HIPAA
Privacy and Security Reference Tool

May 2018

Authored by the GHVHS Compliance, Audit & HIPAA Privacy Office & IT Security Officer
# Table of Contents

What is HIPAA?......................................................................................................................3
What is Protected Health Information (PHI)?..................................................................................3
Can HIPAA be waived?................................................................................................................3
How does HIPAA affect me?.........................................................................................................3

## Part I: HIPAA Privacy

What is HIPAA Privacy?............................................................................................................4
Who are the HIPAA Privacy Officers?..........................................................................................4
What are the Hospitals’ HIPAA Privacy Policies........................................................................4
  - HIPAA Privacy Policy ...........................................................................................................4
  - HIPAA Bin..................................................................................................................................4
  - Fax Transmissions Policy ........................................................................................................5
  - HIPAA Notice of Privacy Practices ..........................................................................................5
  - Patient HIPAA Special Requests ............................................................................................5
  - HIPAA Marketing and Fundraising Opt Out Policies .................................................................6
  - HIPAA Complaint Filing Policy ...............................................................................................6
  - Access to Patient Health Information and Business Information .............................................6
  - HIPAA Violation, Breach Notification & Disciplinary Policy .....................................................7
  - Medical Record Information Disclosure Policy ........................................................................7
  - HIPAA Business Associate Agreement (BAA) Policy .................................................................7
  - Disclosing Health Information to Patient’s Family via Telephone ............................................8
  - Disclosing Protected Health Information to Law Enforcement Officials ....................................8

GHVHS HIPAA Privacy Policies .................................................................................................9

## Part II: HIPAA Security

What is HIPAA Security?...........................................................................................................10
Who is the HIPAA Security Team at GHVHS?..........................................................................10
What are the Hospitals’ HIPAA Security Policies?.....................................................................10
  - HIPAA Security .....................................................................................................................10
  - Information System Audit Logging Policy ...............................................................................11
  - Access to Patient Health & Business Information ................................................................11
  - Anti-Virus Management Policy ...............................................................................................11
  - Disaster Recovery ..................................................................................................................11
  - Workstation Security Policy...................................................................................................12
  - Media/Hardware Use, Re-Use, Destruction and Disposal .........................................................12
  - Accountability & Data Back-Up ...............................................................................................13
  - Network Security, Usage & Controls ......................................................................................13
  - Encryption ................................................................................................................................13
  - Facility Security .....................................................................................................................14
  - IT Security Incident ................................................................................................................14
  - Password Management .........................................................................................................15
  - Mobile Devices ......................................................................................................................15

GHVHS HIPAA Security Policies ................................................................................................16

## Part III: HIPAA Guidelines for GHVHS Staff

How can I protect PHI?...............................................................................................................17
What is a HIPAA Breach?..........................................................................................................17
What should I do if I suspect a HIPAA breach?..........................................................................19
If I report, will I get in trouble?................................................................................................19
What is HIPAA?
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates the protection and confidential handling of Protected Health Information (PHI). The Health Information Technology for Economic and Clinical Health (HITECH) was passed in 2009 and further strengthened HIPAA to address privacy and security concerns associated with electronic transmission of health information. The Omnibus Final Rule, effective in 2013, strengthened both HIPAA and HITECH by adding more requirements described in this document and in our Policies.

What is Protected Health Information (PHI)?
Everyone must keep Protected Health Information (PHI) confidential. We are required to follow a “minimum necessary standard,” meaning only access the PHI necessary to do your job.

PHI is any information that can identify a patient, such as:

- admission or discharge date or information
- diagnosis or prognosis
- treatment plan or treatment options
- conversations about a patient’s care or treatment
- information about a participant in a computer system
- patient’s medical record number or social security number
- any part of the medical record
- images of the participant
- name
- address
- telephone number
- age/date of birth
- or any other information that can identify a patient.

See GHVHS HIPAA Privacy Policy

Can HIPAA be waived?
No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

How does HIPAA affect me?
All GHVHS Staff members (hereinafter meaning ORMC or CRMC employees, physicians, volunteers, contractors, vendors, students, residents or other persons having patient or PHI contact) are required to comply with all HIPAA requirements. If, after an investigation, you are found to have violated the organization’s HIPAA Privacy or Information Security policies then you may be subject to disciplinary action up to termination and the government or others could even bring civil and criminal actions.
PART I: HIPAA PRIVACY

What is HIPAA Privacy?
HIPAA Privacy refers to the protection of privacy of all health information, including forms created and received by GHVHS.

