Medical Protective

a Berkshire Hathaway company

Strength. Defense. Solutions. Since 1899.

HIPAA Update – Focus on Breach Prevention

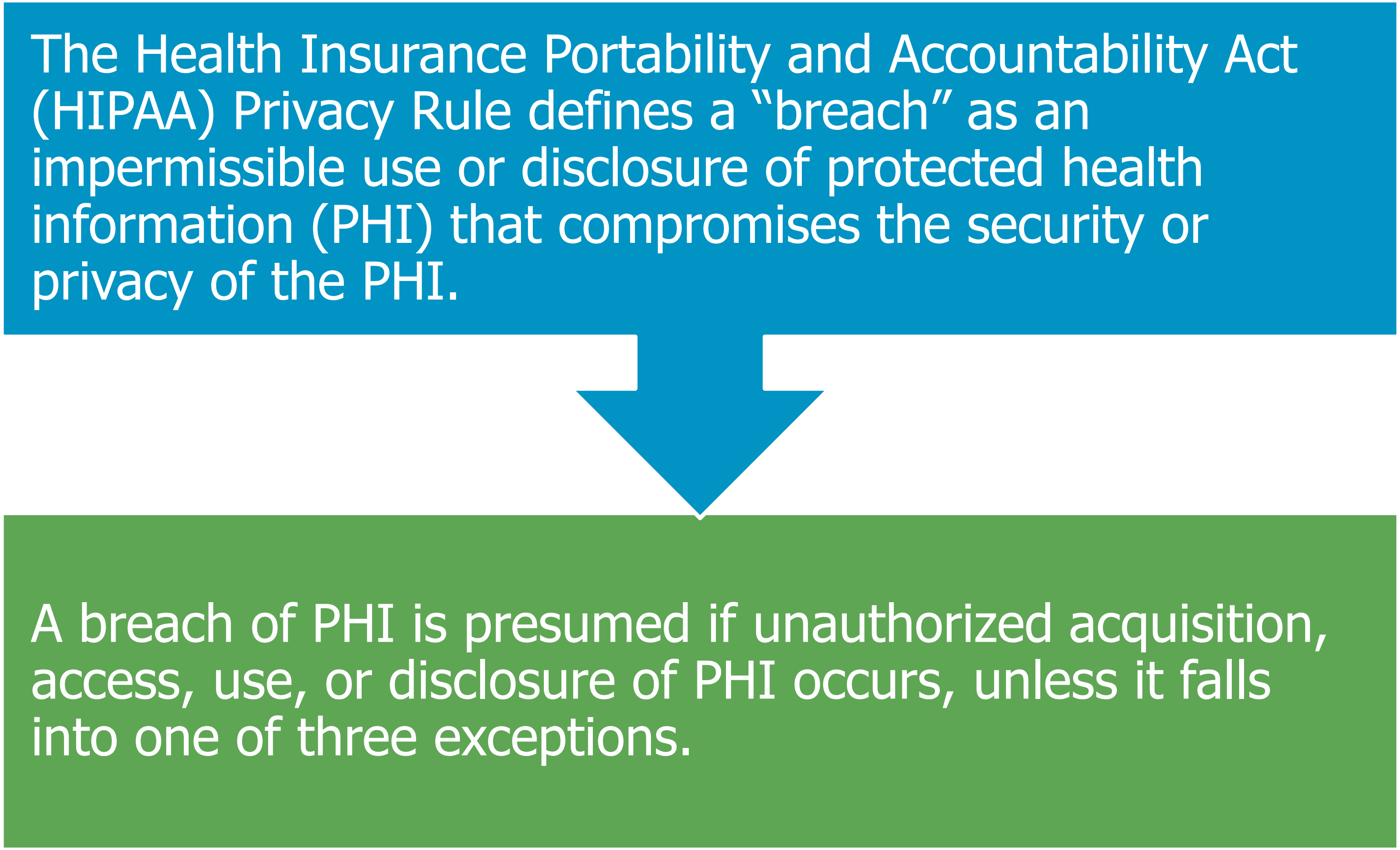
2015

Objectives

By the end of this program, participants should be able to:

- Identify top reasons why breaches occur
- Review the breach definition and notification process
- Discuss best practices for preventing breaches

Definitions



The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule defines a "breach" as an impermissible use or disclosure of protected health information (PHI) that compromises the security or privacy of the PHI.

