How to Determine if an Incident is a HIPAA Data Breach to Ensure Legal Compliance

Rick Kam, CIPP

March 22, 2016

id experts®

Agenda

- What is a HIPAA Data Breach?
- Multi-Factor Risk Assessment
- Data Breach Notification
- Resources
- Q&A

id experts®

Event vs. Incident vs. Breach

- Event – Any observable occurrence in a system or network (NIST)

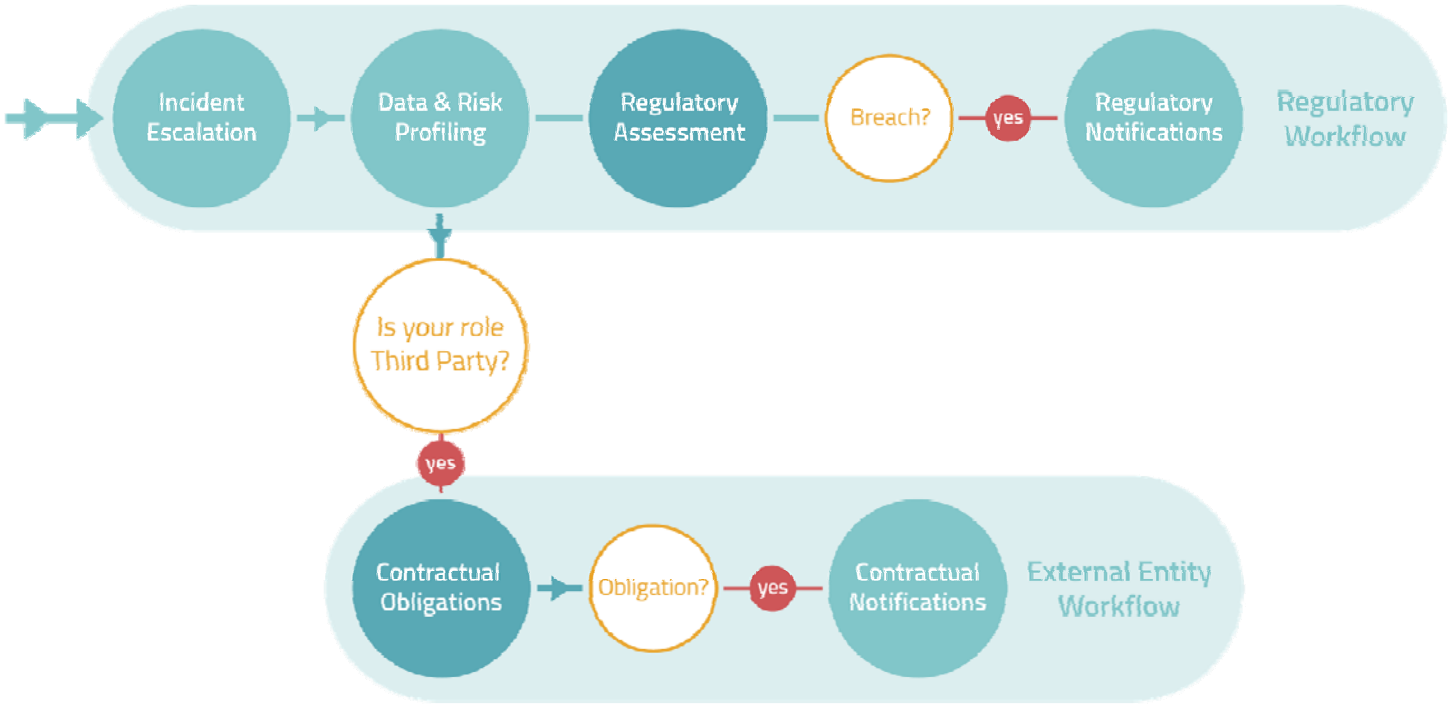
- Incident – Any Event that violates an organization's security or privacy policies involving sensitive information

- Breach – Any Incident that meets specific legal definition per state or federal breach laws and requires notice to affected individuals….
  - Presumption of breach, unless ***low probability*** the PHI has been ***compromised*** after multi-factor risk assessment (HIPAA)
  - Presumption of breach if there risk of harm (most states)

