



Group Health Graduate Medical Education
c/o GHP PLD
Mailstop E2N
320 Westlake Avenue North
Seattle, WA 98109

F: 206-877-0649
www.ghc.org/

Dear Student,

Welcome to Group Health! Please find your required site documents attached below. We will require you to submit:

1. Application for Clinical Training
2. Confidentiality and Security Agreement
3. Privacy Training Exam
4. Hospital Site Documents

These documents must be submitted no later than three weeks prior to the start date of your clerkship. Preferably please scan/email them to graduatemedicaleduca@ghc.org. Otherwise fax or mail contact information are located above. Please note that documents not submitted on time will delay the start of your clerkship.

If you have any questions about the documents, please contact us. Thank you for your assistance.

Confidentiality and Security Agreement



This Agreement applies to all users of Group Health Cooperative information systems. I understand that as a user of Group Health Cooperative information systems, I may have access to or become aware of confidential information and I acknowledge my legal and ethical obligations to protect the confidentiality of all such information. Such confidential information includes, but is not limited to, the following:

- f* Patient/member/enrollee/participant health care and financial information, including but not limited to, medical records, credit card and banking information, health plan information, billing and accounts information, claims data, and peer review activities;
- f* Group Health Cooperative, Group Health Options, Inc. or Group Health Permanente employee personnel, compensation, financial, and health care information; and
- f* Business information relating to Group Health Cooperative and its affiliates and subsidiaries, including but not limited to human resources, administrative, payroll, fiscal, proprietary, research, sales and marketing, planning, risk management, legal, health plan, and management information.

The above will be referred to as "Group Health Information" throughout this Agreement.

By signing below, I acknowledge that I have read and understand this Agreement and hereby agree to comply with its terms. I acknowledge this Agreement is a condition of my employment or affiliation with Group Health Cooperative, Group Health Options, Inc. or Group Health Permanente and my obligations set forth in this Agreement continue after the termination of such employment or affiliation.

Signature _____ Date _____

Print Last/First Name _____ Employee ID _____

Department _____ User ID _____

Manager Name _____

OWNERSHIP OF INFORMATION AND INFORMATION SYSTEMS

- f* I understand that information contained on Group Health Cooperative information systems, whether locally or remotely hosted, is owned by and belongs to Group Health Cooperative, including but not limited to all medical records and other information relating to Group Health Cooperative patients/members/enrollees/participants.
- f* I understand that at any time, with or without notice or consent, Group Health Cooperative may audit, investigate, monitor, access, and disclose information related to my use of Group Health Information and/or its information systems, including any data I create, transmit, or store on Group Health Cooperative information systems.
- f* I will only access or use information systems or devices I am authorized to access with a business need to know.
- f* I agree to complete all privacy, confidentiality, and security training required by Group Health Cooperative.
- f* I agree that I do not have any expectation of privacy with respect to my use of Group Health information systems, including any data that I create, transmit, or store on those systems.
- f* I understand that Group Health Cooperative has the right to access, copy, and make unlimited use of any data which I receive, create, store, or transmit in the course of my employment or relationship with Group Health Cooperative, regardless of where such data is stored. I further agree to provide Group Health Cooperative access to any such data stored on media in my personal possession, whether or not the storage media is owned by Group Health Cooperative.

AUTHORIZATION TO ACCESS, CREATE, USE, AND DISCLOSE INFORMATION

- f* I am only authorized to access, create, use, or disclose Group Health Information required to perform my job/contractual duties.
- f* I will not use my access to Group Health information systems to view my health care or health plan information, unless such access is through MyGroupHealth or the Lawson employee self-service portal.
- f* I will not use my access to Group Health information systems to view information about my family members, friends, Group Health Cooperative, Group Health Options, Inc. or Group Health Permanente employees, or others for personal purposes; instead, I will only view such information if required by my employment/contractual duties. I understand that if I access my own or a family member's health or other information through any means other than Group Health's established processes for patient access to such information, I am subject to termination of my employment, contract, or affiliation with Group Health Cooperative, Group Health Options, Inc., or Group Health Permanente.
- f* I will differentiate between my role as a Group Health employee versus a Group Health patient demonstrating appropriate use of Group Health systems in both roles. I will use secure messaging (and not staff messaging) when I am communicating as a patient with my Group Health provider. I will maintain boundaries between my personal relationships and will not allow friends and family to use my status as a Group Health employee to gain patient information.
- f* I will only obtain my own health care or health plan information or that of a family member's (or others for whom I may legally access information) according to Group Health Cooperative's established processes for patient access to information, such as through the clinic business/medical records office, practitioner, care team, Customer Service, and MyGroupHealth. I understand that if I access my own or a family

member's health or other information through any means other than Group Health's established processes for patient access to such information, I am subject to termination of my employment, contract, or affiliation with Group Health Cooperative, Group Health Options, Inc. or Group Health Permanente.

I will not use Group Health systems or resources for personal use and will abide by appropriate use policies.

VIOLATION OF AGREEMENT

f I understand that my failure to comply with any part of this Agreement may result in disciplinary or other action, including denial of access to Group Health information, and/or termination of my employment, contract or affiliation with Group Health Cooperative, Group Health Options, Inc. or Group Health Permanente, or my right to practice in a Group Health Cooperative facility.

