

Is Your Security Incident a Data Breach? Uncle Sam Wants to Know

Panelists:

Patricia (PC) Shea, Partner, K&L Gates

Laura Merten, Chief Privacy Officer, Advocate Health Care

Asra Ali, Compliance and Risk Manager, HealthScape Advisors

Mahmood Sher-Jan, CEO, RADAR, Inc.

Agenda

Each Panelist will Discuss a Topic, Followed by a Brief Break and Open Discussion

- Patricia (PC) Shea, Partner, K&L Gates
- Laura Merten, Chief Privacy Officer, Advocate Health Care
- Asra Ali, Compliance and Risk Manager, HealthScape Advisors
- Mahmood Sher-Jan, CEO, RADAR, Inc.
- BREAK
- Panel Discussion



K&L GATES

Basic Framework & Compliance Tips

Navigating HIPAA

Patricia Shea

patricia.shea@klgates.com

© Copyright 2017 by K&L Gates LLP. All rights reserved.

K&L GATES

THE FRAMEWORK

- Health Insurance Portability & Accountability Act of 1996 (HIPAA)
- Implementing Regulations
 - Privacy Rule – oral, documents, electronic
 - Security Rule - electronic
 - Breach Notification Rule - unsecured
 - Enforcement Rule

klgates.com

4

OVERSIGHT

- United States Department of Health and Human Services, Office for Civil Rights (OCR)
 - Investigate reports of breaches
 - Investigate complaints from individuals
 - Conduct compliance audits

HIPAA'S LANDSCAPE

- Complex
- Stressful
- Constant
- Evolving



THE Rule for HIPAA Compliance



K&L GATES

KNOWLEDGE IS POWER ...

The more you know about HIPAA and your obligations, the better positioned you will be to comply.

1. KNOW HIPAA'S CORE TERMS

- Individually identifiable health information
- Protected health information (PHI)
- Covered entity
- Workforce
- Business associates

1. KNOW HIPAA'S CORE TERMS (CONT.)

Individually identifiable health information

- Is created or received by a health care provider, plan, or clearinghouse; or employer; and
- Relates to the past, present, or future physical or mental health or condition of an individual (or payment for health care to the individual); and
- Identifies the individual or reasonable could be used to identify the individual

1. KNOW HIPAA'S CORE TERMS (CONT.)

Protected health information (PHI) is *IIHI* that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

1. KNOW HIPAA'S CORE TERMS (CONT.)

PHI **excludes** *IIHI* in:

- Education records covered by the Family Educational Rights and Privacy Act
- Records described at 20 USC 1232g(a)(4)(B)(iv)
- Employment records held by a covered entity in its role as an employer

1. KNOW HIPAA'S CORE TERMS (CONT.)

Covered entity

- Health plan
- Health care clearinghouse
- Health care provider who transmits any health information in electronic form in connection with a standard transaction (e.g., claims for payment for services)

Most important term because it triggers HIPAA.

1. KNOW HIPAA'S CORE TERMS (CONT.)

Workforce

- Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity

1. KNOW HIPAA'S CORE TERMS (CONT.)

Business Associates

- Perform services **on behalf of a covered entity** that require the use or disclosure of PHI.
- Perform services **on behalf of another business associate** that require the use or disclosure of PHI.
- No limit to the number of business associates performing services on behalf of a covered entity or another business associate of the covered entity.

2. KNOW THE KEY PLAYERS

- Privacy Officer
- Security Officer
- Counsel (in-house and outside)

3. KNOW THE KEY DOCUMENTS

- Policies and procedures
- Notice of Privacy Practices
- Business Associate Agreements

4. KNOW THE GOLDEN RULE

You may not use or disclose PHI unless HIPAA permits or requires you to do so.

