GroupHealth

Privacy, Confidentiality and Security Fact Sheet

Handling Confidential Information I

Conversations

- Don't talk to patients or about patients where unauthorized people can hear.
- Never discuss confidential patient information with anyone without a business need or right to know.

Phones

- Hardwired telephones are secure but don't let people overhear confidential information.
- Most cellular phones are secure. Some revert to analog sometimes; know if yours does.
- Cordless phones transmit via radio broadcast and may not be secure.
- Call IT Help Desk for advice on telephones.

Voicemail

- Never leave confidential info on a voicemail unless you have the patient's permission.
- When retrieving messages, don't use your speakerphone and delete messages when finished.

Text & Digital Pagers

- Text pagers are susceptible to "eavesdropping."
- Do not use pagers to transmit patient information.

Use and Disclosure of Patient Information

- GHC/GHP staff are authorized to access and disclose patient information only for legitimate business needs.
- Use & disclosure of patient information must be limited to the minimum necessary to accomplish the purpose, except to support treatment.
- Mental health & substance abuse (from 13 yrs+), STDs & HIV/AIDS (from 14 yrs+), & reproductive care for minors (from 14 yr+) are specially protected. See GHC operational policies on the Group Health Intranet.
- When in doubt about appropriate use or disclosure, ask first. Wrongful disclosure cannot be undone.
- Patient authorized release of information is performed by the Centralized Release of Information Unit located at Capitol Hill (CSB) or Spokane (CSO) Campus.
- Patient access to medical records is facilitated by the Centralized Release of Information Unit and at times by the clinic business offices, including arranging record review with providers.
- Authenticated patients may access portions of their records via MyGroupHealth at www.ghc.org
- Patients are informed of their rights and how to complain about misuse of their information by Group Health staff in the Group Health Notice of privacy practices.

Handling Confidential Information II

Electronic Messaging

- Federal law prohibits e-mailing patient-identifiable information over Internet without encryption.
- Limit patient identifiers in e-mail to CSR# and initials.
- Use Epic Staff Messaging and MyGroupHealth Secure Messaging as appropriate
- See Electronic Messaging policy F-08-503 for more guidance.

Paper Documents

- Keep confidential documents secure; never leave unattended or accessible by unauthorized people.
- Check patient name on After Visit Summaries for the correct patient before distributing to the patient.
- Use ***ConWaste*** bins for confidential waste disposal.

Copy/Scan/Print/Fax Machines

- Never leave PHI on unsecured machines.
- Use Private Print to protect PHI.
- Verify the target fax number carefully before sending.
- When faxing patient information, send only minimum necessary except to support treatment in emergency.
- Use a completed GHC Fax Coversheet every time.
- Use CDS number for internal faxing.
- GHC e-mail PHI rules apply to scan/e-mail functions.

Using Computers Responsibly

- NEVER share your password(s) with anyone else.
- You are responsible for all access & actions under your UserID and passwords.
- Lock up (Ctrl-Alt-Del) your workstation or log off when leaving your work area.
- Secure your Epic screen.
- Position your screen so unauthorized individuals cannot see information. Consider privacy screens for any area where individuals may see screen.
- Observe all GHC confidentiality & security policies & procedures when using laptops, portable devices or Remote Access.
- You may not remove patient information from GHC premises, transmit to, or store it on home computers.

Business Access vs. Personal Access

- You are authorized to use your access to patient information only for legitimate business purposes.
- You do not have the right to use your business access to look up your PHI, or that of family, friends or co-workers.
- Do not use your employment status to ask co-workers to look up information about you, family or friends, or other co-workers.
- Access your PHI or that of others to which you have a legal right only as other patients do.

GroupHealth

Privacy, Confidentiality and Security Fact Sheet

Member/Patient Rights

Federal/state laws provide members/patients the right:

- To privacy.
- To see the GHC Notice of Privacy Practices.
- To authorize use and disclosure of their patient information not otherwise permitted by law.
- To supervised access to their medical records in Business Office/Medical Records & to explanation of records by their providers.
- To request correction or amendment of records.
- To an accounting of disclosures of their health information provided by GHC Privacy Office.
- To request restriction of use and disclosure of their health information through GHC Privacy Office.
- Hospital Directory listing is addressed during admitting process.
- To file a complaint about violations of privacy rights, policies and law with Customer Service, Privacy Office, or the U.S. Office for Civil Rights.

Patient privacy must never be compromised for the sake of expediency.

HIPAA & You

- HIPAA is a federal law that protects patient privacy and places responsibility for confidentiality and security on all GHC/GHP staff.
- GHC/GHP staff are legally required to protect confidentiality and security of patient information.
- HIPAA establishes civil and criminal fines and penalties for violation of patient privacy.
- GHC/GHP staff are required to complete HIPAA privacy and confidentiality/security training.
- Contracts involving use and disclosure of patient information must include GHC business associate agreement language. Managers need to consult with Purchasing Material Management when hiring a vendor to perform services on behalf of GHC.
- Member/patient complaints about privacy may be directed to Customer Service or Privacy Office.
- PHI = Protected health information.

GHC/GHP Staff Obligations

- Staff members are required to protect and preserve member/patient privacy, use and disclose patient information only as authorized, and adhere to all confidentiality and security policies/procedures.
- Managers assure confidentiality & security agreements reviewed/signed annually, arrange for Privacy/HIPAA training, monitor compliance with C&S policies, take timely, consistent action in reporting and responding to incidents and violations.
- Staff are required to report privacy complaints and confidentiality and security incidents/violations. Reporting supports improvement of practices and procedure to preserve patient privacy.
- Confirmed violation of C&S policies/procedures will result in disciplinary action, and may result in civil and criminal fines/penalties.
- Business offices and Centralized Release of Information Units respond to requests for release of information, and patient requested record access, amendment or correction.
- Privacy Office responds to requests for patient accounting of disclosures.

Privacy, Confidentiality, & Security Resources

Privacy Office: privacy.office@ghc.org
206-448-2422 (8-320-2422)

Enterprise Security Assurance: dsec@ghc.org
206-901-6020 (8-600-6020) Select Option 2

For online resources, go to:
http://incontext.ghc.org/privacy/index.html
http://incontext.ghc.org/security/index.shtml
and save it to your Favorites.

Privacy Office

Tools: **C**onfidentiality & security agreement, Privacy training, Privacy incident & complaint reporting, Notice of Privacy Practices
Reference: Confidentiality & security policies, Business associate agreements, Privacy compliance resources
Training: New hire and annual privacy compliance training, Consulting on privacy issues, Privacy awareness and guidance

Information Security Office

Access: Initiate/modify/terminate GHC Systems access, portable devices, remote access
Incident reporting: Report security breaches
Forms: Access, name change,
Resources: Encryption, virus information, Data custodians, Security reviews and risk assessments
FAQs: Answers to common questions