Not A HIPAA Data Breach

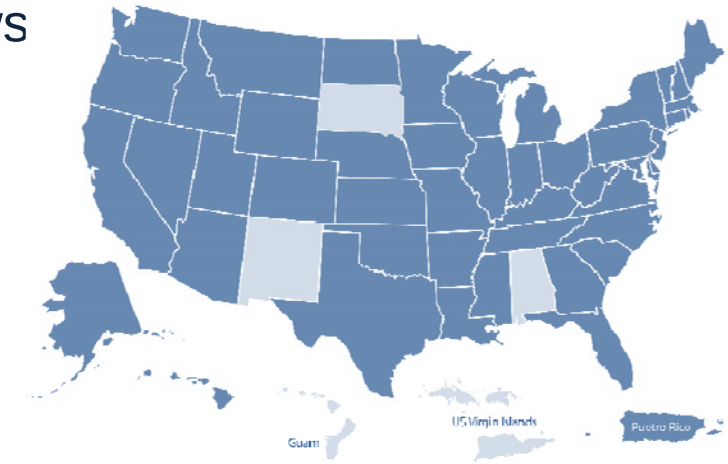
- Electronic PHI has been encrypted
- The media on which PHI is stored or recorded has been destroyed

Incident Lifecycle: Assessment & Compliance



Data Breach Notification Laws

- 51 state and territory breach notification laws
  - Differ with respect to:
    - Definitions
    - Risk of harm
    - Safe harbor
    - Exemptions
    - Timing
    - Content
    - Notice to regulators, agencies, etc.
- A plethora of federal laws & other standards
  - HIPAA Omnibus Final Rule
  - GLBA, PCI



