



Discipline/Corrective Action for Privacy and Security Violations

**Education: Updates to corporate policy 1.HR.04
June 2018**

Introduction

Welcome to UPH Methodist | Proctor | Pekin training on the updates made to corporate policy 1.HR.04: Discipline/ Corrective Action for Privacy and Security Violations..

- This does not replace our annual HIPAA training. This is additional training to educate all staff on the policy changes and to explain how privacy and security violations will impact everyone.
- Protecting the privacy of our patients and their information is one way we Champion Excellence – it's the right thing to do for our patients.

Policy

UnityPoint Health is committed to ensuring compliance with all applicable privacy and security laws, regulations, standards, policies and procedures including the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).



This policy describes the manner in which UnityPoint Health is protecting patient privacy and security. All alleged/suspected violations will be investigated. System-wide standards have been developed to ensure consistency in the discipline/corrective action of its employees.

Why has the policy changed?

- The Health Insurance Portability and Accountability Act (HIPAA) rules have not changed
- The **Office of Civil Rights** (the government agency who enforces HIPAA) expects that covered entities follow their discipline policy consistently throughout the organization when a violation of the privacy or security rule occurs.
- 1.HR.04 Discipline/Corrective Action for Privacy and Security Violations has been updated to add clarity on disciplinary actions that may take place for various types of violations.

Types of Violations

In the revised policy, the level of disciplinary action may range from coaching to immediate termination. Each situation will be evaluated using all the available facts and will fall under one of the following categories:

- **Careless or Inadvertent** - unintentional or careless access, review or disclosure by an employee and/or disclosure of PHI without authority.
- **Failure to Follow Established Privacy and Security Policies and Procedures** - acts resulting from failure to follow established privacy and security policies.
- **Deliberate or Purposeful Violation without Harmful Intent or Malice** - deliberate unauthorized or inappropriate access or use, generally out of curiosity or concern, of PHI without harmful or malicious intent.
- **Harmful Intent or Malice** - intentional access or disclosure of PHI with harmful intent or malice.

HIPAA
violations
RUIN
careers



Examples include but are not limited to...

Careless or Inadvertent

- Discussing confidential patient information in public area (elevator, cafeteria or other public place)
- Leaving a patient medical record unattended and accessible in a public area in either a paper or electronic format
- Forgetting to log off computer
- Faxing to wrong fax number
- Selecting wrong PCP on registration or selecting wrong provider when placing an order
- Failing to de-identify or redact PHI for operations or business use
- Scanning PHI into wrong chart

Failure to Follow Established Policy

- Leaving mobile devices containing PHI unattended or failing to secure electronic PHI
- Releasing Do Not Report patient information
- Failure to take reasonable precautions to prevent disclosure of highly sensitive PHI
- Routinely failing to log off/lock computer
- Sharing more than minimum necessary
- Accessing own personal medical records outside of established policy
- Providing PHI to wrong patient (i.e. After Visit Summary, Discharge Instructions, Scripts)
- Encouraging another coworker to access a record inappropriately

Examples include but are not limited to...

Deliberate or Purposeful Without Harmful Intent or Malice

- Sharing user ID/password
- Looking up PHI of friends/relatives
- Accessing and reviewing medical records for curiosity or concern
- Accessing census lists out of curiosity
- Repeated incidents of unintentional, inappropriate and self reported accidental access

Deliberate or Purposeful With Harmful Intent or Malice

- Accessing or using/disclosing PHI from a personal relationship
- Gathering PHI to be sold
- Tampering with or unauthorized destruction/disposal of PHI
- Deliberate acts that adversely affect integrity, security and/or confidentiality of PHI
- Posting information, pictures or other identifiable information about a patient on a social media site to cause harm to the patient

Reporting Potential Violations

All staff are expected to report potential privacy and security violations. To report a violation, please complete at least one of the following steps:

- Fill out an RL Solutions event
- Send an email to the HIPAA Privacy Officer/ Information Security Officer, Angela.Moore@unitypoint.org, and/or Wendy.Kelly@unitypoint.org
- Communicate all details to your manager or a member of the management team
- Call Angie Moore: 309-672-4865 or Wendy Kelly: 309-672-4831

HIPAA Scenarios

While clinic receptionist, Cecelia, confirms the demographics of the patients and escorts them back to the exam room, her voice carries so that all patients in the waiting area can hear. Cecelia also calls patients back using their full name (first and last).

