Protecting Your Practice From Cyber Threats

Introductions

Mohamed Yassin, MD, FAAAAI, FACAIAI  
Member of the Association of Certified Fraud Examiners  
Allergy, Asthma, & Pulmonary Associates  
Saint Cloud, MN  
(320) 654-8266

Michael Rogers, MS in Cyber Security, SANS GDAT, GOSI, GCIA  
Director – Technical Advisory Services at MOXFIVE  
(833) 568-6695
Disclosure

Nothing to disclose

Is Cybersecurity a Threat For Medical Practices?

• YES, it is a real and imminent threat to any medical practice and hospitals

• 34% of all data breaches in 2021 were in the Healthcare Industry
  (2021 ForgeRock Consumer Identify Breach Report)

• Since 2018 Cyber Attacks are the number 1 way health records are breached
### U.S. Department of Health and Human Services
Office for Civil Rights 2021

#### Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

*Note: The Breach Notification Portal will be offline for maintenance from Fri May 28 12:00 PM EDT to Sat May 29 02:00 AM EDT. Any information being entered when the Portal is up will be lost.*

#### Under Investigation

As required by section 13403(a)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals following breaches have been reported to the Secretary.

#### Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

#### Show Advanced Options

<table>
<thead>
<tr>
<th>Exposed All</th>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity</th>
<th>Individuals Affected</th>
<th>Breach Information</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Harper County Community Hospital</td>
<td>OK</td>
<td>Healthcare Provider</td>
<td>5725</td>
<td>05/01/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>1</td>
<td>Westwood Obstetrics and Gynecology (&quot;Westwood&quot;)</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>12601</td>
<td>05/15/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>2</td>
<td>Trinity Behavioral Care Services</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>207166</td>
<td>05/16/2021</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
</tbody>
</table>

#### Virtual Practice Management Workshop
JULY 23-24, 2021

**Access, affordable, applicable**

### U.S. Department of Health and Human Services
Office for Civil Rights 2021

#### (Displaying 1 - 100 of 774)
OCR (Office of Civil Rights) Data Breach
Financial Penalties

• Penalties range from hundreds of thousands to millions
• Even business associates can pay millions
• Bankruptcy may not protect you from the financial penalties if any of your patients claim “potential harm”
• HIPAA Omnibus modifications grant state attorneys general the ability to bring civil action and seek damages on behalf of their residents for HIPAA violations.

Is Cybersecurity a Threat For Medical Practices?

• Now we agree Cybersecurity is a real threat how can we do and what are the best practices related to cybersecurity?
Cybersecurity Best Practices for Your Medical Practice

• Fact: you are practice is no longer “data secured” because you are practicing in a small town in North Dakota or Idaho
• Fact: your office computers via the internet are potentially accessible to any hacker from Russia, Nigeria or Timbuktu

Cybersecurity Best Practices for Your Medical Practice

• There are three parts to securing in your office:
  • Personnel (employees and business associates e.g. billing company, transcription companies, IT staff....)
  • Hardware (computer terminals, network server, firewall)
  • Software (EMR, Microsoft, WordPerfect, Financial....)
Cybersecurity Best Practices for Your Medical Practice

• Personnel:
  • Establish policies regarding
    • Email; no employee should be allowed to open personal emails using office computers or office network on personal devices
    • Personal devices; no one should be allowed to connect personal devices (computers, tablets, smart phones, removable hard drives and USB drives,..)
    • No internet access to any site in the web for staff except purchasing department/manager
    • Good physical access controls (leaving passwords where they can easily be seen – such as on a sticky note)

• Personnel:
  • Train your staff, update training 5-10 minutes every staff meeting at least every 4 months
  • Office manager or designated staff should have HIPAA agreements with all business associates, and update yearly
Business Associate Definition

- Business Associates (BA’s) are individuals or entities who **create, receive, maintain, or store** private health information on behalf of a covered entity.

- Example:
  - Answering Services, Medical Transcription, IT groups, Billing companies, shredding services are clearly under the auspices of “Business Associate”.

Business Associate

- The OMNIBUS Rule requires business associates to comply directly with HIPAA regulations themselves.

- BA’s must now:
  - Develop policies and procedures for HIPAA – train staff
  - Conduct risk analysis
  - Be subjected to federal inspections
  - Monitor covered entities where a BA exists – have BA’s with sub-contractors
  - Be subjected to the Breach Notification Rule
Cybersecurity Best Practices for Your Medical Practice

• Hardware:
  • Computers; update security upgrade and patches, anti virus software. Example: the recent government hack was successful because they had few Windows XP professional in the network (no security updates available)
  • Server; must have the most recent software version with automatic updates, virus updates
  • Very important to have the best firewall with updated firmware / software
  • Don’t allow any personal computers to access the main office internet and the server
  • Make sure wireless printers are not viewable for any computer or device not part of the office network

Avoiding Risks

• Back up important files using the 3-2-1 rule— create 3 backup copies on 2 different media with 1 backup in a separate location
• Regularly update software, programs, and applications to protect against the latest vulnerabilities (especially the browser, anti- virus program, and operating system)
Avoiding Risks

- Access controls must be in place (i.e. who are you granting access into the system)
- Very strong password policies in place
- Business associate access controls
- Cheap anti-virus (don’t do it!)
- Cheap (non-robust) firewalls (don’t do it!)