- Good news = HIPAA likely permits use and disclosure for majority of covered entity's operations
- Bad news = Lots of ways to unintentionally violate the rule

5. KNOW WHEN YOU MUST DISCLOSE PHI

- To the individual when requested in accordance with HIPAA's provisions
- To the Secretary of the United States Department of Health and Human Services for purposes of investigating compliance with HIPAA

6. KNOW WHEN YOU MAY DISCLOSE PHI

- For treatment, payment, and health care operations purposes
- To your business associates if you have a business associate agreement in place
- Research, law enforcement and other purposes as long as requirements for those disclosures are satisfied

7. KNOW REQUIRED EPHI SAFEGUARDS

Administrative, technical, and physical safeguards are specified

- Some are required
- Some are addressable (but not optional)

Safeguards are designed to protect the confidentiality, availability, and integrity of ePHI

- Risk assessment and risk management plans are key
- Must be updated appropriately

8. KNOW WHEN YOU HAVE A BREACH

- Unpermitted access, acquisition, use or disclosure of PHI not permitted by HIPAA (with some limited exceptions)
- Applies to PHI not secured in the manner specified by the Secretary of the Department of Health and Human Services
- May require notification to the affected individuals, Secretary and others if the PHI has been compromised

9. UNDERSTAND INDIVIDUALS' RIGHTS

- Right to access their PHI
- Right to amend inaccurate PHI
- Right to an accounting of disclosures of their PHI
- Right to complain to you or to OCR about your policies and procedures or your compliance with them
- Right to request additional restrictions on disclosures of their PHI
- Right to request confidential communications

klgates.com

23

10. KNOW THE PENALTIES

Civil penalties up to \$1 million per identical penalty per year

- Typically more than one violation so the penalties can grow substantially very quickly
- Various factors affect the amount, depending on whether the violation was willful

Criminal penalties up to an including incarceration

klgates.com

24


WHEN IN DOUBT

Don't do anything without checking with the
Privacy and/or Security Officers

Keys to Building a Culture of Privacy: CPO Perspective

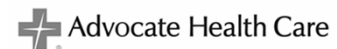
Laura Merten, JD, CCEP

Chief Privacy Officer

 Advocate Health Care

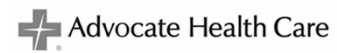
Privacy Thought Leadership

- Strategic Approach
- Prospective versus Responsive
- Stakeholders & Relationships



Cross Functional Support

- CIO, CTO, CISO
- Marketing, Business Development
- HR
- HIM
- Internal Audit
- Supply Chain
- Research, Other Business Functions



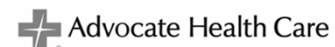
Privacy Compliance Framework

- Types of Data Collected
- How Data is Kept
- Location of Data
- Data Security Measures
- Business Unit or Individual Data Owner
- Privacy Risk Assessments
- Legal Requirements and Compliance Roadmap



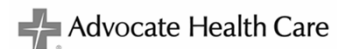
Policies and Internal Controls

- External Policy Statements
- Internal Policies and Procedures
- Procedures Related to Incidents
- Internal Reporting Mechanisms
- External Reporting Mechanisms
- Policies and Procedures for Incident Communication



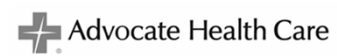
Privacy Compliance Tools

- Risk Analysis
- Event and Incident Tracking
- Incident Analysis
- Vendor Management and Risk Analysis



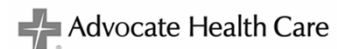
Vendor Management

- Vendor Identification
- Risk Analysis
- Stakeholders
- Process
- Tools



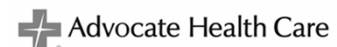
Training and Awareness Programs

- Annual Computer-Based Training
- Incident Response Training
- Trend Training
- Form of Training
- Emails, System Screensavers, Intranet



Revising Program Controls, Policies and Procedures

- New Threats or Risks
- Expansion into New Business Areas
- Evolving Industry Standards
- Law and Regulatory Changes
- Monitoring and Auditing
- Benchmarking and Complaints
- External Program Review