I understand that, in some circumstances, Group Health may report violations of this agreement to the appropriate regulatory authorities.

CONFIDENTIALITY

I understand that in the course of my work, I may see or hear confidential information about Group Health patients, members, enrollees and participants or about Group Health business.

I recognize my legal and ethical obligations to protect the confidentiality of:

Health information including but not limited to medical records, personal finances, billing accounts, claims data, risk management, peer review activities, and other patient, member, enrollee, and participant information.

Business and proprietary information, and other confidential information relating to Group Health Cooperative and its affiliates, such as human resources, payroll, fiscal, research, planning, and management information.

I will access, use, or disclose Group Health Information only when it is my legitimate business/job responsibility to do so and will disclose such information only to individuals with a legitimate need to know such information.

I will not discuss Group Health Information with unauthorized individuals, nor will I discuss Group Health Information in public areas in a manner so that unauthorized individuals may hear such information.

f I understand that laws provide special protections to any and all references to patient sexually transmitted disease treatment or consideration of sexually transmitted disease testing and unauthorized release of such information may subject me to legal and/or disciplinary action.

I understand that the laws provide special protections for mental health and substance abuse health information and that unauthorized disclosure of such information may subject me to legal and/or disciplinary action.

SECURITY

I will protect the security and integrity of Group Health Information from loss, misuse, falsification, and unauthorized access, disclosure, modification, or destruction.

f I will comply with and not attempt to circumvent all security configurations or user security requirements (such as logging off, locking my workstation and positioning screens away from public view, etc.) when accessing and using Group Health Information and information systems, including remote access to Group Health information systems.

I will not take advantage of, use, or disclose unsecured Group Health Information or an unsecured workstation.

f I will keep my passwords secret, change them as required by Group Health's password aging standard, not share them with anyone, and not allow others to use my logon credentials to access Group Health Information and information systems. I will use only my own user ID and passwords to access Group Health Information and information systems.

If I use a portable electronic device, such as a Blackberry or Blackjack, etc. or laptop computer, to store Group Health Information, I will do so in accordance with Group Health Cooperative Policy F-08-508, Security for Portable Electronic Devices and Portable Electronic Devices User Agreement.

I will observe Group Health security procedures when transmitting confidential information, such as faxing, e-mail, secure messaging, staff messaging, or secure file transfer.

I will print information from Group Health information systems only when necessary for a legitimate purpose and I acknowledge that I am accountable for the physical security of all information I print.

f I will not copy, move, and store Group Health information to non-Group Health systems, removable storage media, or local hard drives without the express approval of the Information Security Office.

If, as part of my responsibility, I must take any Group Health information off Group Health premises, I will only do so with permission from my manager and I acknowledge my duty to protect such data from unauthorized disclosure.

I will follow Group Health *ConWaste* and departmental policies and procedures for disposing of confidential information.

I will not ask any other person to access Group Health Information on my behalf that I am not otherwise permitted to access.

REFERENCES, RESOURCES, INCIDENT REPORTING

Privacy, confidentiality, and security policies, procedures, and other resources are available on InContext.

I may also contact the Privacy Office or the Information Security Office about any privacy or information security questions I have.

I may contact the Privacy Office or Information Security for answers to questions and concerns including questions I may have about this agreement.

I will inform my manager and/or the Information Security Office on the same day I observe any actual or suspected security violations, including compromised passwords, or inappropriate access or security actions.

I will inform my manager and/or the Privacy Office on the same day of any actual or suspected inappropriate use, access, or disclosure of Group Health Information, whether by me or another individual, whether intentional or accidental.



Privacy and Security

Basic Training

April 2010



Welcome To Basic Training For Privacy And Security

At Group Health, we are committed to protecting the privacy and security of our member and patient identifiable information. This training will provide you with a foundation of privacy and security principles to help you with your everyday work. When you have completed this training you will understand what privacy and security are and what they mean to you in your role at Group Health.

By the end of this course, you will be able to:

1. Understand what protected health information is and your responsibility to follow Group Health policies.
2. Understand the fundamental concepts of privacy and security.
3. Recognize, reduce, and report privacy and security risks in your work environment.
4. Locate resources for help with privacy and security questions.

Contents

CHAPTER 1

What are privacy and security and why are they so important?.....	4
What is Protected Health Information?.....	5
Group Health Values.....	7
Group Health Consumer Bill of Rights	7
Federal & State Law	8

CHAPTER 2

Fundamental Concepts of Privacy and Security	9
The First Cornerstone	10
The Second Cornerstone.....	14
The Third Cornerstone	16
The Fourth Cornerstone.....	19
The Fifth Cornerstone	19

CHAPTER 3

Standards and Safeguards that Reduce the Risk of Security Breach	20
Workstation Security	21
Privacy Screen	22
Passwords	23
Access.....	25
Email and Email Security.....	26
Mobile Handheld Devices	27
Confidential Documents	28

CHAPTER 3

Your Responsibilities	29
Privacy and Security	30
Confidentiality and Security Agreement.....	31
Manager Responsibility	31
The Three R's.....	32
Quiz Questions	33
For More Information.....	35

