How To Secure your Network, Computers, and Records

Peter J. Cass, OD

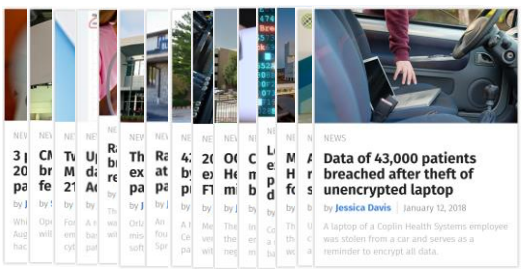
1

Peter J. Cass, OD - Disclosures

- Associate, MyEyeDr Beaumont,
- Vice President, Practice Compliance Solutions
- Past President, Texas Optometric Association
  - Chair HIT Committee, member AOA HIE Workgroup
  - L&L Committee, Third party Committee
- Adjunct Faculty, University of Houston College of Optometry
- Board Member, Elevate Digital Optics Lab
- Consultant/Speaker for ophthalmic companies:
  - Alcon, Bausch & Lomb, BioD, Crystal Practice Management, Diopsys, Solution Reach, Katena, Tear Science, Shire, Weave
- Lecturer for
  - Professional groups: Vision Source, Vision West, ECPN, PERC, Vision Trends, Vision West, TSO, etc.
  - Universities: RSO, UHCO, UAB, etc.
  - State associations: TOA, and over 20 others
- Working relationships with: CodeSafePlus
- Shareholder Essentia, EDO labs, PCS, CVS

2

Scope of problem



3

Scope of problem

- Healthcare is **the most targeted industry** by ransomware attacks
- Ransomware attacks on healthcare almost doubled – 66% of healthcare organizations surveyed were hit by ransomware in 2021, up from 34% in 2020
- Ransom demands reached $2.8 million in special cases
- **The median demand is $10,000**
- **71% of incidents were for small & medium-sized businesses**
- Hackers have also been adding pressure by conducting reconnaissance on their network and **compromising back-ups before deploying malware.**

4

Why small businesses?

- **Larger companies often have more resources** to put better controls in place.
- Smaller companies are **less likely to have properly segmented their backups**
- Smaller companies are **more likely to pay**

5

Data breaches have HIPAA implications

2015 update... $10,000 MINIMUM fine for ANY, even minor HIPAA violation

- **Moderate** ($5,000 - $150,000 per violation per day)
  Compliant but significant omission or breach

- **Severe** (any amount up to $1.5 Million)
  Severe breach; willful neglect; "reckless indifference"

"Reckless indifference"
That can cost you $250,000.00

6

So…Are YOU HIPAA compliant?

To be compliant, you must have:

1. Privacy and Public Information **Officers**
2. **Notice** of Privacy Practice / **Acknowledgement** of

You are legally obligated to do all this and have doctors AND STAFF that are prepared to answer patient's questions about their rights and your policies

7

And you must know how to handle:

- Authorizations
- Medical records review
- Marketing
- Medical records request
- Minimum Necessary Rule
- Request to change medical records
- Incidental Disclosure Rule
- Requests for disclosure documentation
- Business Associates
- Individual privacy accommodations requests
- HIPAA Breach

HIPAA legislation totals 2712 pages of legal mumbo jumbo.

You and your staff must understand all of these issues and they must be addressed in your Privacy Manual

8

And conduct a Security Risk Analysis:

- The Security Standards do not prescribe a
  - ➢specific policy,
  - ➢software or
  - ➢other course of action and
  - ➢do not hold large and small business to the same standard!
- A unique risk analysis conducted by the covered entity is required
  - ➢the OIG says **YOU must participate** in this analysis
- Be wary of "experts" telling you that you MUST do certain things under the Security Rules

9

HIPAA Privacy & Security Clarifications

- 45 CFR164 522-530
  - ➢All covered entities and business associates are required by law to implement measures that "**guard against unauthorized access to PHI that is being transmitted over an electronic communications network**"
- What is an "electronic communications network"?
  - ➢Email
  - ➢Text
  - ➢**Anything involving the internet**
  - ➢FAX?

10

In the context of Cybersecurity

- Infrastructure
- Data
- Communications
- Updates
- IT companies
- Security Policies

11

Infrastructure

- Use as much hardwiring as possible.
  - ➢WIFI is nice, but not as reliable, fast or secure.
  - ➢We use a mix of both in my office, but
  - ➢I try to **plug in as many devices as possible**.

