



CENTER *for*  
INTEGRATIVE  
HEALTH

insight to innovation

Convene.  
Strategize.  
**Activate.**

# Cybersecurity & HIPAA: Protecting Your Organization

**PETE SEEBER**  
**CHRIS RAFFORD**  
**Rocus Networks**



---

***The Single-Source Cybersecurity  
Provider for the SMB***

**Pete Seeber**  
Founder & CEO

**Chris Rafford**  
Cybersecurity Strategist

# Before we begin

**Incident:** A security event that compromises the integrity, confidentiality or availability of an information asset.

**Breach:** An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

**Ransomware???**

**ePHI:** electronic Protected Health Information

**Verizon DBIR:** Data Breach Investigation Report



What is a healthcare employee's biggest priority?

**A. Patient health**

**B. Cybersecurity**

# High expectations

IN A FAST-PACED, STRESSFUL ENVIRONMENT



YOU MUST:



**Do it right**



**Do it fast**



**Stay in compliance**

# DBIR: Cybersecurity suffers

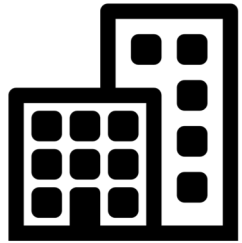
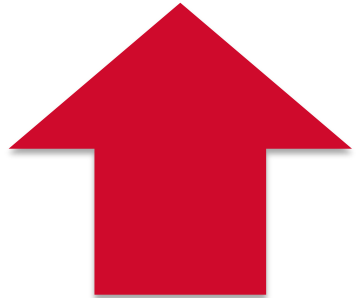


Healthcare is the only sector where the majority of the breaches were tied to insiders.

**59%**  
of breaches  
involve insiders



**HEALTHCARE**



**34%**  
of breaches  
involve insiders

**CROSS-INDUSTRY**

# DBIR: Data compromised



**Medical (72%)**



**Personal (34%)**



**Credentials (25%)**

# DBIR: Top 3 patterns in healthcare

81% of incidents come from 3 things:

**1. Miscellaneous Errors**

**2. Privilege Misuse**

**3. Web Applications**



For threat actors with a motive, financial gain (83%) is #1 motivation

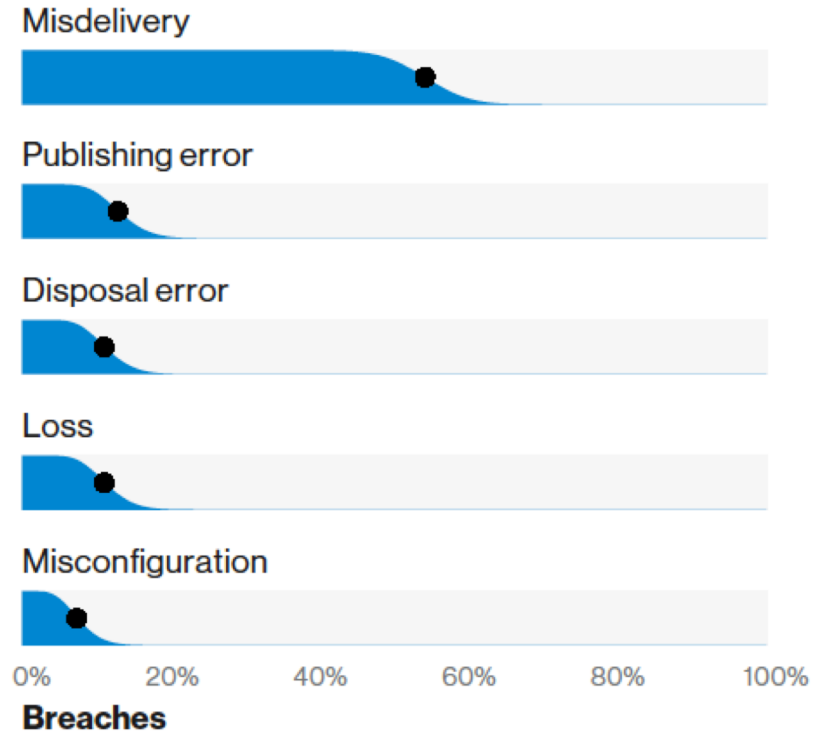


# 1. Miscellaneous errors

## Top error: misdelivery

- Data emailed to the wrong recipient
- Paperwork sent to wrong address

*A form with a life-changing medical diagnosis was accidentally faxed to the patient's workplace instead of the urologist.*