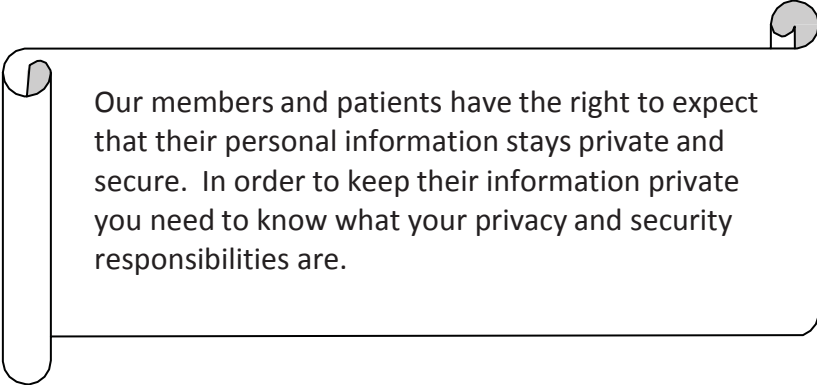
What are privacy and security and why are they so important?

What is Privacy?

Privacy is a member's and patient's right to know that their personal health information is being protected. Privacy means that the member's and patient's private information is being used or shared in a manner for which it can legally be used by Group Health.

What is Security?

Security is the protection of that information from disclosure to unauthorized individuals. Security is also ensuring that the information isn't altered, destroyed or lost.



Our members and patients have the right to expect that their personal information stays private and secure. In order to keep their information private you need to know what your privacy and security responsibilities are.

What is Protected Health Information?

To protect our members' and patients' privacy you need to know what protected health information is, and the various ways you can encounter it.

The following are examples of information that could unintentionally identify a member or patient:

- x A report with patient information left unattended on a desk.
- x A computer screen positioned where the public can view patient information.
- x An unguarded conversation in a hallway about a patient.

<i>Protected Health Information</i>	<i>electronic Protected Health Information</i>
<p>PHI is any information that could identify a member or patient in any form: oral, written, or electronic. PHI refers to the past, present, or future health care of an individual, or to payment for that care. PHI is any information that could identify a member or patient, whether on paper, in a computer file, or spoken aloud.</p>	<p>ePHI includes any medium used to store, transmit, or receive PHI electronically. Here are some examples:</p> <p>Store</p> <ul style="list-style-type: none"><i>f</i> File servers and shared drives<i>f</i> Personal computers<i>f</i> iPods<i>f</i> CDs, DVDs<i>f</i> USB memory sticks<i>f</i> PDAs, Smartphones <p>Transmit</p> <ul style="list-style-type: none"><i>f</i> Personal computers<i>f</i> Blackberries<i>f</i> Smartphones<i>f</i> Email<i>f</i> File transfer<i>f</i> File servers <p>Receive</p> <ul style="list-style-type: none"><i>f</i> Personal Computers<i>f</i> Blackberries<i>f</i> Smartphones<i>f</i> Email

You must always be aware of the information around you. PHI and ePHI come in many forms:

Electronic Hardware
<ul style="list-style-type: none"><i>f</i> GH databases<i>f</i> files servers<i>f</i> network share drives<i>f</i> fax memory

Portable Electronic Devices
<ul style="list-style-type: none"><i>f</i> Laptops<i>f</i> Cell phones<i>f</i> CDs & DVDs<i>f</i> Memory sticks

Paper documents
<ul style="list-style-type: none"><i>f</i> computer printouts with individually identifiable information on your desk, at the fax machine, or on the printer

Electronic Documents
<ul style="list-style-type: none"><i>f</i> Emails<i>f</i> Medical records<i>f</i> Digital images, such as x-rays<i>f</i> Claims data

Group Health Values

Federal and state law, accrediting bodies, and Group Health values are the foundation on which our privacy and security policies are built.

Group Health Consumer Bill of Rights

The Group Health consumer bill of rights was written in 1976, long before many of the laws we have today were written. Why did Group Health feel it was necessary to talk about patients rights when it wasn't required by law?

The answer is simple; it was about doing the right thing. Our members and patients value their privacy – so Group Health needs to value our member and patient privacy.

“You have the right to privacy when receiving care at the Cooperative. Private information, which is necessary for us to receive in order to serve you, will remain private and accessible only to those requiring such information to serve you.”

Federal & State Law

The Federal Privacy Rule (HIPAA) establishes the floor for privacy protections nationally. In some instances state and other federal laws may be stricter than the Privacy Rule. Where state or federal laws offer greater privacy protections, we will follow those stricter requirements.

State laws are similar to federal laws but require Group Health to place extra restrictions on specially protected areas in the medical record.

State law applies special protection to information about:

- f* Mental health illness and treatment
- f* Control and treatment of sexually transmitted diseases
- f* Reproductive care for minors

Group Health creates policies to protect the privacy and security of member and patient information. Policies fulfill our legal requirement but they also help staff know what is expected of them.

Policies guide us, they tell us the proper way to approach privacy and security, and they help us to understand what role each individual plays in the effort to protect patient privacy.

If you work at Group Health, in any capacity, these policies and rules apply to you. It's important to realize that the rules are for the most part about respect and courtesy.

Fundamental Concepts of Privacy and Security

Now that we've talked about what "privacy" and "security" mean, let's talk about some fundamental concepts of privacy and security.

As you will see, there are five cornerstones to privacy. These cornerstones guide you. They help you follow the law and Group Health policies when working with confidential information.