12

Routers

- A good **commercial grade router** (SonicWall makes some really good ones).
- The cheaper small office/home ones are much riskier and less reliable.
- **Separate and segregated the Wi-Fi for patients**

13

Wi-Fi

- **Separate and segregated the Wi-Fi for patients**

14

Workstations

- Install as few programs on workstations as possible.
- As a rule, only install
  - EHR client and
  - antivirus software on workstation

15

Remote access

- There are some decent HIPAA compliant programs
  - www.TeamViewer.com
  - www.GoToMyPC.com
  - www.LogMeIn.com

16

VPNs

- The most secure is a VPN
  - We use **VPN certificates** for secure remote access for doctors & key staff
  - Have your IT company set it up

17

Protecting your EMR - Encryption

- Hard Drive Encryption
  - It is a "must have"
  - Patient data must be encrypted.
  - Windows 10 and higher has a full hard drive encryption option integrated with the OS called **BitLocker**
  - In the event of a breach, doctors who do not have the data encrypted **will be held responsible**
  - Encryption is a get out of jail free card

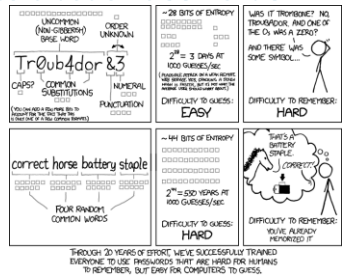
18

Protecting your EMR - Passwords

- Use Strong passwords
- Protect the **EMR**
- Protect the **operating system**
- Don't forget the **server**

19

A note about Passwords



20

Protecting your EMR - Antivirus

- Antivirus software
  - another "must have".
  - www.MacAfee.com
  - www.Norton.com
  - www.TrendMicro.com

21

Protecting your EMR - Firewalls

- Firewalls
  - **Windows** (and most antivirus programs) provide decent firewall protection
  - Having a good IT company configure the firewall on the **router** adds an extra layer of security
  - **Separate any free Wi-Fi paths** from the intraoffice

22

Communication

3 Types

1. **FROM** the patient
2. **TO** the patient
3. **Third Party** (To anyone EXCEPT the patient)

23

Communications FROM the Patient

- The HIPAA Privacy and Security Rules **do NOT apply to communications FROM the patient**. But as soon as the provider receives the email, the information now **must be protected by the provider**.
- For any communication BACK to the patient from their initial response or any contact initiated by the provider, refer to next slides

24

Communications TO the Patient

- "The Security Rule **does not expressly prohibit the use of email** to communicate with a patient. However, the standards require certain procedures to restrict access, protect the integrity of and guard against unauthorized access to PHI."
- What are "certain procedures"?
  - ➢Finally defined in 2015 – "**reasonable precautions… equivalent to encryption**"

25

Communications TO the Patient

- If you elect to communicate with your patient via email, you have two choices:
  1. **Secure the Transmission**
  2. **"Equivalent to encryption"** – *whatever that is*
- We suggest all communications are encrypted.
  - ➢HHS suggests email communication be limited to only secure patient portal systems

26

Communications TO the Patient

- If using non secure transmission, required to **inform the patient**:
  - ➢The communication may not be secure
  - ➢The potential consequences of that
  - ➢Patient must confirm they understand the risks and confirm they wish to continue.

Does not state HOW they confirm this but anything less than **written authorization** would be foolish

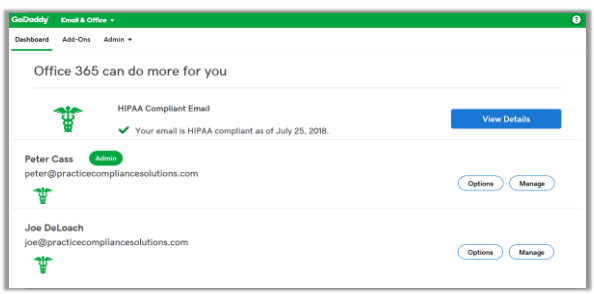
27

Communications TO Third Party

- No stated exception to the encryption criteria and no expressed authority for the patient to "waive" these security measures
  - ➢In fact court rulings to the contrary
- Specifically includes text and email communication (but not FAX – can't encrypt or decrypt FAX)
- This is EVERYONE else – including referral letters!