**Figure 51.** Top error varieties in Healthcare breaches (n=109)

## 2. Privilege misuse

Healthcare workers have access to databases to do their jobs

- Difficult to limit these types of incidents
- Can take years to detect

*Six doctors and 13 employees at UCLA Medical Center viewed Britney Spears' medical records after her 2008 psychiatric hospitalization. Many of the employees were non-medical support staff and none of them had a legitimate medical need to view the PHI.*



#2 threat actor motivation is fun (6%).

# 3. Web applications

Hackers find their way into the application via code vulnerabilities or via user names and passwords

- Phishing emails trick users
- Unlike other industries, Healthcare organizations are required to disclose ransomware attacks, even if there is no data loss

*Indianapolis-based Anthem holds the record for the largest health data breach in US history (2015). The health history of 79 million people was exposed due to an undetected, continuous and targeted cyberattack.*



# Regulation



**90's  
Computerization**



## HIPAA

**The Health Insurance Portability and Accountability Act (1996)**

- **PORTABILITY:** To help maintain health insurance coverage for employees between jobs
- **ACCOUNTABILITY:** To ensure the security and confidentiality of patient data

# 5 HIPAA rules



## HIPAA Privacy Rule

PHI Disclosure Rules

---



## HIPAA Security Rule

Standards to  
safeguard ePHI

---



## Omnibus Rule

Merges HITECH rules  
into HIPAA

---

## Breach



## Notification Rule

60 days to notify HHS

---



## Enforcement Rule

How investigations  
are conducted

---

# HIPAA Security Rule (2005)

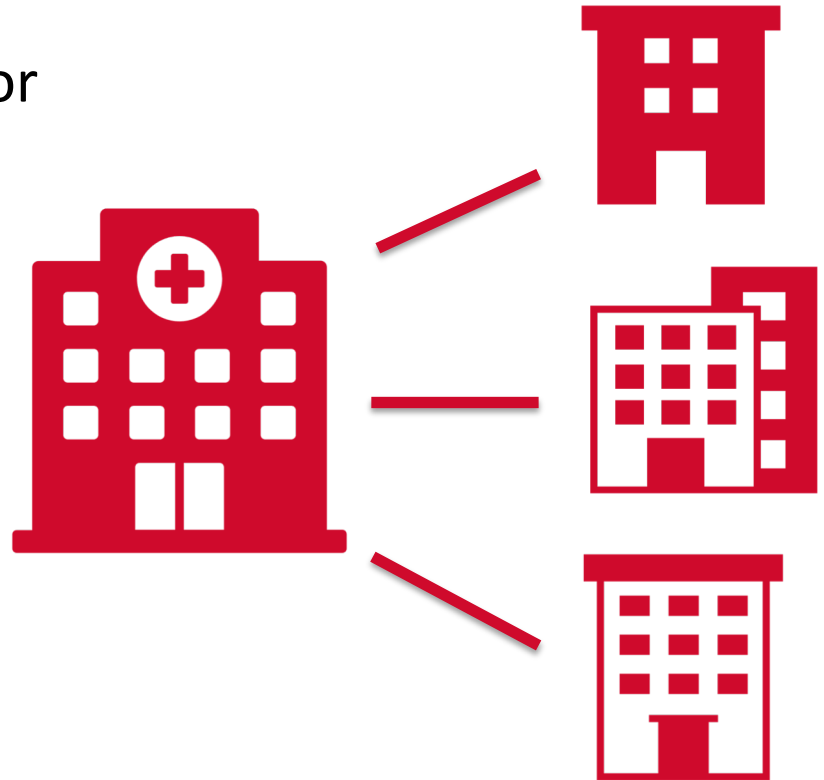
Entities covered by HIPAA **must implement strong data security safeguards** in their environments to ensure the confidentiality, integrity, and availability of all of the electronic protected health information (ePHI) they create, receive, maintain or transmit.



