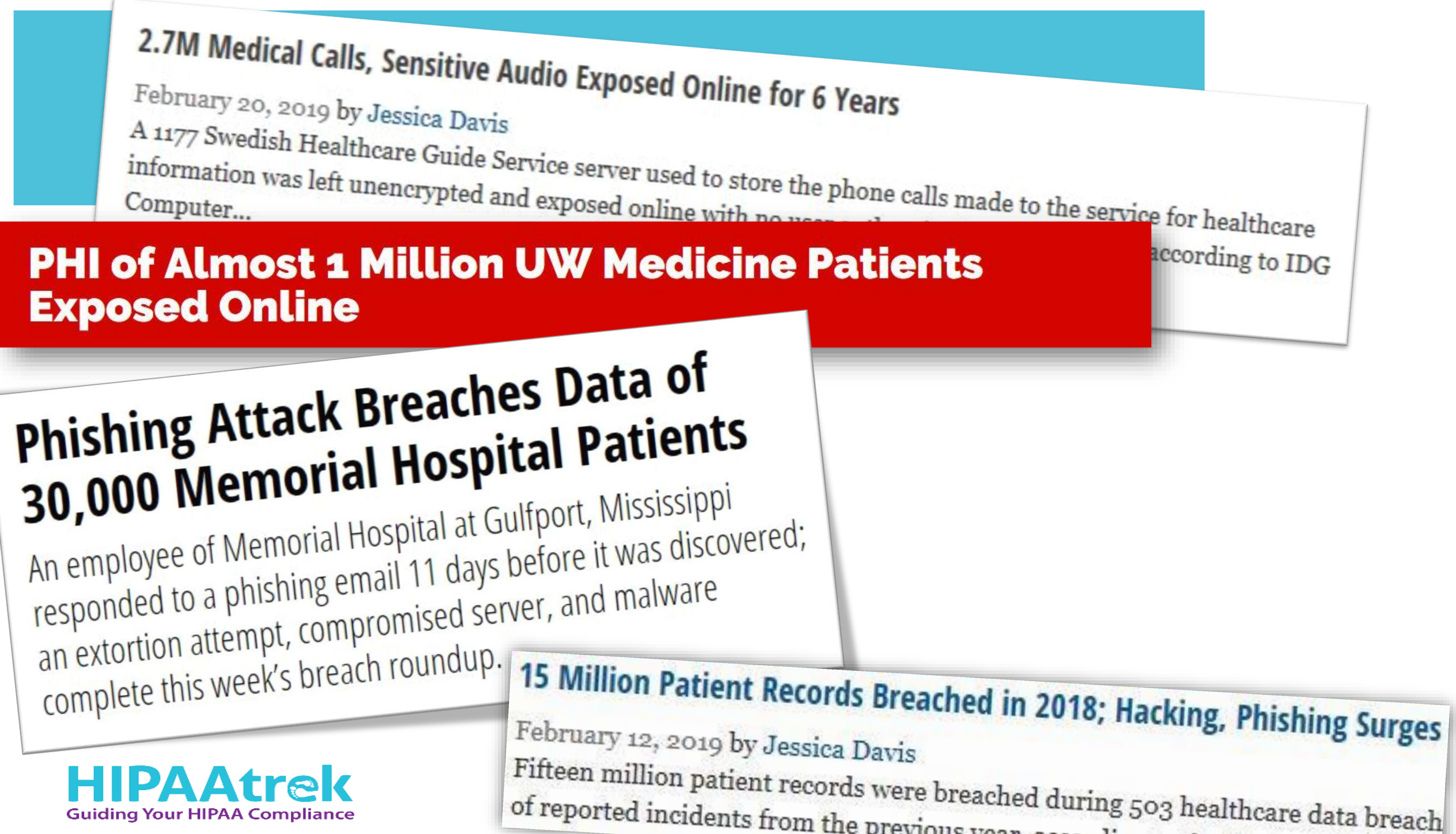
HIPAAtrek

Guiding Your HIPAA Compliance

Sarah Badahman
CEO/Founder, HIPAAtrek

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

Security Over Compliance



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 user auth ccording 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

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

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

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/personal email accounts
  - Shared email accounts
  - Unencrypted email
  - Access 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