28

Are there secure email systems?



29

Summary of Text & Email

- For ALL text or email correspondence to EVERYONE (including the patient) – use only secured, encrypted text or email or a secured patient portal system

Well maybe we can say that…
Feb 2017

Children Hospital, Texas settled with OCR for $2.3 MILLION for failure to encrypt communications with patients

30

Updates - Servers

- It is very important to keep your server up to date.
- It is the **core of our EHR system** and any issues with it can shut the entire office down quickly.
- Use a **high-end machine** from a manufacturer with a good reputation.
- It **needs to run very smoothly** at all times.
- At the first sign of trouble it should be replaced. I do not recommend trying to repair a server, replace it with a better machine.

31

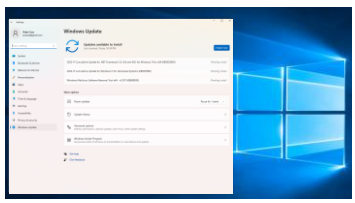
Updates - Workstations

- When one breaks or begins to function poorly, I order an inexpensive replacement online.
- If the workstations have **no patient data** and very few programs they **can be changed out rapidly** and **don't require high end specifications**.

32

Updates – Software

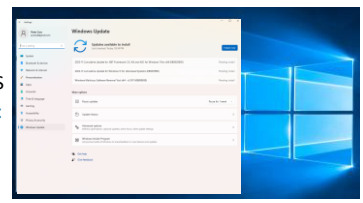
- Update software regularly, especially
  - **operating system,**
  - **antivirus, and**
  - **EHR**
- Not keeping those 3 current increases the risk of breach



33

Updates - Operating Systems

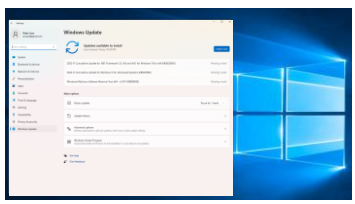
- Can be a pain, but is necessary
- **Get rid of those old machines** with old OS
- **Not HIPAA compliant**



34

Updates – EHR

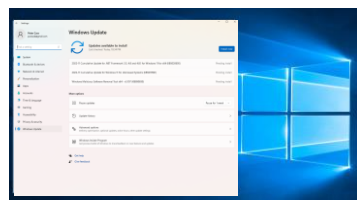
- Update especially
- Usually helpful too



35

Updates - Antivirus

- Should be **automatic**



36

IT Companies

- Establish a relationship with an IT company
- **Most doctors do not have the expertise** to set up commercial routers and firewalls properly
- Be wary of expensive contracts - usually a retainer and periodic updates are fine

37

IT Companies – build a relationship

- **Have them setup your network**
- If you ever have a problem, you will already have someone to contact
- Have them help with **upgrades**
- They can also help with security camera, fire alarms, etc

38

IT Companies in rural areas

- If there is no one in your area **find someone in a nearby city** that is willing to travel
- This should be done **before there is a problem**
  - Most of us are VERY dependent on our computer systems

39

Security Protocols

- Staff training is key. The staff need to know that:
  - They **should** use secure passwords
  - They should **not** share their passwords
  - They should **not** install ANY software without doctor or IT company approval (including screen savers)
  - They should **not** check personal email or social media on company devices
  - They should **not** download ANY attachments to emails, unless they were expecting the attachment.

40

Formal staff training

- In a breach, **you need to be able to prove you trained**
- Need a **formal program**
- You should **test your staff**
- **Must document** that they did training

41

HIPAA Security Rules

Requirements

1. Appoint a **Security Officer**
2. Conduct a **risk analysis** and risk management plan to determine threats or risks in your operational systems
3. Complete the Organizational Requirements
4. Documented policies and procedures for all applicable Security Standards – **Security Manual**

42

HIPAA Security Risk Analysis

- HIPAA Security Standards do not prescribe a
  - specific policy,
  - software or
  - other course of action and
  - do not hold large and small business to the same standard!
- A unique risk analysis conducted by the covered entity is required
  - the OIG says **YOU must participate** in this analysis
- Be wary of "experts" telling you that you MUST do certain things under the Security Rules

43

HIPAA Compliance Basics:

To be compliant, you must have:

1. Privacy and Public Information **Officers**
2. **Notice** of Privacy Practice / **Acknowledgement** of Notice
3. **Privacy Manual**
4. **Security Manual** w/ an SRA that will pass an audit!
5. Documented staff **training** (lack of cost one OD $25K)
6. **Business Associate Agreements** (current format)

44

National Cybersecurity & Communications Integration Center (NCCIC) Tips

- **Update** software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- **Never click on links or open attachments** in unsolicited emails.
- **Backup** data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when browsing the Internet.