Who is the HIPAA Privacy Officer?
The Greater Hudson Valley Health System

Trish Manna
tmanna@ghvhs.org
ORMC - (845) 333-7188
CRMC - (845) 397-3516

Anonymous Compliance Hotline: 845-333-HERO (4376) or report online at www.hotline-services.com

What are the Hospitals’ HIPAA Privacy Policies?

HIPAA PRIVACY POLICY
GHVHS “Staff” are obligated to keep patient health information confidential. Protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. GHVHS follows a “minimum necessary standard,” meaning GHVHS works to limit unnecessary or inappropriate access to and disclosure of PHI.

See the GHVHS HIPAA Privacy Policy

HIPAA Bin
Trash containing any patient information must be placed in a marked HIPAA-bin. GHVHS has contracted with an outside vendor who provides locked containers strategically placed throughout all locations. All paper containing PHI must be placed in these containers. The vendor provides us with a certificate of destruction.

See the GHVHS Protected Health Information Confidential Material Destruction (PHI) Policy
**Fax Transmissions Policy**

When sending patient information or records via fax, we should always ensure that the fax number is correct and should always receive a confirmation that the fax was received. Incoming faxes should be checked and distributed appropriately and receipt should be confirmed according to the requested confirmation method.

See the **GHVHS Fax Transmissions Policy**

**HIPAA Notice of Privacy Practices**

The Hospital displays and distributes a HIPAA Notice of Privacy Practice to all patients that describes:

- How the patient’s PHI may be used without their consent;
- Various patient rights including the rights to:
  - Inspect, amend and request copies of their medical records
  - Request an accounting of certain disclosures of their PHI
  - Request confidential communications
  - Be notified of a Breach of their PHI
  - Opt out of Fundraising and Marketing activities
  - Opt out of facility director and restrict visitors

See the Policies on: **GHVHS HIPAA Notice of Privacy Practices**
 **GHVHS Fundraising Opt Out**
 **GHVHS Marketing Opt Out**

**Patient HIPAA Special Requests**

Patients have a right under HIPAA to make a request to restrict their patient information. There are no approvals necessary for the following requests:

- Exclusions from the Facility Directory
- No Clergy visits
- No Volunteer/Staff visits
- No visitors
- No Foundation/Fundraising Activity
- No Hospital Marketing Activity

Reviewable requests are to be granted or denied by the Nurse Manager/Supervisor in a timely manner. If denied, denial must be documented, communicated to the patient and a copy given to the patient. If granted, Nurse Manager/Supervisor will sign the form and communicate with the patient. Reviewable requests include:

- No incoming phone calls
- Selective visitors

See the **GHVHS Patient HIPAA Special Request Policies**
HIPAA MARKETING AND FUNDRAISING OPT OUT POLICIES
Patients may opt out from marketing and fundraising activities. The GHVHS Marketing Departments and the Foundations maintain the Master Opt-Out Lists.

See the GHVHS Fundraising Opt Out Policy
See the GHVHS Marketing Opt Out Policy

HIPAA COMPLAINT FILING POLICY
GHVHS is required to accept complaints about any aspect of our services including complaints related to improper use or handling of PHI.

The HIPAA Privacy Officer will work with the Patient Advocate and management regarding complaints pursuant to this policy. While the HIPAA Privacy Officer may not be the initial contact, he or she needs to be notified of the filing a complaint. If the matter is HIPAA Security related, HIPAA Security Officer will be involved.

See the GHVHS HIPAA Complaint Filing Policy

ACCESS TO PATIENT HEALTH INFORMATION AND BUSINESS INFORMATION
The “minimum necessary” level of security access to PHI or other hospital information will be used. Managers will be responsible for acquiring each staff’s signature on the User Code agreement and release forms and returning the signed forms to the hospital information systems administrator, as well as educating the new staff during orientation.

Staff members who become aware or are suspicious of a situation, in which patient confidentiality or confidential hospital information has been compromised by another staff or by a business agent, must immediately report the situation to the manager. The manager will then investigate the breach of confidentiality report and notify the Privacy Officer. Failure to do so places the staff and the hospitals at risk for a variety of issues. Staff violations of the rules, regulations, policies, and procedures relating to patient information and confidentiality standards will be subject to discipline.

