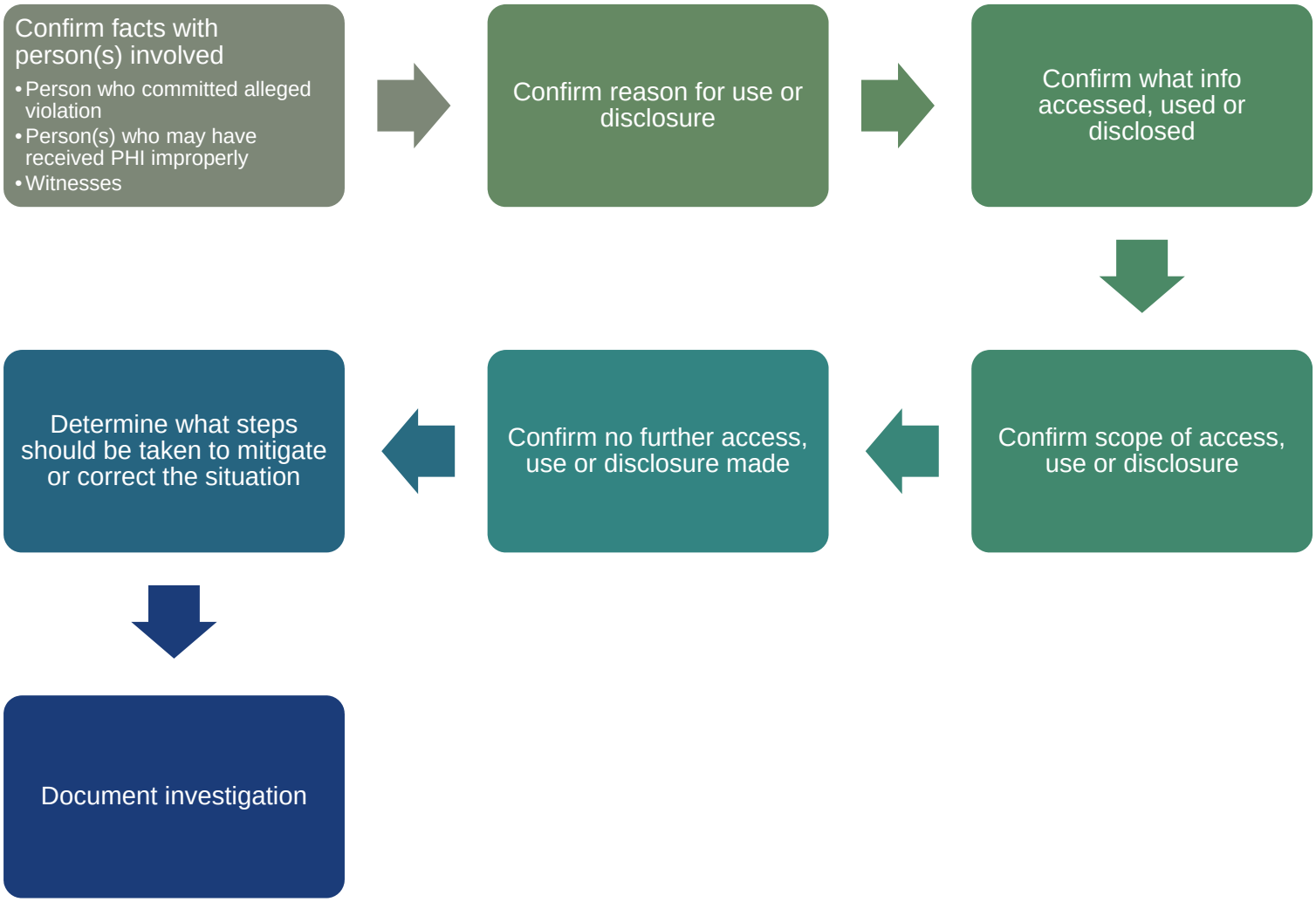
IDENTIFICATION: INCIDENT TRIAGE

- What data is at risk?
- What are the physical locations?
- Where on the network?
- Who are the business owners of the systems and data?
- What possible pivots?

Triage: Identify What Has Been Lost

- Update NIDS/HIDS to search
- Full packet capture
- Dredge email for phishing messages in Sent Items
- Host-based forensics
- Identify legal ramifications
  - HIPAA
  - PCI
  - Contractual Notifications
  - State Breach Notification

IDENTIFICATION: INVESTIGATE PROMPTLY



IDENTIFICATION: IMMEDIATELY REPORT TO PRIVACY OFFICER.

All covered entities must have a privacy officer and security officer designated in writing

Train staff to immediately report suspected PHI breaches to the privacy officer

- Immediate response may help avoid breach reporting obligation and/or penalties
- May avoid penalties if correct violation within 30 days of when knew or should know of violation
- Must report breach within 60 days of when knew or should know of violation
- Business associate agreement may impose shorter deadlines

Privacy officer should investigate

ANALYSIS: CONFIRM WHETHER HIPAA APPLIES.