Avoiding Risks

- Avoid unsecure websites
- Good physical access controls (leaving passwords where they can easily be seen – such as on a sticky note)
- Non-secured data transmissions of sensitive access controls
- Be sure to have a backup copy of your system (full image)
RISK ASSESSMENT

• A risk assessment is not only required by HIPAA but it’s the best way problems can be found within your practice/business and the issues can be mitigated.

• There is no surefire way to do the assessment but just make sure all areas are covered.

• THE RISK ASSESSMENT IS THE FIRST THING THE FEDS WILL WANT TO SEE IN THE EVENT OF A BREACH!!

• RISK ASSESSMENT MUST BE DONE ANNUALLY (AT LEAST)

MUST CONDUCT RISK ASSESSMENT

• As quoted in from HIPAA’s Security Rule (CFR) 164.308(a)(6), a covered entity is required to conduct a Risk Assessment:
  • “identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents known to the covered entity; and document security incidents and their outcomes.”
  • “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306 (a) [(the general requirements of the security rule)]”

• The Risk Assessment is the building blocks for your policies and procedures. In fact, conducting a Risk Assessment is a “required” part of the HIPAA Security Rule!!**
Responding to an Incident/Breach

Common misconceptions:

- **Recovery Time:** “The business will be back up and running within a couple days.”

- **Cyber Insurance:** “Planning isn’t required, I have insurance.”

- **Impact:** “We can just rebuild if needed.”

- **Security Confidence:** “We are secure because of XYZ software.”

- **Preparation/Defense Costs:** “Cyber security is too expensive to invest in.”

Security Risk Assessment

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and their business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA’s administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization’s protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, click here, visit the Office for Civil Rights’ official guidance.

**New! Security Risk Assessment Tool Version 3.0**

ONC, in collaboration with the HHS Office for Civil Rights (OCR), developed a new version of the downloadable Security Risk Assessment Tool (SRT) to help guide you through the process.

Download Version 3.0 of the SRT Tool (ZIP) [45 MB]

For details on how to use the tool, download the SRT User Guide (PDF) [2.2 MB].

Watch videos on contingency planning and what a risk assessment may involve

Read the HHS Press Release on release of SRT Tool 3.0 in October 2018.

Legacy Version: Security Risk Assessment Tool Version 2.0

Note that you can’t directly transfer data from 2.0 to 3.0, but can upload certain portions (e.g., lists of...
Preparing for an Incident/Breach

1. **Backup Isolation:**
   Have the ability to isolate backups immediately.

2. **Priority Asset Listing:**
   Critical hosts identified to restore for the business.

3. **Data Governance:**
   Knowledge of where your sensitive data is stored.

4. **Communication Plan:**
   POCs of vendors, legal, insurance, and internal team members to assist with an incident.

5. **Disaster Plan:**
   If possible, have a plan that will enable you to keep the lights on while the investigation and recovery process is playing out.

---

Top Recommended Actions

1. **Security Gap Assessment**
2. **Multi-Factor Authentication | Two Factor Authentication**
3. **Password Vaults**
4. **Security Awareness and Phishing Training/Testing**
5. **Active Directory Hardening**
6. **Unique Local Administrator Passwords**
7. **Protect Backups**
8. **EDR**
Top Threat: Ransomware

Average Ransom Payment: $220,298 (+43% from Q4 2020)

Resources

• To build use cases and buy in leverage the following resources:
  • Coveware, CrowdStrike, MOXFIVE, PhishLabs Blogs and Reports

• General Cyber Security Resources:
  • Microsoft Security Compliance Toolkit 1.0
  • Security Technical Implementation Guides (STIGs)
  • NIST Check List
  • NSA Logging Recommendations
  • Center for Internet Security
Resources

• Quick checks:
  • https://haveibeenpwned.com/

Resources

• Quick checks:
  • https://www.shodan.io/
MOXFIVE Blogs

- **Blog: The Key to Successful Business Recovery**
- **Blog: Ransomware Recovery Tales: Protect the Kingdom**
- **Blog: Backups: Ahh! To Zzz**
- **Blog: Ransomware Recovery Tales: Prepare for Battle**

Closing Remarks

- The threat is real and evolving
- Being proactive is essential
- Prepare an action plan
- Leverage external resources and your community