See the GHVHS Access to Patient Health Information and Business Information Policy
HIPAA VIOLATION, BREACH NOTIFICATION & DISCIPLINE POLICY
GHVHS “Staff” 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.

See the GHVHS HIPAA Violation, Breach Notification & Discipline Policy

MEDICAL RECORD INFORMATION DISCLOSURE POLICY
Patients have the right to request their medical record information. If the request is made by an inpatient, request should be conveyed to the Nurse Manager or Charge Nurse of the unit. Nursing staff is to notify the attending physician of the request for record review. Unless the physician or institution has a valid objection, access will be granted.

Requests for medical records after discharge are to be made to the Health Information Management (HIM) Department during normal business hours. The patient or qualified person must fill out the Release of Medical Information Form. Within ten (10) days of receipt of completed release, access to records will be granted or the reason why access is withheld or delayed will be relayed to the requestor. Any disclosure, with or without the patient’s authorization, must be the minimum necessary to fulfill the stated purpose.

See the GHVHS Medical Record Information Disclosure Policy
See the ORMC Requests for Release of Patient Records – Rad Onc
See the ORMC PACS: Release of Images – Print films or CD’s; DI

HIPAA BUSINESS ASSOCIATE AGREEMENT (BAA) POLICY
Each vendor or service provider that may receive, view, access, use, disclose or create PHI from GHVHS must enter into a HIPAA BAA in which it is obligated to protect the privacy and confidentiality of such information in accordance with HIPAA regulations.

See the CRMC HIPAA BAA Policy
See the ORMC HIPAA BAA Policy
**DISCLOSING HEALTH INFORMATION TO PATIENT’S FAMILY VIA TELEPHONE**

Upon admission the patient will be presented a card that has an information access number on it *(last 4 digits of Account/FIN#)*. To inquire about the patient’s condition beyond the one word condition, the caller must provide this code (the one word condition- fair, stable, etc. does not require a code).

If upon admission, the patient is unable to or incapable of accepting this information access number, hospital staff, using best professional judgment, will provide the access number to the individual who will be responsible for making decisions about the patients care.

For the Skilled Nursing Unit and Adult Day Health Care Program at CRMC, the individual(s) who may receive PHI will be determined upon admission and will be so designated on the Resident’s/Registrant’s medical record.

See the **GHVHS Disclosing PHI to Patient’s Family/Friends via Telephone**

**DISCLOSING PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT OFFICIALS**

The Health Insurance Portability and Accountability Act of 1996 carved out a special provision regarding PHI disclosed to Law Enforcement Officials. GHVHS may be required to disclose information in response to the following: court-ordered subpoenas, warrants, summonses; and, administrative requests, subpoenas, or summonses. Further, GHVHS may be required to disclose certain information for the identification and location of suspects, fugitives, material witnesses, and missing persons. Under certain circumstances, staff may disclose information about a patient who may have been the victim of a crime to law enforcement officials.

Certain injuries require GHVHS to make a mandatory reporting to the appropriate officials. Further, information regarding prisoners’ treatment may be disclosed to correctional facilities to aid in the prisoner’s care and protect corrections and law enforcement officers.

Please seek advice from your manager and or the Directors of Health Information Management, Risk Management, or the Legal department before discussing PHI with outside parties.

See the **GHVHS Medical Record Information Disclosure Policy**
See the **Reportable Cases to the Police Policy - ORMC**
See the **Reportable Cases (ED) – CRMC**
GHVHS HIPAA Privacy Policies

- HIPAA BAA Policy
- HIPAA Notice of Privacy Practices Policy
- HIPAA Special Request
- GHVHS Access to Patient Health Information and Business Information
- GHVHS Disclosing PHI to Patient’s Family Friends via Telephone
- GHVHS Fax Transmissions Policy
- GHVHS HIPAA Violation, Breach Notification & Discipline Policy
- GHVHS HIPAA Complaint Filing
- GHVHS HIPAA Fundraising Opt Out Policy
- GHVHS HIPAA Marketing Opt Out Policy
- GHVHS HIPAA Privacy Policy
- GHVHS Medical Record Entries Correction Amendment Policy
- GHVHS Medical Record Information Disclosure
- GHVHS Protected Health Information Confidential Material Destruction
- GHVHS Records Retention and Destruction Policy
PART II: HIPAA SECURITY

What is HIPAA Security?
HIPAA Security refers to administrative, technical and physical safety procedures for GHVHS to ensure the confidentiality, integrity and availability of protected health information.

