HIPAA Compliance Does NOT Work

Bruce McCully, CISSP
I am Your Security / Computer Expert

This material does not constitute legal advice and covers only federal law.

For legal advice pertaining to HIPAA/HITECH compliance, contact your personal attorney.
Bruce McCully

My company eliminates computer problems for rural hospitals. We help people succeed by managing their compliance without costing an arm and a leg.
Why Is HIPAA Compliance THAT Important?

Fines?  Guidelines?  Prevention?

72,602 word document from 1996
Quick and Dirty HIPAA Compliance

- Restrict access to PHI?
- Policies and procedures for managing and assessing risk of PHI?
- Termination procedures?
- Disaster recovery plan (tested plan)?
- Security officer on team?
- Staff HIPAA training?
- Business Associates and BAAs?
- Limit physical access to PHI?
- Record of hardware containing PHI?
<table>
<thead>
<tr>
<th>Violation category—Section 1176(a)(1)</th>
<th>Each violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did Not Know</td>
<td>$100–$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>1,000–50,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect—Corrected</td>
<td>10,000–50,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>(C)(ii) Willful Neglect—Not Corrected</td>
<td>50,000</td>
<td>1,500,000</td>
</tr>
</tbody>
</table>
HIPAA Fines Really Aren’t The Scary Part!

Real reason for HIPAA?

Make sure healthcare is keeping patient data safe!

Plain and Simple.
What’s more important than fines?

Patient trust?
Employee trust?
Keeping patients safe?

Bob sits in his office, face in hands.
“But We’re Small... Nobody Would Bother To Hack Us, Right?”

Wrong!

• **One in five** organizations fall victim to cybercrime each year and that number is GROWING.
  *(Source: National Cyber Security Alliance)*

• Small organizations **are low-hanging fruit** because they don’t believe they are a target, and therefore have very loose or no security systems and protocols in place. (Think about your contractors!)

• **Half of all cyber attacks** are aimed at SMBs.
  *(Source: Forbes Article, “5 Ways Small Businesses Can Protect Against Cybercrime”)*
These are all large organizations – they don’t want my data – Right?

- 71% of security breaches target rural healthcare
- 20,765 records are stolen on average per data breach
- $201 is the average cost per record stolen in a data breach
- 60% of hospitals fail after a data breach
The Problem with HIPAA Assessments?

Check lists don’t always catch everything!

Missing pieces if security isn’t thought through

Not sufficient without context

Hospitals are passing HIPAA risk assessments, YET are still getting attacked by ransomware!

HIPAA Requirements ARE NOT updated regularly!
The OTHER Problem with HIPAA Risk Assessments?
Hospitals Are Passing HIPAA Assessments With Flying Colors YET Still Get Ransomware Infections!
Hospitals Are Passing HIPAA Assessments With Flying Colors YET Still Get Ransomware Infections!

I have Backups. I'm safe. Why not pay?
We have always remained compliant with the current regulations concerning our IT systems and have spent untold dollars to take care of our data. In fact, we completed a full security evaluation in November 2017.

On or about the 15th of January 2018 our company was attacked by ransomware. On the 8th page of Bruce’s book, the first paragraph asks you to speculate on how you would react if this happened to you. I can tell you that I no longer have to wonder. We were helpless. Our company was stopped in its tracks. We had over 400 computers and 30 plus servers that had almost every file encrypted. Our IT capabilities were quickly overwhelmed. By the grace of God we were introduced to Bruce’s team.

Bruce and his group immediately sent a disaster recovery team to mitigate the issues and then to repair our systems. I do not believe another company could have done what they did for us. They have worked around the clock to recover our data and to get us back in business. We have truly found a partner for our future.

