



Confidentiality and Security Agreement

Confidentiality and security of patient information are part of providing the best possible care. All Group Health Cooperative patients, including co-workers, have a legal right to privacy. Each of us, including employees, practitioners, contractors, consultants, vendors, students, volunteers, and temporary employees, has legal and ethical obligations to protect confidential information about Group Health patients. Patient information is confidential regardless of the source or form, including paper, computer, and speech.

- I know that I:
 - ✓ May see or hear confidential information about patients and their families, such as medical records, finances, billing accounts, claims data, and conversations.
 - ✓ Will be granted access to Group Health patient information only if I need it to do my job.
 - ✓ Am authorized to access only the patient information I need to do my job.
 - ✓ May only access my own health information through my practitioner, care team, clinic business office/medical records department, or MyGroupHealth, as other patients do.
 - ✓ May only access the records of my family if I have a legal right to do so and only if I go through the practitioner, care team, clinic business office/medical records department or MyGroupHealth, as other patients do.
 - ✓ Must follow department or Group Health **ConWaste** procedures about disposal of confidential information.

- I will not:
 - ✓ Look at, talk about, show, copy, or otherwise disclose any confidential information unless it is my job to do so.
 - ✓ Change, delete, destroy, or throw away any confidential information unless it is my job to do so.
 - ✓ Discuss confidential information outside Group Health or in public places such as elevators, hallways, and open work areas, where it might be overheard by unauthorized individuals.
 - ✓ Use my employee information access privilege to view information about myself, my children, family, friends, or co-workers.
 - ✓ Reveal confidential information even when I am no longer a part of Group Health.

- I am responsible for protecting confidential information, so I will:
 - ✓ Keep my userID and passwords secret, change them often, and not share them with anyone.
 - ✓ Use only my own password to access Group Health computer applications and information.
 - ✓ Protect my computer applications from unauthorized access by logging off, locking my workstation, or by other secure means.
 - ✓ Observe all confidentiality and security requirements when using Group Health Remote/Web Access.
 - ✓ Inform my manager or Information Security if I feel someone else knows or uses my password.
 - ✓ Inform my manager or Information Security of any observed or suspected activities that may lead to a violation of confidentiality or security.

I understand that failure to comply with this agreement may result in disciplinary action that may include termination of my employment, contract or right to practice in a Group Health facility, and/or civil and criminal penalties including fines and imprisonment as prescribed by state and federal laws. By signing this agreement, I acknowledge that I have read, understand, and will comply with it.

Signature _____ Date _____

Print Last/First Name _____ MailStop _____

Employee # _____ Dept/Vendor _____

Responsible Manager Name _____ MailStop _____

QUESTIONS AND ANSWERS

- Q** How do I get help with access questions?
- ✓ Obtain Group Health information systems access for new, and/or existing employees?
 - ✓ Inform Group Health about a transferring employee so that key card access, information systems access, and voicemail follow the employee to the new location and/or job role?
 - ✓ Inform Group Health about a terminated employee to ensure key card access, information systems access, and voicemail are removed?
- A** See InContext ISD Customer Service, Access and Termination
- Q** How do I report privacy, confidentiality, and security incidents and violations?
- A** For privacy concerns, call Privacy Office at 206-448-2422 (8-620-2422) or e-mail Privacy, Office. For security concerns such as inappropriate password use, call Information Security at 206-901-6020 (8-600-6020), Option 2 or e-mail Information, Security.
OR see InContext Privacy, Confidentiality and Security page: <http://incontext/Confidentiality>, Select Reporting a Privacy Concern or the Information Security link.
- Q** How do I access health information or account information about myself or about family members to which I have a legal right?
- A** Contact your practitioner, care team, or your clinic business office/medical records department or access MyGroupHealth. For copies of medical records, your clinic business office/medical records department will facilitate that for you.
- Q** How do I access Group Health Privacy, Confidentiality, and Security resources, tools, and policies?
- A** See InContext Privacy, Confidentiality, and Security Resource Page at: <http://incontext.ghc.org/privacy/privacyhomepage.html>

SOME EXAMPLES OF VIOLATIONS OF CONFIDENTIALITY AND SECURITY:

Accessing information you do not need to know to do your job:

- ✓ Looking up health or account information about yourself, your children, family, friends, or co-workers.
- ✓ Reading a patient's chart when you are not involved in care, or provision of other services.
- ✓ Looking up the phone number, birthday, marital status, or address of a co-worker for any purpose.
- ✓ Using your UserID and password to make appointments for yourself or family members.

Telling, showing, or giving confidential information when it is not your job to do so:

- ✓ Copying parts of a celebrity's medical record to show friends or sell to a publisher.
- ✓ Looking up laboratory results for a neighbor as a favor.

Poor verbal communication practices:

- ✓ Discussing confidential information in a hall, waiting room, or elevator so that unauthorized individuals may overhear or as casual conversation, such as in a restaurant or at social events.
- ✓ Allowing unauthorized individuals to overhear confidential information when talking on a telephone or cell phone.

Not protecting userID and password:

- ✓ Telling a co-worker your password so they can access your work.
- ✓ Telling anyone your password so that they can access information.
- ✓ Obtaining a co-worker's password to access Group Health information.

Not protecting the security of computer-based information:

- ✓ Not logging off a secure application or locking your office door when leaving your computer.
- ✓ Allowing a co-worker to access information using your password.
- ✓ Having your computer screen turned so an unauthorized person may freely see information.

Handling confidential information carelessly or inappropriately:

- ✓ Allowing a patient to handle or review his/her medical record without supervision.
- ✓ Allowing other unauthorized individuals to handle or review a patient's medical record.
- ✓ Throwing labels, labs, or patient records containing patient information in the trash.
- ✓ Leaving a cart containing medical records unattended outside a secure business area.
- ✓ Leaving confidential information in open areas such as counters, mailboxes, conference rooms.
- ✓ Placing consumer cards or labeled information where an unauthorized person may see or take them.
- ✓ Faxing material without double-checking the phone number or without knowing the receiving machine is attended or secure.

Accessing information for unethical purposes:

- ✓ Entering referrals for oneself.
- ✓ Creating covered family members.
- ✓ Initiating coverage that does not exist.
- ✓ Accessing and/or manipulating information to avoid payment