# ELECTRONIC HEALTH RECORDS

| | |
|---|---|
| **Procedure Name:** | ELECTRONIC HEALTH RECORDS (EHR) |
| **Procedure Number:** | 001 |
| **Domain:** | Information Technology |
| **Approved By:** | Rich Petro, HR Director |
| **Created/Written By:** | Rowan McGlasson, Systems Specialist |
| **Effective Date:** | 4/15/20 |
| **Date(s) of Revision:** | |
| **References:** | Electronic Communication Procedure |

## STATEMENT OF PURPOSE

This procedure covers the agency's Electronic Health Record system, including confidentiality of the data as well as use and access of the system.

## AREAS OF RESPONSIBILITY

The Human Resources department and the Systems Specialist is responsible for maintaining and updating the Electronic Health Records procedure.

## PROCEDURE

Family & Children's Center (FCC) recognizes the need to protect the security, confidentiality, integrity and availability of our clients' electronic Protected Health Information (PHI) and to do so in accordance with HIPAA Security Rules and other federal and state regulations. Information used in the course of FCC's business is a vital asset that enhances the agency's continuum of care to clients and requires protection from unauthorized access, modification, disclosure or destruction. This procedure sets forth requirements for incorporation of information security practices into use of FCC systems.

The data stored on the EHR system is the property of FCC, and the EHR system is to be used solely for job-related purposes. All EHR data is confidential and is to be treated as such. The EHR system should be accessed only the minimal amount necessary for the provision of health care services to FCC client(s). Employees are not permitted to access the EHR system for anything other than authorized job-related purposes relating to client treatment, billing or FCC operations. Accordingly, employees are not permitted to access an individual's health

information because of a personal request, personal reasons or personal curiosity. Unauthorized access of the EHR system without the proper security clearance and/or access authorization, for whatever reason, is considered a violation of the agency's Electronic Health Records Procedure. Violations of this Procedure can result in disciplinary action including immediate termination of employment at Family & Children's Center.

Passwords and user identification ("ID") are utilized to access the agency's EHR. Passwords or ID must not be divulged to any other individual or entity. Employees are responsible for ensuring the privacy of PHI displayed on computer screens, including protecting the screen from attempted or accidental exposure to unauthorized users, and will log off the EHR system when stepping away from her or his computer. Employees are responsible for any damages, including monetary damages, for the inappropriate use and/or disclosure of PHI, even if such inappropriate use and/or disclosure was made by another individual, when using another employee's password or ID. Employees who suspect her or his password or ID has been obtained by another individual must immediately change her or his password and inform the System Specialist or HR Director so that appropriate action may be taken.

The EHR system is monitored by the System Specialist, and employees do not have personal privacy rights when using the Electronic Health Records (EHR) system. The EHR system is subject to search, and FCC is able to track and monitor system use, including viewing and modifying client records. Employees are not to use the EHR system for any other purposes such as solicitation for outside business ventures, campaigns, and political or religious causes. Employees are prohibited from storing, displaying, or disseminating obscene, offensive, harassing, or discriminatory textual or graphical materials on the EHR system. The only exception is for scanning into the health record a copy of such data that was created by the client or other person and that is relevant to the client.

Users agree to indemnify, defend and hold harmless, FCC and its affiliates, and their respective members, trustees, officers, directors, employees and agents, from and against any claim, cause of action, liability, damage, cost or expense, including without limitation, reasonable attorneys' fees and costs, arising out of or in connection with any unauthorized or prohibited use or disclosure of PHI, or any other breach of the EHR Procedure.

# ELECTRONIC HEALTH RECORDS

Family & Children's Center

**Confidentiality:** All data contained on the EHR system is confidential and unauthorized disclosure of PHI is strictly prohibited. FCC and the EHR system will provide administrative and IT technical safeguards which are intended to protect the confidentiality, integrity and availability of records received, created and maintained in the EHR system as required by law.

**Access:** Records are accessible to Family & Children's Center (FCC) staff through unique login names and passwords. Based on the program and level of service provided, staff members can be given access to client records as needed. Access is dependent on signed release by client for inter-agency programs.

The EHR system has the capability to grant or deny levels of access as needed. Staff can be given full access to documents and read clinical data for the program(s) which they are assigned. Users will be given access only to the data necessary for them to complete their required tasks. When applicable, read only access can be granted for continuum of care when a client is receiving services through multiple programs at the agency. The Senior HR Specialist will notify the System Specialist when there are changes in employment, including hires, terminations or transfers.

**Data Integrity:** All data in the EHR system is internally time and date stamped at time of creation and last modification, along with the name of the employee who created/modified it, and a snap shot is taken of clinical records, if signed, at the time of signature. Electronic signatures are bound to the electronic content for verification. Data is accessible through web browsers, and no data is held on FCC servers.

**Email:** When necessary for business operations, emails containing PHI may be sent outside the EHR system. With the exception of client initials, all correspondence containing PHI must be encrypted in a password protected ZIP file before emailing. The password should be related verbally (preferred) or in a separate email. Emails where client initials are the only included PHI may be sent to HIPAA-compliant entities without further encryption, though "Client" or other non-identifying terms are to be used wherever possible. To create a ZIP file:

- Open your File Explorer and select the items you want to ZIP. This process will work with a single file, multiple files or a directory.
- Right-click one of the files or folders and go to **7-Zip** then click on **Add to archive**.
- Choose a name for the ZIP file and a new location (if you want). By default, the new ZIP archive will be created in the same folder that its contents were selected from.
- When the ZIP dialog box opens make sure **zip** is chosen in the **Archive format** drop-down menu.
- Enter the password for the ZIP file in the **Encryption** text boxes on the lower right of the dialog box. You will reenter the password in the next box to assure it is correct.
- Finish the ZIP by clicking on **OK** at the bottom of the dialog box.
- The password protected ZIP file can then be emailed like any other attachment.

**Licensing review:** Records for licensing reviews are available at the location the services are being provided. Program Coordinators or other assigned staff members are responsible for facilitating this review. A limited-time password for the visiting auditor must be requested in advance from the System Specialist. The Program Coordinator is responsible for notifying the System Specialist at the conclusion of the review so the password can be disabled.

**Confidential documentation breach:** All users are responsible for immediately reporting any suspected and/or known unauthorized use or disclosure of client data to their supervisor, the System Specialist, or any member of management. In the event of a breach of information FCC will comply with all related state and federal requirements.

**Vendor agreement:** EHR is subject to a licensing agreement with the vendor, Procentive. In the event that either, for whatever reason, terminate this agreement, the data collected in Procentive belongs solely to FCC. In the event of termination a transition plan will be established to cover the transfer of data, including billing information.

## GETTING HELP

Employees with questions regarding the agency's electronic health record system should contact the Systems Specialist at (608) 785-0001 x302 or the Human resources Director at (608) 785-0001 x327.