A breach of PHI is presumed if unauthorized acquisition, access, use, or disclosure of PHI occurs, unless it falls into one of three exceptions.

HIPAA Breach Notification Rule, 45 CFR §164.402

Exceptions

1 Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity (CE) or business associate (BA), if made in good faith and within the scope of authority, and if it does not result in further impermissible use or disclosure

2 Any inadvertent disclosure of PHI by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized healthcare arrangement in which the CE participates, and the information is not further impermissibly used or disclosed

3 A disclosure of PHI in which a CE or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not reasonably have been able to retain the information

HIPAA Breach Notification Rule, 45 CFR §164.402

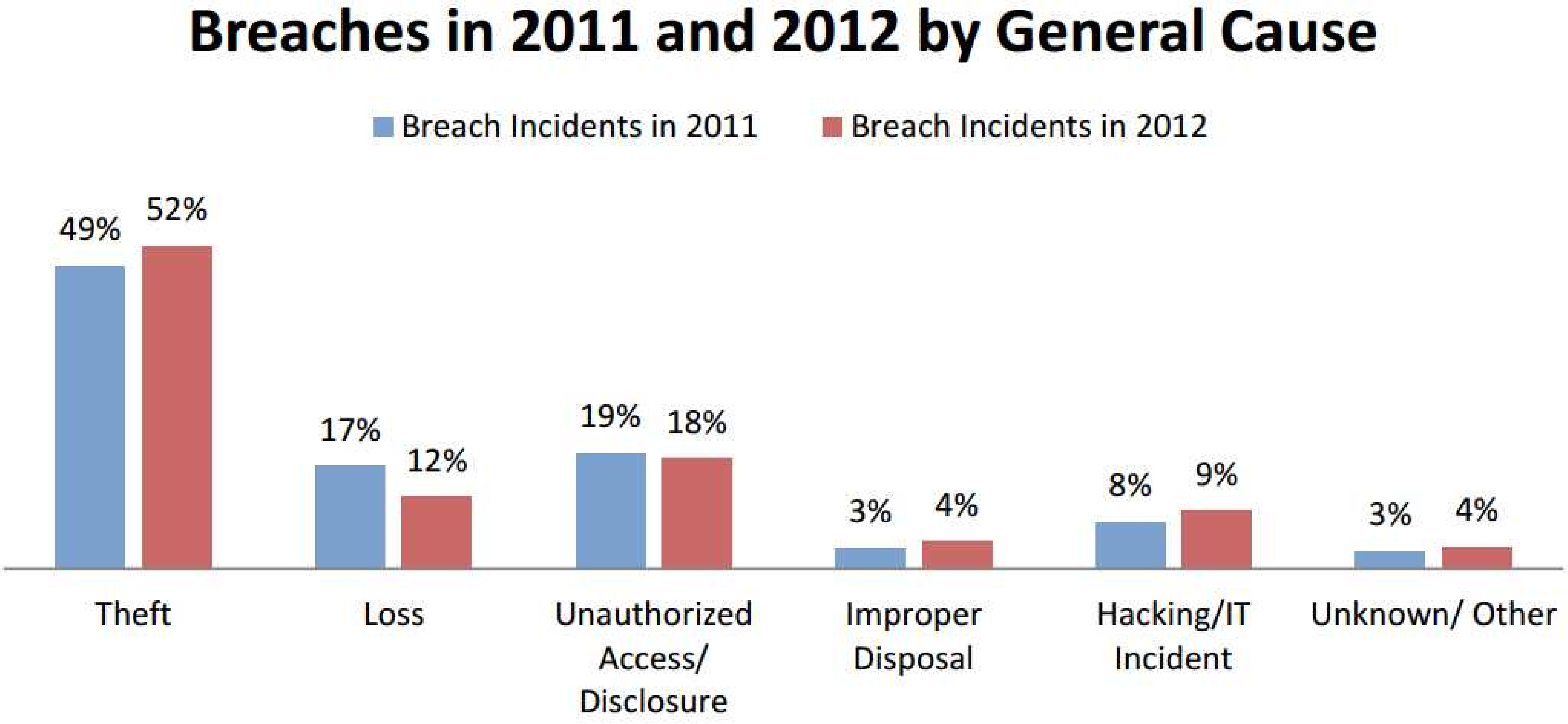
Exceptions

Impermissible use or disclosure also might not be considered a breach if a risk assessment demonstrates that there is a low probability that the PHI has been compromised based on at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
2. The unauthorized person(s) who used the PHI or to whom the disclosure was made
3. Whether the PHI was actually acquired or viewed