FIVE CORNERSTONES

1	<i>Is it permitted by law?</i>	Only use and share protected health information (PHI) for purposes permitted by law.
2	<i>Do you need to know?</i>	Only use and share protected health information (PHI) for purposes permitted by law.
3	<i>Is it the minimum necessary?</i>	Do not use, access, or share more information than is needed.
4	<i>You should never assume.</i>	Confirm that PHI is necessary information. If you don't know, ask your supervisor, privacy officer or information security officer.
5	<i>Your most important possession.</i>	Always treat PHI as if it were your own most important possession. You wouldn't leave your wallet lying around, don't leave PHI where anyone could take it.

The First Cornerstone

Before you use or share information, ask yourself **“Am I legally permitted to access this information?”**

Member and patient information should be accessed **only** when it is needed to provide care or conduct Group Health business.

The bottom line about privacy is this: You may only use and share member and patient information as authorized by the patient or as permitted by law

This means you need to know what use and disclosure is allowed and what isn't. You also need to remember what precautions to take when handling and sharing information.

You are using PHI when you	You are disclosing PHI when you
<ul style="list-style-type: none"><i>f</i> Send an e-mail<i>f</i> Complete a form<i>f</i> Run a report<i>f</i> Create a database<i>f</i> Document in Epic<i>f</i> Discuss a patient	<ul style="list-style-type: none"><i>f</i> Discuss a patient with someone who isn't a Group Health employee<i>f</i> Share information outside of Group Health<i>f</i> Fax information outside of Group Health<i>f</i> E-mail information outside of Group Health

Without Authorization

There are situations when it is appropriate to release PHI without specific authorization from the patient. Some of those situations are for the purposes of treatment, payment, and operations.

For example, Group Health does not need an authorization to

- Share information between providers.
- Share information between departments, such as X-rays and lab work.
- Bill patients for health care Group Health provides.
- Pay others who provided care to patients.
- Protect public health and safety or to prevent or control disease.
- Report vital statistics, such as births and deaths.
- Comply with State and Federal law.

Treatment, Payment and Operations

Generally, you may use and share PHI **without** patient authorization for purposes allowed by law, such as for **treatment, payment** and healthcare **operations**.

In order to provide the best care for our members and patients, we must share information between doctors, nurses, lab technicians and others who are involved in the patients care. For this reason, you do not need patient authorization for **treatment** purposes.

Once a patient has been treated, Group Health is allowed to use patient information for **payment** purposes. This allows us to bill patients for treatment without authorization.

Some examples of payment purposes:

- Determining eligibility
- Billing, claims management, or collection activities
- Reviewing services for medical necessity or coverage

Once a patient has been treated, Group Health is allowed to use patient information for **payment** purposes. This allows us to bill patients for treatment without authorization.

Some examples of payment purposes:

- Determining eligibility
- Billing, claims management, or collection activities
- Reviewing services for medical necessity or coverage

Group Health is allowed to use patient information for **operational** purposes, such as:

- Business planning and development
- Teaching health care professionals
- Quality assessment and improvement activities
- Legal services, auditing functions and to carry out compliance activities

Specially Protected Information

All PHI must be protected, but some information have stricter rules on how you handle them.

This information is considered **specially protected information** and there are four general categories that are considered specially protected:

- f* Mental Health
- f* Chemical dependency treatment
- f* Sexually transmitted diseases, HIV, and AIDS
- f* Reproductive services for minors

Depending on the type of information, minors have the right to consent to treatment and to authorize disclosure of specially protected health information. This includes sharing information with parents and family.

The age of consent depends on the type of information.

Age 13	Age 14
Mental health	STDs, HIV and AIDS
Chemical dependency treatment	Sexual and reproductive care

Access

Every person at Group Health must be aware of the appropriate use and disclosure of PHI.

You need to think about how your actions **protect** or **violate** the privacy of members and patients and the confidentiality of patient information.

The Second Cornerstone

The second cornerstone of privacy is **need to know**. It's an essential step in keeping confidential information private.

Before you access information you need to ask yourself these three questions:

1. Do I **need** to know this information?
2. Do I have a **right** to know this information?
3. Am I accessing this information only because I'm **curious**?

Having a "legitimate business need to know" means you may access clinical or business information **only** when necessary to do your job.

Only staff members with a legitimate business need to know are authorized by Group Health to access, use, or share member or patient information of any kind.

To put it simply, the only information you should be accessing is information you need to do your job.

A legitimate business need to know **does not** include:

- Using your employee systems access to look up health or account information about you, your children (of any age), family, friends or co-workers
- Obtaining a neighbor's lab results
- Looking up the phone number, birthday, marital status, or address of a co-worker
- Looking up information for a coworker because they aren't allowed to look at their own record.

You must talk to your provider or use MyGroupHealth if you need information about your care, just like any other Group Health patient.

Scenario

Chris recently had some lab work done and wants to know the results. He asks his co-worker Jennifer to look in Epic and tell him what the results are. Jennifer tells Chris she can't help him; he will have to get his results some other way.

Question: Did Jennifer do the right thing?

Answer: Yes, Jennifer should not be accessing her co-workers medical record for any reason unless she's involved with his care. Since Jennifer isn't involved with Chris' care, he needs to talk to his care team or log on to MyGroupHealth to get his lab results.

