

# Cyber Attacks in the Healthcare Industry

## Healthcare Compliance Association – Columbus Regional Conference

May 3, 2019

**Paulette M. Thomas, Esq.**  
Counsel  
Baker & Hostetler LLP  
312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202  
513.929.3483  
[pmthomas@bakerlaw.com](mailto:pmthomas@bakerlaw.com)  
Blog: [www.dataprivacymonitor.com](http://www.dataprivacymonitor.com)

BakerHostetler  
BakerHostetler

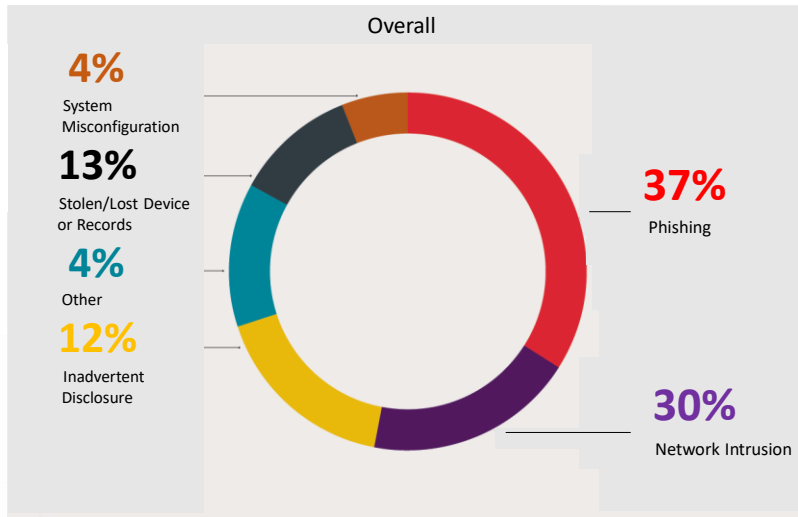
1

## AGENDA

- Cyber Risk Landscape
- Incident Response
- Notification
- Legal Landscape
- Risk Management Strategies
- Questions

2

## Cyber Risk Landscape Incident Causes



Source: BakerHostetler 2019 Data Security Incident Response Report <sup>3</sup> BakerHostetler

## Data Breach Cost Per Record

- Health - \$408
- Financial - \$206
- Technology \$170
- Education \$166
- Commercial \$128

IBM and Ponemon Institute, UC  
July 2018

<sup>4</sup> BakerHostetler

# Most Common Threats to Healthcare Organizations

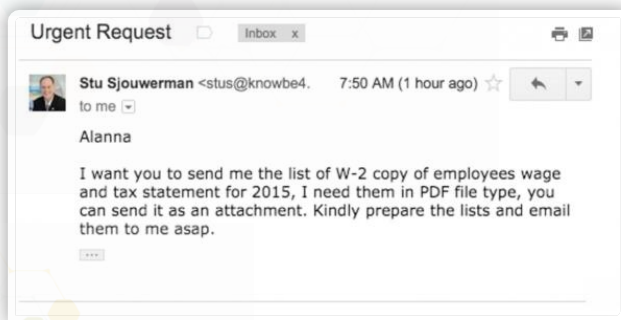
- E-Mail Phishing Attacks
- Ransomware Attacks
- Loss or Theft of Equipment or Data
- Insider, accidental, or intentional data loss
- Attacks against connected medical devices that affect patient safety

Health Industry Cybersecurity Practices:  
Managing Threats and Protecting Patients  
U.S. Department of Health & Human Services  
Healthcare & Public Sector Coordinating Council  
December 28, 2018

5 BakerHostetler

## W-2 & Business Email Compromise

- ♥ Hackers use emails from a target organization's CEO, asking human resources and accounting departments for employee W-2 information:



6 BakerHostetler



7

## The Privacy “Patchwork”

- Federal & state laws govern the handling of PII/PHI
  - Laws covering SSNs / disposal of PII
  - Employment-related laws (e.g. FMLA, ADA, GINA)
  - Other federal and state regulations (e.g. FTC Act, Mass. Regs)
- HIPAA
  - Applies to Covered Entities and Business Associates
  - Preempted except where state law is “more stringent”
- State breach notification laws
- State medical information breach reporting laws
- International data protection regulations