4. The extent to which the risk to the PHI has been mitigated

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Top causes of breaches



Office for Civil Rights. (n.d.). Annual report to Congress on breaches of unsecured protected health information, calendar years 2011 and 2012. U.S. Department of Health and Human Services. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html

Breach prevention strategies

Theft/Loss

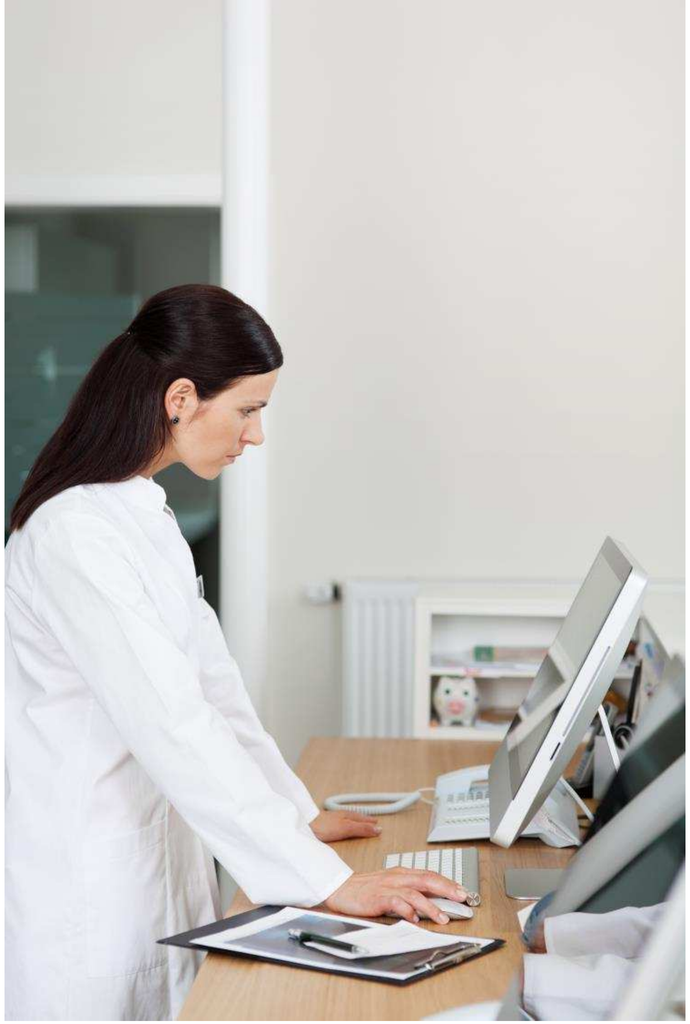
- Utilize data encryption technology for electronic PHI.
- Establish policies prohibiting storage or transfer of PHI on or to laptops, portable media, cellphones, and workstations, and implement IT systems that support these policies (e.g., use of a virtual private network (VPN) or cloud-based storage).

- Establish policies on security of laptops/workstations.

Breach prevention strategies

Unauthorized Access/Disclosure

- Limit discussions with patients concerning PHI in waiting/checkout areas.
- Limit phone messages to basic requests to the return call.
- Ensure that the release of any medical records complies with the specific request in the authorization.
- Place computers where screens are not visible in general areas.
- Routinely perform access audits.



