Highmark FTP Communication Standards

The secure transport system utilized by Highmark is maintained on a Secure FTP (SFTP) server. It utilizes 128-bit HTTPS encryption to safeguard data. The secure transport system provides an Internet-accessible SFTP service over an encrypted data session, allowing our business partners to exchange files with Highmark using a simple SFTP process in an encrypted and private manner. The system is a mature file transfer system that was designed to provide you with enterprise-grade security, reliability, scalability, and performance.

Highmark offers the following Internet file transfer options to its business partners:

HTTPS Encryption, or SFTP Using SSH Encryption:

The above solutions can be accessed via standard file transmission clients that can transmit using HTTPS or SCP/SFTP and provide for user ID and password authentication.

Standard SCP or SFTP Clients:

Highmark also has the ability to accept files via a SCP or SFTP client. These are clients that are provided with most Unix systems, and available for free for Windows systems. These clients use the encryption and communications provided by SSH (Secure Shell) software. Each external customer that wishes to use this type of client will be responsible for obtaining and implementing this software from a source with which they feel comfortable.

Software Requirements

As with any SFTP connection, customers will need a third-party transfer application in order to transfer files using the secure transport system. The following two options are available from Highmark:

1. A standard SFTP or Secure Copy Protocol (SCP) client.
2. Any state of the art browser that supports strong encryption (128 bit) and is set to allow cookies for session tracking purposes.

SFTP: Configuration

Business partners will need to configure their third-party transfer application or browser to access either of the following server URLs: **ftp.highmark.com** or **mft.hmhs.com**[1]. These credentials must be supplied to gain access to the secure transport system. SFTP clients should be configured to utilize port 22 for SFTP over SSH.

Additional Capabilities Offering Increased Security:

PGP encryption: If desired, the secure transport system can support PGP encryption. Please note that the transmission of the files must still be done via HTTPS or scp/sftp. In this case, we must provide the Highmark public PGP encryption key to be used to encrypt the file before it is put to the Highmark Secure FTP server and saved with a file extension of .pgp. If a file is received with a file extension of ".pgp," the service will automatically PGP decrypt the file. Customers should contact Highmark EDI Operations at 800-992-0246 to obtain a public PGP encryption key directly from Highmark.
The secure transport system also supports file reception of zipped and compressed files, and virus scans all files that are placed on the Highmark server for protection of internal and external systems.

Firewall Considerations:

Both HTTPS and SSH are implemented by Highmark using the standard port numbers of 443 (HTTPS) and 22 (SSH). Customers must configure their network and firewalls to allow the system exchanging files to communicate with Highmark via one of these two standard methods. Below are the IP addresses that should be opened for traffic. Connections should be made to the hostname, and will resolve to one of our internal servers.

Protocol	Port	Hostname/URL[1]	IP Address
Web Browser - HTTPS	443	https://ftp.highmark.com	157.154.7.34 167.164.7.34
Web Browser - HTTPS	443	https://mft.hmhs.com	157.154.4.135
SFTP Client - SSH	22	ftp.highmark.com	157.154.7.34 167.164.7.34
SFTP Client - SSH	22	mft.hmhs.com	157.154.4.135

[1]As of Oct. 2020, HM Health Solutions is undergoing a migration to new secure transport servers. While both servers are operational, please refer to your prior documentation to identify the appropriate server for your connection.

External Access NOT Supported:

Highmark does **NOT** support the use of the FTP transport protocol. The standard ftp transport protocol does not provide any encryption of session (login and password) or data transmission, and therefore, jeopardizes the integrity of the data on our system.

Highmark does **NOT** support the use of the FTPS transport protocol. Although this software provides encryption of session and data, our firewall will not permit this data to pass over the standard port number. Its use of non-standard ports requires complex firewall rules to be implemented by both parties engaged in the transfer.

Highmark does **NOT** support SSH with key authentication. Our system requires user ID and password authentication. SSH key authentication is not supported.