HIPAAtrek

Guiding Your HIPAA Compliance

Sarah Badahman
CEO/Founder, HIPAAtrek

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

Why Are Hackers Targeting Healthcare?

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

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

COVID Complicated EVERYTHING – even cybersecurity

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.

Why Are We Being Attacked?

- Predators go after the weakest link
  - 72% increase in healthcare attacks since 2013
- Protected Health Information is worth 10x credit card information on the black market
  - Average of $363 per healthcare record
  - Up to $20 per financial or credit card record
- Hackers exploit the fact that healthcare professionals are nurtures and caregivers by nature – we *want* to help
- Adoption of technology in healthcare has grown at a higher rate than the adoption of security measures

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

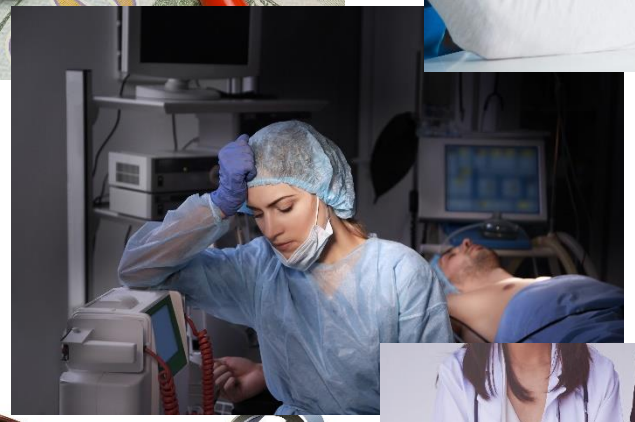
Why Are We Vulnerable?

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

Know How an Attack Can Effect You

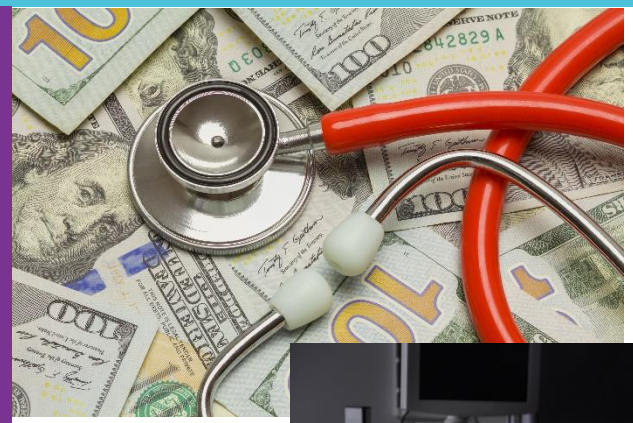
- Financial Impact
  - Fines
  - Lost Revenue
  - Cost to Quickly Adopt Tech/Safeguards
  - Legal Fees
  - Cost to Mitigate
- Operational Impact
  - Increased Workloads
  - Employee Dissatisfaction
  - Loss of Workforce Members
  - Change Management
  - Potentially have to reroute patients (Presbyterian 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

GI Joe was right…Knowing is Half the Battle!

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

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

Common Attacks

It used to be believed that social engineering was reserved for governments and organizations with enemies. However, it's becoming as mainstream as any other kind of cybercrime and social media is making it far easier to stage an attack. The answer lies in education of the workforce, and, as with any other type of security measure, diligence.

Social Engineering

- ***Ransomware*** - a type of malicious software designed to block access to a computer system until a sum of money is paid.
- ***Phishing*** - the activity of defrauding an online account holder of financial information by posing as a legitimate company.
- ***Pretexting*** - is a form of social engineering in which an individual lies to obtain privileged data. A pretext is a false motive.
- ***Malvertising*** - (from "malicious advertising") is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
- ***ClickBait*** - content, especially that of a sensational or provocative nature, whose main purpose is to attract attention and draw visitors to a particular web page.
- ***Quid Pro Quo*** - is a request for your information in exchange for some compensation. It could be a free T-shirt or access to an online game or service in exchange for your login credentials, or a researcher asking for your password as part of an experiment in exchange for $100. If it sounds too good to be true, it probably is quid pro quo.
- ***Tailgating*** - is when someone follows you into a restricted area or system. Traditionally, this is when someone asks you to hold the door open behind you because they forgot their company RFID card. But this could also take form as someone asking to borrow your phone or laptop to perform a simple action when they are actually installing some malicious software.