Breach prevention strategies

Improper Disposal of PHI

- Use locked waste boxes for documents containing PHI.
- Shred documents so they can't be reproduced or read.
- Use a certified disposal company to ensure proper destruction of PHI.

Hacking

- Comply with HIPAA Security Safeguards (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf)

Other Digital Risks

- Prohibit texts containing PHI unless a secure texting platform is in place (http://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf)

Breach notification process

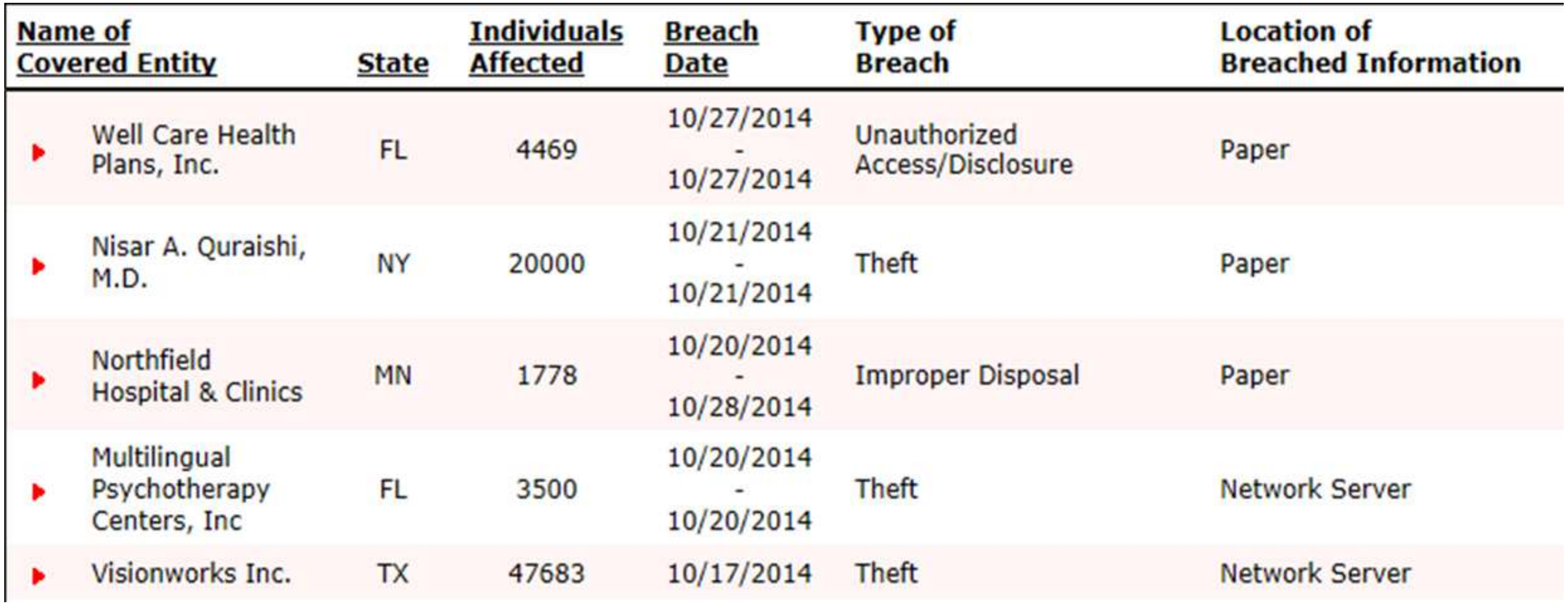
Fewer Than 500 Individuals

- Notice to the individual no later than 60 days following discovery of the breach via first-class mail or email
- Notice must include:
  - A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known
  - A description of the types of unsecured PHI involved in the breach
  - Steps that individuals should take to protect themselves from potential harm resulting from the breach
  - A brief description of what the CE is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
  - Contact information for individuals to ask questions or learn additional information

Breach notification process

Greater Than 500 Individuals

- Same timeframe and elements for individual notice
- Must provide notice to prominent media outlets serving the state or jurisdiction
- Breach is posted on the U.S. Department of Health and Human Services (HHS) website