Sydney Sawyer
CEO, Lackey Memorial Hospital
What Are We Protecting?
Eye Spy PHI

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Affinity Health Plan – Photocopyer Hard Drive Not Securely Wiped
$1,215,780
$100,000

Alaska Dept. of HHS – Unencrypted USB
$1,700,000

NAS Insurance Services – Records Placed In Recycling Bin
Legal and Patient Notification Costs
$85,000

Triple-S Management Corp. – $6.8 Million For Improperly Handling Medical Records of 70,000 Patients
PHI is everywhere!

Who Wants My PHI and WHY?
Who Depends On Medical Records?

Radiology?
Nursing?
ER?
Pulmonary?
Dietary?
Medical Records?

Medical Billing?
Who Depends On Medical Records?

Radiology?
Nursing?
ER?
Pulmonary?
Dietary?
Medical?
Medical Billing?

EVERYONE!
CONFIDENTIAL

February 24, 2017

Dear [Name]

We are pleased to confirm the engagement of Kroll Cyber Security, LLC ("Kroll") by [Company Name] ("Client", and together with Kroll, the "Parties") pursuant to this letter of engagement (the "Agreement").

1. **Kroll Services**

Client has engaged Kroll to perform certain services regarding cyber investigation and incident response, as outlined below (the "Assignment").

**Kroll will conduct the following:**

**Phase 1** - Budget - $28k to $32k

- Determine timeline of events relating to possible network breach.
- Collect, preserve, and analyze available logs as collected by SIM/SIEM device for evidence of unauthorized activity.
- Analyze up to (2) computers for evidence of malware.
Cash Flow Is Critical To Keeping The Lights On!

(Business side of healthcare depends on medical records too!)

$50K ransom, why not pay it? $2M in AR wrapped up in Encrypted Files
Why Healthcare is Behind on Cybersecurity?

- Poor training
- Hard to recruit
- Hard to retain
- IT not specialized on healthcare
- Focused on passing a test (HIPAA) NOT on securing their patient data

Unencrypted backups that could be accessed by anyone in the organization...
Eyes On The Prize: Healthcare

Majority of cyberattacks targeting healthcare!

Attacks on healthcare in 2018 up by 25%

Targeted hospital cyber attacks: 477 successful attacks

Hospital spending on HIPAA: $100 Billion
What is the Dark Web?
Finding Data On The Dark Web?

http://3g2upl4pq6kufc4m.onion/
The Digital Underground’s Thriving Black Market

Credit card details: $2 to $90
Social Security Numbers: $30
Date of Birth: $11
Health Records: $1,200
Your Data (Ransom): $10,000+

Anyone can easily buy training, tools, and services for committing fraud, hacking systems, buying stolen credit cards, setting up fake web sites, etc.

Trojan Kit for as little as $1,000
16:04 @BB>> HEY - I WANT INTO A NETWORK.
16:50 @BB>> HEY - I WANT INTO A NETWORK. HELP ME?
17:12 @BB>> WANT INTO A NETWORK. HELP ME?
17:14 @TZ>> y0u 0ff3r1n6?
17:15 @BB>> BIT COIN. HAVE NAME. HAVE IP.
17:21 @TZ>> ?yp3 Of n37w0rk?
17:22 @BB>> WINDOWS. NAT FIREWALL. WANT ACCESS.
17:35 @TZ>> 0.02 b7c 4 d4y
Growing Hacks From Unloved Networks

VULNERABILITY RISK

EXTERNAL FACTORS

1. Identified
2. Disclosed
3. Published Proof of Concept
4. Scanner Availability
5. Weaponised in Malcode
6. Commoditized in Exploit Kits

LEVEL OF RISK

Copyright © 2018 Dynamic Edge, Inc. All rights reserved.
Attacks are targeting MANY vulnerabilities in your system
One Little Flaw Leads To A BIG Hack

Vulnerability
Notification
Dark Web Chatter
Exploit Created
Recruitment
Campaign
Disaster
One Recent Case: SamSam

Day 1: Infection—300 Users Down
Day 2: Fiddle thumbs
Day 3: Fiddle thumbs
Day 4: Called for help
- 
- 
- 
Day 6: Data Recovery
- 
- 
- 
Day 15: Remediation Recovered

15 Days to get critical services back online (Medical Billing)

IT Director middle of EHR rollout.
BUT, I have Cyber Insurance!

