HIPAAtrek

Guiding Your HIPAA Compliance

Sarah Badahman
CEO/Founder, HIPAAtrek

www.hipaatrek.com
sarah@hipaatrek.com
314-272-2598

Security Over Compliance

Checkbox Compliance

- HIPAA enacted in 1996
  - HITECH 2009
  - Omnibus 2013
- Security Rule has not been updated
- Does not address modern healthcare workflows and technologies
- Focusing on HIPAA is NOT enough

2.7M Medical Calls, Sensitive Audio Exposed Online for 6 Years

February 20, 2019 by Jessica Davis

A 1177 Swedish Healthcare Guide Service server used to store the phone calls made to the service for healthcare information was left unencrypted and exposed online with no [illegible] according to IDG Computer...

PHI of Almost 1 Million UW Medicine Patients Exposed Online

Phishing Attack Breaches Data of 30,000 Memorial Hospital Patients

An employee of Memorial Hospital at Gulfport, Mississippi responded to a phishing email 11 days before it was discovered; an extortion attempt, compromised server, and malware complete this week's breach roundup.

15 Million Patient Records Breached in 2018; Hacking, Phishing Surges

February 12, 2019 by Jessica Davis

Fifteen million patient records were breached during 503 healthcare data breach of reported incidents from the previous year

HIPAAtrek
Guiding Your HIPAA Compliance

THE STATISTICS

- For the first time, criminal hacking has surpassed human error as the main cause of healthcare data breaches – costing healthcare as much as $6B!
- As hackers become more sophisticated, is is predicted that there will be a 125% increase in the number of intentional attacks over the next 5 years.
- Not only do data breaches affect an organizations' reputation, legal, and financial perceptive, but also drastically impacts the real risk to an affected patient's health. Loss of access to medical records can cause misdiagnosis, delayed treatment, incorrect prescriptions/diagnostic orders. Complete loss of those records is particularly harmful as patients can be poor historians of their own medical history.
- A recent Ponemon Institute Survey stated that more than 50% of the respondents in a survey said their organizations internal incident response teams were either understaffed or underfunded and roughly 1/3 of the respondents didn't have any incident response plan in place whatsoever.
- 40% of the health organizations in the study admitted that they had reported more than 5 breaches in just the past 2 years – accounting for more than 90 million records!
- The results of the Ponemon Institute study reveal the need for organizations in the healthcare industry to better protect themselves and their records from social engineering attacks.

Hacking has surpassed all other breach types!

