**Name:** Robert Shea

**Date:** 9/25/2025

**Student ID:** 5476462

**Task 1: HIPAA Rule Violations (10 points)**

Identify which HIPAA rules were violated. Check all that apply and provide a brief explanation for each selection.

☑ **HIPAA Privacy Rule** Explanation:

The privacy rule was violated because protected health information was disclosed to an unauthorized individual. This included full names, social security numbers, diagnoses, insurance IDs, and dates of recent services. The disclosure did not fall under any of the exceptions such as treatment, payment, healthcare operations, required by law, public health activities, health oversight activities, or law enforcement purposes. This was sent from a current employee to a former employee from the riverside medical center.

☑ **HIPAA Security Rule** Explanation:

The security rule was violated because the organization failed to implement technical safeguards to prevent accidental disclosure of electronic PHI. They didn’t have strong enough digital locks to mistakes like this. Sending private patient data to the wrong person shows they didn’t have the right protections in place such as email checks or secure systems that could’ve prevented this.

**Specific violations identified:**

1. Private patient data was shared with someone who wasn’t allowed to see it.
2. Patients sensitive details were put at risk such as names, social security numbers, diagnoses, and more.
3. Insufficient safeguards to prevent misdirected email transmissions.

**Task 2: Four-Factor Breach Risk Assessment (15 points)**

Apply the four-factor breach risk assessment from Chapter 10. For each factor, analyze the scenario and determine the risk level (Low/Medium/High).

**Factor 1: Nature and extent of PHI involved**

* Risk Level: ☐ Low ☐ Medium ☑ High
* Analysis: The spreadsheet shared with the unauthorized recipient contained highly sensitive identifiers such as SSN, DON, and diagnoses. Leaking this information exposed those patients to identity theft and medical fraud.

**Factor 2: Unauthorized person who used/received the PHI**

* Risk Level: ☐ Low ☑ Medium ☐ High
* Analysis: The recipient was a former employee and not known to be a malicious hacker. However, they were no longer authorized to access the patient health information.

**Factor 3: Whether PHI was acquired or viewed**

* Risk Level: ☐ Low ☐ Medium ☑ High
* Analysis: The former employee confirmed they opened the file, meaning the PHI was accessed. This increased the severity as opposed to an unopened accidental transmission.

**Factor 4: Extent to which risk has been mitigated**

* Risk Level: ☐ Low ☑ Medium ☐ High
* Analysis: The former employee stated they deleted the email and attachment. While this reduces some risk, there is no guarantee copies weren’t saved or that they were properly removed from the accessed device.

**Overall Breach Determination:** ☑ Breach Occurred ☐ No Breach Justification:

PHI was disclosed to an unauthorized party and included highly sensitive identifiers. This qualifies as a breach under HIPAA definitions.

**Task 3: Breach Notification Timeline (10 points)**

Discovery Date: March 20, 2024

Legal requirements: Notifications must occur within 60 days of discovery.

| **Notification Date** | **Recipient** | **Method** | **Legal Requirement** |
| --- | --- | --- | --- |
| By May 19th, 2024 | Individual Patients | Written notice by first-class mail. | Within 60 days of discovery |
| By May 19th, 2024 | U.S. Department of Health & Human Services (HHS) | Electronic submission | Required for breaches affecting <500 individuals. |
| By As soon as possible | Media | N/A | Not required unless it’s less than 500 individuals affected. |
| By May 19th, 2024 | Riverside Medical Center workforce | Internally and possibly training | Assuming this is an organizational policy. This ensures awareness and mitigation. |

**Additional considerations for this timeline:**

All notifications must go out no later than 60 days after discovery and the notifications must include what happened, what info was exposed, and the steps patients should take to protect themselves.

**Task 4: Preventive Safeguards (15 points)**

List 5 specific preventive measures that could have prevented this incident. Categorize each measure as Administrative (A), Physical (P), or Technical (T) safeguard.

| **#** | **Safeguard Type** | **Preventive Measure** | **How It Would Prevent This Incident** |
| --- | --- | --- | --- |
| 1 | ☑A ☐P ☐T | Workforce training on correct email procedures | Training ensures employees confirm the recipient addresses before sending patient health information. |
| 2 | ☐A ☐P ☑T | Data loss prevention (DLP) software | Automatically blocks emails with patient health information sent to unauthorized outside domains. |
| 3 | ☑A ☐P ☐T | Access authorization and termination procedures | Prevents former employees from receiving sensitive data. |
| 4 | ☐A ☐P ☑T | Email encryption with recipient verification | Requires confirmation that recipient is authorized before it decrypts the sensitive information. |
| 5 | ☐A ☑P ☐T | Clear workstation privacy practices | Helps employees focus when dealing with patient health information handling tasks which would reduce the likelihood of an error. |

**Task 5: Ethical Decision-Making Matrix (10 points)**

Apply the 8-step ethical decision-making matrix from Chapter 13 to this scenario.

**1. What is the question?**

How should Riverside Medical Center respond to the accidental patient health information disclosure ethically and legally.

**2. What is my "gut" reaction?**

My gut reaction is immediate concern for those affected and concern for their privacy and potential identity theft.

**3. What are the facts?**

* Known facts: The patient health information of 50 patients was sent to a former employee who was no longer to receive the information. The data was opened.
* Facts to be gathered: It needs to be confirmed that the data was properly deleted, the extent of the exposure, and if any PHI was further shared.

**4. What are the values?**

* Patient perspective: Right to privacy, transparency about the exposure, and protection from harm.
* Healthcare professional perspective: They must act with beneficence and nonmaleficence.
* Organization perspective: Obligation to comply with HIPAA and maintain trust.
* Society perspective: Secure handling of sensitive health information.

**5. What are my options?**

Option A: Notify the patients and HHS as soon as possible. Start implementing safeguards.

Option B: Since the file was supposedly deleted, minimize the reporting.

Option C: Investigate first before reporting it to the proper parties.

**6. What should I do?** Selected option:

A) Be transparent and notify the patients and HHS as well as strengthen the safeguards

**7. What justifies my choice?** ☑ Justified ☐ Not justified Reasoning:

It is the right thing to do because being open, honest, and transparent aligns with HIPAA and helps patients feel safe and supported.

**8. How can I prevent this problem?** Future prevention strategies:

1. Use stricter email safeguards. Set up systems that block or warn when sending patient data to the wrong address.
2. Provide regular staff training. Teach employees how to double check patient health information before sending.
3. Require encryption for patient health information emails. This would make sure sensitive files can only be opened by the correct person.

**Grading Rubric**

| **Task** | **Points** | **Criteria** |
| --- | --- | --- |
| Task 1 | 10 | Correctly identifies violated rules with accurate explanations |
| Task 2 | 15 | Thoroughly analyzes all four factors with appropriate risk assessments |
| Task 3 | 10 | Creates accurate, complete timeline with all required notifications |
| Task 4 | 15 | Provides relevant, specific safeguards properly categorized |
| Task 5 | 10 | Completes all 8 steps with thoughtful, relevant responses |
| **Total** | **60** |  |

**Submission Instructions**

* Complete all sections of the template
* Save your file as: LastName\_FirstName\_Week5\_CaseStudy.pdf
* Submit via the course management system by [Due Date]
* Late submissions will be penalized 10% per day