Breach Investigation and Determination

Real World Scenarios

Asra Ali, CHC, CHPC, Compliance and Risk Manager at HealthScape Advisors



Breach Investigation and Determination

- Four factor analysis per HIPAA
- Collect facts as soon as possible
 - Interviews
 - Incident Intake Form
- Core Team
 - Privacy Office
 - Manager
 - Associates involved
 - If a breach is determined, involve a high level executive to determine next steps
 - Outside Counsel

Real World Scenario #1

- Employee Data Disclosed through Unencrypted Email
 - Email sent by HR to insurance carrier with sensitive employee data
 - Method: Unencrypted email
 - Investigation
 - Core team: Compliance, IT, HR
 - Interviews
 - Determination
 - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - The unauthorized person who used the protected health information or to whom the disclosure was made;
 - Whether the protected health information was actually acquired or viewed;
 - The extent to which the risk to the protected health information has been mitigated.
 - Mitigation
 - Credit monitoring?
 - Notification
 - Employee training

Real World Scenario #2

- Stolen Laptop in combination with paper records
 - Employee left laptop in a backpack.
 - Vehicle parked on private property.
 - Vehicle is broken into and the backpack is stolen. Paper medical records are also missing.
 - Investigation
 - Police report?
 - Interviews
 - Core team: Executive presence
 - Determination
 - Was the laptop encrypted?
 - What data was included in the medical records?
 - Type of “records”?
 - Mitigation
 - Notification
 - Call center?
 - Insurance coverage?

Current Industry Issues

Cybersecurity/Cyberliability

Phishing

Cybersecurity/Cyberliability

- **Internal Practices**
 - Penetration Testing
 - Mobile Devices and Wireless Networks
 - Cloud Services
 - Risk Assessments
 - Employee Data
 - Policies and Procedures
- **Vendor Contracts**
 - Risk Assessments
 - SOC Reports
 - Insurance Coverage
- **Definition of Data**
 - State level
 - Other key statutes

Trending Issues

- W2 Scams
- FTC email scam
- Phishing
- Ransomware

Phishing

- What is “Phishing”?

'fiSHiNG/

Noun

The activity of defrauding an online account holder of financial information by posing as a legitimate company.

- 1990s: inspired by *fishing*, on the pattern of *phreaking* .



What Does a Phishing Email Look Like?

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form;

http://www.facebook.com/application_form

Links in email

Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.

Popular company

Source: <https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx>

Real World Scenario #3

- Phishing
 - Scenario #1: Employee clicks on a link through email that looks like it coming from the CEO, asking for payroll information.
 - Information hacked: employee names, SSNs, 2015 wages earned, states of residence, states of work, employees' contributions to their retirement accounts, taxes withheld
 - Breach?
 - Investigation
 - Core Team
 - Remediation
 - Notification

Ransomware

Cybersecurity/Cyberliability

Phishing

Ransomware

Ransomware

- Ransomware
 - ran·som·ware
 - *noun*
 - a type of malicious software designed to block access to a computer system until a sum of money is paid.
 - Uses cryptotechnology to encrypt files
- Why is it so successful?
 - Victim generally do not use scrutiny when receiving emails (email overload)
 - Employees generally are not trained on what to look for
 - Email is primary vector for attacks
 - Cyber criminals getting better at creating content to trick users
 - Oversharing of personal information through public social media outlets
 - Allows cyber criminals to personalize content



What Does Ransomware Look Like?



Tips and Tools on Incident Response

- Determine basic level of severity
 - Laptop missing versus lost work badge
- Determine which team(s) you want to engage
 - Core team?
- Conduct formal risk analysis
 - Radar
- Document all steps
- Does outside counsel need to be involved?

External versus Internal Review and/or Investigations

- When to involve outside counsel?
 - Company culture
 - Internal role
 - Transactions and business initiatives
 - Compliance Department
 - Familiarity with privacy and state laws
 - Level of severity
 - Risk analysis
 - Policies and procedures
 - Independent review



Trends in Changing Data Breach Laws

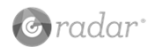
Mahmood Sher-Jan, CHPC, CEO and Founder of RADAR, Inc.