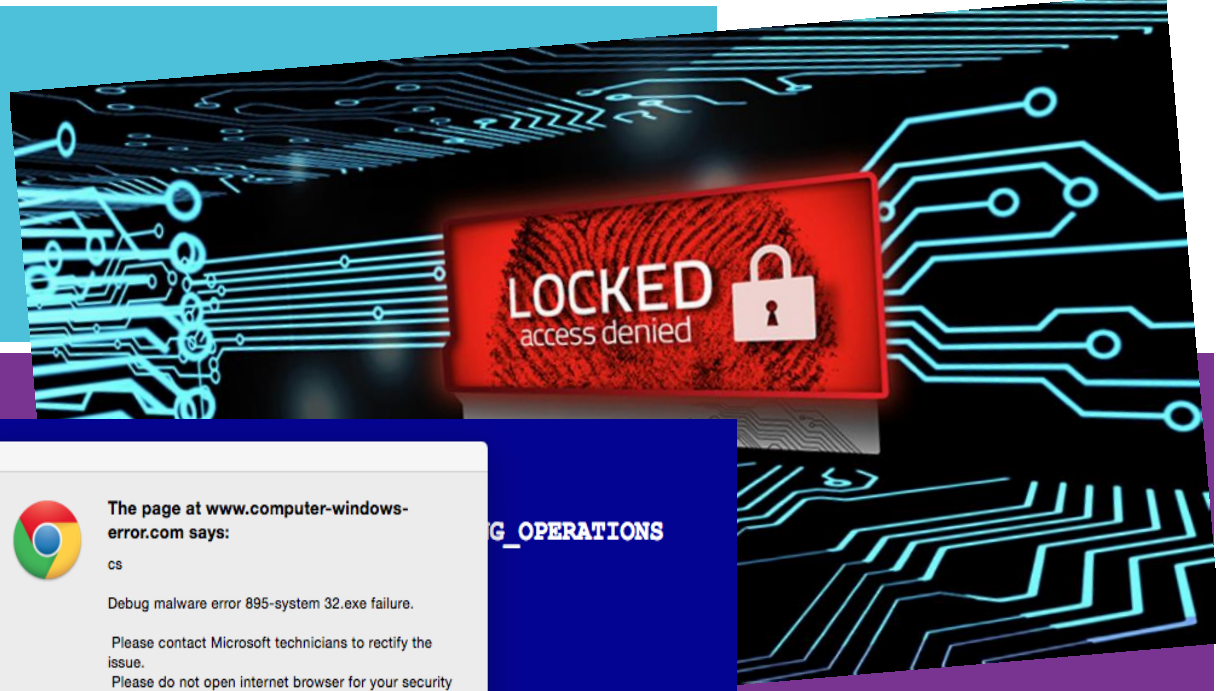
Most Attacked Locations

- Network Servers
- EMR
- Email
- Desktop Computers
- Laptops

- Most hacking events will affect more than one location
- Most attacks are preventable with proper attention to security
- Healthcare is the most attacked industry in the US
- Attacks are coming from overseas as well as in country

HIPAAtrek
Guiding Your HIPAA Compliance

Threats to Healthcare



HIPAAtrek
Guiding Your HIPAA Compliance

Why Are We Vulnerable?

Security Remains Minimally Addressed…WHY?

- Not viewed as critical to patient care
- Shortcuts to adoption of technology are culturally "OK" in healthcare
- Budget – Tech is EXPENSIVE to adopt and maintain
- Interruption of existing workflows are met with resistance
- Belief that your hospital or clinic is too small to be targeted or breached
- Assuming the cost of a potential breach will not outweigh the cost to implement the appropriate controls

Why Are We Vulnerable?

Weak or Missing Security Measures Include…

- Lack of Authentication
  - 2-factor authentication
  - Weak password policies
- Lack of Encrypted Data at Rest (Stored Data)
- Use of insecure email
  - Free email accounts
  - Personal email accounts
  - Shared email accounts
  - Unencrypted Email
  - Email accessible on mobile devices

Why Are We Vulnerable?

Weak or Missing Security Measures Include…

- Lack of Comprehensive Inventory
- Lack of Basic Security Procedures
  - SSL/TLS on websites and applications transmitting PHI
  - Data Backup/Disaster Recovery Planning
  - Auditing and Monitoring Procedures
- Use of outdated technologies
- Training of staff on recognizing potential malware

The Best Defense: A Robust Security Program

Focus on Security and compliance will follow…

HIPAAtrek
Guiding Your HIPAA Compliance

HIPAA is **NOT** a Security Framework

Regulation is not Security!

- OCR/HHS refer to NIST security framework
- Need to up healthcare's security game
- Over 340 breaches reported so far in 2019
  - 212 were Hacking/IT incidents

NIST Cybersecurity Framework

HIPAAtrek
Guiding Your HIPAA Compliance

Breaking it down…
Asset Management

Cybersecurity goes beyond your workstations and mobile devices…

All Devices Connected to the Internet or Network

Connected Devices Are a Growing Security Concern

- Unsupported Operating Systems
- Not considered in Risk Analysis/Security Evaluations
- Do not support common security protocols
  - Unique User ID
  - 2-Factor Authentication
  - Audit Controls
- Store rich PHI
- Easily breached with low likelihood of immediate discovery

Asset Management Action Steps:

- Identify ALL devices, workstations, mobile devices, and personal devices which access, store, or transmit PHI
- Identify ALL softwares which create, access, store, or transmit PHI
- Application and Data Criticality Analysis
- Controls (policies, procedures)

Breaking it down…
Risk Assessment/Risk Management

Risk =
(Threats x Vulnerabilities
x Impact x Probability)
– Controls

What is a Vulnerability?