Did the event happen to an entity acting in its capacity as either:

A covered entity

- Healthcare provider who engages in certain electronic transactions
- A health plan, including employee group health plan
  - With 50 or more participants
  - Administered by a third party

Business associate

- An entity that creates, maintains, transmits, or uses protected health info on behalf of a covered entity

(45 CFR 160.103)

ANALYSIS: CONFIRM WHETHER HIPAA APPLIES

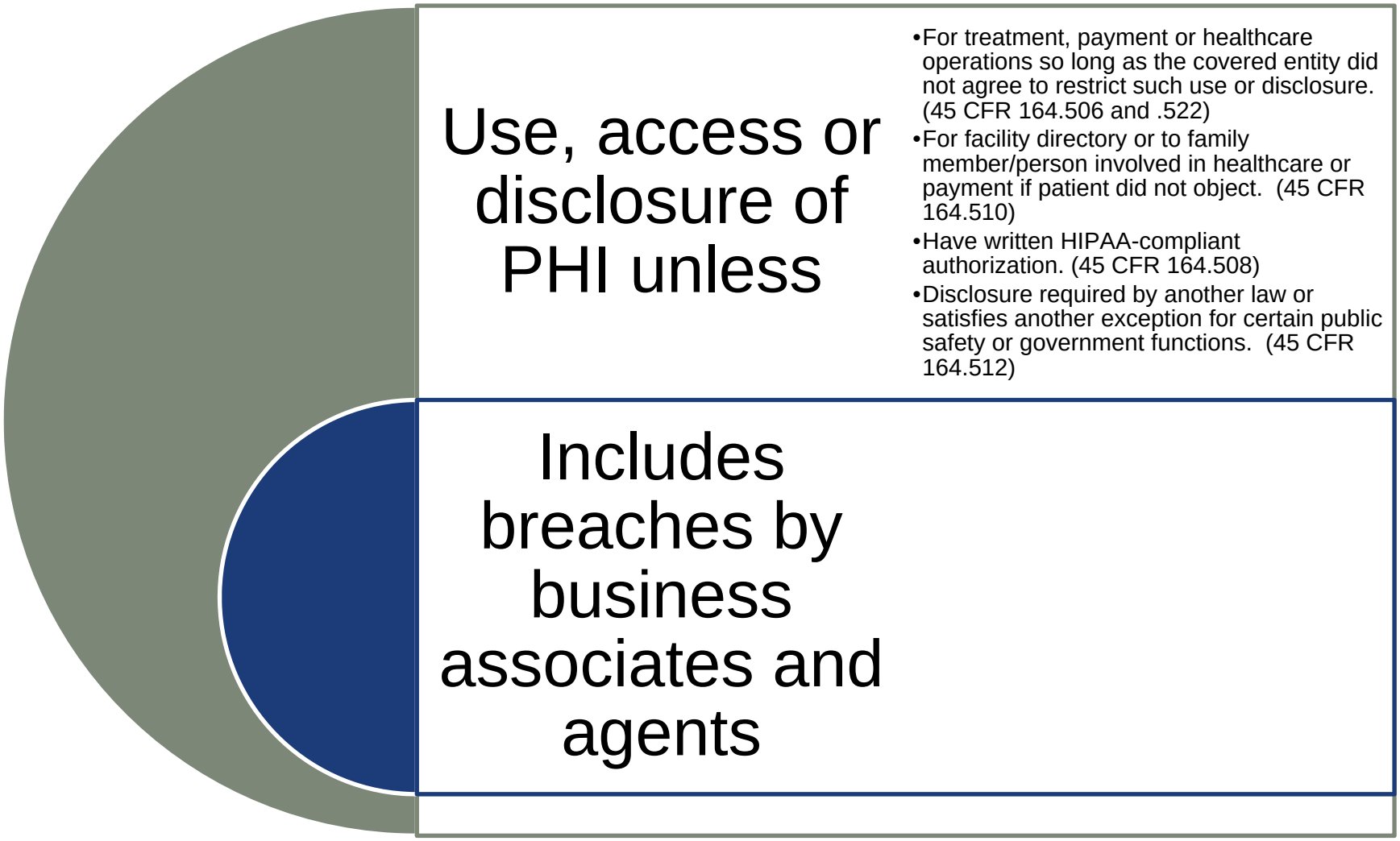
Is the info "protected health info"

- Created or received by a healthcare provider or health plan
- Relates to the past, present or future health, healthcare or payment for healthcare; and either
  - Identifies the individual
  - There is reasonable basis to believe the info can be used to identify the individual

Not de-identified info

(45 CFR 160.103, 164.514)

ANALYSIS: CONFIRM WHETHER HIPAA VIOLATED



(45 CFR 164.502)

ANALYSIS: CONFIRM WHETHER HIPAA VIOLATED

Use, disclosure, or request for more PHI than the minimum necessary to accomplish the intent of a permitted use, disclosure or request

The "minimum necessary" standard does not apply to

- Disclosures to or requests by another healthcare provider
- Uses or disclosures made per an authorization.
- Uses or disclosures required by law

(45 CFR 164.502(b))

ANALYSIS: CONFIRM WHETHER HIPAA VIOLATED

Incidental disclosures do not violate HIPAA and are not reportable.

