



CHFC Policy Number POL-3

SECURITY AND CONFIDENTIALITY OF PATIENT HEALTH INFORMATION POLICY

Date: May 5, 2004

1. Background

CHFC is responsible for instituting reasonable safeguards to protect the confidentiality and security of its patient health information.

2. Policy

CHFC will endeavor to protect the confidentiality and security of its patient health information against inappropriate access, inappropriate use, tampering, loss/destruction and inappropriate disclosure through the use of reasonable safeguards.

Reasonable safeguards include properly selected equipment/software, procedures guiding the access, use, maintenance and disclosure of its patient health information, education and training, system measures, contractual requirements imposed upon individuals and entities who are authorized to access its patient health information and sanctions for noncompliance.

3. Purpose

The purpose of this policy is to set forth the general principles and procedures for maintaining the confidentiality and security of CHFC's patient health information.

4. Definitions

- 4.1 **Patient Health Information:** Information that is (i) created or received by CHFC; (ii) relates to past present or future physical or mental health or condition of a CHFC patient or the provision of health care to a CHFC patient; and (iii) identifies the CHFC patient or can be used to identify the CHFC patient.
- 4.2 **Medical Record:** Any paper or electronic record, file, document or other written material relating to a CHFC's patient's medical history, diagnosis, condition, treatment or evaluation.
- 4.3 **Sensitive Information:** Patient Health Information that requires heightened confidentiality, such as alcohol/drug abuse, mental health, HIV/AIDS. State and federal laws specially protect this type of information.
- 4.4 **User:** Any person issued a logon password to the CHFC computer system that uses the computer system to input Patient Health Information or use Patient Health Information from reports.

5. Procedures

- 5.1 Every individual and entity allowed access to Patient Health Information shall maintain the confidentiality and security of such information in accordance with this policy, their contractual obligations (if any) and applicable law.

- 5.1.1** This obligation begins at the time of initial access to Patient Health Information, continues during such ongoing access and use of all such information and continues even after the individual's or entity's affiliation with CHFC ceases.
 - 5.1.2** Failure to maintain the confidentiality and/or security of Patient Health Information will result in sanctions against the violator, which may include termination of the violator's affiliation with CHFC.
- 5.2** Internal access to and usage of Patient Health Information shall be limited to those individuals and entities entitled to access and use such information on the basis of their specific patient care and administrative functions.
 - 5.2.1** Employee and volunteer job descriptions shall identify the scope of access to and usage of Patient Health Information authorized for the position.
 - 5.2.2** Contracts shall identify the scope of access to and usage of Patient Health Information authorized for the contracting entity or individual.
 - 5.2.3** Heightened confidentiality shall be maintained for Sensitive Information. Internal access to and usage of all Sensitive Information shall be restricted to those persons who have a need to know the information for the purpose of providing care to the patient.
- 5.3** Patient Health Information, whether on paper, PC terminals, facsimile machines, printers or any other source, shall be kept in secure areas and not left unattended in areas accessible to unauthorized individuals.
- 5.4** Electronic Patient Health Information shall be maintained and protected with the same level of security as a patient's paper Medical Record. Special access and usage policies and procedures for Users will apply, including the following:
 - 5.4.1** The Clinic Director is responsible for providing Users with unique identification and password assignments and authorization to modules or commands to enable Users to access Patient Health Information. The scope of such access shall be based upon position classifications and job requirements.
 - 5.4.2** Users shall sign and comply with the Information Security Agreement.
 - 5.4.3** Users shall comply with the Internet Access/Patient Confidentiality Policy.
- 5.5** Patient Health Information shall not be removed from CHFC premises, unless otherwise authorized by this policy or the Clinic Director.
 - 5.5.1** Medical Records are to remain on CHFC premises at all times.
 - 5.5.2** Any hardware containing Patient Health Information shall be purged before it is removed from use by CHFC.
- 5.6** The integrity of Patient Health Information shall remain intact and tampering with, or the unauthorized destruction or removal of, all or any part of the Medical Record is strictly prohibited.

- 5.7** CHFC shall retain its Medical Records until the patient is 25 years old and 7 years after the last treatment at CHFC. After this time, Medical Records may be destroyed by shredding them (if in paper format) or deleting them (if in electronic format).
- 5.8** Patient Health Information shall be disclosed only in accordance with applicable law.

 - 5.8.1** Patient Health Information may be disclosed to patient or person/entity authorized by the patient upon written request by the patient or the patient's legal representative using a CHFC's authorization to release records form.
 - 5.8.2** Patient Health Information may be disclosed for treatment purposes to health care providers that do not provide services at CHFC subject to obtaining the patient's written authorization to do so.
 - 5.8.3** Patient Health Information may be disclosed pursuant to a valid subpoena or court order only in accordance with applicable law. The Clinic Director, following receipt of legal advice, must authorize all such disclosures.
 - 5.8.4** Sensitive Information may be disclosed only in accordance with applicable law. The Clinic Director, following receipt of legal advice, must authorize all disclosures of Sensitive Information.

