



Privacy, Confidentiality and Security Fact Sheet

Handling Confidential Information I

Paper Documents

- Keep confidential documents secured; never leave unattended or accessible by unauthorized people.
- Keep medical records, TRFs, schedules face down and out of reach of unauthorized people when not in use.
- Don't let patient information remain on faxes or printers unsecured.
- Use **ConWaste** guidelines for waste disposal.

Conversations

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

Phones

- Telephones are secure but don't let people overhear confidential information.
- Most digital phones are secure. Some revert to analog sometimes; know if yours does.
- Cordless phones transmit via radio broadcast and may not be secure. Call Info Security for advice.

Text & Digital Pagers

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

Use and Disclosure of Patient Information

- Users of GHC information & systems 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 of 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 policies, Release of Info Manual, Use & Disclosure on InContext.
- Legally mandatory reporting of patient information is documented in the medical record.
- When in doubt about appropriate use or disclosure, ask first. Wrongful disclosure cannot be undone.
- Patient authorized release of information is performed by Business Office/Medical Records.
- Patient access to medical records is facilitated by MyGroupHealth or GHC Business Offices/Medical Records.
- Members/patients are informed how to complain about misuse of their patient information by GHC/GHP staff.

Handling Confidential Information II

Voicemail

- Never leave confidential info on a voicemail unless you have the patient's permission.
- Other people may have access to the voicemail.
- When retrieving messages, don't use the phone's speaker and delete messages when finished.

Fax Machines

- When disclosing patient information, send only minimum necessary except to support treatment in emergency.
- Verify the fax number carefully before sending.
- Use a completed GHC Fax Coversheet every time.
- Use CDS number if available for internal faxing.

Email

- Messages sent outside GHC's network are not secure; Send only CSR# and initials or patient information locked in a password protected attachment document.
- Messages within GHC network are secure if not forwarded outside.
- Avoid placing patient names in subject line.

Questions to Privacy Office or Information Security

Using Computers Responsibly

- Never share your password(s) with anyone else.
- You are responsible for all access & actions under your userID and password.
- Log off or lock up (Ctrl-Alt-Del) your workstation when leaving your work area.
- Position your screen so unauthorized individuals cannot see information.
- You are authorized to use your access to patient information only for legitimate business purposes.
- Access your personal information or that of others you have a legal right to only as other patients do.
- You may not remove patient information from GHC premises, transmit to, or store it on home computers.
- Patient info stored on laptops or personal digital assts (PDAs) must be password protected and authorized. For information, call Info Security.
- Observe all GHC confidentiality & security policies & procedures when using Remote/Web Access.



Privacy, Confidentiality and Security Fact Sheet

<p style="text-align: center;">GHC/GHP Staff Obligations</p> <ul style="list-style-type: none"> • GHC/GHP staff is required to protect and preserve member/patient privacy, use and disclose patient information only as authorized, and adhere to all GHC confidentiality and security policies/procedures. http://incontext.ghc.org/about/org-pol/oppolhome.html • Managers obtain signed confidentiality & security agreements, arrange for Privacy/HIPAA training, monitor compliance with all C&S policies, take timely, consistent action in response to violations. • Business Office/Medical Records responds to requests for release of information, access to records, amendment or correction, accounting for disclosures. • Confirmed violation of C&S policies/procedures will result in disciplinary action, and may result in civil and criminal fines/penalties. 	<p style="text-align: center;">HIPAA & You</p> <ul style="list-style-type: none"> • HIPAA is a federal law that protects patient privacy and places responsibility for confidentiality and security on GHC/GHP staff. • HIPAA establishes civil and criminal fines and penalties for violation of patient privacy. • GHC/GHP staff is required to complete HIPAA training. • Contracts involving use and disclosure of patient information must include GHC business associate agreement language; managers may consult Materiel Mgmt, ISD Finance/Info Security, Privacy Office, Legal Dept as appropriate. • Member/patient complaints about privacy are directed to GHC Customer Service. • PHI = Patient-identifiable health information
<p style="text-align: center;">Member/Patient Rights</p> <ul style="list-style-type: none"> • Members/patients have the right to privacy. • They have the right to see the GHC Notice of Privacy Practices. • They have the right to authorize use and disclosure of their patient information not otherwise permitted by state & federal law. • They have the right to supervised access to their medical records in Business Office/Medical Records & to explanation of records by their providers. • They have the right to request correction or amendment of their medical records. • They have the right to an accounting of disclosures of their health information provided by Business Office /Medical Records. • They have the right to request restriction of use and disclosure of their health information through GHC Privacy Office. Hospital Directory listing is addressed during admitting process. • They have the right to file a complaint about violations of privacy, rights, GHC policies, and law with Customer Service, Privacy Office, or the U.S Office of Civil Rights. <p style="text-align: center;">Patient privacy must never be compromised for the sake of expediency.</p>	<p style="text-align: center;">Privacy, Confidentiality, & Security Resources</p> <p>Privacy Office: privacy.office@ghc.org 206-448-2422 (8-320-2422)</p> <p>Info Security: information.security@ghc.org 206-901-6020 (8-600-6020) Select Option 2</p> <p style="text-align: center;">For online resources, go to http://incontext.ghc.org/him/privacy/index.html and save it to your Favorites.</p> <p>Tools:</p> <ul style="list-style-type: none"> • GHC Confidentiality & Security Agreement • Vendor/Consultant Non-disclosure Agreement • Authorizations for Release of Information • GHC Fax Coversheet <p>Reference:</p> <ul style="list-style-type: none"> • <i>Practical Guide to Confidentiality & Security</i> • GHC Release of Healthcare Information Manual • ConWaste Guidelines Chart & Program • GHC Confidentiality & Security Policies • Signing Contracts Involving Patient Information • HIPAA Resources <p>Access & Information Security:</p> <ul style="list-style-type: none"> • Initiate/Change/Terminate GHC Systems Access • Incident Reporting for Conf/Security Breaches <p>Training:</p> <ul style="list-style-type: none"> • Request Confidentiality & Security Training • GHC Online Privacy training available