Incidental disclosure =

Incident to a use or disclosure that is otherwise permitted or required

The covered entity otherwise complied with

The "minimum necessary" standard

Implemented reasonable safeguards to protect against improper disclosures

(45 CFR 164.502(a)(1))

ANALYSIS: CONFIRM WHETHER HIPAA VIOLATED

"An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule", e.g.,

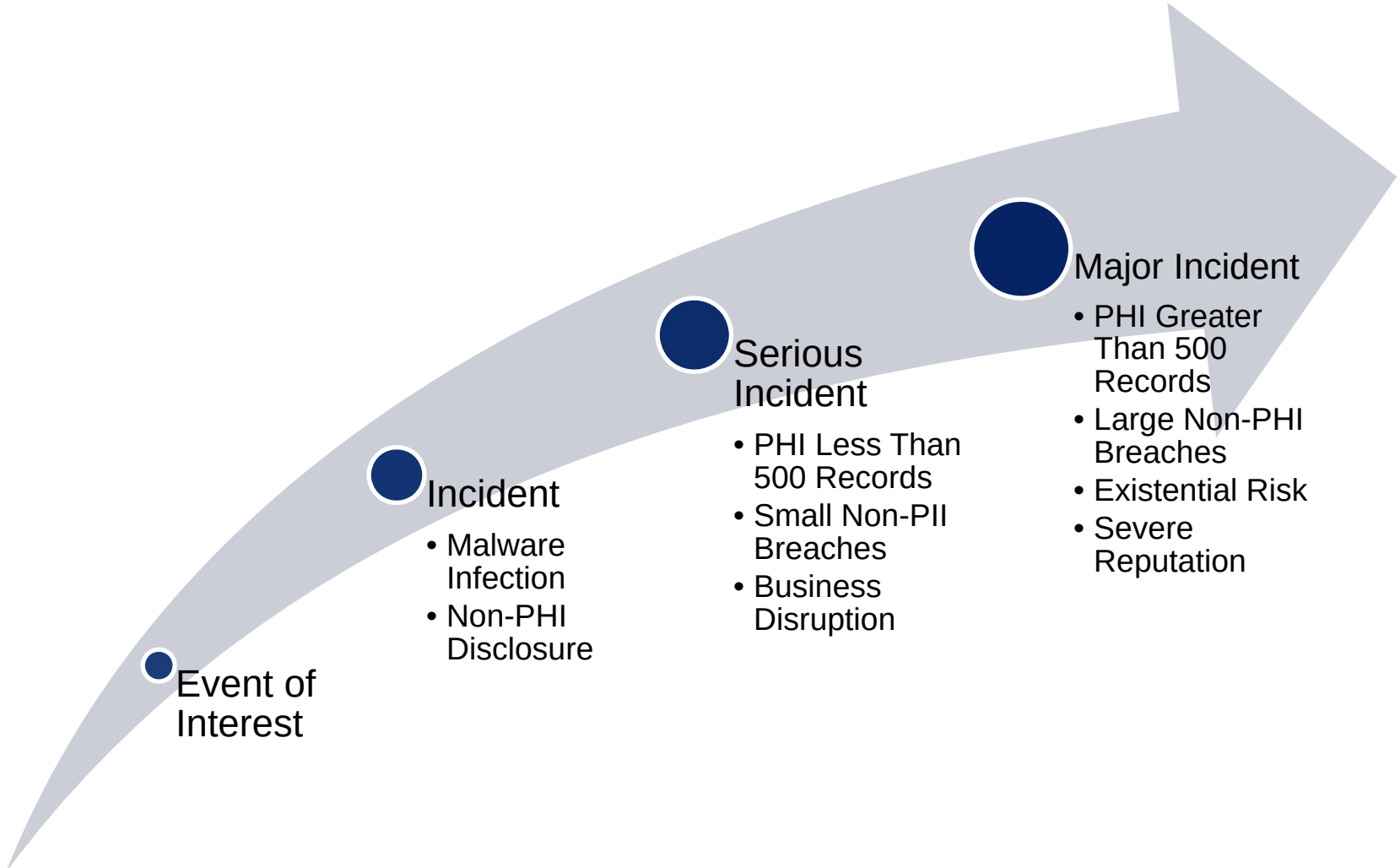
- A hospital visitor may overhear a provider's confidential conversation with another provider or a patient
- A hospital visitor may glimpse a patient's PHI on a sign-in sheet or nursing station whiteboard