8 BakerHostetler



# HIPAA

## Breach by a Covered Entity

- **Applies To:** A health plan, health care clearinghouse and health care provider who transmits any health information in electronic form in connection with a covered transaction.
- **Information Covered:** Unsecured PHI– individually identifiable health information that is transmitted or maintained in electronic media or any other form or media (*encryption=safe harbor*).
- **Definition of Breach:** The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, which compromises the security or privacy of the PHI.
- **Who Must Be Notified:** The patient or their personal representative, HHS, and the media if more than 500 residents of a state or jurisdiction are affected.
- **Notification Timeframe:** Without unreasonable delay and in no case later than sixty (60) calendar days after the breach is discovered.
- **Preemption:** HIPAA preempts state law unless state law is more restrictive.

9 BakerHostetler

## Definition of “Breach” in Final Rule

- Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the HIPAA Privacy Rule is **presumed** to be a breach. . .
- **Unless** the Covered Entity or Business Associate can demonstrate that there is a **low probability that the PHI has been compromised** based on a risk assessment.



10 BakerHostetler

# HIPAA Breach Risk Assessment

- Must be documented
- Must evaluate at least the following 4 factors:
  1. *The nature and extent of the PHI.*
  2. *The unauthorized person involved.*
  3. *Whether the PHI was actually acquired or viewed.*
  4. *Extent to which any risk has been mitigated.*

## Ransomware

1. *Integrity and availability of PHI.*



11

BakerHostetler

## Incident Response Plan

### 1. Preparation

- Review and update response plan. Develop response capabilities. Test response plan. Promote awareness of plan.

### 2. Identification

- Initial incident detection, triage, and escalation to appropriate incident response team members. Formation of appropriate response team. Determine need to notify external parties.

### 3. Assessment

- Conduct analysis necessary to properly prioritize response activities, including resource needs. Begin to form communication and containment action plans. Assess preservation and mitigation needs.

### 4. Communication

- Finalize and execute any initial notification plans to internal and external parties.

### 5. Containment

- Take incident specific actions to stop the incident from continuing.

### 6. Eradication

- Determine and eliminate the cause of the incident. Repair any unauthorized changes. There is often a cycle back to identification, analysis, and containment in this phase.

### 7. Recovery

- Finalize mitigation of incident and restore system to normal operational state and implement measures to prevent incident recurrence.

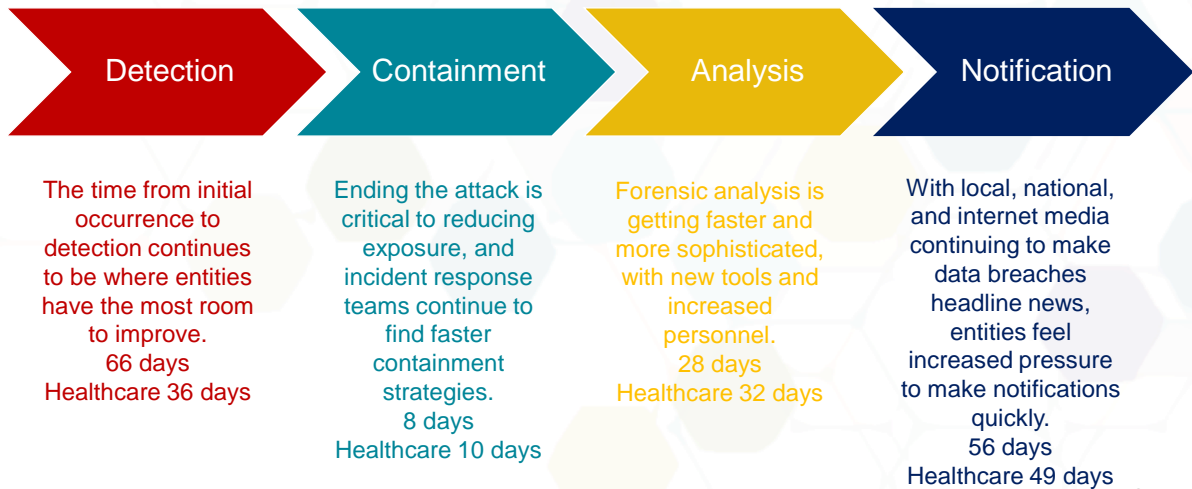
### 8. Follow-Up

- Analyze plan effectiveness and areas for improving response and security measures to prevent future incidents and be better prepared to respond to future incidents (a return to the preparation phase).

