
TITLE: CORRECTIVE ACTION TO DETER VIOLATIONS OF PATIENT PRIVACY AND SECURITY

POLICY:

All Hospital staff whose activities are such that they may have access to patient information must comply with the Hospital's Privacy and Security policies. Non-compliant staff shall be subject to corrective action and discipline up to and, including termination. All confirmed violations will result in discipline to be determined on a case by case basis depending on the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of patient information, and other relevant considerations.

PURPOSE:

The purpose of this policy is to provide a framework of appropriate consistent discipline for violating privacy and security policies as outlined and included in, but not limited to, the Hospital Code of Conduct, the By-Laws of the Medical Staff and the Human Resources Corrective Action/Disciplinary Policy.

APPLICABILITY: All Hospital Staff

PROCEDURES:

1. **INVESTIGATION**

The Privacy Officer and/or the Information Security Officer shall investigate violations of privacy and security policies, with the assistance of the alleged transgressor's department, Legal Affairs or others as deemed necessary. Investigations may include interviews of complainants, patients and staff, review of work schedules, auditing of electronic information systems, chart reviews, among other processes.

If it is confirmed that a violation of NYP's privacy and security policies has occurred, the findings of the investigation with a recommendation in accordance with this policy, and to include potential mitigating factors, will be forwarded to a committee who will make the final determination of appropriate discipline.

The committee will be comprised of the Vice President of Internal Audit and Compliance, the Compliance and Privacy Officer, the Vice President(s) of Human Resources and the respective SVP of the campus where the employee works, or Chief Medical Officer as appropriate. Legal Affairs will provide the committee with legal and regulatory guidance, including advice on the potential financial and legal exposure associated with any disciplinary decision.

2. VIOLATIONS OF PRIVACY AND SECURITY POLICIES

To assist in determining the significance and impact of violations of privacy and security policies, on page 3 of this policy are four progressive categories of potential violations with examples and the appropriate discipline for each category. This is not an exhaustive list – please review the Privacy and Security policies for more information.

CATEGORY	VIOLATION	DISCIPLINE
Category 1	Accidental or Inadvertent Violation: ✓ Carelessness such as misdirecting patient information via email, fax or incorrectly identifying patient records.	▪ Mandatory Privacy and Security Education ▪ Note: a second occurrence of such a violation or a single occurrence that results in the misdirection of numerous patient records should be treated as a Category 2 violation
Category 2	Failure to Comply with NYP's Privacy and Security Policies: ✓ Releasing PHI without proper authorization ✓ Failure to sign off of an IT application ✓ Sharing user ID and/or passwords ✓ Failure to safeguard portable devices ✓ Transmitting PHI using an unsecured method	▪ Final Written Warning and ▪ Mandatory Privacy and Security Education
Category 3	Deliberate or Purposeful Violation Without Harmful Intent: ✓ Accessing PHI without Harmful Intent	▪ Final Written Warning and a three day suspension plus ▪ Mandatory Privacy and Security Education ▪ and Report to appropriate licensing board as required
Category 4	Willful Disclosure of Patient Information and/or Accessing Patient Information with Malicious or Harmful Intent: ✓ Examples of willful disclosure include disclosure of PHI to an unauthorized individual or entity; posting PHI on social media sites or disclosing PHI to the media. Examples of access with malicious or harmful intent include accessing PHI to use against the patient in a dispute, legal proceeding or to otherwise extort, embarrass or humiliate the patient.	▪ Termination and ▪ Report to appropriate licensing board as required

A subsequent violation after receiving a final written warning will result in termination. The Mandatory Privacy and Security Education course must be taken and completed within 7 days of the issuance of discipline.

To successfully complete the required privacy and security course, the transgressor must score at least 90% on the post-course examination.

DEFINITIONS:

Protected Health Information (PHI) is information about a patient, including demographic information that may identify a patient that relates to the patient's past, present or future physical or mental health or condition, related health care services or payment for health care services.

Hospital Staff is any New York- Presbyterian employee, member of the medical staff, resident, student or volunteer.

RESPONSIBILITY:

Human Resources, Patient Services,
Chief Operating Officers, Chief Medical Officer,
Compliance and Privacy Officer
Information Security Officer.

POLICY DATES:
ISSUED: April 2003
Revised: April 2005; April 2013; **June 2013**
Reviewed: April 2007; April 2009; April 2011; **July 2015**