Must use reasonable safeguards, e.g.,

- Speak quietly or do not discuss PHI in public areas
- Do not use patients' names in public areas
- Isolate or lock file cabinets or records rooms

(OCR Website, "Incidental Disclosures")

ANALYSIS: CLASSIFY THE INCIDENT



SAFE HARBOR: BREACH OF PHI

Currently, only two methods to secure PHI
With Guidance updated annually

Encryption of electronic PHI

- Transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- Notice provides processes tested and approved by Nat'l Institute of Standards and Technology (NIST)

Destruction of PHI

- Paper, film, or hard copy media is shredded or destroyed such that PHI cannot be read or reconstructed
- Electronic media is cleared, purged or destroyed consistent with NIST standards

(74 FR 42742 or www.hhs.gov/ocr/privacy)

Risk Analysis: Breach of PHI

Acquisition, access, use or disclosure of PHI in violation of privacy rules is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the info has been compromised based on a risk assessment of the following factors

- nature and extent of PHI involved
- unauthorized person who used or received the PHI
- whether PHI was actually acquired or viewed
- extent to which the risk to the PHI has been mitigated
- unless an exception applies

(45 CFR 164.402)

RISK ANALYSIS: BREACH OF PHI

"Breach" defined to exclude the following

- Unintentional acquisition, access or use by workforce member if made in good faith, within scope of authority, and PHI not further disclosed in violation of HIPAA privacy rule
- Inadvertent disclosure by authorized person to another authorized person at same covered entity, business associate, or organized health care arrangement, and PHI not further used or disclosed in violation of privacy rule
- Disclosure of PHI where covered entity or business associate have good faith belief that unauthorized person receiving info would not reasonably be able to retain info

(45 CFR 164.402)

When is PHI "Compromised"?

"Breach": Risk Assessment

Determine the probability that the data has been "compromised" by assessing

- Nature and extent of PHI involved, including types of identifiers and the likelihood of re-identification
- Unauthorized person who used PHI or to whom disclosure was made
- Whether PHI was actually acquired or viewed
- Extent to which the risk to the PHI has been mitigated
- Other factors as appropriate under the circumstances

Breach Risk assessment is unnecessary if you make a report

(45 CFR 164.402)

"BREACH": RISK ASSESSMENT

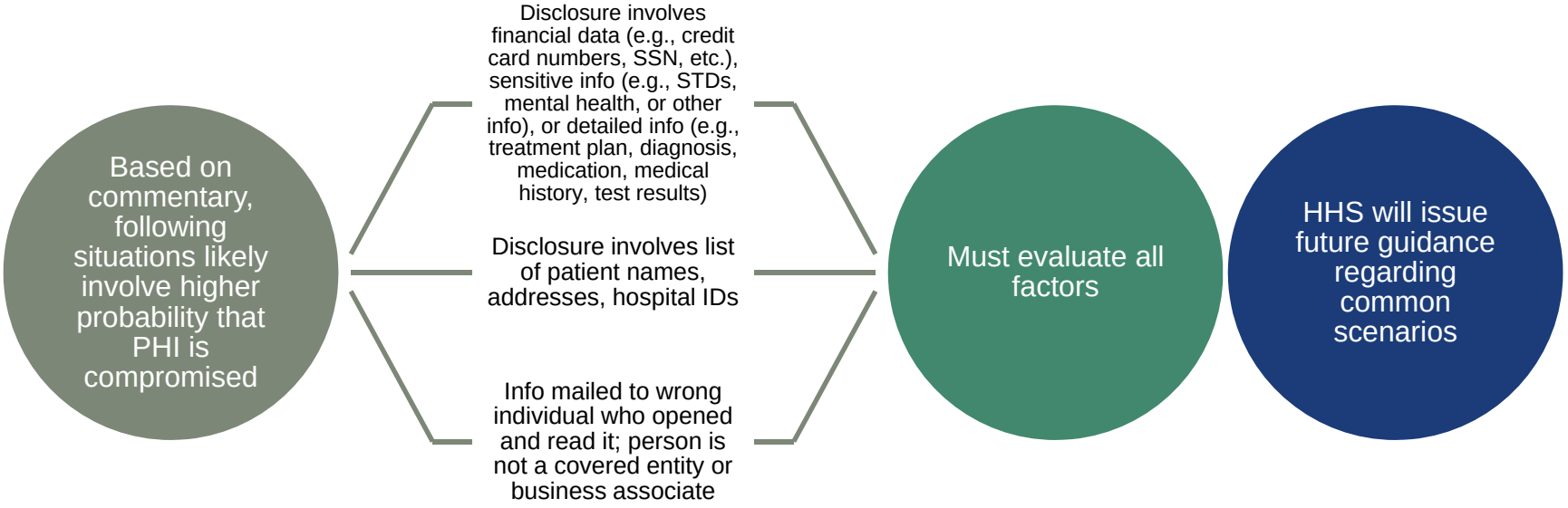
Based on commentary, following situations likely involve lower probability that PHI would be compromised