45

National Cybersecurity & Communications Integration Center (NCCIC) Tips

- **Restrict users' permissions** to install and run software applications, and apply the principle of "least privilege" to all systems and services.
  - Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- **Use application whitelisting** to allow only approved programs to run on a network.

46

National Cybersecurity & Communications Integration Center (NCCIC) Tips

- Enable **strong spam filters** to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- **Configure firewalls** to block access to known malicious IP addresses

47

48

Ransomware

- Ransomware is becoming a significant threat to small providers
  - A type of malware that: *"attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key."*
- Taking steps to prevent and avoid attacks are important
- Especially in light of the more aggressive pursual of HIPAA violations.

49

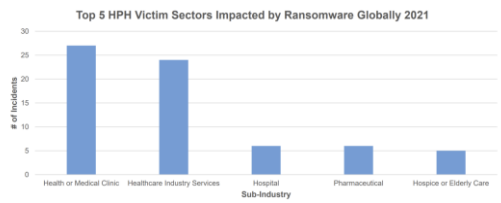
HHS Statistics

- According to HHS:

*"Ransomware is the fastest growing malware threat, with more than **4,000 ransomware attacks occurring daily** since January 2016"*

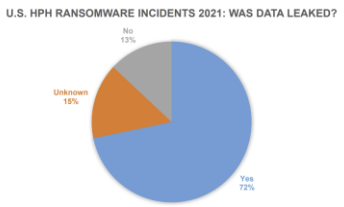
50

HHS Statistics



51

HHS Statistics



52

Ransomware as a breach

- HHS notes that
  - *"[w]hen [ePHI] is encrypted as a result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired[,] and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."*
- In other words, you are required to presume a ransomware incident **is a breach** unless the evidence demonstrates a low probability of compromise based on risk assessment factors

53

Risk assessment factors

- The risk of compromise is based on 4 things:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

54

Discovering a breach

- Rans
  1. to
     to
     nd/or
  2. on

55

Next steps

- Most victims **check to determine whether sufficient backups** exist to restore the encrypted files and avoid paying the ransom.
- But be careful, **IT assistance should be sought**, to determine how the ransomware accessed the system.
- For healthcare providers, it is imperative to **determine whether there the data was actually compromised**.
- If the computer is formatted, **you may not be able to determine**, and will have to notify all individuals whose information was on the affected computer

56

How to spot CYBERATTACK emails

- **Emails describing**:
  - Account verifications
  - Unclaimed property / packages
  - Requests for money
  - Unrealistic threats
  - Update payment details
- **Don't know the sender**…don't open
- Look for **valid usernames** and domain names
  - Domain at the end – domain@joe.com vs joe@domain.com
  - Check the hyperlinked address (mouse hover in outlook)
  - Spelling and grammatical errores (oops)
  - Emails from the government (they don't work that way!)

57

How to spot CYBERATTACK emails

- Message asks for personal information
- They tell a story leading you to take action
- **Sender and domain don't match**
  - xx. From: Paypal <paypal@imacrook.com>
- Slightly **misspelled domain** – ex. fedex.com vs fedez.com
- Check the link (again, mouse hover)
- Emails with **generic domains** (Gmail, Hotmail, etc)
- Offers that seem **too good to be true** (they always are)
- If it looks suspicious, it probably is!

58

Avoiding

- Most importantly, users should ask themselves if they were **expecting to receive a document** or link from this user.
- To confirm, users should call the sender – not email – to **confirm** whether an email is legitimate
  - unauthorized actors often remain in the email box, responding affirmatively to questions of legitimacy

59

HHS also suggests

- **Implement proven and tested response procedures** when employees click on phishing emails
  - By conducting phishing simulations
- Establish cyber threat information sharing with other healthcare providers.

60

Questions?

peter@practicecompliancesolutions.com

61