

FamilyCare Medical Group, P.C. (“FamilyCare” or “practice”) Patient Portal Security

Patient Portal Security Features

- The Patient Portal can be accessed by logging onto the FamilyCare website, www.fcmg.org, and clicking on the “Patient Portal” tab. The web server does not permanently store any Protected Health Information (PHI). The portal communicates with the FamilyCare Electronic Health Record (EHR) database over secure VPN.
- The Patient Portal uses HTTPS when communicating with users' browser which provides encrypted communication and secure identification of the Patient Portal web server.

Account Activation & Secure Login

- In order to activate a portal account and have access to health information, the patient will need to receive an activation code from FamilyCare, the practice. Each patient has his or her own unique activation code randomly generated by the system. The practice is provided with a letter containing the activation code which can be mailed or physically given to the patient during an office visit. The activation code cannot be sent to the patient electronically via email.
- During the activation process, the patient will have to enter personal information and the activation code for identity verification. The patient will then create a unique login name and password. The password is case sensitive and must be at least seven characters long.
- The patient must select and provide answers for three different security questions. These questions are used to verify the patient's identity when logging into a computer the system does not recognize. The patient will also be asked to answer a security question if it has been a week or more since the last login.
- The patient must select a site ID image and create a site ID phrase. This will be presented each time the patient logs in (prior to entering a password), to confirm that the patient is logging into the correct website. This specific security feature protects the patient from phishing websites trying to obtain personal information fraudulently.

Password

- Only the patient has access to his or her password. The practice cannot view this information and therefore cannot accidentally provide login information to a person not authorized by the patient.
- The account cannot be accessed without the password, nor can changes be made to the account profile. In order for a patient to change his or her current password, email address, login name, security questions and answers, or site ID image and phrase, the patient will need to re-enter his or her password once logged in.
- If the patient has forgotten his or her current password, the patient can request a password reset. In order to do so the patient must enter the email address and login name that the practice currently has on file. If these first two fields match what is entered in the practice's EHR system, the patient is then required to answer a security question to further verify his or her identity. The patient must answer the security question, even if using a computer the system recognizes. The temporary password is then sent to the patient's email account.
- The patient's portal account will automatically be frozen after five failed password entries. Each failed attempt is logged in the practice's EHR system and only the practice can unfreeze the portal account.

Login Name

- If the patient has forgotten his or her login name, the patient must submit a form to receive a new activation code from the practice. The form requires the patient to enter his or her personal information and create new login information. In order to login with the new name, the patient must enter the new activation code received from the practice.
- The new activation code is randomly generated and treated with the same security as the initial activation code. The practice gives the patient a new code in the form of a login reset letter, which can either be mailed or physically given to the patient. The code cannot be sent to the patient electronically via email.

Security Questions

- The answers to the patients' security questions are not viewable in the account profile. Like all other areas of the profile, the patient must re-enter his or her password in order to make changes.
- The practice does NOT have access to the patient's security questions and answers. Therefore, the practice cannot accidentally provide login information to a person not authorized by the patient.

Email Address

- PHI is NOT sent to the patient's email address. All messaging and exchange of health information is done through the secure Patient Portal website.
- The patient will receive an email from the practice when there is something new to view on the portal, but to access the information the patient will need to login to his or her portal account.

Session Timeout and Automatic Log Out

- The practice has set a session timeout of minutes. If the patient's portal account has been inactive for the set amount of time, the patient will automatically be logged out.
- The patient is automatically logged out of his or her portal account if the patient logs in from a different computer. Two users cannot be logged into the same portal account from 2 different computers.
- The patient is automatically logged out of his or her account if the patient closes the browser window without manually logging out.