- Fax sent to wrong physician, but physician reports fax and confirms he has destroyed it
- Disclosure to or use by persons who are required by HIPAA to maintain confidentiality
- Disclosure without identifiers or to entity that lacks ability to re-identify the PHI
- Stolen laptop recovered and analysis shows that PHI was not accessed

But must evaluate all factors

(78 FR 5642-43)

"BREACH": RISK ASSESSMENT



(78 FR 5642-43)

Breach of Unsecured PHI: Summary

No breach notification required if

- No privacy rule violation
  - "Incidental disclosures" do not violate the privacy rule
- PHI is "secured", i.e., encrypted per HHS standards
- Exception applies, i.e.
  - Unintentional acquisition of PHI by workforce member acting in good faith and no further use or redisclosure
  - Inadvertent disclosure by authorized person to another person authorized to access the PHI
  - Unauthorized recipient of PHI is unable to retain PHI
- Low probability that data has been compromised

Covered entity has burden of proof

Breach of Unsecured PHI: Summary

Until we receive further clarification, safer to err on the side of reporting all but clearly "inconsequential" breaches

Covered entity has burden of proving "low probability that PHI has been compromised."

Failure to report may be viewed as willful neglect resulting in mandatory penalties

Breach of Unsecured PHI: Summary

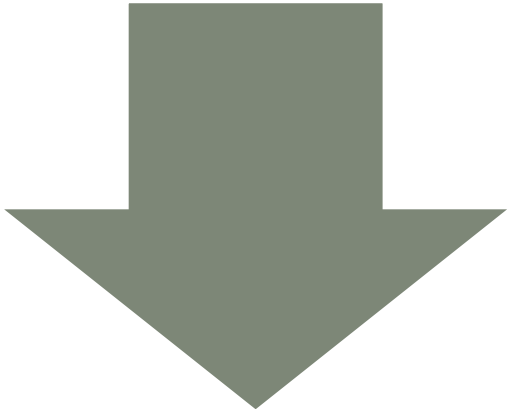
According to HHS, the following constitutes "willful neglect", requiring mandatory penalties

"A covered entity's employee lost an unencrypted laptop that contained unsecured PHI…. [T]he covered entity feared its reputation would be harmed if info about the incident became public and, therefore, decided not to provide notification as required by 164.400 et seq."

Beware missing PHI or devices containing PHI

(75 FR 40879)

Breach of Unsecured PHI: Summary

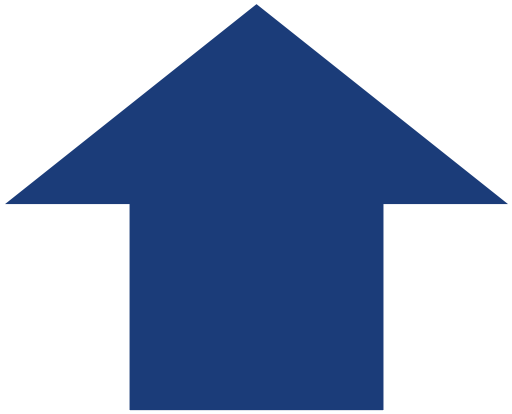


Reporting may reduce risk of significant penalties

- Willful neglect and mandatory penalties
- Excessive penalties

Reporting will increase risk of

- OCR investigation, which may uncover other problems
- Patient complaints or suits.
- AG suits
- Costs of reporting



Incident Handling Lifecycle

Preparation

- Key Contact List. TEST your plans (table top)
- Funding, Human Resources, Contracts in Place
- Written Procedures, Process, Roles & Resp.

Identification & Analysis

- Events of Interest
- Incident Type
- Vitals: system, location, owner, data, pivot, etc.

Communication & Containment

- Stop the bleeding, kill chains, run book
- Identify data lost, Isolate, track pivots
- Once contained, Immediately commence notification

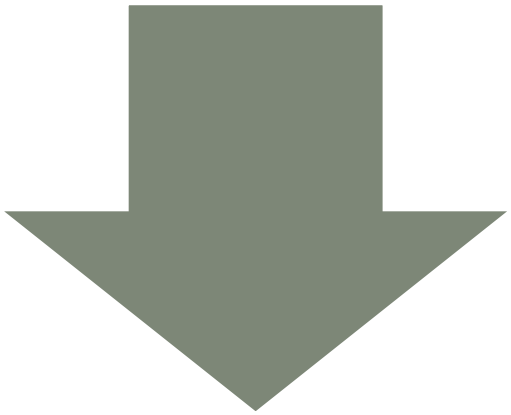
Eradication & Notification

- Close access, remove accounts
- Address vulnerability
- Clean up

Recovery

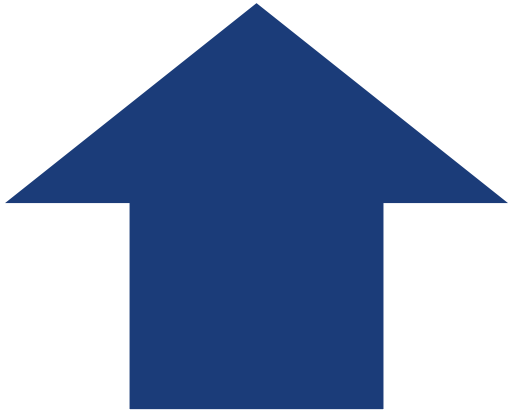
- System restore
- Test

COMMUNICATE: INTERNAL COMMUNICATIONS



Upon Identification:

