HIPAA & Confidentiality 101

Katie Malinski, LCSW
www.HIPAAforTherapists.com

Who I am

• Katie Malinski, LCSW
• Therapist in private practice in Austin
• Specialist in parenting & childhood sexual development
• The founder of HIPAA for Therapists, an in-person and online HIPAA training program for private practice therapists.
Who I am not

• An attorney (this is not legal advice)
• A security expert
• A member of your agency (i.e., I’m not in the know about all current procedures, etc.)
• The source of everything HIPAA that you need to know.

Course Objectives

• Increase knowledge of basic HIPAA requirements as applied to front-line staff.
• Identify typical problems that might arise in an agency setting
• Understand possible solutions, and their ethical implications
• Increase the agency culture of prioritizing privacy & security
Basic Terms

**HIPAA**: Health Insurance Portability & Accountability Act.

**PHI**: Protected Health Information.
- Clients' individually identifiable information: name, contact information, diagnosis, treatment, progress, appointment times, fee, status, etc.

Basic Terms 2

**Texas Medical Privacy Act/TMPA**: This is a *Texas* law passed 2012. Also known as HB300 & TMRPA/TMPA. It is more strict than HIPAA in several ways, most significantly: the definition of Covered Entities.

**Covered Entities**: Providers/organizations that have to follow HIPAA. Before TMPA, Texas therapists that didn’t file insurance electronically might not have had to comply. TMPA pretty much says that anyone who has contact with *any* PHI has to follow HIPAA guidelines.
The Bird’s Eye View: HIPAA in 4 Sentences

Think very hard and methodically about privacy and security in your agency.
Identify all places where privacy and security might be at risk.
Develop a plan to address those risks, & take action.
Document everything, continually maintain & update those documents, and keep thinking, evaluating, training, learning and mitigating.

Agency-Level HIPAA Requirements, over-simplified

• Designated Privacy & Security Officer
• Risk Assessment.
• Identify, evaluate, and mitigate risk of all possible PHI loss/breach events.
• Strong technical security measures.
• Strong procedures & agency policies that protect privacy & security.
• Appropriate employee training
• Agency culture of PHI privacy & security
• Formal agreements with 3rd parties.
• Lots of paperwork.
HIPAA vs. Mental Health Ethical Codes

- Under HIPAA
  - Easier for family to have involvement in care
  - Allows release of PHI for treatment or financial reasons without consent

- Mental Health Ethical Codes
  - Client has control of who can be involved
  - Consent required even for treatment purposes, financials

- Follow Ethical Codes or State Laws that are more strict

Top 6 Reasons to Care about HIPAA

1. The laws changed in 2013. Enforcement has been increased, penalties are higher.
2. Overall community awareness of HIPAA and privacy standards is increasing rapidly. HIPAA is becoming a ‘standard of care’ & clients expect it.
3. Clients can complain to the federal government, triggering investigations.
Top 6 Reasons to Care about HIPAA

4. Random audits.
5. The penalties are potentially huge: reports of fines from 50K-5.5M. Can be more or less.
6. And probably the most important reason: focusing on privacy and security generally increases privacy and security, and that’s good for everyone.

Worth Repeating

PHI must be kept secret and safe.

It must not be accessed, overheard, or overseen by anyone without authorization & an official sanctioned reason to access it.

The agency must evaluate, anticipate, and mitigate possible risks.
Common Problem: Laptops

- Lost/stolen laptops are a very common cause of HIPAA breaches.
- Encryption is very strongly recommended.
- Agencies need to prioritize laptops in their Risk Assessments, and create strong policies, training and support to mitigate this risk.

Common Problem: Unsecured Paperwork

- Client PHI is on most paperwork that is generated in an agency.
- Unfiled, unlocked paperwork is at risk for being seen, taken, copied, lost, stolen, etc.
File Safekeeping

• Your clients may not be famous, but the world is very small and all too often, unsecured paperwork magically finds its way to the worst possible outcome.
• Go ahead and be a little bit paranoid.
• Charts shouldn’t be left out.
• File cabinets should always be locked when not in use.
• Most professional training programs recommend 2 locks. (i.e., cabinet and room.)
• Use secure methods to travel with files if necessary.

Common Problem: Leaving Messages

• Get permission from a client before leaving a message at any number.
• Double-check the number.
• Leave the “minimum necessary” amount of information.
• ACGC permits leaving voicemails--limited to scheduling.
Common Problem: Faxing

- Double- and triple-check that the number is correct before sending.
- Use cover letter with confidential label.
- Don’t walk away.
- Agency needs policy (& training) about where fax machines are kept, who can retrieve faxes, where the incoming faxes are stored temporarily, etc.
- Good article on fax risks here:

Common Problem: Device Retirement

- Laptops, mobile devices, desktops, and fancy printers/copiers have hard drives that likely have PHI on them.
- When you or the agency retires those devices, they must be properly sanitized or destroyed. This must be planned for & documented.
Common Problem: The Walls Have Ears

• Be aware and very conservative when discussing client info with others.
• Think about who is even remotely close enough to hear.
• Complete visual and auditory privacy is your safest bet. If you don’t have a private room, point this out to the client and proceed according to their wishes (and maybe also whisper.)
• The world is much smaller than we think it is. Talking about clients, even without using their name, is very dangerous.

