Minimizing HIPAA Liability:
Tips from a healthcare law attorney

Leslie Rojas Whitworth
Rojas Law, PLLC
leslieannnerojas@gmail.com
No Conflicts

- I do not have any financial disclosures to make or conflicts of interest to report.
Healthcare = Risky Business

- HIPAA violations can result in significant monetary damages.
- Learn to manage the risk and minimize your HIPAA liability.
What are the risks?

HIPAA Breach Case Examples:

× A 12-physician dermatology practice paid $150,000 for alleged HIPAA violations arising out of a lost, unencrypted flash drive containing protected health information.

× An orthopedic clinic failed to execute a business associate agreement prior to turning over 17,300 patients’ PHI to a potential business partner. The settlement included a monetary payment of $750,000 and a comprehensive corrective action plan.
What are the risks?

HIPAA Breach Case Examples:

- A urology group in Ohio fell victim to a ransomware attack this year where the hackers took over control of their medical records and computer systems.
- The attack was discovered by the practice administrator who received a fax demanding payment of $75,000 via Bitcoin in order to regain access to their encrypted files.
- The practice contacted an IT firm, who used a third-party to pay the ransom demand.
- The ransomware attack was complex, going deep into their computer systems, taking them 48 hours to recover. The practice told police their loss in revenue due to downtime was between $30,000–$50,000 per day. So about $60,000–$100,000 plus the $75,000 ransom payment.
HIPAA Liability Exposure

- HIPAA breaches are inevitable.
- Liability can result from a breach report (whether reported by you pursuant to breach reporting requirements or reported by someone else), and a government investigation will likely follow.
- Routine Government HIPAA Compliance Audits.
- The government reports that the compliance issues discovered during investigations are:
  1. Insufficient HIPAA policies and procedures;
  2. Insufficient safeguards to protect PHI;
  3. Lack of an investigation after a possible breach;
  4. Lack of sanctions against responsible parties (e.g., employee discipline; terminated business associate).
Minimizing Liability: Pre–Breach Checklist

1. A HIPAA Privacy Manual and HIPAA Security Policies that are *tailored* to your practice
2. Annual employee HIPAA training.
3. Updated Notice of Privacy Practices
   - Updated after 2013?
   - On practice’s website?
4. Updated Medical Record Release Authorizations
   - Updated after 2013?
   - Special rules for STDs, mental health, substance abuse
Minimizing Liability: Pre-Breach Checklist

5) Annual Security Rule Risk Analysis (hire an IT forensic expert under the attorney client privilege)
   - Evaluate the risk to PHI when at rest. (ePHI on removable media, mobile devices, computer hard drives, as well as PHI on paper (where are paper charts stored/secured? how are papers such as prescription refill requests disposed of?)
   - Store all e-PHI to a network
   - Encrypt data stored on portable devices & media
   - Remote device wipe to remove data when lost/stolen
   - Consider appropriate data backup procedures
   - Train workforce members on how to effectively safeguard data and timely report security incidents
6. Business Associate Agreements.

- A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. (Excludes a member of the covered entity’s workforce.)

- Examples:
  - Third-party billing company
  - IT company
  - Your healthcare attorney
  - EMR company
  - Medical record storage company (old paper charts)

  - Does not include those with incidental exposure to PHI. For example, janitorial staff or electrician.
Minimizing Liability: Pre-Breach Checklist

7. Documentation!!!

8. Follow-through.
   ❖ Do not have any policies on paper that you are not going to follow in practice.

   ❖ Not required by law...but DO IT!
Minimizing Liability: Preparing for the Inevitable

If you’ve implemented my Pre-Breach Checklist, then you have implemented basic HIPAA compliance in your practice.

But, HIPAA breaches are inevitable…
Minimizing Liability: What to do when there is a possible breach.

- Prompt investigations of possible breaches are critical.
- Work with health care legal counsel and IT experts.
- Document everything
- Rapid Response and Notification
  - “Without undue delay” rule
- Two Tracks (Important!)
  1) Initial Breach Response
  2) Prepare for the investigation/get your house in order!
Minimizing Liability: Possible Breach Checklist

If you suspect a breach:

1) Immediately notify health care legal counsel and IT forensic experts to establish a plan of action for the investigation and analysis. (Attorney-client privilege)

2) Secure the premises.