id experts®

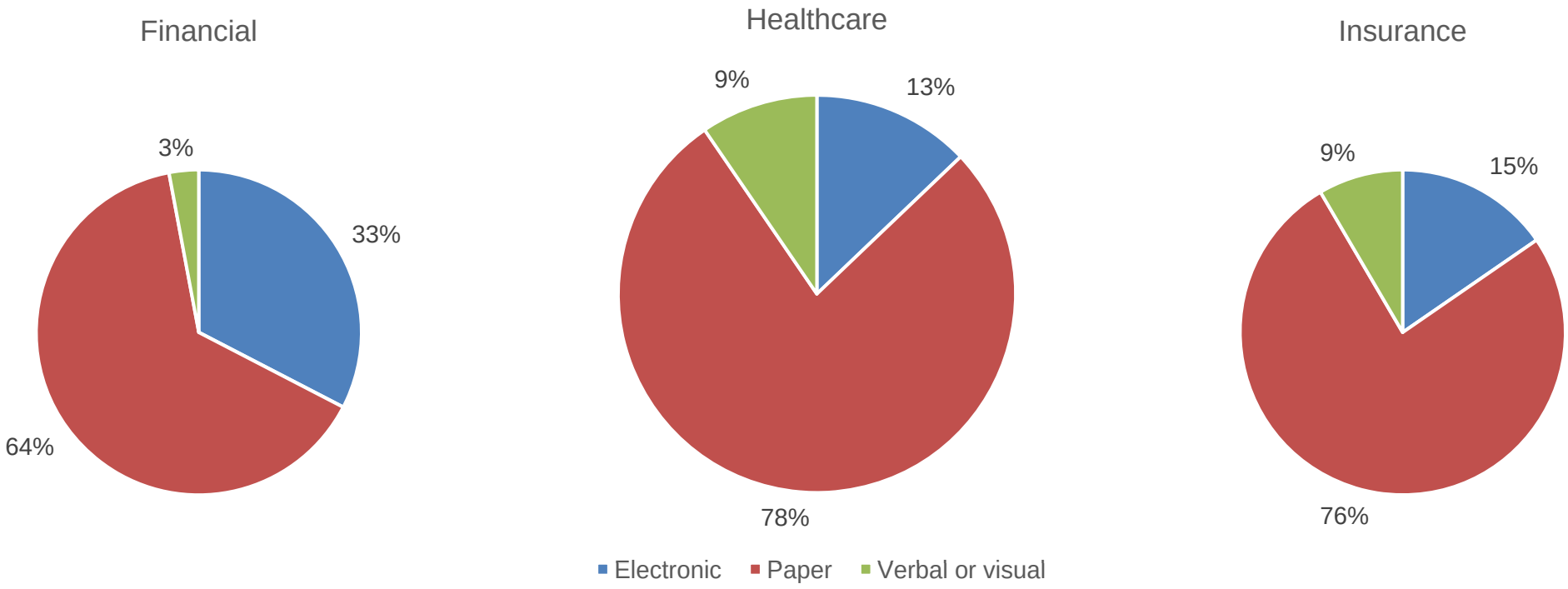
Recent Changes To Breach Laws

	Effective Date	Notification Content Required (New)	AG Notice (New)	PII Expansion / Revision	Medical and Insurance info. (added)	Medical Record Info. (added)	Health Insurance ID # (added)
Wyoming (SF 35 & 36)	7/1/15	Y		Y	Y		
Nevada (AB 179)	7/1/15			Y			Y
Washington (HB 1078)	7/24/15	Y	Y				
North Dakota (SB 2214)	8/1/15		Y	Y			
Montana (HB 74)	10/1/15		Y	Y		Y	

Multi-Factor HIPAA Risk Assessment

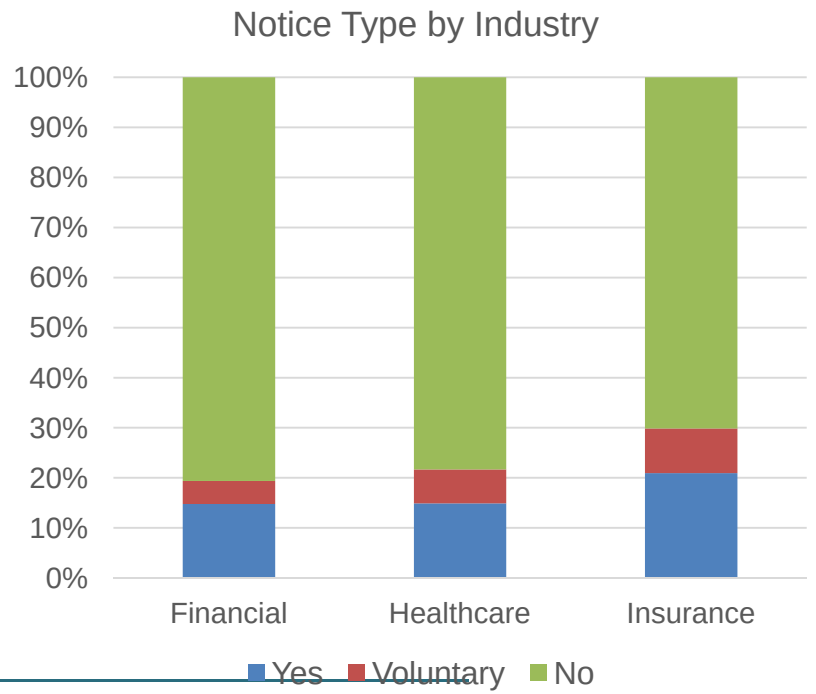
- Nature and extent of PHI involved
- Recipient & intent
- Access/viewing/re-disclosing
- Risk mitigation

Incident Categories by Industry



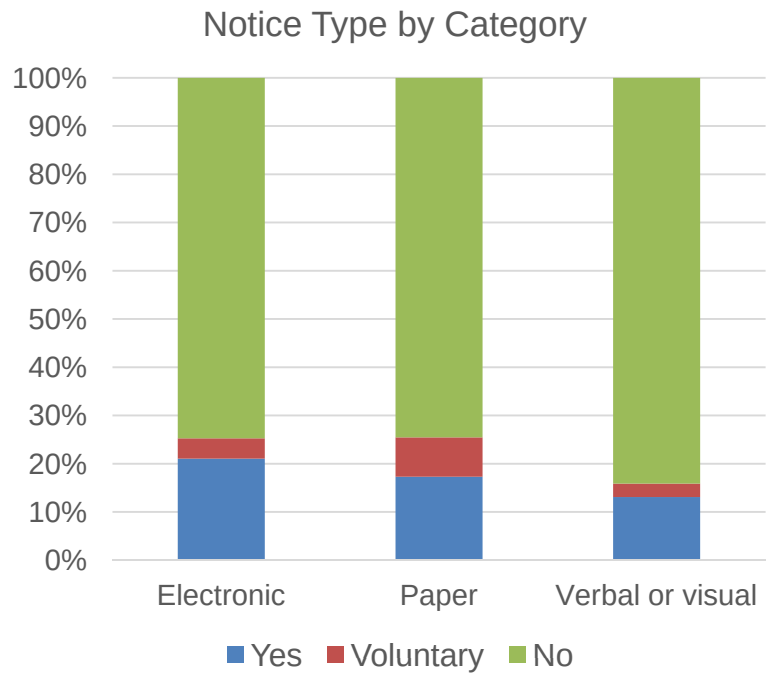
Decision to Notify

	% Decision to Notify
Financial	15% to 19%
Healthcare	15% to 22%
Insurance	21% to 30%
Aggregate	18% to 25%