A flaw/weakness in system security procedures, design, implementation, or internal controls that could accidentally or intentionally be exercised and result in a security breach or violation of an organization's security policies.

Technical vulnerabilities:

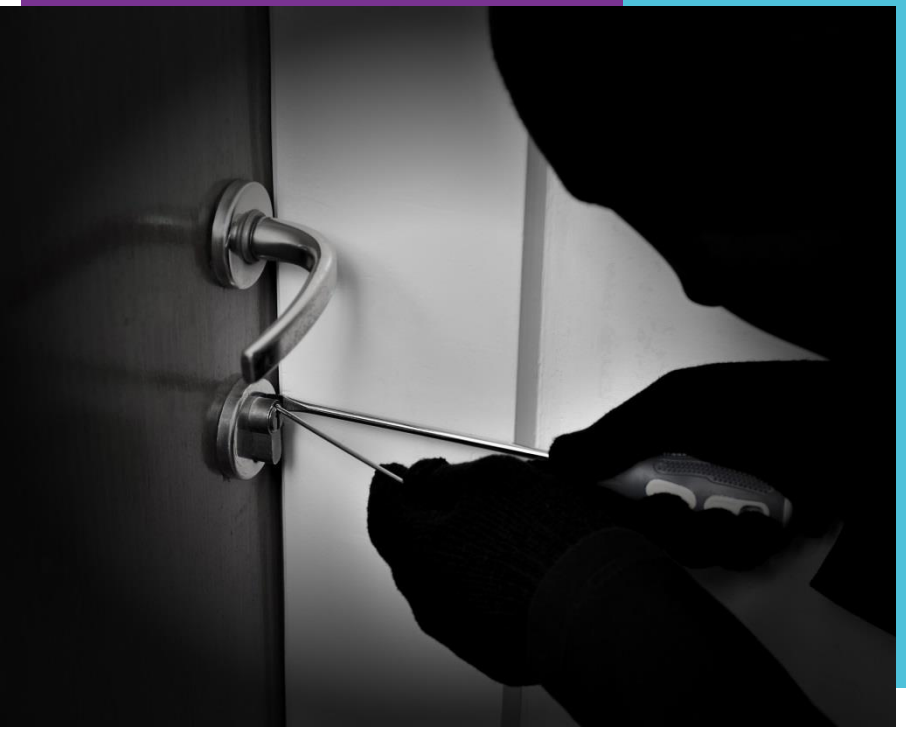
- Holes, flaws, & weaknesses in development of information systems
- Incorrectly implemented/configured systems
- Lack of technical safeguards (ex. Poor password management, insufficient anti-malware)

Nontechnical vulnerabilities:

- Ineffective/non-existent policies, procedures, standards, or guidelines

What is a Threat?

The potential for a person or thing to accidentally trigger or intentionally exploit a specific vulnerability.



Types of threats:

- Natural
- Human
- Environmental

Where threats occur:

- Information systems
- Operating systems
- Environment

What is Risk Probability?

The likelihood that a threat could exercise a vulnerability.

What is Risk Impact?

The effect on an organization if a vulnerability is exercised.

Impacted areas could include:

- Availability of systems and/or data
- Financial cost
- Legal repercussions
- Reputational harm

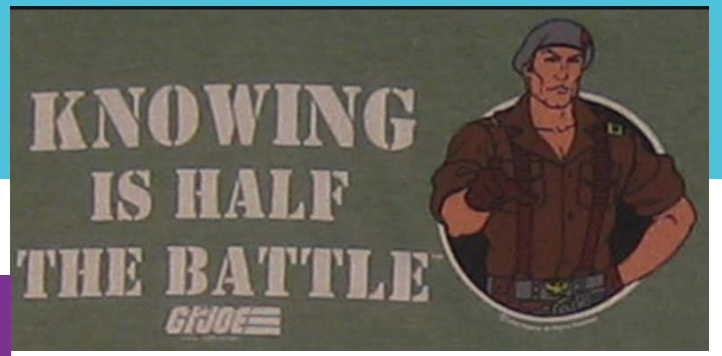
What are Controls?