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

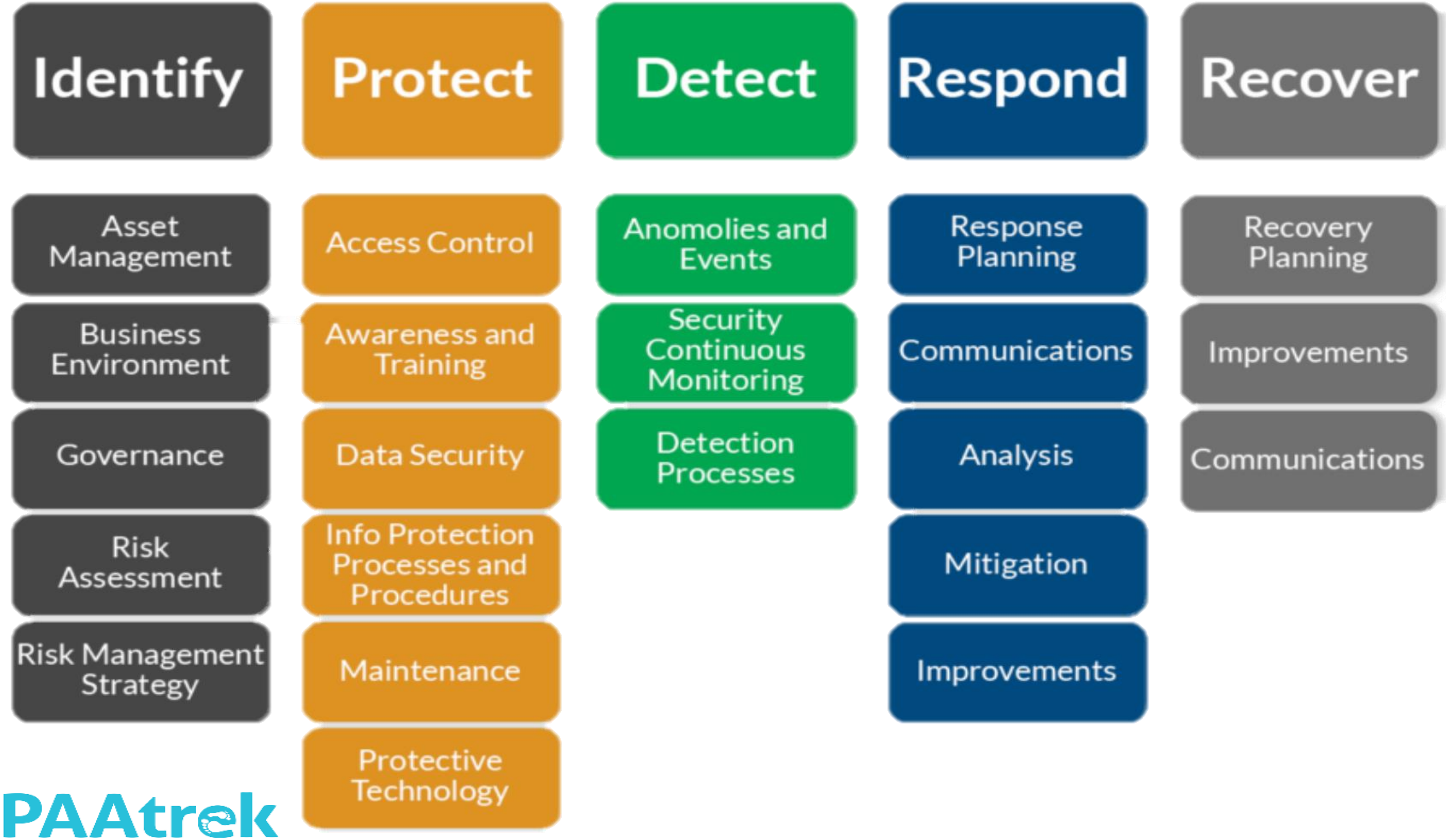
- Physical security
  - Portable devices
  - Storage
  - Maintenance records
- Employee
  - Training
  - Hiring
  - Terminating
- Policies and procedures
  - More than just a binder
- Third parties
  - Business Associate Agreements
  - Security assessment of third-party vendors

HIPAAtrek
Guiding Your HIPAA Compliance

The Best Defense: A Robust Security Program

Focus on security and compliance will follow

NIST Cybersecurity Framework



Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomolies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Cybersecurity must include 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 ePHI
- 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 ePHI
- Identify ALL software that creates, accesses, stores, or transmits ePHI
- Application and Data Criticality Analysis
- Controls (policies, procedures)

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

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 an on-going process

Your data is valuable. Your cybersecurity and compliance programs must protect them!