Overall: Increased Stringency and Growing Complexity



- 20 states and one territory now specify the contents of required notifications to individuals.
- 12 states and one territory now regulate medical information as PII.
- 23 states now require notice to the attorney general under specified circumstances.



Expanding Scope of Personal Information

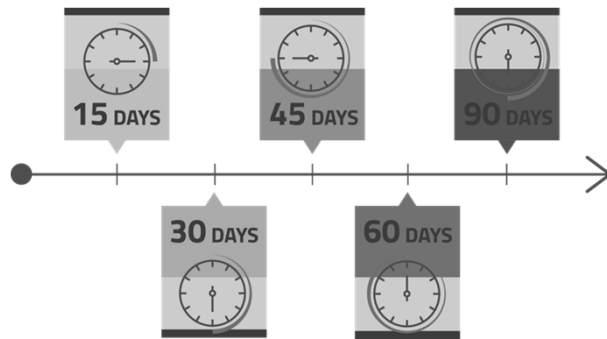


How a state defines personal information hugely impacts what's acceptable in terms of disclosure and access. States that have recently expanded the definition of personal information:

- Illinois (HB 1260)
- Nevada (AB 179)
- Oregon (SB 601)

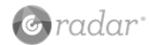


Increased Specificity of Timelines



Many state breach notification laws have ambiguous timelines when a breach of personal information requires notification to impacted individuals. States that have recently added more specific timelines:

- Connecticut (SB 949)
- Washington (HB 1078)
- Rhode Island (SB 134)
- Tennessee (SB 2005)

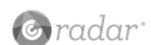


Specifying Notification Contents



In many states, initial data breach notification legislation didn't include guidance as to what information a notice to affected individuals should contain. States that have recently updated their notification requirements:

- California (SB 570)
- Wyoming (SF 35)
- Rhode Island (S 0134)



Adding the Requirement to Notify State Attorney

General

With the number of high profile data breaches on the rise, state attorneys general are adding requirements to be notified under certain circumstances. Recently:



- Illinois (HB 1260)
- Montana (HB 74)
- Oregon (SB 601)
- Rhode Island (SB 134)



Operationalizing Incident Response Management

Five Things to Operationalize



1. Timely & Efficient Intake
2. Multi-Factor Risk Assessment
3. Breach Notification Letters
4. Trend Analysis & Reporting
5. Staying Current with Laws



1. Incident Intake

- Configurable Web Forms
- Efficient for getting the required incident details
- Automated alerts to privacy & security
- APIs for Integration
- Purpose-built Workflow



Manual,
ad-hoc intake



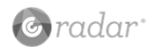
Purpose-Built
Workflow



2. Multi-Factor Risk Assessment



- a) Consistency
- b) Efficiency & Agility
- c) Collaboration
- d) Legal Oversight
- e) Decision-Support
- f) Burden-of-proof



Four-Factors Risk Assessment

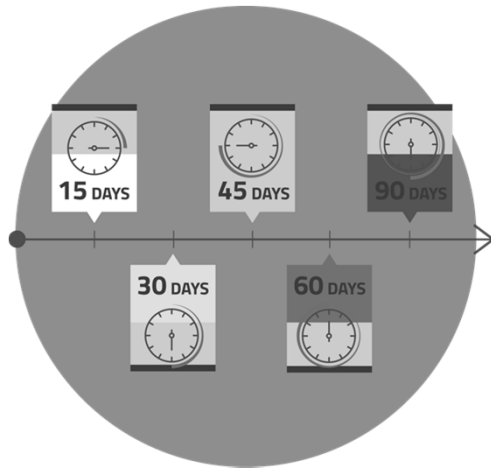


HIPAA Breach Notification Rule **Risk Factors**

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
2. The unauthorized person 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