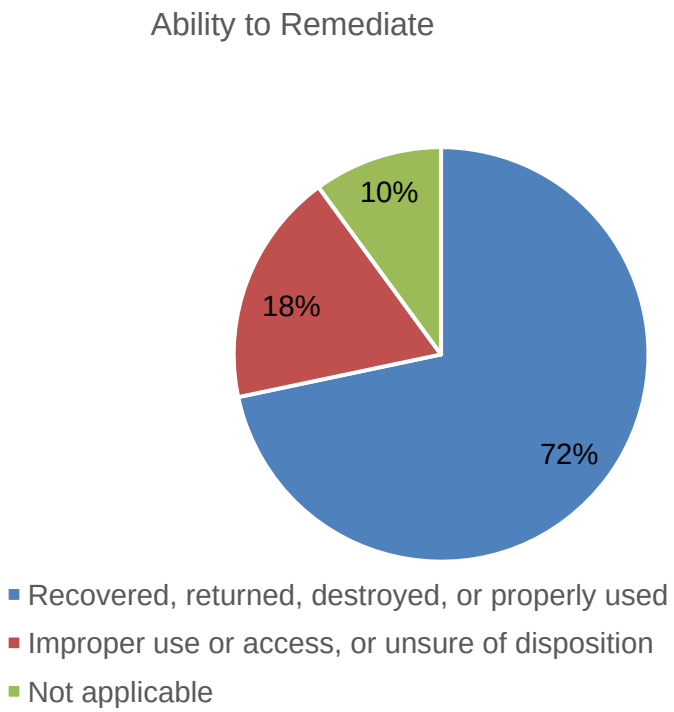


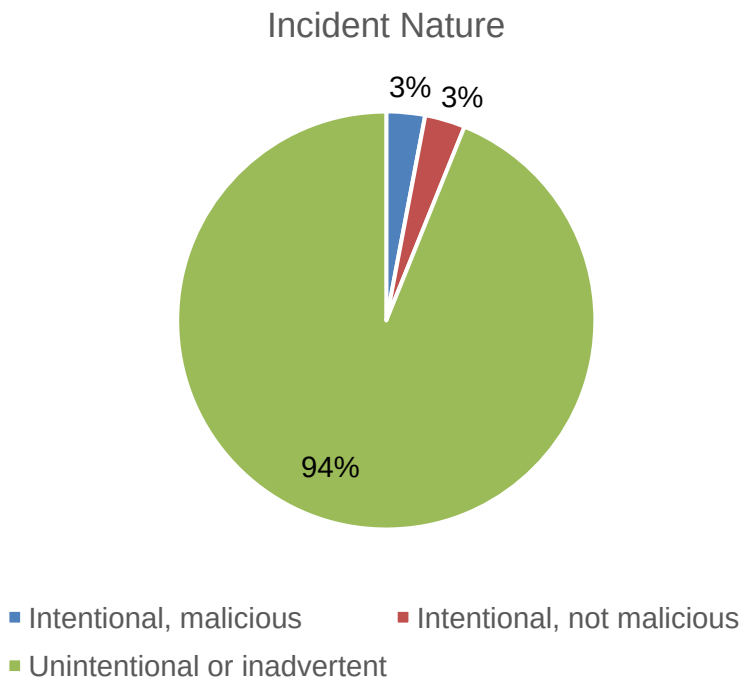
Notification by Category

	% Decision to Notify
Electronic	21% to 25%
Paper	17% to 25%
Verbal or visual	13% to 16%
Total	18% to 25%



Ability to Remediate and Incident Nature





Resources

- HHS.gov Health Information Privacy website
- OCR Breach Portal
- ID Experts Guide to Breach Response whitepaper

Q&A

Rick Kam

Rick.Kam@idexpertscorp.com

971-242-4705