Safeguards to control, mitigate, or prevent a vulnerability from being exercised.

Safeguards include:

- Policies & procedures
- Processes to control/prevent threats exercising vulnerabilities

GI Joe was right...



Conduct a Security Risk Analysis!

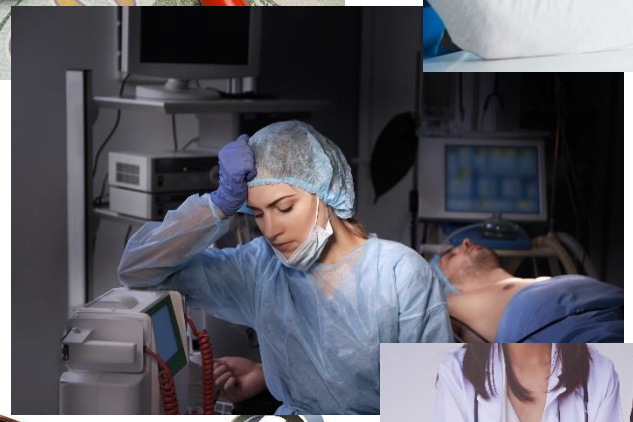
- Scope the Assessment
- Gather Information
- Identify Realistic Threats
- Identify Potential Vulnerabilities
- Assess Security Controls
- Assess Risk Impact
- Assess Risk Probability
- Document Findings
- Develop and Implement a Risk Management Plan

TIP: Use a Multi-Disciplinary Approach!

HIPAAtrek
Guiding Your HIPAA Compliance

Know How an Attack Can Effect You

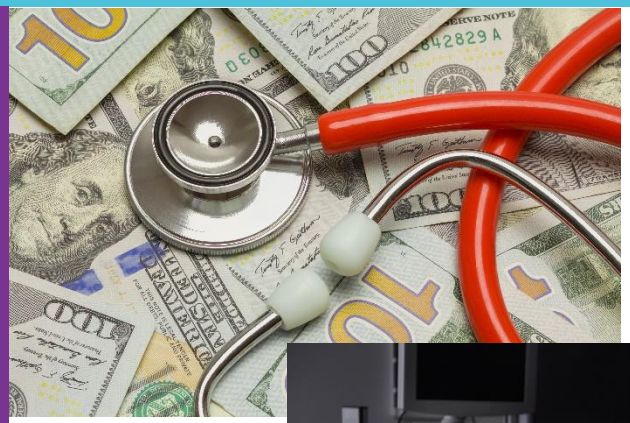
- Financial Impact
  - Fines
  - Lost Revenue
  - Cost to Quickly Adopt Tech/Safeguards
  - Legal Fees
  - Cost to Mitigate
- Operational Impact
  - Increased Workloads
  - Employee Dissatisfaction
  - Loss of Workforce Members
  - Change Management
  - Potentially have to reroute patients (Presbyterian Hospital in Hollywood, CA did)
- Patient Impact
- Legal Impact
- Reputational Impact



HIPAAtrek
Guiding Your HIPAA Compliance

Know How an Attack Can Effect You

- Financial Impact
- Operational Impact
- Patient Impact
  - Patients are poor historians
  - Misdiagnosis
  - Delayed Treatment
  - Incorrect Lab/Diagnostic Order
  - Lack of Access to Care/Records
  - Wrong or missing Rx
- Legal Impact
  - Corrective Action Plans
  - If criminal, potential malpractice
  - Civil HIPAA suits
- Reputational Impact
  - Loss of patient population/revenue
  - Loss of community support
  - Damaging press coverage



HIPAAtrek
Guiding Your HIPAA Compliance

Risk Management Action Steps:

- Prioritize identified vulnerabilities
- Create a project management plan for each vulnerability that will be mitigated
- Use a multi-disciplinary approach to mitigation
- Document EVERYTHING
- Remember risk management is on on-going process

Breaking it down…
Protect

Your data is valuable. Your cybersecurity and compliance programs are arsenal to protect them!

