Do I Fall Under HIPAA?

- Do you furnish, receive, or bill for healthcare?
  - No: No HIPAA For You
  - Yes: Do you transmit covered transactions electronically?
    - Yes: Welcome To HIPAA
    - No: No HIPAA For You

Network Types

What network fits my needs?
**On Premises Network**
- All hardware, software & data is onsite under your control.
  - Complete control.
  - High upfront cost.
  - Requires IT staff.
  - You own your data.
  - High Risk

**Hybrid Cloud Network**
- You pick what’s in the cloud & what’s on premises
  - Some control.
  - Medium upfront cost.
  - Low to medium monthly payments.
  - May require IT staff.
  - High to Low risk based on setup.
  - Simpler backup and disaster recovery.
  - Who owns your data?

**Cloud Network**
- Let someone else deal with it.
  - Little control.
  - Low upfront cost.
  - Monthly fees based on users or usage.
  - Low risk based on setup.
  - Backups and disaster recovery provided.
  - Who owns your data?
HIPAA 201: Security Considerations

<table>
<thead>
<tr>
<th>HIPAA Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Administrative</td>
</tr>
<tr>
<td>- Physical Security</td>
</tr>
<tr>
<td>- Technical Safeguards</td>
</tr>
<tr>
<td>- Training</td>
</tr>
<tr>
<td>- Incident Response</td>
</tr>
</tbody>
</table>

Administrative Safeguards

- **Security Management Process 164.308(a)(1)**
  1. [R]Risk Analysis 164.308(a)(1)(i)(A)
  2. [R]Risk Management 164.308(a)(1)(i)(B)
  3. [R]Sanction Policy 164.308(a)(1)(i)(C)
  4. [R]Information Systems Activity Review 164.308(a)(1)(i)(C)
  5. [R]Assigned Security Responsibility 164.308(a)(2)

- **Workforce Security 164.308(a)(3)**
Administrative Safeguards
- Information Access Management 164.308(a)(4)
  1. (R) Isolating Health Care Clearinghouse Functions 164.308(a)(4)(ii)(A)
  2. (A) Access Authorization 164.308(a)(4)(ii)(B)
  3. (A) Access Establishment & Modification 164.308(a)(4)(ii)(C)

Administrative Safeguards
- Security Awareness & Training 164.308(a)(5)
  1. (A) Security Reminders 164.308(a)(5)(i)(A)
  2. (A) Protection from Malicious Software 164.308(a)(5)(i)(B)
  3. (A) Log-in Monitoring 164.308(a)(5)(i)(C)
  4. (A) Password Management 164.308(a)(5)(i)(D)

Administrative Safeguards
- Security Incident Procedures 164.308(a)(6)
  1. (R) Response & Reporting 164.308(a)(6)(i)
Administrative Safeguards
- Contingency Plan 164.308(a)(7)
  1. [R] Data Backup 164.308(a)(7)(i)(A)
  2. [R] Disaster Recovery Plan 164.308(a)(7)(i)(B)
  5. [A] Applications & Data Criticality Analysis 164.308(a)(7)(ii)(B)
  6. [R] Evaluation 164.308(a)(7)(ii)(C)

Administrative Safeguards
- Business Associate Contracts & Arrangements 164.308(b)(1)
  1. [R] Written Contract or Other Arrangements 164.308(b)(1)(A)

HIPAA Security
- Administrative
- Physical Security
- Technical Safeguards
- Training
- Incident Response
Physical Safeguards

• Facility Access Controls 164.310(a)(1)
  1. (A)Contingency Operations 164.310(a)(i)
  2. (A)Facility Security Plan 164.310(a)(ii)
  3. (A)Access Control & Validation Procedures 164.310(a)(iii)
  4. (A)Maintenance Records 164.310(a)(iv)
  5. (R)Workstation Use 164.310(b)
  6. (R)Workstation Security 164.310(b)

Physical Safeguards

• Device & Media Controls 164.310(b)(1)
  1. (R)Disposal 164.310(b)(2)(i)
  2. (R)Media Re-use 164.310(b)(2)(ii)
  3. (A)Accountability 164.310(b)(2)(iii)
  4. (A)Data Backup & Storage 164.310(b)(2)(iv)

HIPAA Security

• Administrative
• Physical Security
• Technical Safeguards
• Training
• Incident Response
Technical Safeguards

Access Control 164.312(a)(1)

1. [R] Unique User Identification 164.312(a)(2)(i)
2. [R] Emergency Access Procedure 164.312(a)(2)(ii)
4. [R] Encryption & Decryption 164.310(a)(2)(iv)
5. [R] Audit Controls 164.312(b)

Technical Safeguards

Integrity 164.312(c)(1)

1. [A] Mechanism to Authenticate Electronic Protected Health Information 164.312(c)(2)
2. [R] Person or Entity Authentication 164.312(d)

Technical Safeguards

Transmission Security 164.312(e)(1)

1. [A] Integrity Controls 164.312(c)(2)(i)
2. [A] Encryption 164.312(e)(2)(ii)
Training

