



PROVIDER ALERT



Alert # 16 2007-12-14 HCAL, HCYA, HCBK, HCCH, HCNE, HCCMP, HCNC, WBH, UPMC for Life, UPMC for Kids

Authorization Process Revisions

Effective January 2008, Community Care will revise the process for authorization report mailings. Based on feedback from providers related to mailing time for the weekly reports, we will not be sorting authorization reports by network. This means that providers who have contracts for more than one HealthChoices network will receive a separate authorization mailing each week for each network. Providers who submit Outpatient Registrations either via the web or by teleform should note that the number of units will be designated as one (1) on the report. This indicates a registration that is valid for one year.

Given that this procedural change may have an impact on some providers we would like to inform you that we do have the ability to provide these reports via Electronic Data Interchange (EDI). Since these reports contain protected health information as defined by HIPAA, there is some set-up that is required to assure that we can be compliant with the privacy and security standards.

To set up your process to complete secure EDI with Community Care, we will ask you to review the following External Trading Partner requirements and complete the attached application form. If you have any questions, please contact your Provider Relations Representative who will work with IT to get you an answer as quickly as possible.

Overview:

This External Trading Partner Document defines a standard process that permits companies outside UPMC/Community Care to exchange application data files with UPMC/Community Care. This document is based on the standard defined in the 1.0 release of this UPMC/Community Care Enterprise File Movement Model.

The Enterprise File Movement process is a standard file movement control process for all file movements of application data between UPMC/Community Care trusted computers or external trading partners. This process maintains standards such that all UPMC/Community Care file movements have the same level of security and functionality. The process is designed to be consistent with HIPAA security and privacy mandates.

Enterprise File Movement Process with External Trading Partners

The Enterprise File Movement process has established a server outside the UPMC/Community Care firewall as a drop off location or pick up location for external trading partner files. Any inbound file movement from an external trading partner will be dropped on that server. The process will know that the file has been dropped and will pull the data across the firewall and send the file to the final destination. Likewise any outbound file movement to an external trading partner will be dropped on this server by the Enterprise

File Movement process for pickup by the external trading partner. The external trading partner is expected to move the file from that location to their desired destination. If required, an email will be sent to the external trading partner to note a file has been received or a file is ready for pick-up.

As part of the file movement set-up process, the external trading partner will be given an IP address, user name and password that will allow access to a specific folder on the server outside the UPMC/Community Care firewall. The file movement process is not name oriented and therefore can move any file between the source and destination. A file movement is not bi-directional.

All data files must be encrypted between the UPMC/Community Care firewall and the external trading partner. UPMC/Community Care expects all files to be encrypted with a PGP (RSA algorithm) key. UPMC/Community Care uses GnuPG software for encryption and decryption. This software effectively encrypts and decrypts data and exchanges keys with trading partners using either PGP or GnuPG. The software is available at <http://www.gnupg.org>. The software can be used manually in a desktop environment or in an automated server environment.

Enterprise File Movement Process

All file movements with external trading partners, like any trusted file movement, are subject to a standard set of features. UPMC/Community Care has established a server on the UPMC/Community Care trusted network to control all file movements within the Enterprise File Movement Model. This server represents a controlling “check point” for all included movements between trusted trading partners or trusted and non-trusted trading partners. This server is an intervening step between the source and destination of any file movement. The following features are built into the Enterprise model such that each file passing through the Enterprise server is processed in the same manner.

- All files are archived for 14 days.
- An email error message is generated to note an error in the file movement process.
- An optional email message can be generated to note a file has been moved as planned.
- An optional email message can be generated that notes an anticipated file movement has not been completed because the file was not available.
- An event log is built for each normal or exceptional condition such that support staff can monitor movements.
- A database record is built for each file movement. This database will be the source for as needed file movement history reporting.

Enterprise File Movement (EFM) Request

Company Information:

Company Name:	
Address:	
City, State, Zip:	
Department:	

Which Region(s) are you Contracted with?

Northeast: North Central: Carbon, Monroe, Pike:

Chester: York, Adams, Berks: Allegheny:

Data Steward:

Name:	
Phone Number:	
Email Address:	

Technical Support Contact:

Name:	
Phone Number:	
Email Address:	

Who should receive conformation Emails when files are available?

External IP Address(s) (Please Obtain this from your ISP)

IP Address:	
IP Address:	

Please submit your EFM request to:

Mike Burke, Manager Data Communication Networking
 Community Care
 One Chatham Center
 112 Washington Place
 Pittsburgh, PA 15219