Is this a HIPAA privacy or security violation? Yes - This is a privacy violation. This behavior is Careless/Inadvertent. Cecelia fails to provide privacy by discussing more than the minimum necessary in an area where others may be able to hear. Cecelia's manager would create a disciplinary/corrective action plan with her.

Office Coordinator, Kathy, collects completed paper patient intake forms for her clinic. Once Kathy has entered the information into the computer, she puts the forms in her unsecured "shred" area (a cardboard box under her desk). Her normal procedure is to empty this box into the locked shred box every night, but tonight she forgets. The next morning, she discovers the cleaning service had removed her cardboard box and its contents, believing it was garbage. All the patient intake forms with SSN and insurance information from the day before were placed in the regular garbage.

Is this a HIPAA privacy or security violation? Yes - This is a privacy violation. This behavior is Careless/Inadvertent. Kathy fails to properly secure and dispose of PHI. She should dispose of paper PHI in the proper bin on a regular basis throughout the day. Kathy's manager would create a disciplinary/ corrective action plan with her.

Counselor Joe takes his laptop to a conference in Chicago. After the conference, he stops at the American Girl doll store and leaves his computer in the back seat of his car, in plain sight. When he returns to his car, he notices his lap top bag has been stolen.

Is this a HIPAA privacy or security violation? Yes - This is a security violation. This behavior comes under the category of Failure to Follow Policy/Procedure. Joe left a mobile device containing PHI unattended and fails to properly secure his lap top and take steps necessary to prevent loss. He should have locked his work lap top in the trunk while he was not in his car. Joe could receive a final warning or be terminated.

Nurse Hannah receives a call from somebody who says they are a patient's neighbor and wants to know how the patient is doing. The neighbor had been present one time while Hannah was providing care and the patient was alright with the neighbor being present, and to give the neighbor the nurse's number "just in case." Hannah shares that the patient's prognosis is not good and the patient had recently decided to elect for hospice care. The neighbor talks to patient and expresses their sympathy, and finds out the patient had not yet told anyone of her decision.

Is this a HIPAA privacy or security violation? Yes - This is a privacy violation. Hannah's behavior comes under the category of Failure to Follow Policy/Procedure. Hannah specifically failed to verify the neighbor was authorized by the patient to receive this information. She inappropriately assumed the patient did not need to approve the disclosure. Hannah should have checked with the patient first to determine if release of information was approved by her. If the patient is not able to give permission, Hannah would need to check with the patient's representative who makes decisions for the patient. Hannah could receive a final warning or be terminated.

Security Guard, Lucy, was stationed in the ED. At one point, ED RN, Jen, asked Lucy to watch an intoxicated patient, who happened to be the city's mayor. Jen reported to Lucy the patient's name, blood alcohol level, expected disposition and past ED visit history. Several hours later, Lucy takes a break and sees her friend, Theresa, in the cafeteria. While on break together, Lucy shares everything she knows about the mayor.

Is this a HIPAA privacy or security violation? Yes, this is a privacy violation. Jen's behavior falls into Failure to Follow Policy. Jen shared more information than the minimum necessary for Lucy to watch the patient. She should have provided the patient's first name, so Lucy could address the patient personally if she needed to. All other information was more than Lucy needed to know to provide a safe environment for the patient. Jen could receive a final warning or be terminated. Lucy's behavior falls into Deliberate or Purposeful Violation without Harmful Intent. Lucy specifically shared PHI with Theresa, who had no need to have any information about the mayor's emergency department visit. Although she meant no harm, Lucy could be terminated.

Nurse Mandy has completed her night rounding documentation and wants to grab lunch from the cafeteria. Before she leaves the floor, Mandy wants to ensure she will not be receiving any patients soon. Mandy reviews the ED and ICU patient lists and discovers her neighbor is in the ED. Mandy then proceeds to open and review her neighbor's chart just to see what happened.

Is this a HIPAA violation? Yes, this is a privacy violation. Mandy's behavior falls into Deliberate or Purposeful Violation without Harmful Intent for reviewing lists of patients she is not caring for and reviewing her neighbor's records. If staffing is a concern, Mandy should use appropriate resources such as her supervisor, manager, Patient Care Coordinator (PCC) or Bed flow coordinator. She also could have called the ED and ICU to inquire about any pending admissions or transfers to her floor. Mandy could be terminated for accessing patient census lists for patients she is not caring for and/or accessing her neighbor's chart.