12

BakerHostetler

# Incident Response Timeline



Source: 2019 BakerHostetler Data Security Incident Response Report <sup>13</sup> BakerHostetler

## Let Forensics Drive the Decision Making

- ❖ Know your environment, have accurate network diagrams, log access, and internal imaging/collection capabilities to identify and locate critical data and assets.
- ❖ Vet several vendors and negotiate the MSA before an event happens.
  - ❖ Do on-boarding with primary forensic firm before an incident
  - ❖ Review technical incident response capabilities and run books pre-incident.
  - ❖ Cyber insurance carrier panel of approved firms
- ❖ Have a backup – one firm may not be available or appropriate for all events.
- ❖ Retain legal counsel for incident response that understands technology and cyber issues to reduce response time.
- ❖ Establish protocols to maintain privilege
- ❖ Establish relationships with local law enforcement, FBI
- ❖ Perform tabletop exercises with your vendors

<sup>14</sup> BakerHostetler

# Credit Monitoring

## Why Offer?

- ✦ It mitigates harm, positively changes affected individuals' expectations and regulators' expectations.

## Why Not Offer?

- ✦ It does not prevent fraudulent charges on payment cards.
- ✦ It may impact litigation position.
- ✦ Low redemption rate.

70%

Offered Credit  
Monitoring When  
Notification Occurred

BakerHostetler, 2019 Data Security Incident Response Report

15 BakerHostetler

# Rise of the Regulators

- ✦ State Attorney Generals (AGs)
- ✦ Office for Civil Rights (OCR)
- ✦ European Union
- ✦ Other Regulators



Agencies issue Civil Investigative Demands (CIDs) that request:

- ✓ Information Security Plan
- ✓ Remediation Steps
- ✓ Digital Environment Details and its Physical, Technical, and Administrative Controls

16 BakerHostetler



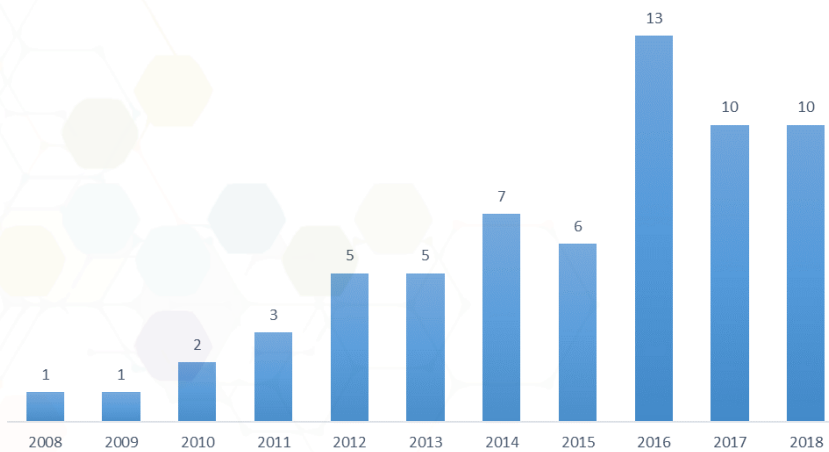
# OCR Hot Buttons

- **Recent Focus on Hacking Related Safeguards**
  - Intrusion Detection Software
  - Anti-Virus Software
  - Logging
  - Access Controls
- **Mobile Device and Transmission Security**
  - Encryption
  - Device Inventory, Tracking, and Monitoring
  - Facility Security and Theft Prevention
- **Security Risk Analysis and Risk Management Plans**
- **Third Party Access to PHI / Business Associates**
- **Staff Training and Education and Sanctions**