3) Isolate affected system to prevent further intrusion, data release, or damage. Take infected machines offline, but leave the power on.

4) Use telephone to communicate. Attackers may be capable of monitoring email traffic.
Minimizing Liability: Possible Breach Checklist

5) Activate all **auditing software** (if not activated).

6) IT experts should preserve all pertinent system logs (firewall, router, intrusion detection system, etc.). Files on the affected systems should **never be deleted, moved, or altered** in any way.

7) If files are damaged/ altered, IT should **create backup copies and store in a secure location**.

8) Identify **systems that connect** to the affected system and where the affected system resides within the network topology.
9) Identify the programs and processes that operate on the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

10) Locate backup, if any.

11) Take an inventory of missing items and their locations.

12) Review keycard and surveillance data for unusual activity.
13) Retain an external **forensic** IT expert to assist and to image the data.
14) Determine whether **breach notification** is required.

⋆ Even if there has been an “incident,” you have to determine, with the assistance of healthcare legal counsel, whether there has been:

A **reportable** breach under HIPAA.
Minimizing Liability: Breach Reporting and Investigation Checklist

15) If there is a reportable breach, after consultation with health care legal counsel, notify **affected patients** and the appropriate **law enforcement agenc(ies)**.

   a) **Document** all conversations with law enforcement, if any, and the steps taken to restore the integrity of the system.

   b) In the event the affected system is collected as evidence, make arrangements to provide for the **continuity of services**, i.e., prepare redundant system and obtain data back-ups.

16) Log the unauthorized use or disclosure in the patient’s disclosure tracking log.

Breach Notification Rule

General Rules:

- 500 or more = notify government within 60 days (but without unreasonable delay).
- More than 500 individuals in the same jurisdiction/state = notify media within 60 days (but without unreasonable delay).
- Less than 500 individuals = notify the government at least 60 days after the end of the calendar year.
  - Usually March 1 or February 29 during a leap-year.

***Tip for breaches of less than 500: Don’t do it earlier than you need to.
Minimizing Liability:
Breach Reporting and Investigation Checklist

18) After the investigation and notification (if necessary) are completed, conduct a post-investigation review of the events and make necessary adjustments to the technology and/or response procedure to reflect the lessons learned.

Remember the 2 Tracks!

Track 1 was the initial breach response (steps 1–17 above). Now that the notifications have gone out, the government may come knocking, so…

Track 2 is…Get your house in order!!!

- Update Notice of Privacy Practices
- Update breach notification policies and implement safeguards
- Conduct and document employee training.
- Conduct and document risk assessment.
- Update BAAs and document satisfactory assurances from BAs.
Government Investigation: Overview

HIPAA Privacy & Security Rule Complaint Process

- Complaint
  - Intake & Review
    - Possible Privacy or Security Rule Violation
  - DOJ
    - Accepted by DOJ
    - DOJ declines case & refers back to OCR

- Resolution
  - OCR finds no violation
  - OCR obtains voluntary compliance, corrective action, or other agreement
  - OCR issues formal finding of violation

- Resolution
  - The violation did not occur after April 14, 2003
  - Entity is not covered by the Privacy Rule
  - Complaint was not filed within 180 days and an extension was not granted
  - The incident described in the complaint does not violate the Privacy Rule
OCR Investigation: Step-By-Step

1) OCR receives a complaint or a breach notice.
2) OCR conducts intake & review to determine if a possible Privacy or Security Rule violation occurred.
3) At any time, the OCR may refer the complaint to the DOJ if a possible criminal violation occurred.
4) If no Privacy or Security Rule violation, case closed.
5) If there is a possible violation, then OCR will notify the complainant and the CE.
   - The CE will receive a letter from the OCR asking for specific information to be submitted for review.
   - In some cases, the letter will not have any requests, but will instead list corrective actions for the CE to take.
6) Respond to OCR’s information requests/compliance demands.
OCR Investigation: Step–By–Step

7) After receiving CE’s response, OCR reviews evidence to determine if a violation occurred. If there was non–compliance, then OCR will suggest:
   - Voluntary compliance;
   - Corrective action; and/or
   - Resolution agreement.

8) Sometimes OCR will request additional information (e.g., follow–up requests about whether the CE actually took the corrective actions it said it would).

9) If CE does not take action to resolve the matter that is satisfactory to OCR, then OCR may impose fines and CE may request an evidentiary hearing.