HIPAAtrek
Guiding Your HIPAA Compliance

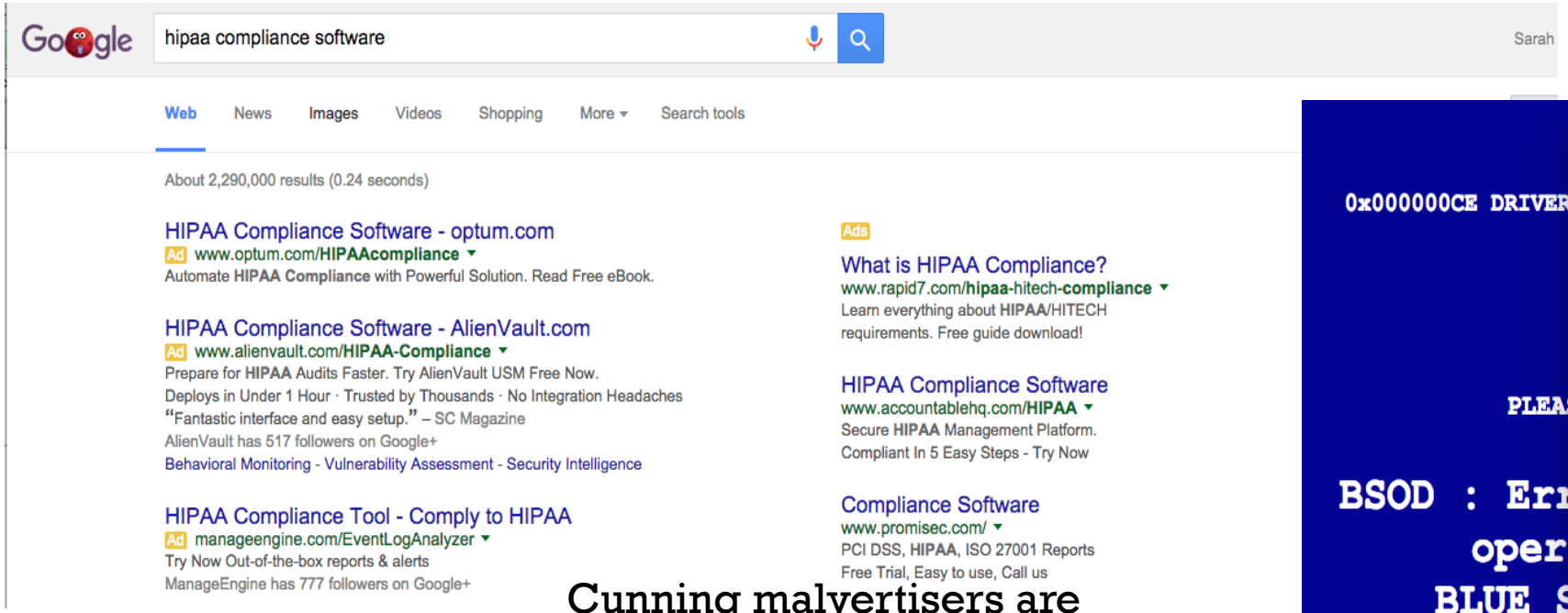
Social Engineering

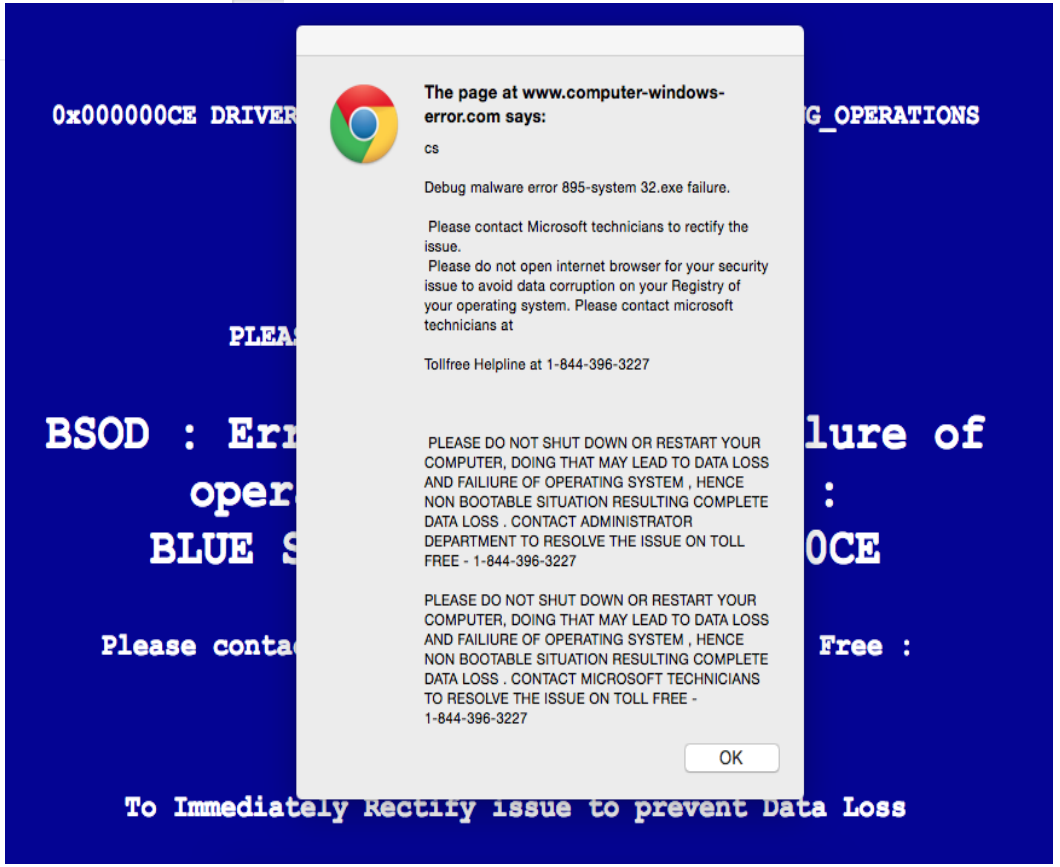
Social Media's role in luring users

- Facebook is well-known for having clickbait
  - Which Disney Princess Are You?
  - How to eliminate dental plaque in 5 minutes, without the dentist!
  - You won't believe this really exciting cool thing that we know will make you click here because of our algorithms that know your interests!
- Most of these sites just want your click (thank you Ad Revenue!) – but can you tell the ones that have malware from the ones that don't?
- ClickBait can automatically post onto your Social Media page to further spread its malware to all your friends!

The Dawn of Malvertizing

Sneaky Hacker Devils





Cunning malvertisers are bidding on keywords that are highly searched. They are also using reputable company names to launch their attack.

Interested in an ad? Type the name directly in your browser.