17 BakerHostetler

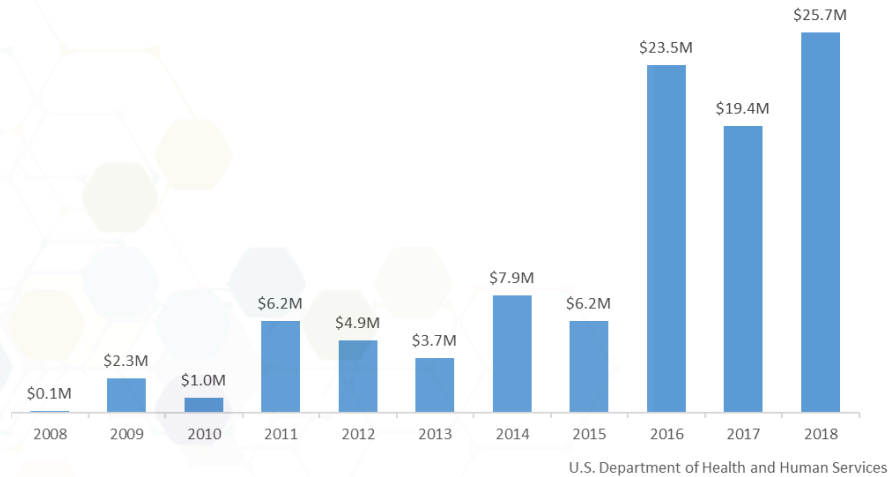
## OCR Resolutions on the Rise



U.S. Department of Health and Human Services

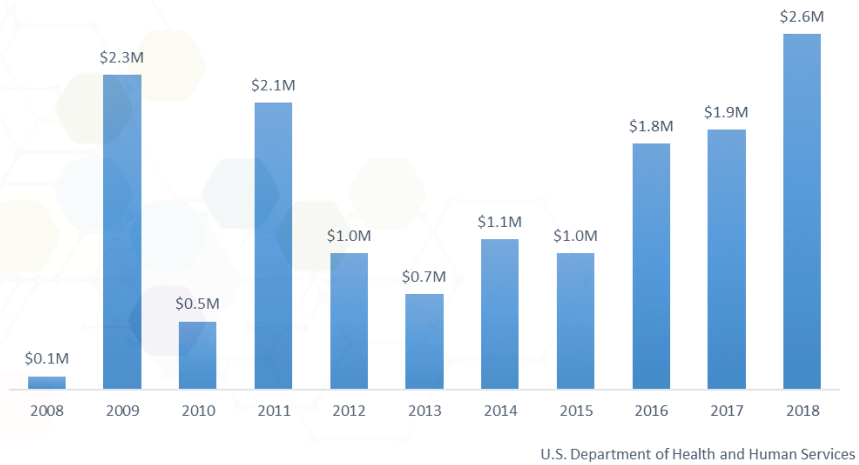
18

## HIPAA Penalties Assessed



19

## HIPAA Penalties - Average Penalties



20

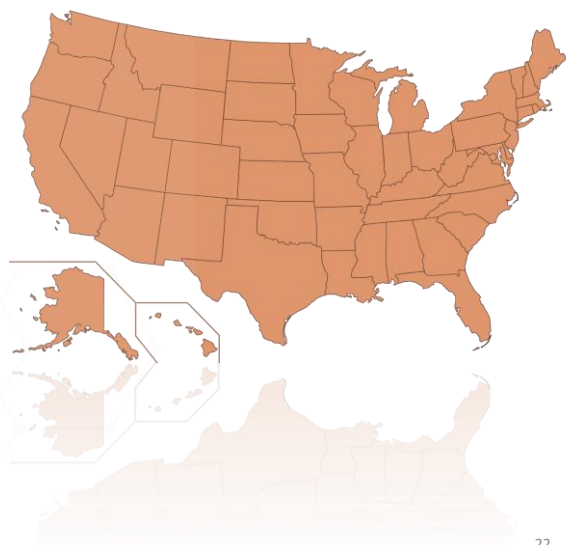
## 2018 HIPAA Fines and Settlements

Covered Entity	Amount	Reason
Presenius Medical Care North America	\$3,500,000	Risk analysis failures; impermissible disclosure of ePHI; lack of policies covering electronic devices; lack of encryption; insufficient security policies; insufficient physical safeguards.
Filefax, Inc.	\$100,000	Impermissible disclosure of PHI
University of Texas MD Anderson Cancer Center	\$4,348,000	Impermissible disclosure of ePHI; No Encryption
Massachusetts General Hospital	\$515,000	Filming patients without consent
Brigham and Women's Hospital	\$384,000	Filming patients without consent
Boston Medical Center	\$100,000	Filming patients without consent
Anthem, Inc.	\$16,000,000	Risk Analysis failures; insufficient reviews of system activity; failure related to response to a detected breach; insufficient technical controls to prevent unauthorized ePHI access
Allergy Associates of Hartford	\$125,000	PHI disclosure to reporter; no sanctions against employee
Advanced Care Hospitalists	\$500,000	Impermissible PHI Disclosure; No BAA; insufficient security measures; No HIPAA compliance efforts prior to April 1, 2014
Pagosas Springs Medical Center	\$111,400	Failure to terminate employee access; no BAA


21

## State Data Protection Laws

- 50 States, D.C., & U.S. territories
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent



22  
BakerHostetler



## California Consumer Privacy Act of June 28, 2018

- Takes effect June 2020
- Stated Purpose:
  - to give consumers more control and transparency regarding use of private information.
- Recent amendments would prohibit application of act to PHI collected by HIPAA-covered entities; however, may still apply to other types of personal information.

<sup>23</sup>  
BakerHostetler

## International Breach Notification

- ❖ Several Non-U.S. jurisdictions have security breach notification requirements
  - ❖ Some are specific to certain industries.
  - ❖ Some only require notification to a regulator.