The Third Cornerstone

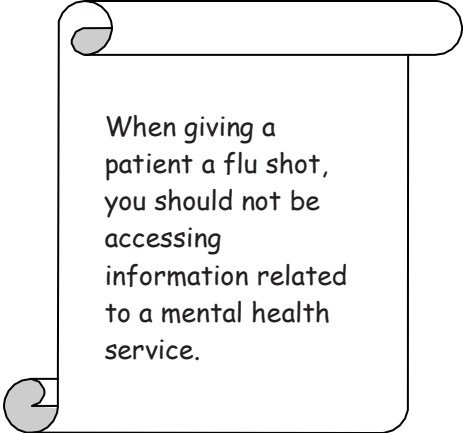
When you have established the first two cornerstones – you know you are **legally** permitted to use the member or patient information and you know you **need** to access it to do your job – you must consider the **minimum necessary rule** before accessing the information.

What is Minimum Necessary?

"Minimum necessary" means you are only allowed to access the minimum amount of member or patient information you need to do your job.

In some situations the minimum necessary rule does not apply, such as when:

- Exchanging information between providers who are caring for a patient.
- Disclosing information to the patient.
- The patient authorizes in writing the use and disclosure of their information.
- We are legally mandated to share information, such as reporting suspected child abuse.



When giving a patient a flu shot, you should not be accessing information related to a mental health service.

Scenario

Suzy is a Patient Care Representative. While checking a patient in, she discovers they have a mutual hobby. Later, Suzy is curious to know where the patient lives and is thinking about calling her to talk more about the hobby.

Suzy decides not to look in the medical record for this information because she doesn't think it's the right thing to do.

Question: Would it have been okay for Suzy to get that information from the medical record?

Answer: Suzy did the right thing by not looking at the patient's medical record for her address and phone number. Suzy should only be looking at information she needs to do her job.

Requesting Information

Another part of the third cornerstone is sharing. You should never share more information than is needed to care for the patient.

When you receive a request, if the requestor is not known to you, **verify** their identity and authority before providing PHI.

The same rules apply when you are requesting information; limit your request to only the information you need to do your job.

Scenario

Dr. Smith calls and asks for copies of Mrs. Johnson's radiology report from her car accident. You don't know who Dr. Smith is.

Question: Is it okay for you to fax the radiology report to him?

Answer: Maybe. Before faxing the x-rays you must first verify that Dr. Smith is who he says he is.

In this case, Dr. Smith wasn't really a doctor. He worked for the car insurance company involved in Mrs. Johnson court case.

The Fourth Cornerstone

Once you have established the first three cornerstones of privacy

- x you know it's **permitted**
- x you **need to know** the information
- x you are using the **minimum necessary**

now you need to confirm that PHI is **necessary information**.

Ask yourself if the information you are accessing is really necessary to care for the member or patient or to do your job.

If you are able to accomplish your task without accessing PHI, then don't access it.

The Fifth Cornerstone

You must always treat PHI as if it were your most valued possession.

You wouldn't leave your car unlocked with the keys in the ignition; you would practically be asking for someone to steal it.

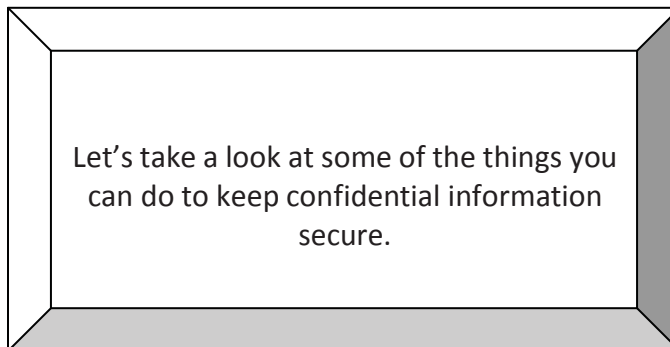
By leaving PHI out where anyone could take it you are tempting someone to steal it. Remove the temptation by putting it away.

Standards and Safeguards that Reduce the Risk of Security Breach

At Group Health we have the responsibility to ensure that we are protecting confidential information from harm and unauthorized use.

The best way to ensure we are meeting this responsibility is to have standards and safeguards which reduce the risk of security breaches.

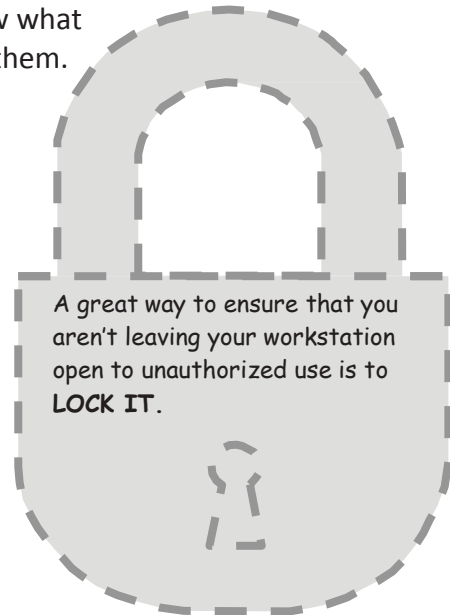
Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information is stolen, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.



Workstation Security

Much of the information you use at Group Health will be accessed through your workstation. It is especially important for you to know what the workstation security rules are and how to follow them.