Access Control

- Establish Access
- Modification of Access
- Review of Access
- Don’t forget PHYSICAL Access
- Minimum Necessary Rule

Employee Training

- Training on HIPAA 101
  - HIPAA requires training on YOUR policies and procedures
  - HIPAA 101 is a good starting place; but not sufficient
- Training as a checkbox vs an opportunity to increase security practices
- Routine security reminders
- Training prior to granting or modifying access to PHI
- Training when a security/privacy incident occurs
- Employee access to policies and procedures

BYOD Policies

- Types of devices included in the BYOD policy (laptops, tablets, mobile phones, company owned, employee owned, non-employee owned)
- Rules regarding what is allowed based on operating systems
- Rules regarding what devices, data types or applications are restricted
- Rules regarding monitoring of devices (for example, rules requiring apps to be run on each device to allow remote verification of proper configuration, audit logging, and remote wipe capability)
- Basic controls required for each device (device profile/image, system configuration, malware prevention, endpoint protection)
- Enhanced controls required for certain devices (for example, whole disk encryption and multi-factor authentication)

Encryption Practices

- Encrypt data at rest
  - Full Disk encryption
    - Only effective on an unbooted computer. The second it's turned on, the encryption is no longer effective
      - May prove ineffective in most environments as workstations are rarely powered down when not actively being used
    - Files are not protected when moved as they are decrypted during the process
  - File Encryption
    - Stay encrypted regardless of where they are stored
    - As long as the file is 'at rest' the file is encrypted, even if the computer is booted
- DON''T Send unencrypted communications containing ePHI
  - Text
  - Email
- Most thefts involving portable devices are laptops that are unencrypted
- Don't forget to encrypt smart phones and tablets that store, transmit, access ePHI

Information System Maintenance

Outdated technology costs the health industry $8.3B annually

- Patch Management
  - Automate as much as possible
  - Assess Legacy Systems
  - Ignoring updates leads you vulnerable
- Cleaning Machines
  - Temporary Files
  - Recycling Bins
- Older Technology
  - Incompatible with newer softwares and patches
  - Prone to crash
  - Lost productivity/revenue
  - Higher prevalence of cyber attacks
  - Less likely to be supported

HIPAAtrek
Guiding Your HIPAA Compliance

Breaking it down…
Detect

Early Detection Saves Data!

Detection Software

NEVER use Home Versions!

Keep libraries up to date

Review Quarantines frequently

Disallow users from disabling

Ensure it can scan root folders

Scan email attachments

Scan websites

HIPAAtrek
Guiding Your HIPAA Compliance

Employee Training

- Educate staff on recognizing a potential attack
  - Slow moving machines
  - Executable starts running
  - Pop-Ups
  - Browser Toolbars not added by the user
  - Strange network patterns
- Instruct them on what to do if they suspect an attack
  - Disconnect from the network
  - Unplug the workstation
  - Power Off the workstation
  - THEN call IT

No Detection Software Catches 100%

Breaking it down…
Respond and Recover

Stop the Attack FIRST!

Don’t Panic!

- Assemble a multi-disciplinary task force
- Contain the breach or attack
- Assess severity and extent of the breach
- Notification
  - Patients
  - Staff
  - Management
- Document along the way
  - You will need this to avoid future breaches

Contingency Planning

Disaster Recovery Plan

- Healthy Data Backup Planning and Processes Essential
- Recovery Time Objective
- Recovery Point Objective
- Application and Data Criticality Analysis
- Testing the Process Frequently!

Ransomware Response Plan

Do you have a plan specific to Ransomware?

- To pay the ransom or not to pay the ransom – that is the real question!
  - FBI warns against paying the ransom
  - Many hospitals and clinics have been forced to pay
  - What will YOU do?
- Have you simulated a ransomware attack?
- Employee training on ransomware is NOT an option!