- You can pay for online training.
- What would a training outline look like?
  1. What are HIPAA & the HITECH Act?
  2. Why is my clinic covered?
  3. What is the Privacy Rule?
  4. What is the Security Rule?
  5. What is meaningful use?
  6. Breach notifications
  7. Enforcement (Inside / Outside the clinic)
- Training should be tailored to individual’s role/access to PHI
- Periodic re-training should occur
## HIPAA 201: Security Considerations

### HIPAA HIPPO

![HIPAA HIPPO Image]

*IS DISPLEASED WITH YOUR HANDLING OF PROTECTED HEALTH INFORMATION.*

### Healthcare Data Breaches > 500 Individuals Affected

- Unauthorized Access / Disclosure: 6%
- Theft / Loss: 75%
- Improper Disposal: 1%
- Hacking / IT Incident: 7%
- Other / Unknown: 11%

### Estimated Data Breach Cost

<table>
<thead>
<tr>
<th>Source of Cost</th>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of records maintained by clinic</td>
<td>10,000</td>
<td></td>
</tr>
<tr>
<td>Legal, forensics, media &amp; public relations costs</td>
<td>@ $100 /h</td>
<td>$10,000</td>
</tr>
<tr>
<td>Internal research &amp; investigation labor cost</td>
<td>@ $75 /h</td>
<td>$7,500</td>
</tr>
<tr>
<td>Credit monitoring servers for one year</td>
<td>@ $10 per record per month for 50% of clients affected</td>
<td>$600,000</td>
</tr>
<tr>
<td>Notifications costs</td>
<td>@ $1.00 per letter</td>
<td>$10,000</td>
</tr>
<tr>
<td><strong>TOTAL COST WITHOUT LITIGATION</strong></td>
<td></td>
<td>$667,500</td>
</tr>
<tr>
<td>Class action litigations are $1,000 per record. The legal costs would significantly increase as well.</td>
<td></td>
<td>$10,000,000</td>
</tr>
<tr>
<td><strong>Total cost WITH litigation settled at 10%</strong></td>
<td></td>
<td>$1,667,500</td>
</tr>
</tbody>
</table>
Incident Response

- Dr. Scott, I may have taken photos of my client and posted them on Facebook. Also when I was driving here to tell you, his medical record blew out my car window.

- So now what? Let’s get the following information.
  1. Name of individual making the report.
  2. The individual’s contact information.
  3. Location where the incident took place.
  4. Time and date that the incident occurred.
  5. Brief synopsis of the incident.
  6. Rationale behind making the report.

Incident Response

- And review.
  1. Confirmation
  2. Analysis
  3. Notification
  4. Containment
  5. Eradication
  6. Recovery
  7. Review
  8. Retraining?

HIPAA Timeline

- Fall
- Spring
- Summer
- On Going
Fall Tasks
- Spend the fall semester getting familiar with HIPAA & HITECH.
  1. Gather up the information you already have, even if it's old and out of date.
  2. Review how your clinic works.
     - Follow a client record from start to archiving
     - Where do clients wait?
     - What can the everyday visitor see?
  3. How do students access PHI?
  4. Where is your PHI located?
  5. Make a list of what documents you have and what you need.
  6. Think of internal and external threats to the clinic.

HIPAA Timeline
- Fall
- Spring
- Summer
- On Going

Spring Tasks
- Review the clinic’s IT systems.
  1. Think of training, what has happened in the past?
     1. How has it occurred?
     2. Who's been trained? According to their role?
     3. Records of training stored?
     4. Periodic retraining?
  2. Mitigation plans
  3. Data monitoring
  4. Sanctions policies
  5. Incident response plans
  6. Disaster recovery plans


**HIPAA Timeline**
- Fall
- Spring
- Summer
- On Going

---

**Summer Tasks**
- Use this slow time in the year to update systems and test new policies & procedures.
  1. Applying software and settings to comply with HIPAA.
  2. Review access controls.
  4. Review EMR systems.
  5. Generate how-to guides for end-users.
  6. Test audit.
## HIPAA Review Timeline

<table>
<thead>
<tr>
<th>Month</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Access</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Inventory</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Vulnerability Testing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Training</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Walk - Audit</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### HIPAA Myths

- My electronic medical record software is HIPAA compliant so that makes me HIPAA compliant.
- My Business Associate handles my security so I'm HIPAA compliant.
- I have Policies and Procedures in place, Now I am HIPAA compliant.
Myths

- I did a self audit years ago and nothing has changed, I’m good to go. Correct?
- I won’t be audited.
- I won’t have a data breach.
- I do not need a privacy or security official.

Questions

Our IT department has set up a secure HIPAA drive that can only be used on campus computers in our building. This surely limits what students/supervisors can do at home. IT & Legal say they do NOT want to move forward off campus because of expense & risk.

- How did you design a secure encrypted model that works both on and off campus?
Questions

Contact Information

- Dr. Lisa Scott
  - Florida State University
  - 850-322-8727 (cell) or 850-644-2238 (work)
  - Lisa.Scott@cci.fsu.edu

- Thomas Turner
  - McGladrey
  - 281-684-1882
  - Thomas.Turner@McGladrey.com