# The HITECH Act (2009)

Health Information Technology for  
Economic and Clinical Health Act

Extends the reach of HIPAA to  
**Business Associates**



# The big 2 for cybersecurity compliance

1. **Protect** the data and systems (You and your Business Associates)
2. **Notify** if you fail to protect the data and systems





# You decide how

The HIPAA Security Rule is designed to be **technology-neutral**.

HIPAA doesn't require the use of a specific cybersecurity framework.



# NIST is most popular

*Table 17: Security Frameworks*

Framework	N	percent
<b>NIST</b>	<b>103</b>	<b>57.9%</b>
HITRUST	47	26.4%
Critical Security Controls	44	24.7%
ISO	7	18.5%
COBIT	13	7.3%
Other	9	5.1%
No security framework has been implemented at my organization	30	16.9%
Don't know	15	8.4%

*Q. Which of the following security framework(s) does your organization use? Please select all that apply.*

<https://www.himss.org/2018-himss-cybersecurity-survey>

National Institute of Standards and Technology (U.S. Department of Commerce) established its first cybersecurity framework (CSF) in 2014

- Widely considered the **GOLD STANDARD**
- Any industry, entity type or size
- 5 functions: Identify, Protect, Detect, Respond, Recover



# IDENTIFY

## Asset Management

What do you have, where, how access, who can access?

## Business Environment

What is your business' mission, what do you do, who is involved or affected?

## Governance

What rules and requirements apply to your business?

## Risk Assessment

What is the likelihood of an incident vs. its impact on your business?

## Risk Management Strategy

Decisions are made about how your business will handle risk. Policies and procedures created.



# IDENTIFY

## Immediate action:



- Know who has access to your data
- Ensure background checks are conducted on anyone with access to your data
- Require individual user accounts for each employee
- Create cybersecurity policies and procedures



# PROTECT

## Access Control

Limit employee and 3<sup>rd</sup> party access to data, devices, transactions

## Awareness and Training

Provide cybersecurity awareness training to your employees and partners

## Data Security

Manage information and records to protect confidentiality, integrity, and availability

## Information Protection Processes and Procedures

Maintain security policies, processes, and procedures to manage protection of information systems and assets

## Maintenance

Perform maintenance and repairs of information system components and necessary patching

## Protective Technology

Technical security solutions used (e.g. network firewalls, email security, endpoint security)



## Immediate action:



- Limit who has access to data
- Install surge protectors and uninterruptible power supplies
- Patch operating systems and applications
- Install firewalls on all networks
- Set up email and device security filters
- Use encryption for sensitive info
- Dispose of old computers, hard drives and media safely
- Train your employees on cybersecurity policies and awareness



## Anomalies and Events

---

Anomalous activity is detected in a timely manner and the potential impact of events is understood

## Security Continuous Monitoring

---

The information system and assets are monitored to identify cybersecurity events and verify effectiveness

## Detection Processes

---

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events





# DETECT

## Immediate action:



- Install and update anti-virus, spyware, and malware programs
- Maintain and monitor data logs



# RESPOND

## Response Planning

Response procedures to ensure timely response to detected cybersecurity events

## Communications

Response activities coordinated with internal and external stakeholders, including law enforcement and victims notified

## Analysis

Analysis is conducted to ensure adequate response and support recovery activities

## Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident

## Improvements

Response plan improved by incorporating lessons learned from current and previous detection/response activities



# RESPOND

## Immediate action:



- Have an Incident Response Plan in place for disasters and information security incidents
- Ensure the plan is reviewed and updated regularly



# RECOVER

## Recovery Planning

Recovery procedures executed to ensure timely restoration of systems or assets affected by cybersecurity events

## Improvements

Recovery plan improved by incorporating lessons learned

## Communications

Restoration activities coordinated with all necessary parties, public relations managed for reputation repair



# Additional tips

- **Track** all attempts to access patient data
- Implement **dual factor** authentication – not convenient but necessary
- **Teach employees** about how to avoid falling for phishing tactics and to report questionable emails, calls, and webpages
- Ensure employees **think twice** before delivering, publishing, or disposing of patient data



Thank you!