- x During the work day, lock your workstation by pressing the **Ctrl/Alt/Delete** keys then select **Lock Computer** whenever you are away from your desk.
- x From a Point of Care workstation, click the “Secure” button on Epic and close out of all applications before leaving the exam room.




Remember, it's your responsibility to protect any information in your possession. All system access is logged and monitored and you are accountable for all information accessed using your account.

Group Health workstations may not be used by unauthorized individuals for any purpose. This means your friends and family members are not allowed to check their e² mail on your workstation.

- x Don't download or install unauthorized software such as screensavers. By installing a personal screensaver you are increasing the risk of spyware or virus attack.
- x Never bypass your workstation security, it's there to protect you. Not only does it protect you, it also protects Group Health assets.

Privacy Screen



Your computer screen must be positioned in a way so it is not visible to unauthorized individuals.

If your computer screen could be seen by the public, you should have a privacy screen installed.

If you don't have a privacy screen and need one, your manager can request one through ISD.

Passwords

You must **never** share any of your passwords.

In addition to keeping your own passwords secret, you must never use someone else's user ID and password to access Group Health computer applications and information.

Treat your password as you treat your debit card pin, never give it out and change it if you suspect a breach.



Here are a few easy things you can do to support password security:

- Choose a password that is hard to guess, one that includes numbers, letters and special characters
- Never write down your passwords
- Change your password immediately if you think someone has inappropriately accessed your account

Think Before You Click

Be cautious about clicking “ok” on web pop opening unknown emails. You run the risk of attracting spam, phishing attacks, and other malicious programs.

You should never plug personal equipment such as thumb drives, USB drives, or iPods in to Group Health’s network.

Don’t download or install unauthorized software such as screensavers. By installing a personal screensaver you are increasing the risk of a virus attack.

Ⓜaps



Access

Systems Access

We protect our patients' privacy by controlling access to their health information. This means that we must always know who's using the information and how they are using it. That is why the level of access you have is based on your job function or role.

Remote Access

For individuals granted remote access, all workstation rules as well as confidentiality and security requirements apply when using remote access.

When using remote access you should limit the amount of confidential information accessed to only what you need to do your job. Never save confidential documents to a personal device.

Email and Email Security

When confidential information is sent electronically outside of the Group Health network it must be encrypted to avoid confidentiality breaches due to interception. Encryption makes the information unreadable by anyone who isn't authorized to access it.

Email – There are 3 types of appropriate messaging that can be used at Group Health:

- x **MyGroupHealth secure messaging** – Patients should be using secure messaging to communicate with their doctor.
- x **Staff messaging through Epic** – Clinic staff should use staff messaging to communicate with each other.
- x **Outlook email** – When using Outlook, users should be limiting patient and confidential information to the minimum needed to satisfy the request. If PHI is involved, users must encrypt that information before it can be sent outside of the Group Health network.

Scenario

Amy works in marketing. She received an email from an employer group and responded to the request with the member's social security number.

After sending her email, Amy received a message telling her that the email she sent was blocked.

Question: Why was Amy's email blocked?

Answer: When Amy responded to the message she didn't remove the patient information. Amy's email was blocked by the content filter because the social security number from the original message wasn't deleted from her reply.

Amy should remove any PHI from the original message before sending her reply.

In this case, Dr. Smith wasn't really a doctor. He worked for the car insurance company involved in Mrs. Johnson court case.

Mobile Handheld Devices

Pagers

Text pagers aren't secure, they are susceptible to "eavesdropping". You shouldn't use a pager to transmit confidential information.



Cell phone & Smart Phones

Mobile handheld devices such as cell phones, Blackberries, and Blackjacks are easily lost, stolen, or misplaced. ~~They~~ **They** never store confidential information on these devices.

When using a mobile phone, be conscious of others who can overhear your confidential conversations. For safety reasons, you should never use your cell phone when you are driving. You should also use the password lock available on your cell phone.

Confidential Documents

You should **always** keep printed confidential documents somewhere secure, like a locked drawer or file cabinet. Don't leave a document containing PHI where a visitor can see or take it.



All confidential information should be stored on the G: and H: drives for proper backup and security. You should never save files on your C: drive.

All confidential waste must be disposed of in locked confidential waste bins to protect the security of information until it is destroyed. Confidential waste isn't just paper, it's any material that has confidential information on it.

Some examples of non-paper items that should be disposed of in special confidential waste bins:

- Patient wristbands
- Labeled IV bags
- Diskettes
- CDs & DVDs

Your Responsibilities

Safeguarding private information is everyone's responsibility. If you have access to member, patient or personal information in any format, you are responsible for keeping it **safe** and **confidential**.

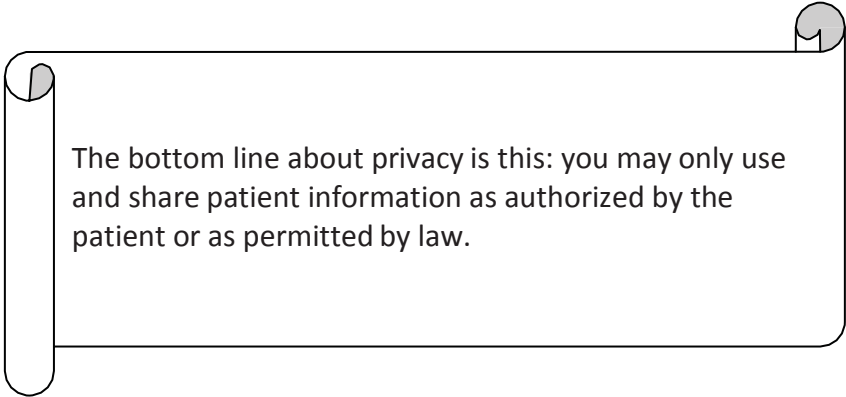
This means you need to know what kind of information disclosure is allowed and what isn't. You need to remember what precautions to take when handling and sharing information.