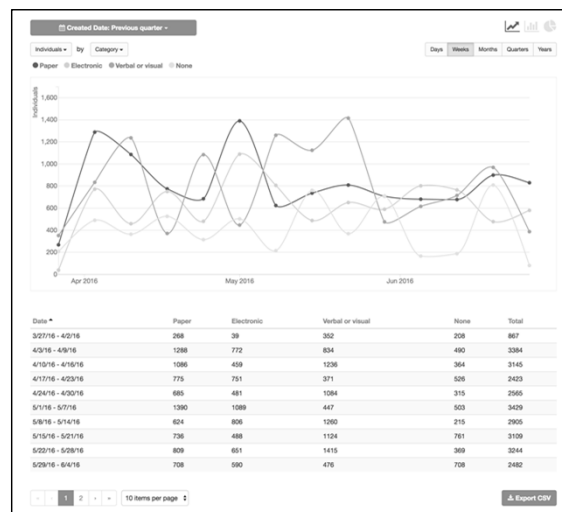
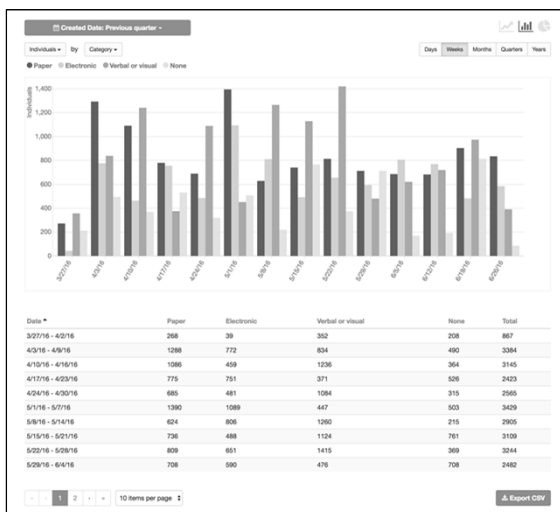
3. Breach Notification Letters & Documentation



- Integrated system that manages complete IR lifecycle
- Approved Letter Templates for Individuals, Agencies, Clients
- Central repository of all notifications to Prove Compliance
- Pay special attention to deadlines, content, format – even font size.



4. Analyze Trends, Measure, and Improve



Example Key Performance Indicators



- Average time between incident discovery and reporting to privacy office, from incident creation to closure, or to perform a multi-factor risk assessment



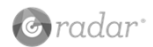
- Percentage of incidents requiring mandatory notification, contractual notification, or involving multiple jurisdictions



- Frequency of missing notification due dates (regulatory & contractual)



- Trends in incident volume by category (electronic, paper), incident type and number of records, or incident source (internal or 3rd party) & root cause



5. Staying Current with Regulations

Difficulties keeping up with changing laws and strict notification timelines

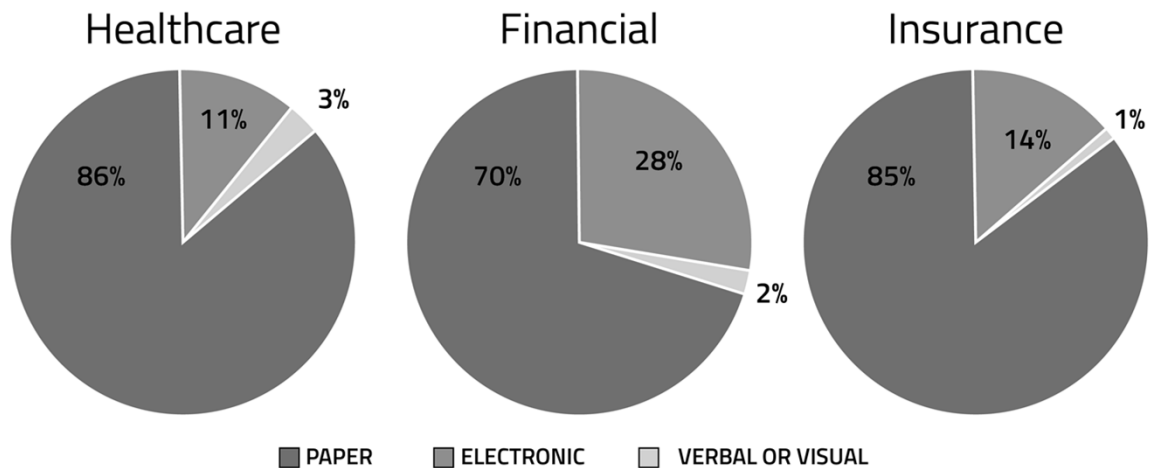
Always current with breach laws, exceptions and notification deadlines