HIPAAtrek
Guiding Your HIPAA Compliance

The Dawn of Malvertizing

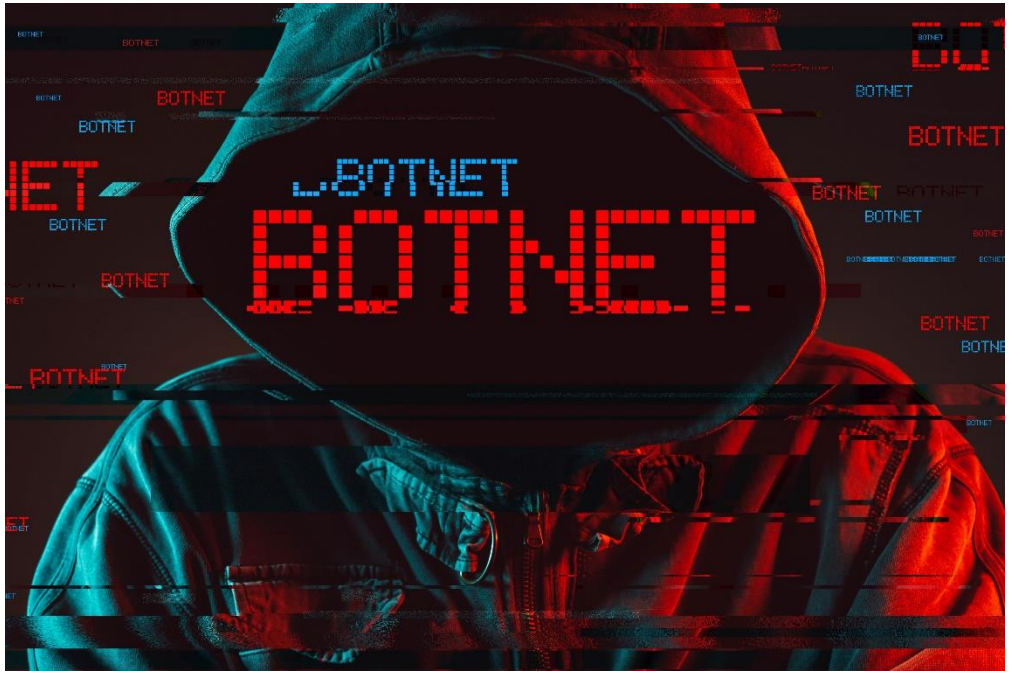
Sneaky Hacker Devils

Malvertising is a silent killer because malicious ads do not require any type of user interaction in order to execute their payload. The mere fact of browsing to a website that has ads (and most sites, if not all, do) is enough to start the infection chain.

Botnet

Zombies are real and scary…

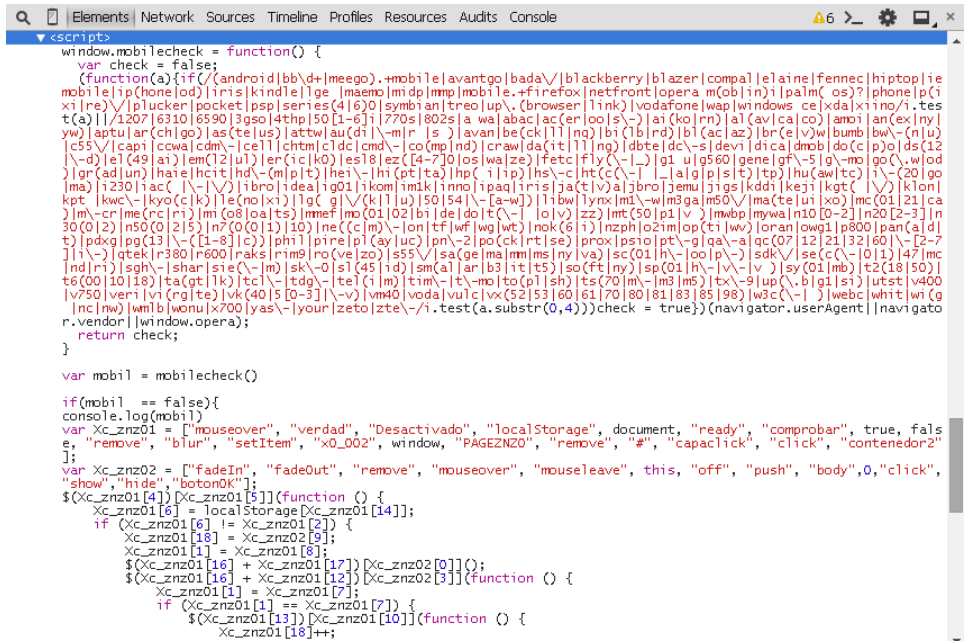
- Allows an attacker to take over a computer
  - Affected machines are called zombies
- Stealing of information
  - Identity Theft
- Denial of Service (Dos)
  - Ransomware
- Clickfraud
  - Fraudulently increasing click-based ad revenue



X Marks the Spot

But the Treasure is for the Hacker

Remember that X icon that was supposed to close the popup? It was loading a hidden iframe. This one was different from the SEO-spam-style hidden iframes that are only seen by search engines and hidden somewhere off-screen. No, this iframe needs to be clickable.