Dr. Bob had a stressful shift in the ED and posted on his Facebook, “this was one of the worst days. I treated 3 motorcycle accident patients – one was an 18-year-old male who attempted to ramp over some cars and didn’t make it. He died while we were contacting his family. He was too young to die.”

Is this a HIPAA violation? Yes, this is a privacy violation. Dr. Bob has posted patient information that can be used to identify a patient on his social media account. There was enough information provided for the patient to be identified. This is a Deliberate or Purposeful Violation without Harmful Intent. PHI disclosed on social media does not have to include the patient name in order to be a privacy violation. Dr. Bob could be terminated for his actions. Some health care professionals may also face consequences from their licensing boards if they violate rules of the licensing board.

Patient Care Technician Steve’s best friend/ co-worker did not show up for his shift. Through the grapevine, Steve finds out his friend is in the hospital. Steve wants to send some “get well” flowers, but doesn’t know the patient’s room number. Steve opens and reviews several census lists to locate his friend’s room number. He then discovers his friend is listed as Do Not Report.

Is this a HIPAA violation? Yes, this is a privacy violation. Steve used the electronic health record to locate his friend. His behavior falls into Deliberate or Purposeful Violation without Harmful Intent. Steve should have used to Facility Directory (accessed through the hospital operator – dial O). The facility directory would not have listed his friend because he was a Do Not Report. Steve could be terminated for his actions, even though he was concerned for his friend.

Student Therapist, Tiffany, heard about an interesting knee injury that requires a specialized therapeutic procedure. Without direction from her instructor, Tiffany reviews the patient's chart under her own login credentials and claims she accessed the chart to educate herself about the procedure.

Is this a HIPAA violation? Yes, this is a privacy violation. This behavior falls into **Deliberate or Purposeful Violation without Harmful Intent**. She accessed a medical record without authority solely out of curiosity about the procedure. She is not taking care of the patient. It would have been appropriate for Tiffany to ask her instructor about the procedure so the instructor could provide education to all students. Tiffany could be terminated.

Nurse Manager Robin has been a recent patient in the clinic. She is worried about her health and anxious to get her lab results back. She logs into the electronic record and accesses her own chart, and is immediately relieved to find her results are normal.

Is this allowed? No – this is not allowed. Although this is not considered to be a HIPAA privacy or security violation, it is a **UnityPoint Health policy**. **UnityPoint Health Information Security policies require you to access your information in the same way any other patient would.** This behavior falls into **Failure to Follow Policy/Procedure**. Access to the electronic health record system is for the purpose of doing your job and access must be work-related, not personal. Robin could receive a final written warning and suspension without pay or termination.

Nurse Manager Robin's 25-year-old daughter had a recent appointment and has been asking Robin to look at her test results because, 'mom, you are a nurse and you will be able to explain them to me'. Robin looks up her daughters lab results.

Is this a HIPAA violation? Yes, this is a HIPAA privacy violation. Accessing the records of any other person without a work-related need to know is Deliberate and Purposeful without Harmful Intent. Verbal permission from the other person does not meet HIPAA authorization requirements. Robin could be terminated for a first offense. Be prepared to let your family and friends know it is not appropriate for you to access their records, even if they tell you they are okay with it.

Patient Access Associate Scott has some gambling debts that need paid. Scott discovers he can sell social security numbers to make some extra money. During his next shift, he runs a report on all patients seen in the last 30 days and proceeds to gather these patients' social security numbers. Scott sells this information to earn extra cash.

Is this a HIPAA violation? Yes, this behavior falls into Harmful Intent or Malice. Scott specifically wants to make money selling the social security numbers and patient information. Scott would be terminated.

Acknowledgement

Thank you for taking this education module and acknowledging the following:

- I have reviewed and understand the requirements under the HIPAA privacy requirements and UnityPoint Health policy, including when I can use, disclose, or access PHI and when I need to report potential inappropriate uses, disclosures, and accesses.
- I will ask my supervisor or the Compliance Department for any clarifications needed.
- I understand that inappropriate access, use, or disclosure of protected health information (PHI) is grounds for corrective action including immediate termination of employment.