	Name of Covered Entity	State	Individuals Affected	Breach Date	Type of Breach	Location of Breached Information
▶	Well Care Health Plans, Inc.	FL	4469	10/27/2014 - 10/27/2014	Unauthorized Access/Disclosure	Paper
▶	Nisar A. Quraishi, M.D.	NY	20000	10/21/2014 - 10/21/2014	Theft	Paper
▶	Northfield Hospital & Clinics	MN	1778	10/20/2014 - 10/28/2014	Improper Disposal	Paper
▶	Multilingual Psychotherapy Centers, Inc	FL	3500	10/20/2014 - 10/20/2014	Theft	Network Server
▶	Visionworks Inc.	TX	47683	10/17/2014	Theft	Network Server

Civil Monetary Penalties

- Failure to comply with policies and procedures may result in corrective action.
- CEs (including individual employees) and BAs are subject to civil monetary penalties (fines) and criminal penalties.

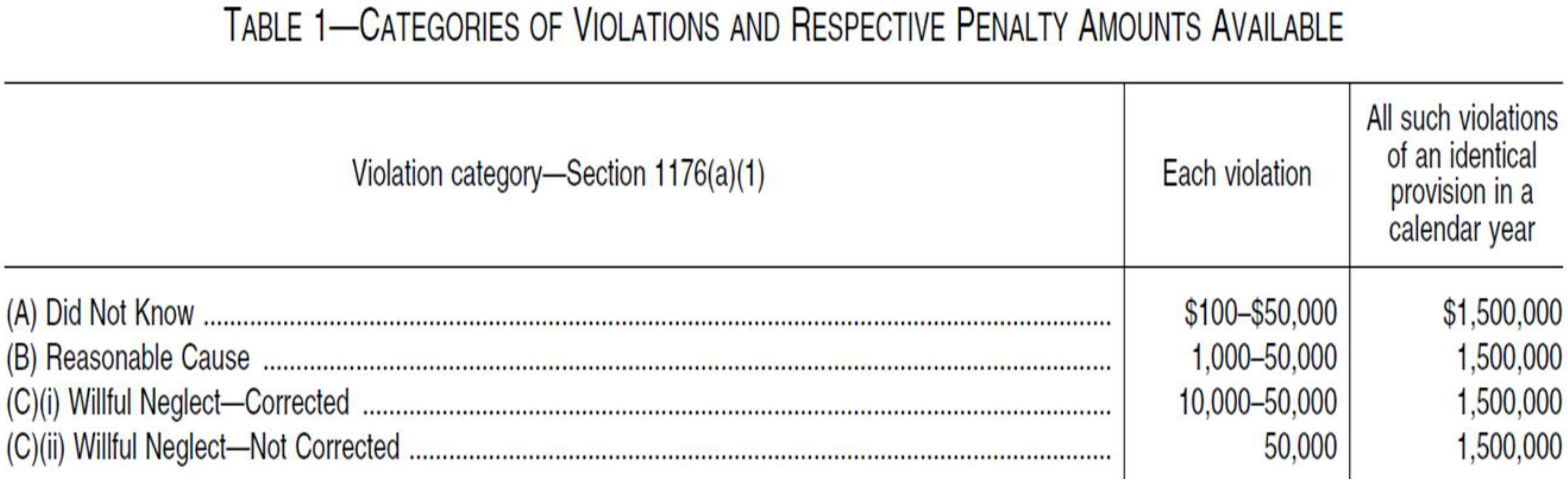