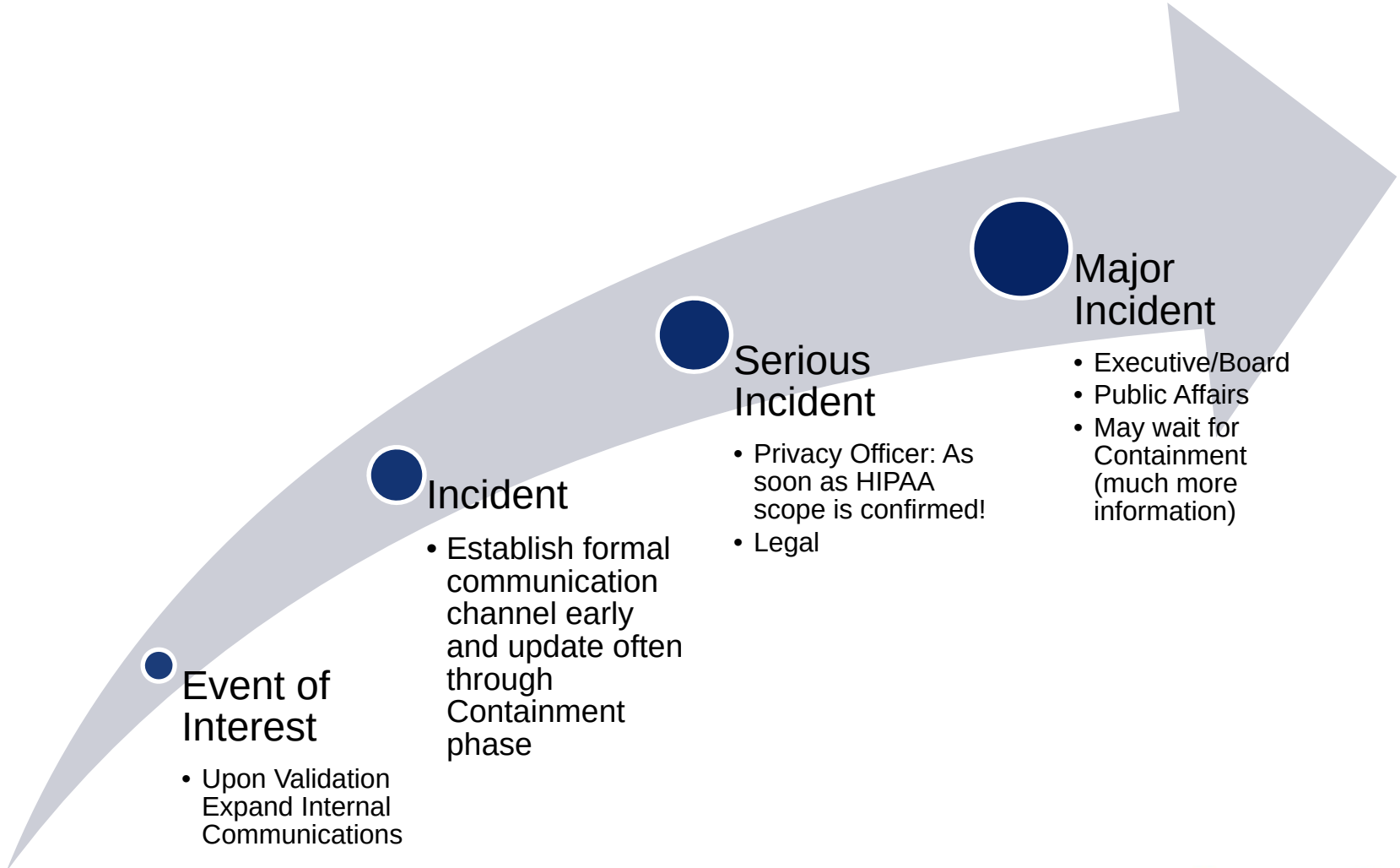
- CIRT Lead
- Validate suspected incident first!
- Incident classification determines stakeholders
- Don't raise false alarms
- **Categorize Severity & Impact (per policy)**
  - **Minor**
  - **Serious**
  - **Major**



Upon Validation

- Privacy Officer
- Security Officer, IT Director
- System Owner
- Affected Business Line

INTERNAL COMMUNICATIONS (CONT.)