Who is the HIPAA Security Team at GHVHS?

HIPAA IT SECURITY OFFICER
Jacqui Budakowski
jbudakowski@ghvhs.org
(845) 333-2509

IT SECURITY ANALYST
Katie DeRigge
kderigge@ghvhs.org
(845) 333-2560

What are the Hospitals’ HIPAA Security Policies?

HIPAA SECURITY
It is the job of the HIPAA Security Officer to understand the HIPAA Security Rule and how it applies to the GHVHS, develop and maintain appropriate policies and procedures to ensure compliance with the Security Rule, oversee the security of PHI within all of the components of the GHVHS, and identify and evaluate threats to the confidentiality and integrity of PHI throughout. The HIPAA Security officer, along with the IT Department and Human Resources Department, conduct periodic education for all staff. In the event of a suspected incident, GHVHS staff shall immediately report the possible incident in one of the following ways:

- For immediate emergencies, call the IT Help Desk at 845-333-2020.
- Directly report to management, the HIPAA Security Officer, HIPAA Privacy Officer or CIO.
- Call the Anonymous Compliance Hotline at 845-333-HERO (4376) or report online at www.hotline-services.com

See the GHVHS HIPAA Security Officer Policy
INFORMATION SYSTEM AUDIT LOGGING POLICY
All systems that handle confidential information or make access control (authentication and authorization) decisions record and retain audit-logging information. These logs are reviewed to ensure compliance with our policies.

See the GHVHS Information System Audit Logging Policy

ACCESS TO PATIENT HEALTH & BUSINESS INFORMATION
The purpose of this policy is to limit access to Protected Health Information (PHI) and Business Information (BI). Access will be granted based on the individual’s role and his/her need for such access of confidential patient and/or business information; this access will be determined based on the “minimum necessary” level of access and requested by managers and approved by IT. Managers shall request appropriate access for all new staff members using the User Access Request Form. All users will be given a unique username (created by IT) and password (to be created by user after initial log-in) for access to system components or sensitive data.

See the GHVHS Access to Patient Health Information and Business Information Policy

ANTI-VIRUS MANAGEMENT POLICY
The IT department takes appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect machine from the network. The IT department monitors anti-virus alerts and log files for any suspicious activity or threats detected on Greater Hudson Valley Health System machines.

See the GHVHS Anti-Virus Management Policy

DISASTER RECOVERY
Disasters come in all shapes and sizes. They can be natural or man-made. They can be hurricanes, earthquakes, floods, fires or chemical spills/releases. They can come with days of prior warning or can happen without any warning at all.
At GHVHS we work hard to ensure that, in the event of a disaster, we are still able to treat patients and access electronic health information. We are able to do this by using an off-site disaster recovery location for our Electronic Health Records (EHRs). Our electronic information is constantly replicating itself over to the disaster recovery site, allowing us to pull information from this site in the event we ever lose our information here. This plan also includes emergency access, emergency training, and the individual roles of the emergency response team members.

**Workstation Security Policy**

User workstations must not be left unattended when logged into sensitive systems or data; users are required to logoff of all systems when they leave their workstation for more than a few minutes. Generic IDs may only be used to access workstations that do not themselves store PHI. Sensitive data may not be stored on a portable workstation.

All workstations must be operated in a manner that ensures:

- Confidentiality of PHI,
- Virus scanning of media prior to use on any workstation,
- Only approved software is used, and
- Used in accordance with contract agreements and copyright laws.

For example: make sure WOW and computer screens are turned away from patients and visitors to limit inadvertent viewing; secure any and all equipment containing patient information to deter theft; and report any suspected unauthorized access/use of a workstation to the IT Help Desk and your manager immediately.

See the **GHVHS Workstation Security Policy**

**Media/Hardware Use, Re-Use, Destruction and Disposal**

GHVHS will properly dispose of all media containing identifiable health information. All staff should consult the IT Department before disposing of any electronic hardware or digital media owned by GHVHS (or one of its entities) to ensure it is disposed of in a compliant manner. Media will be sanitized (wiped) before being reused or should be destroyed completely whether or not they are known to contain any confidential data. GHVHS has contracted with an outside vendor to dispose of such media.