Common Problem: Inappropriate Access

• HIPAA says PHI must not be accessed unless there is a legitimate reason to do so.
• Looking at a record w/o authorization is a violation.
Common Problem: Log In Sharing

• Agency should be tracking access to records.
• If your co-worker uses your login to check out records they should not have access to, you might be held responsible.
• Letting someone use your login might make you appear to be the culprit of a state & federal crime.

Common Problem: Screens

• Can any screens be seen by anyone unauthorized?
• Position screens
• Use screen privacy filter
• Close your laptop, turn off your monitor.
Common Problem: Social Media

- Individuals should never, ever talk about clients or the work you do on social media.
- If your agency uses social media as part of their marketing, advertising, or outreach practices, it should be included in the risk assessment. This is an important thing about which to have thoughtful, clear policies & procedures.

Common Problem: Redisclosure

- Redisclosure is releasing someone else’s document. IE, an external psychological assessment, a hospital discharge summary, etc.
- Redisclosure not recommended in general
- Substance Abuse information redisclosure generally prohibited by law
- Mental Health redisclosure sometimes prohibited.
Common Problem:
Email and Texting

- In general: it’s not secure!
  - PHI transmitted when emailing or texting
  - PHI is available to companies/providers
  - Open to hacking
  - Could be misdelivered or seen by wrong person
  - Phishing

- Solutions (agency-level)
  - Consider an encrypted email portal
  - Always exercise great caution (individuals)
  - Informed consent is important.

Phishing
(never click on anything suspicious)

© HIPAA for Therapists, LLC
Please do not duplicate.
Common Problem: Mobile Devices

• **Huge** potential HIPAA problem.
• If you text with/about clients, email with/about clients, or store their info in your contacts, you have PHI on your phone.
• **Apps** can access that PHI, too.
• Easily lost/stolen, & then: breach.
• Mobile devices are included in the agency’s Risk Assessment. Agency needs strong policies, training & tech support here.
• For today, at least make sure you have the password feature turned on.
• For the future, consider separate work/personal devices.

Breach example: Hospice of N Idaho

• Hospice of North Idaho
• Stolen unencrypted laptop
• 50K fine
• Significant because it was the first settlement for <500 cases PHI (441)
Breach example: Anchorage Community Mental Health Services

- Breach resulted from malware (hacking)
- 2700+ incidences PHI
- ACMHS had adopted the sample Security Rule policies and procedures in 2005, but they were never followed.
- Significant because their fine was largely due to not regularly updating their IT resources with available patches and running outdated, unsupported software.
- 150K fine

Breach example: Alaska DHHS

- Alaska DHHS.
- Unencrypted USB drive w 501 cases PHI was stolen from employee’s car
- Investigation found no risk assessment, no security, no training:
- 1.7M fine.
Breach example: NYP & CU

- New York Presbyterian & Columbia University hospitals
- 6800 patients’ PHI searchable via internet.
- Physician attempted to deactivate a personally-owned computer server on the network.
- Lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual’s deceased partner, a former patient of NYP, on the internet.
- 4.8M fine—largest ever to date.

Breach example: Phoenix Cardiac Surgery

- Posting clinical and surgical appointments for their patients on an Internet-based calendar that was publicly accessible
- 2012
- 100K fine
Breach example: Arkansas nurse

- AR Nurse, shared PHI w spouse, who called patient & threatened legal use of PHI. 2006
- Fired
- Convicted: 14 months probation and 100 hours community service
- Criminal charges carried maximum penalties of 10 years jail 250K fine or both.

Risk Assessment

- The assessment and mitigation of risk is a TOP priority item in HIPAA compliance.
- It’s an ethical issue as well.
- HIPAA technically only requires ePHI to be included in the Risk Assessment, but I strongly recommend including all PHI.
Risk Assessment: Step 1

Where is PHI stored, created, or transmitted?

- Laptop
- Cell phone
- Faxing
- Email
- paper files
- printer’s hard drive
- deleted computer files
- desk or file cabinet

Risk Assessment: Step 2

- What could possibly go wrong?
- What is the likelihood of that happening?
- What size mess would it cause?
- Document.
Risk Assessment: Step 3

- Make a plan to address identified risks.
- Prioritize those that are High Risk and/or High Impact
- Document

Crowd-Sourced Brilliance (DIY Risk Assessment*)

- Brainstorm problems that might be included in a risk assessment for your division. See next slide.
- For each problem, propose potential procedural or security solutions.

* Not the real thing.
<table>
<thead>
<tr>
<th>Location</th>
<th>Problem</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal cell phone</td>
<td>Driving files to court</td>
<td></td>
<td></td>
<td>Etc, etc, etc</td>
</tr>
<tr>
<td>Fax machine</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Etc, etc, etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Thank you!

Katie Malinski, LCSW

www.HIPAAforTherapists.com