TABLE 1—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

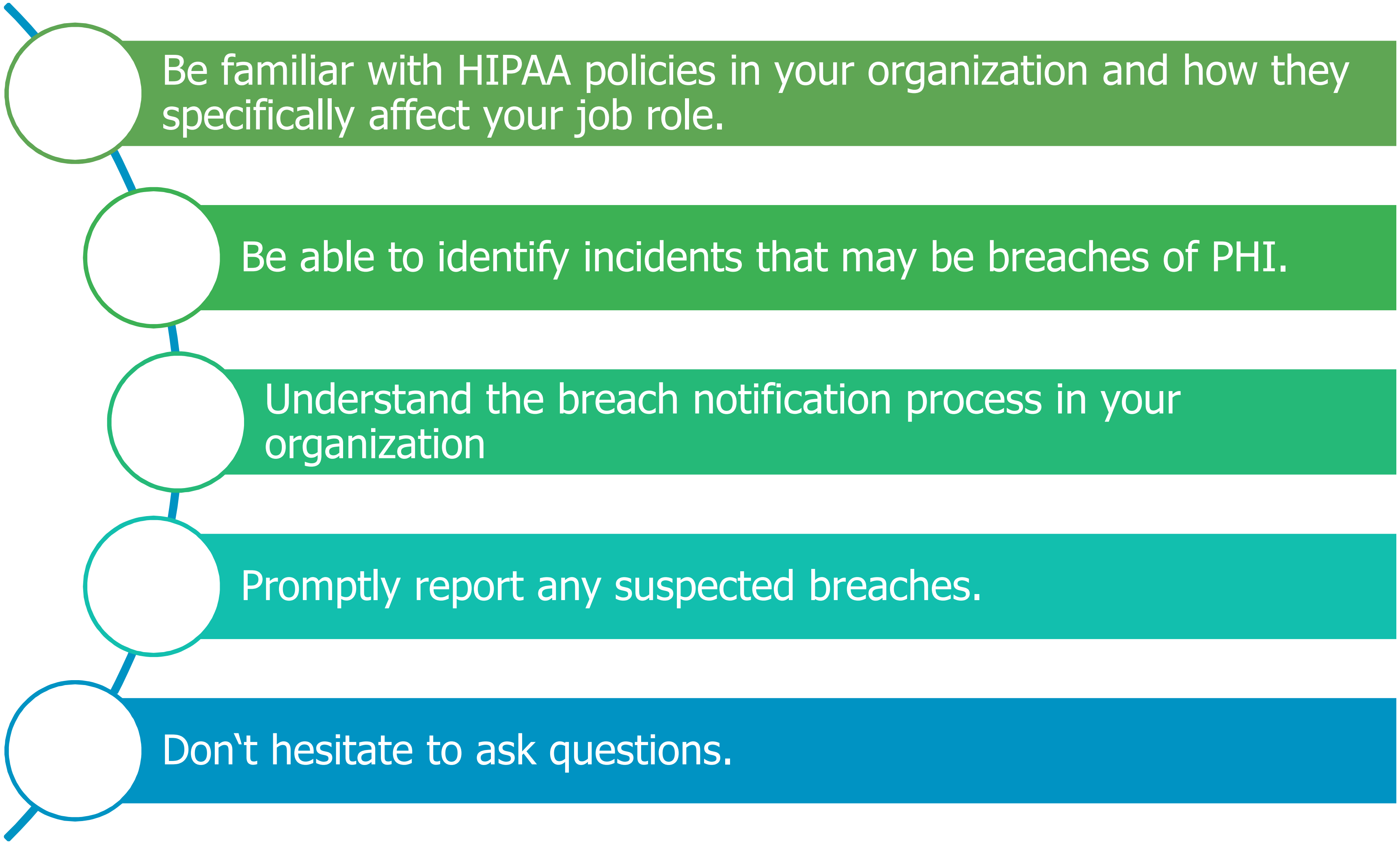
Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

Criminal Penalties

Prohibited Conduct	Penalty
Knowingly obtaining or disclosing PHI without authorization	Up to $50,000 fine and 1 year in prison
If done under false pretenses	Up to $100,000 fine and 5 years in prison
If done with intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm	Up to $250,000 fine and 10 years in prison

42 U.S.C. § 1320d-5(d)

Summary



- Be familiar with HIPAA policies in your organization and how they specifically affect your job role.
- Be able to identify incidents that may be breaches of PHI.
- Understand the breach notification process in your organization
- Promptly report any suspected breaches.
- Don‘t hesitate to ask questions.