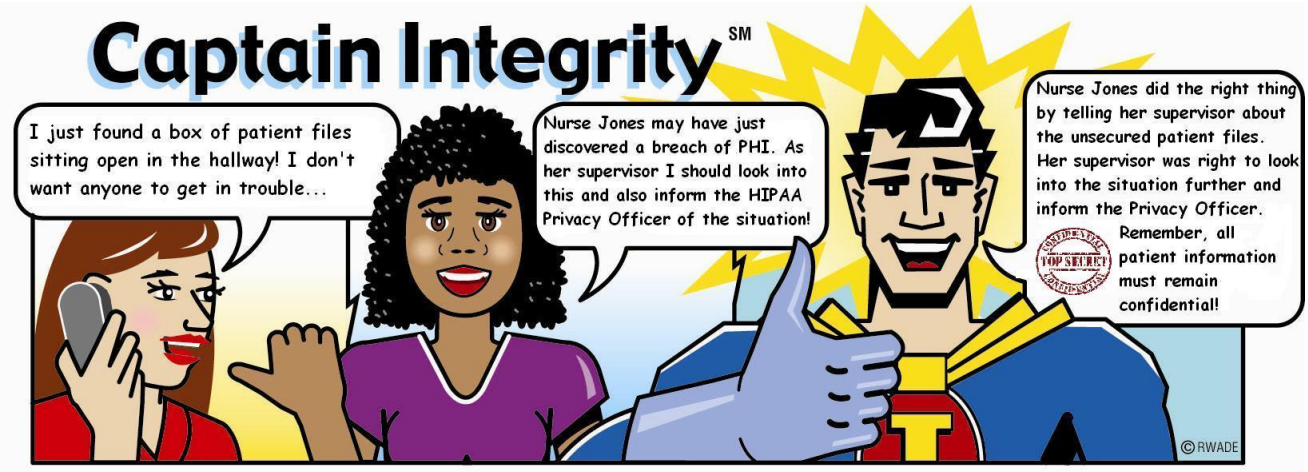
Greater Hudson Valley Health System
Policy/Procedure

Manual: Hospital Wide - Compliance
Section: HIPAA

Policy #:	
SUBJECT: HIPAA Violation, Breach Notification and Discipline Policy	
Implementation : (updated version) 7/13	Concurrences: I.T. Security Officer Chief Human Resources Officer Chief Information Officer Chief Nursing Officer Chief Operating Officer Medical Group Executive
Reviews: 7/13	
Revisions: 12/13, 4/14, 6/15, 11/15, 4/17	
Initiator: Compliance Office	
Approval: President/Chief Executive Officer	
Attachment(s): Breach Notification Risk Assessment Tool	



PURPOSE:

GHVHS needs to provide appropriate notification(s) in the event of an unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI). GHVHS staff are to report any and all possible breaches of PHI to their Director and to the HIPAA Privacy and/or Security Officer(s) who will then address the situation according to state and federal regulations, laws, and policies. Failure to adhere to this policy may result in disciplinary action per HIPAA regulations.

DEFINITIONS:

- **GHVHS "Staff"** - meaning ORMC, ORMC Foundation, CRMC, CRMC Foundation, GHVHSMG, ORMG, CRMG employees, physicians, volunteers, contractors, vendors, students, residents, DSRIP Affiliates, Board Members, or other persons having patient or PHI contact or doing business with GHVHS.

- **GHVHS "locations"** – meaning Orange Regional Medical Center, Catskill Regional Medical Center, Grover M. Herman Hospital, Catskill Regional Skilled Nursing Unit, Catskill Regional Adult Daycare, Livingston Manor, Greater Hudson Valley Medical Group, Orange Regional Medical Group, Orange Regional Medical Pavilion, Catskill Regional Medical Group, Monroe Primary & Urgent Care, Goshen Patient Service Center, Orange Regional Medical Center Family Program for Alcoholism/Chemical Dependency, Outpatient Rehabilitation Center, Ambulatory Surgery Centers, DSRIP related functions, Arden LDC, and all locations where GHVHS conducts business.