See the **GHVHS Media-Hardware Use, Re-Use, Destruction and Disposal Policy**
**ACCOUNTABILITY & DATA BACK-UP**
All electronic information considered of value to GHVHS should be copied onto secure storage media on a regular basis (i.e. backed up), for disaster recovery and to facilitate business continuity.

**NETWORK SECURITY, USAGE & CONTROLS**
GHVHS provides computer devices, networks, and other electronic information systems. These systems are effectively managed to ensure that the confidentiality, integrity, and availability of information assets. All network equipment and software will be installed and maintained by IT; users are prohibited from personally installing anything. Use of tools that compromise security are strictly prohibited. All network access points are protected by a firewall and intrusion prevention system that monitor and control communication. GHVHS reserves the right to access the contents of any messages or data sent over its network and use that information to enforce its policies.

See the **GHVHS Network Security Usage and Controls Policy**

**ENCRYPTION**
When necessary, appropriate encryption must be used to protect the confidentiality, integrity, and availability of PHI contained on GHVHS information systems. This policy outlines appropriate encryption standards for removable media, email, transmissions, and mobile devices. Anytime it is necessary to email confidential or sensitive information, the subject line must contain the word “encrypt” to ensure the security of the email. It is never appropriate to email PHI to a private email address.

See the **GHVHS Encryption Policy**
FACILITY SECURITY

Both ORMC and CRMC have a Security Director who is responsible for developing, implementing and enforcing facility security policies and procedures at their respective campuses, in addition to security personnel (security officers). All staff members are required to report any and all security concerns to the security officer on duty.

Identification badges/wristbands must be worn at all times while on GHVHS property. All staff members, partners, and vendors will be provided with a photo identification badge by Human Resources and the Security Office. Staff member badges have a blue box around the individual’s photo, while non-staff member badges (i.e. vendors) have a red box around the individual’s photo. These badges must be visible at all times and must be worn above the waist. Patients are provided with wristbands upon their admission. These wristbands must not be taken off or tampered with while the patient is still on GHVHS property.

See the ORMC Facility Security Policy & the CRMC Facility Security Policy

IT SECURITY INCIDENT

It is the Policy of GHVHS to rapidly identify and appropriately respond to all security incidents, regardless of their severity. A “security incident” is an adverse effect on people, process, technology, data or facilities. An “information security incident” is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. A “non-electronic information security incident” is the real or suspected theft, loss or other unauthorized access to sensitive or restricted information stored in non-electronic form, such as printed documents and files.

Immediately upon observation, GHVHS staff must report any suspected and known security incident(s) in one of the following ways:

- For immediate emergencies, call the IT Help Desk at 845-333-2020 and notify your supervisor.
- Direct report to management, the HIPAA Security Officer, HIPAA Privacy Officer or CIO.
- Call the Anonymous Compliance Hotline at 845-333-HERO (4376) or online at www.hotline-services.com

See the GHVHS IT Security Incident Policy
**PASSWORD MANAGEMENT**

GHVHS requires the use of strong passwords by all staff members who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable health information. All passwords shall be at least 8 characters in length and require the use of the following: capital letters; lower case letters; and numbers. Passwords must be changed at least every 90 days. Staff should follow these guidelines for passwords:

- Don’t reveal a password over the phone to ANYONE;
- Don’t reveal a password in an email message;
- Don’t talk about a password in front of others;
- Don’t hint at the format of a password, like, “my family name”;
- Don’t reveal a password on questionnaires or security forms;
- Don’t share a password with family members;
- Don’t reveal a password to co-workers or anyone;
- Don’t write passwords down and keep them near computer or workstation.

If any staff member loses, forgets, or experiences compromise of their password they shall immediately notify the IT Help Desk. Proper password management should be emphasized during staff trainings.

See the **GHVHS Password Management Policy**

**MOBILE DEVICES**

GHVHS extends all the privacy and security protections required by HIPAA to Protected Health Information accessed, used, transmitted, and stored on mobile devices operated by members of our workforce.