**GENERAL INFORMATION**

<table>
<thead>
<tr>
<th>Name of Applicant:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>City:</th>
<th>State:</th>
<th>Zip:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web Address:</th>
<th>Total Revenues:</th>
<th>Total Assets:</th>
<th>Employees:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
</tbody>
</table>

**UNDERWRITING QUESTIONS**

1. Does the Applicant have:
   - [ ] Up-to-date, active firewall technology
   - [ ] Patch management procedures
   - [ ] Multi-factor login for privileged access
   - [ ] Remote access limited to VPN
   - [ ] Incident response plan
   - [ ] Media and website content controls
   - [ ] Require service providers to demonstrate adequate network security
   - [ ] Updated anti-virus software active on all computers and networks
   - [ ] Intrusion detection software
   - [ ] Valuable/sensitive data backup procedures
   - [ ] Procedure to test or audit network security controls
   - [ ] Disaster recovery plan, business continuity plan
   - [ ] A person or department responsible

2. If applicable, is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)?
   - [ ] Yes  [ ] No  [ ] N/A

3. If applicable, is the Applicant HIPAA compliant?
   - [ ] Yes  [ ] No  [ ] N/A

4. Does the Applicant encrypt private or sensitive data?
   - [ ] At Rest  [ ] In Transit  [ ] On Laptops and Mobile Devices

Copyright © 2018 Dynamic Edge, Inc. All rights reserved.
How Ransomware Infects Healthcare

Network-Wide Attacks

Patches
Ports
People
Perimeters
Security NOT A Focus In Most Hospitals

Physical PHI (Medical Billing, Medical Records)

Electronic PHI (unlocked computers, no encryption)

Failed Integrations

No Accountability

Issues with Interfaces
Door Openers For Ransomware
Hospitals – here is the scary part...

75% of small businesses (under 250 employees) believe that they are safe from hackers!
Business Associates are Your Achilles heel...

75% of small businesses (under 250 employees) believe that they are safe from hackers!

AND MANY OF THEM HAVE ACCESS TO YOUR PHI!

Controller / Bank
$400,000 because you don’t have your BAA up-to-date?


My EHR is cloud based! I’m safe, right?

22% of ransomware is traceable to cloud vendors.
How Can Healthcare Improve?

Bring context to checklists and frameworks

Change Our Culture!
CHANGE CULTURE?

EDUCATE

Get staff interested in security
Build alliances
CHANGE CULTURE?

LEARN FROM MISTAKES
Share real life events.
What went wrong?
How do we prevent this next time?
CHANGE CULTURE?

REWARD

Engage your team with metrics.

Set goals.

Celebrate small wins.
Patch Management Tracking

Most ransomware caused by unpatched machines— including big attacks like Equifax!

“Too many damn patches!”

Legacy vulnerabilities remain unpatched

Most cyberattacks targeting unpatched systems lag at least a month after a security patch is released (plenty of time to apply it!).
Understandable Security Policies

Making policies easy to follow and remember

Dealing with BYOD

Keeping sensitive data encrypted

Eliminating or limiting risks
Lists Of Hacked Passwords

Hackers have lists of hacked password

(Your password may be more commonly used than you’d think.)
When was the last time you updated any of your passwords?

Do not use the same passwords for your accounts....
From: James S. Meyer [mailto:jsmeyer@stgregorys.edu]

Sent: Monday, January 23, 2017 12:33 PM

Subject: Total Held Email: 25 Contact Messages

Office 365

Total Held Email: 25 Contact Messages
Date: 01-23-2017

Please continue below in order to view your important contact messages.