10) If OCR is satisfied with the CE’s corrective actions, OCR will typically request a phone call to “offer HIPAA technical assistance” to the CE. This is usually an indication that OCR is closing the file.

11) Once investigation is closed, OCR will send a letter.
Best Practices for Response Letter

❖ **Overreact.** Don’t underreact.
   • Show the OCR that the CE takes HIPAA compliance very seriously.

❖ Put your **best foot forward**.
   • Even if not specifically requested by the OCR, make sure to state the ways in which the CE is HIPAA compliant and the corrective actions taken to become/remain compliant.
   • Focus on reputable compliance history and what CE has done correctly.

❖ **Don’t highlight, but don’t hide from weaknesses.**
   • OCR wants to see that the CE is acting in good faith, learning, and taking corrective actions to ensure compliance. Highlight this when discussing your weaknesses.

❖ **Highlight the CE’s compliance barriers**, but don’t rely on this too heavily.
   • E.g., small practice with few employees/resources doing the best it can.
   • If breach was caused by a BA, seriously consider terminating relationship.
Summary: 3 takeaways

1. Good-faith efforts at HIPAA compliance before the government ever comes knocking will demonstrate to the government that you take HIPAA seriously.
   - This will lower your fines, and may result in no fines at all.
   - These include: HIPAA Privacy Manual, HIPAA Security Policies, Updated NPP (on website), Updated Release Forms, Updated BAAs.

2. Proper handling of the potential breach response (with IT forensic experts and healthcare legal counsel) will ensure that you can put together an effective response to a government investigation. Follow the check list.

3. Timely notification of a reportable breach (to patients, government, media) and a well-thought out response to an investigation. This should include a response to the allegations, why you were lacking in certain compliance areas, in which areas you have robust HIPAA compliance (even if unrelated to the allegations), and the changes you have made since discovering the breach.
   - It looks best if these changes were implemented BEFORE the government investigation began, i.e., before the government had to request that you implement those changes.
Cybercriminals are becoming more sophisticated. It’s no longer a matter of IF but WHEN you will be attacked. Security incidents are extremely expensive. Verify that you have cyber insurance (not always included in your basic policy) to help cover these costs.

Consider Cybersecurity Insurance
Resources

- https://www.hhs.gov/hipaa/for-professionals/index.html
- https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- https://www.hhs.gov/hipaa/for-professionals/faq/index.html

Feel free to email me with questions at leslieannerojas@gmail.com.
FAQ’s

Does HIPAA require you to obtain a new acknowledgement of receipt of the Notice of Privacy Practices from patients if you change your privacy policy?

Answer:

➢ No. A covered health care provider with a direct treatment relationship with individuals is required to make a good faith effort to obtain an individual's acknowledgement of receipt of the notice only at the time the provider first gives the notice to the individual -- that is, at first service delivery. See 45 CFR 164.520(c)(2).
FAQ’s

May physician's offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

Answer

Yes. You may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. HIPAA explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).
FAQ’s

Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?

Answer:

- Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object.
FAQ’s

Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with a person who is not married to the patient or is otherwise not recognized as a relative of the patient under applicable law (e.g., state law)?

Answer:

- Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) permits covered entities to share with an individual’s family member, other relative, close personal friend, or any other person identified by the individual, the information directly relevant to the involvement of that person in the patient’s care or payment for health care. In addition, HIPAA allows a covered entity to disclose information about a patient as necessary to notify, or assist in the notification of (including by helping to identify or locate), such a person of the patient’s location, general condition, or death. The Privacy Rule defers to a covered entity’s professional judgment in these cases and does not require the entity to verify that a person is a family member, friend, or otherwise involved in the patient’s care or payment for care.
FAQ’s

Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with a person who is not married to the patient or is otherwise not recognized as a relative of the patient under applicable law (e.g., state law)?

Answer:

- Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) permits covered entities to share with an individual’s family member, other relative, close personal friend, or any other person identified by the individual, the information directly relevant to the involvement of that person in the patient’s care or payment for health care. In addition, HIPAA allows a covered entity to disclose information about a patient as necessary to notify, or assist in the notification of (including by helping to identify or locate), such a person of the patient’s location, general condition, or death. The Privacy Rule defers to a covered entity’s professional judgment in these cases and does not require the entity to verify that a person is a family member, friend, or otherwise involved in the patient’s care or payment for care.