This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and are capable of receiving, processing, or transmitting Protected Health Information, including Mobiles Devices, fax machines and printers. Mobile Devices include, but are not limited to, digital music players, hand-held computers, laptop computers, tablets, personal digital assistants (PDAs), iPads, Smart phones and devices, etc. Further, this Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased by, and provided by GHVHS.
Mobile Devices which cannot be or have not been configured to comply with this Policy are prohibited. GHVHS will also limit the access, use, transmittal and storage of Protected Health Information on mobile devices to the Minimum Necessary. GHVHS is required to train workforce members on the safe and secure usage of mobile devices that are utilized to access, use, transmit, or store Protected Health Information.

“Transmitting of Greater Hudson Valley Health System sensitive information (e.g., Business Sensitive Information (BSI) or Protected Health Information (PHI)) through non-Greater Hudson Valley Health System approved methods is prohibited. These include texting, paging, personal email and social networks. Electronic communications containing PHI should be done through Greater Hudson Valley Health System applications.”

See the Mobile Device Acceptable Use Policy

GHVHS HIPAA Security Policies

- GHVHS HIPAA Security Officer Policy
- GHVHS Information System Audit Logging Policy
- GHVHS Access to Patient Health Information and Business Information Policy
- GHVHS Anti-Virus Management Policy
- GHVHS Workstation Security Policy
- GHVHS Media-Hardware Use, Re-Use, Destruction and Disposal Policy
- GHVHS Network Security Usage and Controls Policy
- GHVHS Encryption Policy
- ORMC Facility Security Policy
- CRMC Facility Security Policy
- GHVHS IT Security Incident Policy
- GHVHS Password Management Policy
- Mobile Device Acceptance Use Policy
PART III: HIPAA GUIDELINES FOR GHVHS STAFF

How can I protect PHI?
These measures should be taken to protect the security of PHI:

- Avoid faxing PHI
- Keep paper records in locked drawers
- Be sure that the areas where patient charts are kept are supervised or locked
- Place PHI that will not be saved (discarded arm bands, temporary lab reports, etc.) in the HIPAA bin to be destroyed
- Log out after electronically accessing PHI
- Never make copies of PHI and take then with you when you leave the hospital
- Always use hospital encryption methods for transfer of PHI
- Turn computer screen so it cannot be seen by others
- Do not share passwords
- Safeguard laptops and other mobile devices
- Don’t gossip about patient’s health
- Don’t look up records you shouldn’t
- Don’t post PHI on Social Media

What is a HIPAA Breach?

Breach: the acquisition, access, use, or disclosure of PHI in a manner which compromises the patient’s HIPAA Privacy or Security rights. PHI is any information that can identify a patient and includes but is not limited to the following examples:

Breaches are categorized into Level One, Level Two, and Level Three, based upon the significance of comprised PHI.

Level One Breach: Examples:

- Discussing patient information in public areas
- Leaving a copy of patient information in public areas
- Giving a patient another patient’s discharge instructions
- Leaving a computer unattended in an accessible area with PHI unsecured
Level Two 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 Three 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

The HIPAA Privacy and/or Security Officer will investigate all reports of Violations or Breaches utilizing the Breach Notification Risk Assessment Tool. 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.

For breaches of certain size (more than 500) the hospital may have to necessitate other requirements such as media notification, etc.

See the GHVHS HIPAA Violation, Breach Notification & Discipline Policy
What should I do if I suspect a HIPAA breach?

When a breach (or potential breach) is discovered, it must **immediately** be reported to the Department Director and the HIPAA Privacy and Security Officer. The Department Director is required to perform an investigation in consultation with the HIPAA Privacy and/or Security Officers. This investigation should focus on:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

This Risk Assessment will assist in the determination whether or not there was a low probability that the PHI was compromised. Under certain circumstances, the event may not be considered a “breach” including instances where the PHI is “Secured” pursuant to the HIPAA Final Rule. The HIPAA Privacy or Security Officer will make that determination.

If the occurrence is found to be a breach after the Risk Assessment has been conducted, the Compliance Officer will follow the mandatory reporting methods.

See the **GHVHS HIPAA Violation, Breach Notification & Discipline Policy**

If I report, will I get in trouble?

No staff may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. In fact, reporting is not optional it is **mandatory**.

See the **Non-Retaliation Policy**

Call the GHVHS HIPAA Privacy Officer or HIPAA IT Security Officer with any questions.