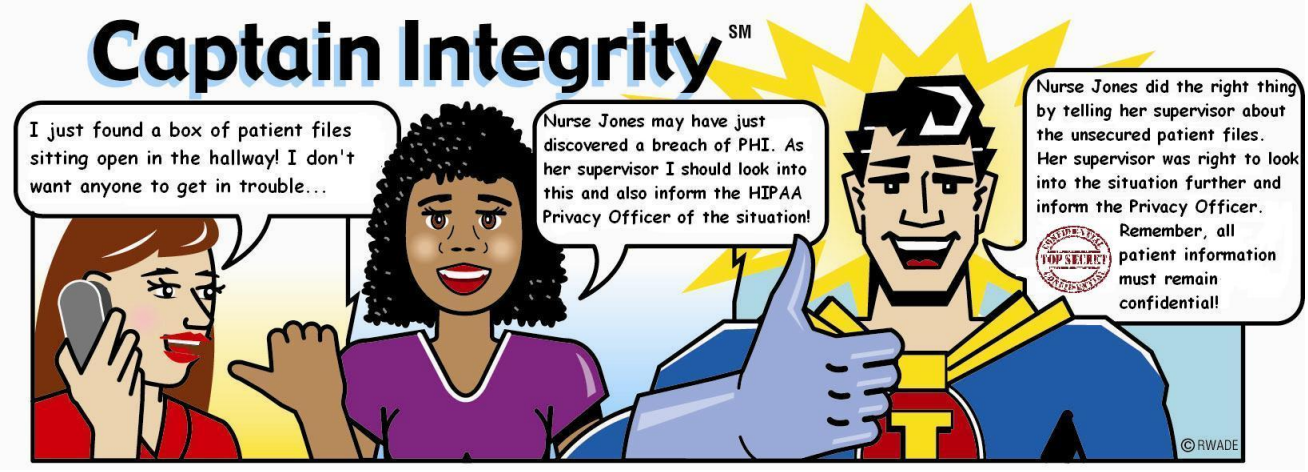
GREATER HUDSON VALLEY HEALTH SYSTEM
ORANGE REGIONAL MEDICAL CENTER
CATSKILL REGIONAL MEDICAL CENTER

Policy/Procedure

Manual: Hospital Wide - Compliance
Section: HIPAA

Policy #:	
SUBJECT: HIPAA Breach & Discipline Policy	
Implementation : (updated version) 7/13	Concurrences: I.T. Security Officer
Reviews: 7/13	
Revisions:	
Initiator: Vice President, Compliance & HIPAA Privacy Officer	
Approval: President/Chief Executive Officer	
Attachment(s):	



PURPOSE:

GHVHS "Staff" (hereinafter meaning ORMC or CRMC employees, physicians, and contractors) are 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:

- **Breach**: the acquisition, access, use, or disclosure of PHI in a manner which compromises the patient' HIPAA Privacy or Security rights. 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
- or any other information that can identify a patient.

The following situations ***may not*** be a breach (please confirm with the HIPAA Privacy Officer):

- Any unintentional acquisition, access or use of PHI by Staff, or a person acting under the authority of the hospital or business associate, so long as made in good faith, within the scope of authority, and does not result in further unpermitted use.
- Any unintentional disclosure by a person who is authorized to access PHI at the hospital or a business associate to another person authorized under the hospital or business associate, so long as the disclosure is not further used or disclosed in an unpermitted manner.
- A disclosure of PHI where the hospital or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

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. Employees should not access their own records. This includes other employees, family and friends. The Department Director will determine the level of access an individual requires.

3. GHVHS will perform random audits of to ensure that only staff with a “need to know” have accessed particular PHI.

There are two levels of Breach: Level 1 and Level 2

4. Level 1 Breach : Examples:
    - Discussing patient information in public areas
    - Leaving a copy of patient information in public areas
    - Leaving a computer unattended in an accessible area with PHI unsecured
    - Accessing a patient record of PHI out of curiosity
    - Looking up images, pictures, addresses of relative or friends or high profile individuals

    A Level 1 Breach may result in a mandatory re-education, disciplinary action process, suspension and/or termination of employment.

5. Level 2 Breach: When PHI is accessed or disclosed for personal gain or with malicious intent; or when PHI may be compromised as a result of reckless disregard for the protected information. Examples:
    - Multiple Level 1 breaches
    - Accessing or disclosing PHI of relatives or friends of high profile individuals relating to the provision of their healthcare (i.e. reason for visit, diagnosis, legal status, etc.)
    - Compiling a mailing list for personal use or to sell
    - Taking a laptop or patient file containing PHI for some personal use
    - Loss of laptop, Blackberry, IPhone, Ipad, or 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)

    A Level 2 Breach may result in mandatory re-education, suspension and/or termination of employment, reporting to authorities, and reporting to applicable licensing/certification and registration agencies.

6. All breaches regardless of whether they are believed to be Level one or Level Two, including staff, public, Business Associate, or patient complaints of breaches are to be investigated and reported to the Department Director and the HIPAA Privacy or Security Officer as soon as they are discovered. The hospital is required to keep investigation files for 7 years.

7. If you are unsure whether an incident qualifies as a breach you should contact your Director or the HIPAA Privacy or Security Officer. Breaches can also be reported anonymously via the Compliance Hotline: 333-HERO (4376).

8. When a breach (or potential breach) is discovered, the Department Director is required to perform an investigation in consultation with the HIPAA Privacy and/or Security Officers. This investigation should focus on:
    - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    - The unauthorized person who used the protected health information or to whom the disclosure was made;
    - Whether the protected health information was actually acquired or viewed; and
    - The extent to which the risk to the protected health information has been mitigated.
    - This Risk Assessment will assist in the determination whether there was a low probability that the PHI was compromised. Under certain circumstances, the event may not be considered a “breach,” for example where the PHI is “Secured” pursuant to the HIPAA Final Rule. The HIPAA Privacy or Security Officer will make that determination.

9. Hospital follow-up: the hospital may be required to notify the party breached by Standard Breach Notice (hospital breach disclosure template) via first class mail within 60 days of discovery of the breach. For breaches of certain size (more than 500) the hospital may have to require other requirements such as media notification, etc. Additionally, notification requirements to HHS and other government agencies, as well as next of kin may be required. The HIPAA Privacy Officer will advise on this process.

10. Well-intentioned or “innocent” release of information is still a violation of the policy.

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