Guiding Your HIPAA Compliance

Access Control

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

HIPAAtrek
Guiding Your HIPAA Compliance

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

Information Systems 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

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

No Detection Software Catches 100%

HIPAAtrek
Guiding Your HIPAA Compliance

Employee Training

- Educate staff on recognizing a potential attack
  - Slow moving machines
  - Executable starts running
  - Pop-ups
- 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

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

Disaster Recovery Plan

- Healthy data backup planning and processes essential
- Recovery time objective
- Recovery point objective
- Application and Data Criticality Analysis
- Test the process frequently!

Ransomware Response Plan

Do you have a plan specific to ransomware?

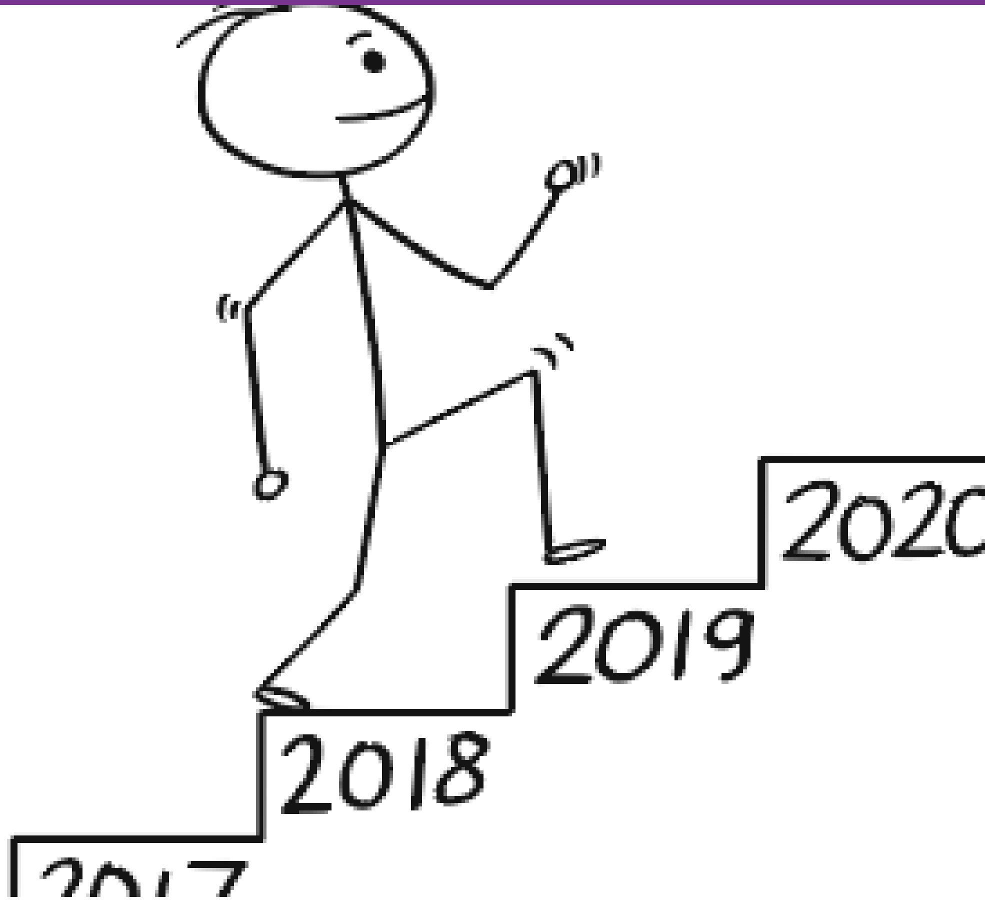
- To pay the ransom or not to pay the ransom – that is the question!
  - FBI warns against paying the ransom
  - Many hospitals and clinics have been forced to pay
  - What will YOU do?
- Have you simulated a ransomware attack?
- Employee training on ransomware is NOT an option!

Compliance is a Journey

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

sarah@hipaatrek.com
314-272-2600

Questions?

HIPAAtrek
Guiding Your HIPAA Compliance