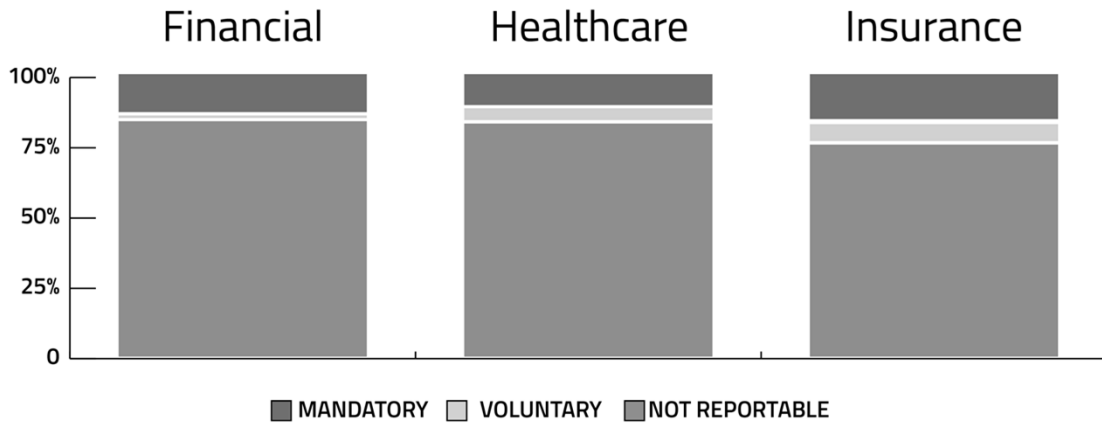
Data Driven Insights

Incidents vs Breaches

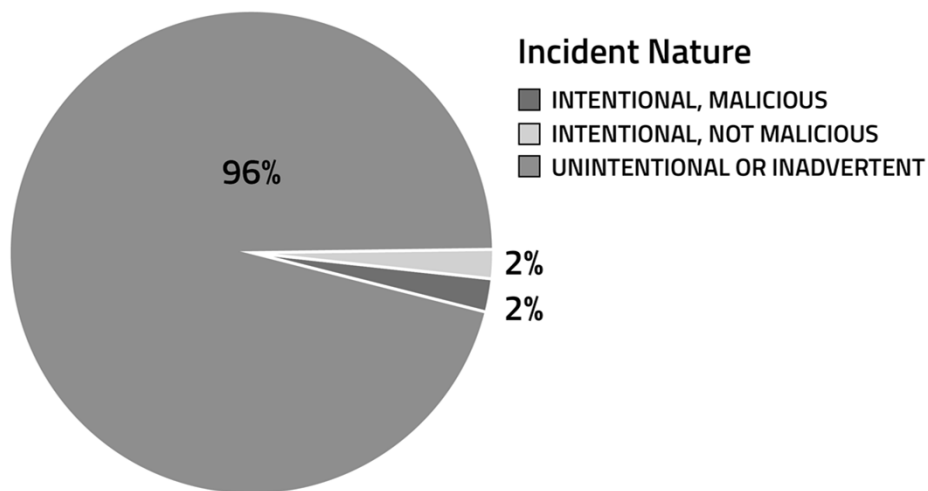
Electronic incidents may expose more records per incident, but paper incidents are much more commonplace