Communicate: Check on insurance

Many companies carry cyberliability or other potentially applicable insurance

Check with broker

When in doubt, report

- Delay in reporting may give insurer excuse to deny coverage
- Insurer may accept coverage despite terms in policy
- Insurer may provide resources to help you respond

Document communications with insurer.

CONTAINMENT: MITIGATE HARM

A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure by the covered entity or its business associate of PHI in violation of its policies or the privacy rule

If a covered entity or business associate knows of a pattern or practice or a business associate or subcontractor that violates HIPAA, they must either

Take steps to cure the breach or end the violation

Terminate the BAA

(45 CFR 164.530(f)) and *(45 CFR 164.504(e))*

ERADICATION: CORRECT THE VIOLATION

- Mitigate the harm
- Sanction employees
- Revise policies and procedures
- Implement new or different safeguards
- Train personnel
- Enforce the policies and rules
- Maybe notify affected individuals
- Take other appropriate steps
- Document actions

ERADICATION

Capture evidence of wrong doing

Forensically image impacted disk drives, replace with clean installs

Maintain chain of custody on all drives and forensic images

Use working copies for analysis while preserving original drives

Advanced attacks are only discovered in RAM, do not write to drive

Close all outbound data exfiltration channels

Close and patch all vulnerabilities

CONTAINMENT: SANCTION EMPLOYEES.

A covered entity must have policies and apply appropriate sanctions against members of its workforce who fail to comply with HIPAA rules or privacy policies

Document the sanctions

Ensure the punishment fits the crime

(45 CFR 164.530(e))

CONTAINMENT: SANCTION EMPLOYEES

CONTAINMENT: CORRECT THE VIOLATION

THIS IS REALLY IMPORTANT!

It is an affirmative defense to HIPAA penalties if the covered entity or business associate

- Did not act with willful neglect, and
- Corrected the violation within 30 days

(45 CFR 160.410)

Incident Handling Lifecycle

Preparation

- Key Contact List. TEST your plans (table top)
- Funding, Human Resources, Contracts in Place
- Written Procedures, Process, Roles & Resp.

Identification & Analysis

- Events of Interest
- Incident Type
- Vitals: system, location, owner, data, pivot, etc.

Communication & Containment

- Stop the bleeding, kill chains, run book
- Identify data lost, Isolate, track pivots
- Once contained, Immediately commence notification

Eradication & Notification

- Forensic images, evidence
- Close access, remove accounts
- Address vulnerability, Clean up

Recovery

- System restore
- Test
- Lessons Learned

Breach Notification

If there is "breach" of "unsecured PHI"

Covered entity must notify

- Each individual whose unsecured PHI has been or reasonably believed to have been accessed, acquired, used, or disclosed
- HHS
- Local media, if breach involves > 500 persons in a state
- Business associate must notify covered entity

(45 CFR 164.400 et seq.)

NOTIFICATION

NOTIFICATION

Know reasonably well before going public:

- Incident is not ongoing
- Type of incident
- Size of breach
- Medium of data: hard copy, electronic or both?
- Location, jurisdictions and controlling law
- Timing of incident:
  - First discovered
  - Internal communications
- Data affected, elements compromised

NOTIFICATION

NOTIFICATION

Establish a call center

Notify all at once, not in waves driven by statutory time limits

Use consistent language to describe the nature of the incident and the affected data, across all external communications to the public, regulators, international entities

Communicate internally to employees

Some employees may also be customers, consistent messaging, proximate in time

Instruct employees to refer inquiries to designated spokesperson/group

Victim Notification Letters

For Non-PHI Notification many states have different requirements for content, notification period, procedure, hotline for questions

Tone of letter: conciliatory, respectful, focused

Include contact information, special twitter feed, or website for continuous updates

LOG THE IMPROPER DISCLOSURE

(45 CFR 164.528) and (45 CFR 160.103)

LOG THE IMPROPER DISCLOSURE

Must include the following info in accounting

- Date of the disclosure
- Name and address of the entity who received the PHI
- Brief description of the PHI disclosed
- Brief statement of the purpose of the disclosure or copy of written request for disclosure

As a practical matter, this will require covered entities and business associates to maintain a log of disclosures

(45 CFR 164.528)

BA REPORT TO COVERED ENTITY

- Any use or disclosure of PHI not provided for by the BAA of which it becomes aware
- Any security incident of which it becomes aware, i.e., "attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an info system."
- Breaches of unsecured PHI per the Breach Notification Rule
- Business associate agreements often contain additional requirements

45 CFR 164.314(a), .410, and .504(a)(2))

INCIDENT HANDLING LIFECYCLE

Preparation

- Key Contact List. TEST your plans (table top)
- Funding, Human Resources, Contracts in Place
- Written Procedures, Process, Roles & Resp.