Member and patient information should be accessed only when it is needed to provide care or conduct Group Health business. You need to think about how your actions protect or violate the privacy of patients and the confidentiality of patient information.

You can't take back a mistake. Mistakes may result in harm to Group Health patients and even lawsuits and government fines.

Failure of any individual to consistently comply with Group Health privacy & security policies puts us at risk for loss of:

- patient **trust**
- **reputation** within the community
- **accreditation**

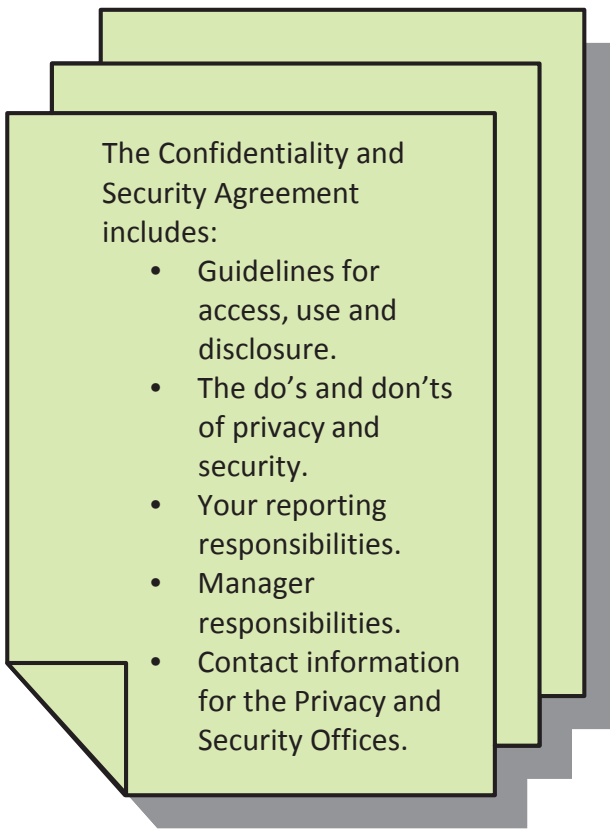


The bottom line about privacy is this: you may only use and share patient information as authorized by the patient or as permitted by law.

Privacy and Security

Did you know you may be violating Group Health confidentiality and security policies when you:

- Allow a patient to review his or her medical record without supervision.
- Leave a cart containing paper medical records or films unattended outside a secure business area.
- Read the medical record of a friend, acquaintance, or co-worker who is a patient when you aren't involved in their care.
- Leave consumer cards, films, or other patient information where an unauthorized person may see or take them.
- Walk away from your desk and leave a provider schedule face up on your workstation counter.
- Fail to use a fax cover sheet when faxing patient information.



The Confidentiality and Security Agreement includes:

- Guidelines for access, use and disclosure.
- The do's and don'ts of privacy and security.
- Your reporting responsibilities.
- Manager responsibilities.
- Contact information for the Privacy and Security Offices.

Confidentiality and Security Agreement

Each year you will sign a Confidentiality and Security Agreement. The agreement is a reminder of your responsibilities and your agreement to protect the privacy and security of member and patient information.

Manager Responsibility

Managers are responsible for ensuring employees have taken all required training.

Managers also need to be able to answer staff questions and ensure their staff have all the resources they need to fulfill their privacy and security responsibilities.

You may have specific training procedures within your work area relating to privacy and security – ask your manager.

The Three R's

Group Health staff are required to:


Recognize risks to the privacy and security of Group Health data.
Part of protecting our members and patients privacy is being able to recognize privacy and security opportunities. If you see a chart left out in the waiting room, pick it up. Make sure you keep your voice low when speaking to patients in a common area and if the confidential waste bin is overflowing, make sure it gets emptied.
Everyone must play a part in recognizing privacy issues and taking care of them right away.

Report suspected risks or breaches of privacy and security.		
As a Group Health staff member, you are required to report any suspected risks or breaches in privacy and security. If you feel there are privacy violations that need to be addressed, contact:		
<table border="1"><tbody><tr><td>Group Health Privacy Office 206-448-2422 (CDS 320-2422) privacy.office@ghc</td><td>Group Health Info Security Office 206-901-6789 (CDS 600-6789) dsec@ghc.org</td></tr></tbody></table>	Group Health Privacy Office 206-448-2422 (CDS 320-2422) privacy.office@ghc	Group Health Info Security Office 206-901-6789 (CDS 600-6789) dsec@ghc.org
Group Health Privacy Office 206-448-2422 (CDS 320-2422) privacy.office@ghc	Group Health Info Security Office 206-901-6789 (CDS 600-6789) dsec@ghc.org	

Reduce those risks.
You must actively work to reduce risk. Everyone has the opportunity to contribute to privacy and security.
Look at your business practices, make sure you are aware of the risks in your work area and have taken steps to reduce them.