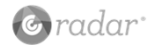
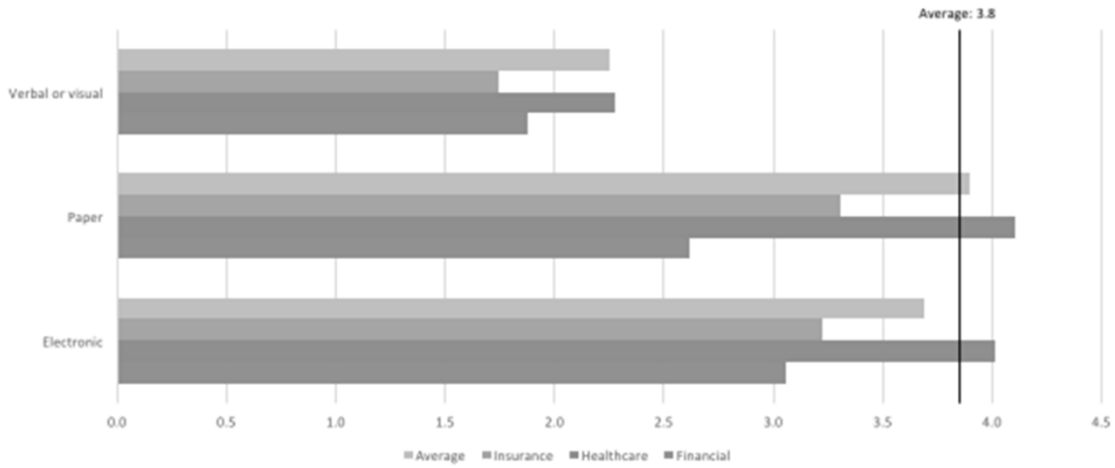
The majority of incidents, risk mitigated and run through a multi-factor risk assessment, do not meet breach threshold.



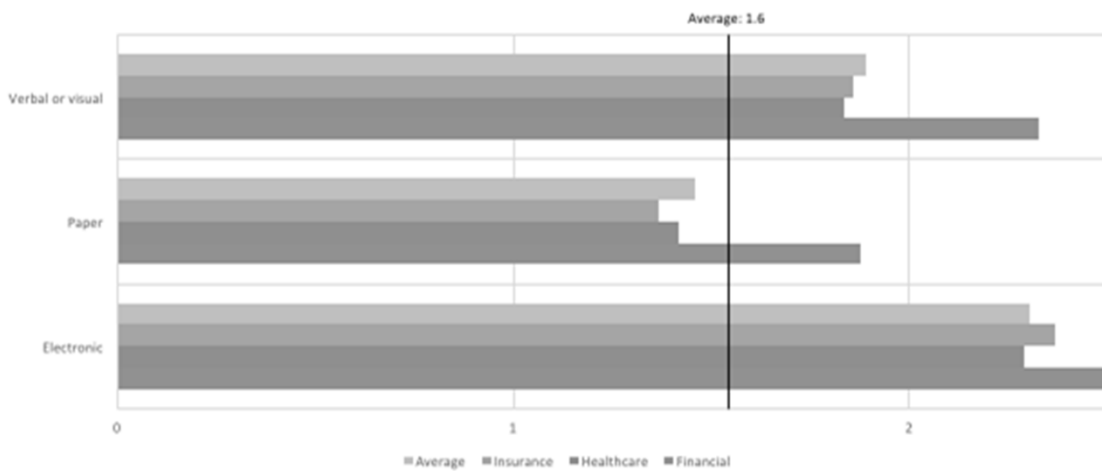
The majority of incidents occur due to human error, not malicious intent. Prepare for scenarios resulting from malicious activities & mishaps



Number of Data Elements per Incident (by Category and Industry)



Number of Jurisdictions per Incident (by Category and Industry)



10 Minute Break, Followed by Panelist Discussion

Panel Discussion



Questions?