Common Cyber Security Mistakes

HIPAAtrek
Guiding Your HIPAA Compliance

Treating Your Work Environment Like Your Home Environment

- Computing habits
  - Browsing
  - Email
  - Social Media
- Physical Security
  - Leaving unlocked and unattended
  - Leaving mobile devices in vulnerable areas
- Security Practices
  - Passwords
  - Firewalls
  - Audit Procedures

Ignoring Non-Technical Vulnerabilities

- Physical Security
  - Portable Devices
  - Storage
  - Maintenance Records
- Employee
  - Training
  - Hiring
  - Terminating
- Policies and Procedures
  - More than just a binder
- Third Parties
  - Business Associate Agreements
  - Security Assessment of third party vendors

Technical Vulnerabilities

Non-Technical Vulnerabilities

HIPAAtrek
Guiding Your HIPAA Compliance

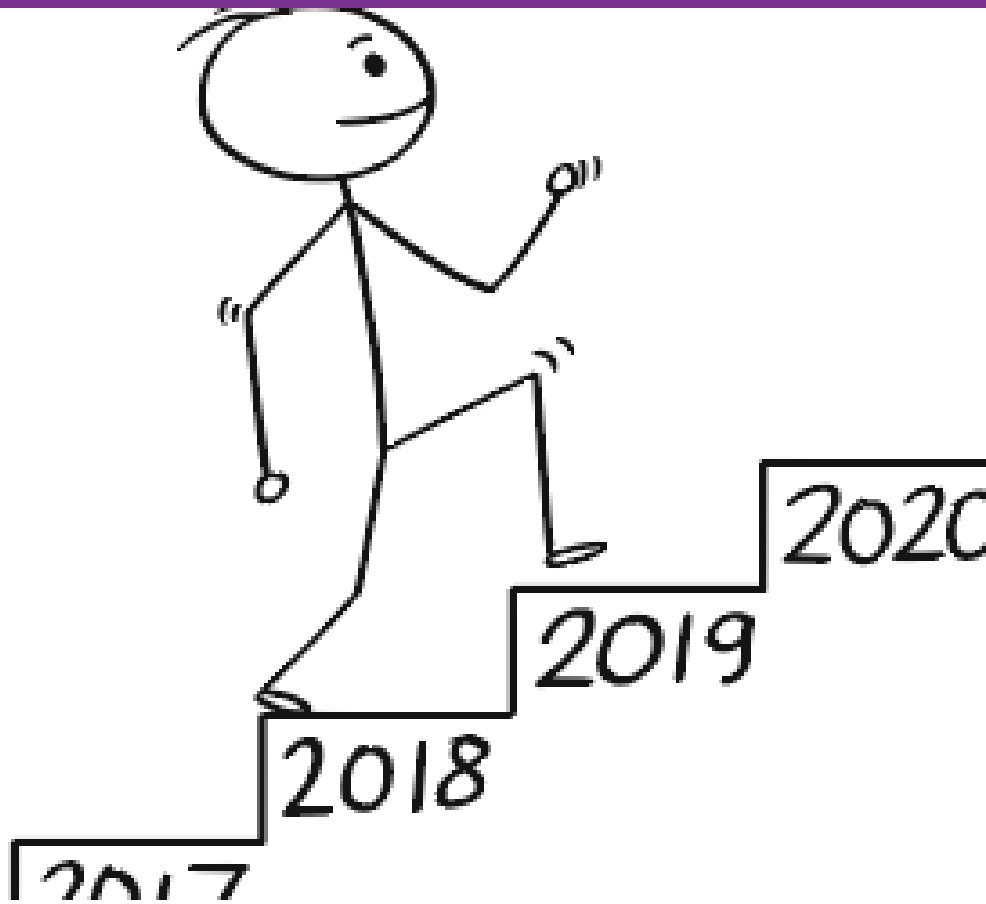
Slow to Adopt to Changing Security Landscape

- Healthcare historically lax in security protocols and technology advancements
- Outdated Technology
- Cost major deciding factor for adoption of newer techniques and technologies
  - ***Less than 6% of operational expenses*** spent on technology and security
- Lack of education around security

Compliance as a Destination

Compliance is a Journey…NOT a Destination!

- Be sure to stay on top of all HIPAA requirements – many are ongoing tasks that must be completed daily, monthly, quarterly, or annually
- There is no such thing as HIPAA certified – don't buy the snake oil that a certification means anything to the OCR



HIPAAtrek
Guiding Your HIPAA Compliance

HIPAAtrek
Guiding Your HIPAA Compliance