Quiz Questions

1. Alison received an e-mail from an employer group which contains a member's consumer number, social security number and date of birth. She needs to reply back to this e-mail, what should Alison do before she sends her reply?
 - A. Encrypt her response.
 - B. Remove the confidential information from the e-mail.
 - C. Confirm she hasn't added any new confidential information.
 - D. Either A or B is correct.
2. Becky works in the maternity ward. She is walking out to her car at the end of her shift and sees Brad Pitt being wheeled into the ER. She is really curious to know why he's there and she knows that his personal business is always in the news anyway. Is Becky allowed to peek in his medical record?
 - A. Yes, movie stars shouldn't expect the same level of privacy as other people.
 - B. No, Becky shouldn't look in the medical record unless she's involved in his care, regardless of whether he is famous or not.
3. You are working at your desk and need to make a quick trip to the copier. Is there anything you need to do to your computer before you leave your desk?
 - A. Yes, put a post-it over any confidential information on my screen.
 - B. Yes, secure or lock my computer.
 - C. Yes, turn the monitor off.
 - D. No, there is nothing I need to do if I'm only running to the copier.
4. Group Health has privacy and security policies because they:
 - A. Help protect the privacy and security of member information.
 - B. Fulfill legal requirements.
 - C. Help staff to know what is required of them.
 - D. All of the above.
5. When a doctor is emailing, what type of messaging should be used?
 - A. MyGroupHealth Secure Messaging.
 - B. Staff Messaging through Epic.
 - C. Outlook e-mail.
 - D. A personal e-mail.
6. If you have access to Epic, are you allowed to use your employee access to view your own medical record?
 - A. Yes, it's your medical information; you can look at it when you want.
 - B. No, you are not allowed to use your employee access to look at your own medical record.

-
7. You need to dispose of patient labels; they have a patient's name and consumer number printed on them. Where should they be disposed of?
 - A. In the locked paper confidential waste bin.
 - B. In the garbage.
 - C. In the special confidential waste bin for non  paper
 - D. In the recycling bin with all the other plastic recyclables.

 8. A 14 year old patient comes in for a pregnancy test. The patient's mother calls the clinic, she didn't know her daughter was going in for care and wants information about why her child is there. Can you tell the mother why the patient is being seen?
 - A. Yes, the patient is still a child and the mother has the right to know.
 - B. No, 14 year olds have the right to choose if reproductive information is shared with family.

 9. Why are all employees required to sign the Confidentiality and Security Agreement every year?
 - A. To check if you still work at Group Health.
 - B. No reason, Group Health just likes paperwork.
 - C. To remind every one of what their responsibilities are.
 - D. None of the above.

 10. Chris notices his coworker looking at her own medical record in Epic. Is Chris required to report his coworker?
 - A. Yes, as a staff member, Chris is required to report all privacy breaches.
 - B. No, only managers are required to report privacy breaches.

 11. Dana wants to send flowers to her coworker for his birthday. Is Dana allowed to get her coworker's address from a Group Health system?
 - A. Yes, she knows the coworker would like the flowers and wouldn't have a problem with her looking up that information.
 - B. No, Group Health information should only be used for business purposes.

 12. What are some ways you can support password security?
 - A. Choose a password that is hard to guess, one that includes numbers, letters and special characters.
 - B. Never write down your passwords.
 - C. Change your password immediately if you think someone has inappropriately accessed your account.
 - D. All of the above.

For More Information

InContext provides access to resources on privacy and security.

The [Privacy Office](#) is available to answer privacy and confidentiality questions, provide resources, and hear concerns and complaints at (206) 448-2422 (CDS 320-2422), or by email at privacy.office@ghc.org

The [Information Security Office](#) is available to answer questions and take reports about information security concerns and breaches at 206-901-6789 (CDS 600-6789), or by email at dsec@ghc.org



YOU HAVE COMPLETED BASIC TRAINING ON PRIVACY AND SECURITY.



**Privacy Office
Office of Compliance & Ethics**

privacytraining@ghc.org



GroupHealth.

***PLEASE ATTACH YOUR LETTER OF GOOD STANDING FROM ACADEMIC AFFAIRS AND VERIFICATION OF MALPRACTICE AND BRING THESE FORMS ON YOUR FIRST DAY OF THE CLERKSHIP**



OVERLAKE Hospital Medical Center

Medical excellence every day™

1035 116th Ave NE
Bellevue, WA 98004
(425) 688-5000
www.overlakehospital.org

MEDICAL SCHOOL STUDENT SPECIAL PRIVILEGES

NAME: _____ DATE: _____

PHONE: _____ DOB: _____

SS#: _____

MEDICAL SCHOOL/PROGRAM: _____

YEAR: _____

Student is in good standing per Medical School:

ANTICIPATED DURATION OF SPECIAL PRIVILEGES: _____

SCOPE OF ACTIVITIES: _____

I _____ agree to assume responsibility for any care or treatment provided by this student at Overlake Hospital Medical Center. I agree that the student will not engage in any patient care, treatment, or activity which exceeds the student's educational background, knowledge, training, experience, or legal capability.

Physician's Signature

Date