- ❖ In certain countries, authorities have issued “guidance” for providing breach notification.
- ❖ GDPR imposes a 72-hour notification requirement.



<sup>24</sup>  
BakerHostetler

# GDPR Breach Notification

**“Personal data breach”**: incident in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

Data controller must notify the competent Supervising Authority without undue delay and, where feasible, not later than 72 hours after discovery

If more than 72 hours later, must give reason for delay

Content: (1) Description of incident (number affected, categories of data subjects and data records); (2) DPO contact information; (3) likely consequences of incident, including mitigation efforts

Individual notification required if there's a high risk (with exceptions)

Data processor must notify data controller “without undue delay” but no strict deadline  
Entities operating in the EU should prepare a GDPR-compliant data security incident response plan

25  
BakerHostetler

# GDPR Applicability

❖ **GDPR applies to organizations outside of the EU to the extent that they offer goods and services to or monitor the behavior of EU data subjects.**

## ❖ **Key Questions**

### ❖ **1. Offering goods in services**

- ❖ **Do you have any representatives or offices in the EU?**
- ❖ **Does your website have a domain with an EU extension (e.g. .fr, .es, .de)?**
- ❖ **Do you provide a telephone number with an EU country code?**
- ❖ **Do any of your promotional or marketing materials mention EU-based clientele?**

### ❖ **2. Monitoring the behavior of EU data subjects**

- ❖ **Do you track subjects on the internet (e.g. cookies)?**
- ❖ **Do you use data processing techniques to profile data subjects, their behaviors or attitudes?**

26  
BakerHostetler

## DATA SECURITY BEST PRACTICES

### Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

#### 10 Recommended Cybersecurity Practices

- Email Protection Systems
- Endpoint Protection Systems
- Access Management
- Data Protection and Loss Prevention
- Asset Management
- Network Management
- Vulnerability Management
- Incident Response
- Medical Device Security
- Cybersecurity Policies

US Department of Health & Human Services  
Healthcare & Public Health Sector Coordinating Councils  
December 28, 2018

27

BakerHostetler

# Questions?

28

BakerHostetler