Since the popup is controlled by JavaScript, the best option is to disable the execution of any scripts (by configuration or browser add-ons). This will impact how most websites look and feel, however you can always add sites to the exception list once you know they are ok, or test them by temporarily allowing them.

Another option is to force quit the browser when a popup appears.

Another good piece of advice is: never trust the links, especially those clickbait ones!

HIPAAtrek
Guiding Your HIPAA Compliance

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

Outdated Technology

- Outdated technology costs the health industry $8.3B annually according to a Ponemon Survey
- Reliance on legacy systems
- Older technology more prone to crashes
- Incapability with newer softwares
- Higher prevalence of cyber attacks and malware
- Less likely to be supported by the manufacturer
- Lost productivity and revenue
- Use of home or non-commercial technology

HIPAAtrek
Guiding Your HIPAA Compliance

BYOD Policies Lacking

- 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)

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

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

Inadequate Encryption Practices

- Failure to 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
- Sending 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

Improper and Lacking 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
- Lack of routine security reminders
- Lack of training prior to granting or modifying access to PHI
- Lack of training when a security/privacy incident occurs
- Lack of access to policies and procedures

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

Secure Compliance

Focus on Security and compliance will follow…

HIPAAtrek
Guiding Your HIPAA Compliance

Testing your Vulnerabilities

What are your weakest points?

- Human
  - Conduct social engineering penetration testing
    - Email spoofing
    - Pretexting
    - Malicious email attachments
  - Tailgating
    - Technical
    - Non-technical
- Social
  - Search for your workforce members on social media – do their public profiles violate your social media policy?
  - Google your employees – what can you see that could hurt your organization?
- Technology
  - Do you have Anti-Exploit, Anti-Malware and Anti-Virus installed, up to date, and continuously monitored?
  - What is your contingency planning in case all fails and you fall victim?

Plan of Action: Implementing Policies

- Project Management
  - Think of procedures as tasks to be completed
    - Set up reminders for repeating tasks
    - Many projects have common threads
  - Compliance is NOT a one and done – it is an on-going process

Tying projects together can help staff and providers see the bigger picture and develop a culture of compliance

- Delegate
  - Compliance is the responsibility of everyone
    - Tasks get overlooked and forgotten when tasks are not properly delegated

- Documentation and Tracking
  - Document all efforts – it will help in the event of a breach or audit
  - Review efforts to determine if the procedure is still effective – revise as necessary

Important Steps

- Workforce Training
- Security Reminders
- Social Engineering Penetration Testing
- Evaluating for technical and non-technical vulnerabilities
- Social Media Policies are a MUST
- Up-to-date anti-malware that is being monitored for attacks (Trojans are a popular tool for social engineer hackers and are difficult to be caught by many anti-malware solutions)
- Anti-Exploit software
- Ensure you are using a positive security model logically and administer privileges with a 'least-access-necessary' mindset. Less people with access to sensitive data both from a network standpoint and a logical access standpoint significantly reduces your risk in losing data in a social engineering attack.

Six Step Checklist

- Assessment: Choose and prioritize specific objectives from a universe of possibilities that can be accomplished with a specific time frame.
- Definition: Define the chosen objectives in terms that are specific and measurable. The objectives must be well defined so that it's clear when the project has been completed.
- Delegation: Assign a specific individual to supervise, complete and be fully accountable for the completion of the task.
- Scheduling: Give the project a deadline that is communicated to the accountable person, and gets that person's consent for the deadline.
- Review: Periodically review and evaluate each project at regular intervals between assignment and completion.
- Document: Ensure the project is documented at each milestone. This will not only provide proof to external auditors, but will also assist you in determining effectiveness of the project.
- Organization: Stay focused, organized and on task. Change is the one thing that remains constant through all regulations and initiatives. Have one person, in-house, who will stay on top of everything (this could mean partnering with the right people to help outside of the practice).

Sarah Badahman
sarah@hipaatrek.com
314-272-2598
https://hipaatrek.com

HIPAAtrek
Guiding Your HIPAA Compliance