Identification & Analysis

- Events of Interest
- Incident Type
- Vitals: system, location, owner, data, pivot, etc.

Communication & Containment

- Stop the bleeding, kill chains, run book
- Identify data lost, Isolate, track pivots
- Once contained, Immediately commence notification

Eradication & Notification

- Forensic images, evidence
- Close access, remove accounts
- Address vulnerability, Clean up

Recovery

- System restore
- Test
- **Lessons Learned**

Recovery: Post-Mortem

Executive

- Is this a cost of doing business?
- Is this a case for meaningful change?
- Avoid blame, use incident to improve capability
- Explain details by analogy

Technical

- Learn from tactics used against you
- Address vulnerabilities with 20 Critical Controls
- Make a solid business case for information security investment
- Translate security goals into business goals

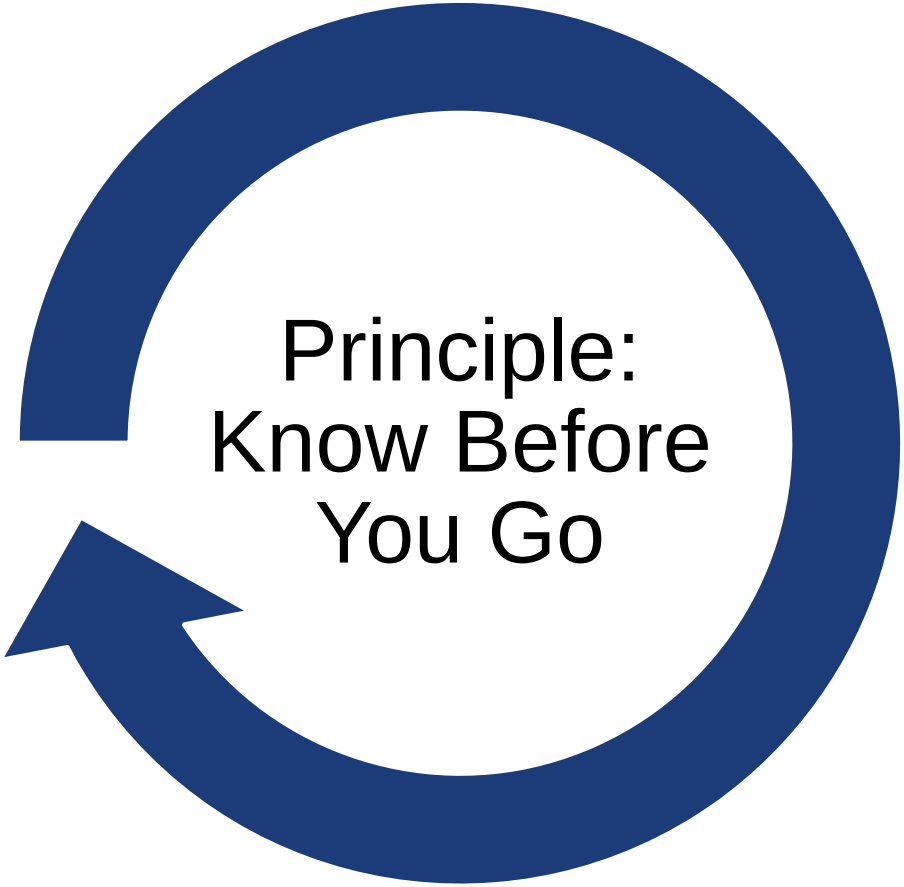
SUMMARY: IF YOU THINK YOU HAVE A BREACH

- Act immediate action to minimize breach
- Notify privacy officer
- Confirm whether HIPAA applies
- Confirm whether HIPAA was violated
- Check on insurance
- Investigate promptly
- Mitigate any harm
- Sanction workforce members
- Correct any process that resulted in improper disclosures
- Log the improper disclosure
- Report if required
- Document the foregoing

Remember: prompt action may allow you to

- Satisfy your duty to mitigate
- Avoid disclosure and breach reporting obligation
- Defend against HIPAA penalties

SUMMARY: PREPARE



- Create a Model Process (Stakeholders, Communications)
- Contract now with service providers
- Stay on top of changes in Data Breach Notification Laws
- Know your regulator; OCR Enforcement Actions
- Draft all templates now
- Tabletop test your plan

Action Plan

When you get back to your office

- Inquire about your incident response plan, review it
- Call a stakeholder meeting to plan improvements to breach readiness

In the first 30 days

- Update incident response plan
- Update key contacts
- Initiate review of data breach notification requirements (state, federal, intl., contract)

By 90 days

- Draft all templates
- Identify and source external service providers
- Finalize roles & responsibilities

End of year

- Complete table top exercise
- Complete post-mortem on all incidents
- Improve security program to prevent incidents (Safeguards, CSF and 20CC)

THANK YOU

QUESTIONS?

MATT SORENSEN
HOLLAND & HART
CMSORENSEN@HOLLANDHART.COM

HOLLAND&HART