



## Confidentiality and Security Agreement

This agreement applies to all Group Health Cooperative, Group Health Options, Incorporated, and Group Health Permanente workforce members including employees, practitioners, interns, agency personnel, visiting professionals, invited guests, contractors, consultants, vendors, students, volunteers, and temporary employees regardless of the nature of their affiliation with these entities.

I have read and understand **BOTH PAGES** of this agreement and hereby agree to the stipulations below. I know that this signed agreement becomes part of my permanent employment or volunteer record. A copy of this agreement has been made available to me. I acknowledge this agreement is a condition of my employment or association with Group Health and my obligations as outlined in this agreement continue after the termination of my employment or affiliation.

Signature \_\_\_\_\_ Date \_\_\_\_\_

Print Last/First Name \_\_\_\_\_ Employee # \_\_\_\_\_  
(if GHC Employee)

Dept/Vendor \_\_\_\_\_

Manager Last/First Name \_\_\_\_\_

### OWNERSHIP OF INFORMATION AND INFORMATION SYSTEMS

- I understand that information regarding the business and operations of Group Health is owned by and belongs to Group Health, which may audit, investigate, monitor, access, and disclose information related to my use of its information and information systems at any time.
- I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with Group Health.
- I will access or use only information systems or devices I am officially authorized to access.
- I agree to complete all privacy, confidentiality, and security training required by Group Health.

### AUTHORIZATION TO ACCESS, CREATE, USE, AND DISCLOSE INFORMATION

- I am authorized to access, create, use, and disclose only patient, member, consumer, and/or business information required to perform my job.
- I will not use my employee information access privilege to view healthcare, plan or other information about my children, family, friends, co-workers or others for personal purposes but only for legitimate business purposes as required by my job responsibilities.
- I will access my own health or health plan information, and other business information or that of family or others for whom I may legally access information according to established processes and channels for member access to information, such as through the clinic business/medical records office, practitioner, care team, Customer Service, and MyGroupHealth.

### VIOLATION OF AGREEMENT

- I understand that my failure to comply with any part of this agreement may result in disciplinary action that could include termination of my employment, contract, or right to practice in a Group Health facility.

### MANAGER RESPONSIBILITIES

- Managers are responsible and accountable for workforce compliance with all Group Health privacy, confidentiality, and security policies and procedures.
- Individuals responsible for contracts with agencies, vendors, business associates, and contractors are required to provide protection for the confidentiality and security of Group Health information through contractual and business associate agreements.

**READ THE REMAINDER OF AGREEMENT ON REVERSE SIDE OF DOCUMENT**

## CONFIDENTIALITY

- I understand that in the course of my work, I may see or hear confidential information about Group Health patients, members, and consumers 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, and consumer 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 (talk about, show, print, copy, transmit, provide access) patient, member, consumer, or business information only when it is my responsibility to do so and will disclose such information only to individuals with a legitimate business need to know it.
- I will not discuss confidential information about members, patients, or consumers with unauthorized individuals nor will I have conversations in public areas of Group Health such as elevators, hallways, and open work areas in a manner so that unauthorized individuals may hear.
- I understand that law specially protects any and all references to patient HIV testing, including any test for HIV or consideration of a test, and unauthorized release of such information will may make me subject to legal and/or disciplinary action.
- I understand that laws specifically protect mental health and substance abuse health information and that unauthorized disclosure of such information may make me subject to legal and/or disciplinary action.

## SECURITY

- I will protect the security and integrity of health care and business information from loss, misuse, falsification, and unauthorized access, disclosure, modification, or destruction.
- I will observe all user security requirements such as logging off, locking my workstation, and positioning screens away from public view when accessing and using Group Health information and information systems, including Remote Access.
- I will keep my passwords secret, change them often, and not share them with anyone. I will use only my own userID and passwords to access Group Health computer applications and information.
- If I use a mobile electronic device such as a personal digital assistant or laptop computer to store patient information, I will provide security protection for that information and ensure that my supervisor knows of and has approved such use.
- I will observe Group Health security procedures when transmitting confidential information, such as faxing, encrypted e-mail over the Internet, secure messaging, staff messaging, and secure file transfer.
- I will print information from information systems only when necessary for a legitimate purpose with the knowledge that I am accountable for the security of this information.
- I will not create fictitious patients and related information outside required Group Health procedure and standards.
- If, as part of my responsibility, I must take any confidential information off the premises, I will do so only with permission from my manager and will protect it from unauthorized disclosure.
- I will follow Group Health **ConWaste** and departmental procedures for secure disposal of confidential information.

## REFERENCES, RESOURCES, INCIDENT REPORTING

- Privacy, confidentiality, and security resources and references are available on InContext.
- 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 Information Security at 206-901-6020 (8-600-6020), Option 2 or e-mail Information Security within the same business day of any observed or suspected security violations including compromised passwords, or inappropriate access or security practices.
- I will inform my manager and/or Privacy Office at 206-448-2422 (8-620-2422) or e-mail Privacy Office within the same business day of any actual or suspected inappropriate use, access, or disclosure of confidential information, whether by me or another individual, whether intentional or accidental.