Click to follow link

Continue

25 contact email messages will be automatically deleted after 24 hours

Sincerely,
James S. Meyer
The Microsoft Online Services Team
Heuristic-trained firewalls

Encapsulate ALL sensitive data

Channels through firewall for vendors

Monitor network and capable detecting suspicious activity

Right configuration is key!
Educate Your Team: Know How To Recognize A Scam

http://www.dynedge.com/email-phishing-scams-are-getting-more-sophisticated-is-your-team-prepared/
Protecting EHR Data

EHR vendors don’t necessarily keep data secure

BUT many expect you to have your security in order (written explicitly in their contracts)

EHR systems inherently buggy (some hospital staff may have unsafe workarounds!)

How do you make sure your PHI is protected housed in your EHR?
Backing Up Data OFF Network

Onsite vs Offsite backups?
Scheduled backups?
Test the backup?
Disaster recovery (what if your laptop is stolen)?
Don’t Just Check A Box?

No golden checklist for cybersecurity.

Know the context to security.

Revise your security checks as you go (no checklist is complete or even comprehensive).

Experts rely on checklists as reminders, NOT an end to resolving security.
Identify and Prioritize Your Vulnerabilities

1. Scan for systems to hack.

2. Install software to scan, compromise, and infect agents.

3. Agents are loaded with remote control attack software.

4. The client issues commands to handlers that control agents in a mass attack.
In Doubt? Get A Second Opinion!
Accountability
Annual Check List

Review Simple Contingency Check List
  • Update numbers, contact names, and account information
  • Redistribute to list

Review backup and recovery log sheets
  • Are they being completed?
  • Are they taking long enough?
  • Does it appear as though enough data is being backed up?

Check office safety equipment
  • Fire extinguishers
  • Emergency / First Aid Supplies

Remind team locations of safety equipment

Perform Bare Metal Restore of server and key workstations

Perform HIPAA Security Risk Assessment

Submit breach log to HHS
Due to the recent ransomware attacks on healthcare and breaches in our community, we decided we should do an assessment with Bruce and his team after seeing Bruce’s ransomware presentation at a local IT managers meeting. I wanted a better idea of how secure our hospital was from ransomware.

Bruce’s team provided a detailed report and, most importantly, spent time to explain it. I am happy I decided to invite our CFO to the meeting. It was good for him to have someone else explain our risks other than me in terms that he understood.

Bruce’s team explained everything at an executive level for our CFO, then turned around and broke down the details for my entire technical team. Bruce’s team brought to light security concerns my technical team or I were not aware of. Even if you have had a recent HIPAA risk assessment, I’d suggest you have the Healthcureity team out for a ransomware assessment. Certainly worth the investment.

Brian Howell
IT Director, War Memorial Hospital
Next Step...
Learn How You Are Doing

Performing 5 FREE Network Assessments

HEALTHCURITY
Healthcare IT Support & Security

Copyright © 2018 Dynamic Edge, Inc. All rights reserved.
What are the main causes of economic loss?

- **Loss of Reputation**: 61%
- **Business Interruption**: 49%
- **Damages Paid to Customer**: 45%
- **Loss of Trade Secrets**: 20%
- **Subsequent Requirements**: 11%
- **Website Downtime**: 9%
- **Notification Costs**: 9%
- **Extortion**: 7%
- **Other**: 0%

Allianz Security Study 2015
What is preventing organizations being better prepared against cyber risks?

- Risk is underestimated: 73%
- Budget constraints: 59%
- Haven't analyzed the problem: 54%
- Infrastructure to sensitive to changes: 30%
- Haven't identified the right personnel: 10%
- Other: 8%

Allianz Security Study 2015

Copyright © 2018 Dynamic Edge, Inc. All rights reserved.
$400,000 because you don’t have your BAA up-to-date?


Are you auditing your Business Associates?
Next Step...
Learn How You Are Doing

Performing 5 FREE Network Assessments