- **PHI** is any information that can identify a patient, and includes, but is not limited to the following examples:
    - admission or procedure
    - diagnosis
    - prognosis
    - treatment plan or treatment options
    - discharge
    - name
    - address
    - telephone number
    - age/date of birth
    - Images
    - or any other information that can identify a patient.

- **Violation/Breach**: the acquisition, access, use, or disclosure of PHI in a manner which violates the HIPAA Privacy or Security Rules and/ or GHVHS Policy. A Violation/Breach may be subject to two consequences:

    1) Patient and government notification requirements. The HIPAA Privacy Officer makes this determination upon investigation, utilizing the Breach Notification Risk Assessment Tool **"Attachment A."**

    2) Discipline as determined by GHVHS Human Resources.

PROCEDURES

1. All new Staff shall receive information and training concerning the standards for Confidentiality of Patient Information and HIPAA at the time of employment and on an annual basis.

2. Staff should not access or request from another person ANY information on ANY patient unless it is within their job function to do so or they have prior written authorization from the patient or their Supervisor. Staff should only access the "minimum necessary" amount of PHI to do their job. Staff should not access records out of curiosity or for patients they are not assigned without written permission from their supervisor.

3. Staff should not access their own records or those of other staff, family and friends. The acceptance of being someone's assigned heath care proxy does not give an employee the right to access the patient's medical record. The Department Director will determine the level of system access an individual requires.

4. Any sharing of PHI with a vendor or contractor requires a written HIPAA Business Associate Agreement.

5. GHVHS will perform random audits to ensure that only staff members with a "need to know" have accessed particular PHI.

There are 3 Levels of Violation/Breach:

Level 1 Breach Examples:

- Discussing patient information in public areas
- Leaving a copy of patient information in public areas
- Giving a patient another patients discharge instructions
- Leaving a computer unattended in an accessible area with PHI unsecured

Level 2 Breach Examples:

- Multiple Level 1 breaches
- Inappropriately accessing or disclosing PHI of individuals not under your care or without permission (including family and friends)
- Loss of mobile device, such as laptop, iPhone, iPad, etc
- Loss of patient file containing PHI
- Loss of a media device, such as flash drive containing PHI
- Accidental transfer of patient data to unintended vendors (non-business associates)
- Sharing a password
- Accessing a patient record out of curiosity
- Looking up images, pictures or addresses of relatives, friends or high profile individuals
- Unintentional installation of unauthorized software

- Unintentionally discarding of PC hard drives, CDs or other devices containing PHI without following the approved destruction/disposal guidelines.

Level 3 Breach Examples:

- Accessing, Compiling or transmission of PHI for personal gain or malice
- Any theft of PHI, or a device or media, containing PHI
- Disclosure of PHI via social media

Discipline:

The HIPAA Privacy and/or Security Officer will investigate all reports of Violations or Breaches utilizing the Breach Notification Risk Assessment Tool **"Attachment A."** Disciplinary decisions are at the discretion of the Human Resources Department and may include mandatory re-education, suspension and/or termination of employment, reporting to authorities, and reporting to applicable licensing/certification and registration agencies based on the Level of severity and level of the breach. In addition to any disciplinary action, the HIPAA Privacy Officer will determine if the matter qualifies as a Reportable Breach which triggers additional action, such as patient and governmental notification.

Attachments:

HIPAA Breach Notification Risk Assessment Tool – Attachment A

References:

- HIPAA HITECH Act of 2009
- HIPAA Final ("Omnibus") Rule
- NYS Public Health Law
- Compliance Plan
- 45 CFR 164.400, 402, 408, 414
- 45 CFR 164.530 (a), (d), (g)
- 13402(h)(2) Pub.L. 111-5
- 74 Federal Register, Pages 42, 740-742
- GHVHS I.T. Security Policies
- GHVHS HIPAA Privacy & Security Reference Tool