

Nebraska Hospital Association Nebraska Hospital Information System

NHIS Claims Data Formats

The Nebraska Hospital Information System (NHIS) will continue its strategic role as a data aggregator for the NHA and Nebraska hospitals. The collaboration between NHA, Blue Cross and Blue Shield of Nebraska, and the Nebraska Health and Human Services System allowed for the creation of an effective and efficient process of collecting hospital claims data. The use of DataTrac as a collection tool was the basis for creating the NHIS before the industry's adoption of the HIPAA transaction standards.

Because of changes brought about with HIPAA transactions standards, NHA redesigned the NHIS claims collection process. The new process is a non-proprietary design that will allow a hospital to submit copies of their claims data directly to the NHA. Under this new process, a hospital may use any software or clearinghouse of their choice. To facilitate the direct submission of claims for the NHIS, NHA has implemented two key components. First, NHA licensed a software product to "translate" the claims into a NHIS usable format. Second, a secure transmission process was developed for Internet use. This process uses a secure connection, or "tunnel" to transmit a file from your facility to the NHIS.

To accomplish the claims submission, a hospital will need:

- Ability to produce a claims data file that can be sent to the NHA in
 - HIPAA compliant 837i claims transaction, or
 - flat file extract matching predefined layout.The NHA process is designed around these standard formats. Other formats are possible, but each must be customized and coordinated with NHA. The NHA encourages all facilities to become compliant with the 837i standard.
- Internet access to transmit files. Internet access is through an Internet Service Provider (ISP) over an IP address.
 - A static IP address is preferred, but not necessary.
 - Allow outbound communication through port 22 on the firewall and proxy servers.
- Use remote client software. NHA will supply the software utility to conduct the transmission of claims information over the Internet. If the hospital already uses a similar utility, it may work with the NHA system.

The new process allows for your choice of the following formats to submit your claims data. It is possible to use a combination of the formats;

- Submission of HIPAA 837i compliant transaction directly to the NHA
 - PC-ACE PRO32 claims submission facilitates this format.
- Submission of proprietary flat file directly to the NHA

To process the inbound files, NHA installed Pervasive as a data conversion software. Pervasive can read a compliant 837i (current version 4010A1) and create an extract file for the NHIS. The default inbound claim format is an 837i. Other data formats are possible, but each must be processed uniquely.

Accepted Formats:

HIPAA 837i transaction with clearinghouses or direct submission to payer

The NHA is set to receive copies of HIPAA compliant 837i transactions files as part of the data collection. The 837i files can be created for any clearinghouse. BCBS of Nebraska deploying PC-ACE PRO32 as a claims processing package for their claims. The NHIS claims submission process will work with the PC-ACE software. As part of the PC-ACE process, a copy of the 837i file will be created for the NHA.

If your hospital doesn't elect to use PC-ACE, the NHA can receive your claims data. We ask that the hospital send the NHA a copy of the HIPAA compliant 837i transaction created for the clearinghouse or payer.

The NHA plans on the hospital using Internet data transmission to send the 837i claims data file. Each hospital must have a unique user account supplied by NHA to send claims data over the Internet. There are several utilities the NHA will provide at no cost to allow the transmission over the Internet.

Flat File to NHA

If the hospital is able, they can create a flat file using an NHA pre-defined record layout. The NHA can process this proprietary file structure in place of 837i claims data file. Documentation on the predefined flat file format is available on request. The NHA would prefer daily or weekly submission of flat files. A monthly cycle is the longest we would want you to use.

The hospital needs to contact the NHA when they explore this option. The NHA plans on the hospital using Internet transmission to send the 837i claims data file. Mailing the file on a CD is an option if the hospital is unable to use an Internet connection.

All Claims Data

Part of what makes the NHIS valuable to the Nebraska hospitals, is the ability to process inpatient and outpatient claims data, and "all payers" claims data, including self-pay. Using one or more of the methods outlined above allows your hospital to continue sending claims data to the NHA.

PC-ACE does not have the capability of sending self-pay claims to the NHA. If you are using PC-ACE, you need to send self-pay claims by submitting an 837i directly to the NHA, or using the flat file extract.

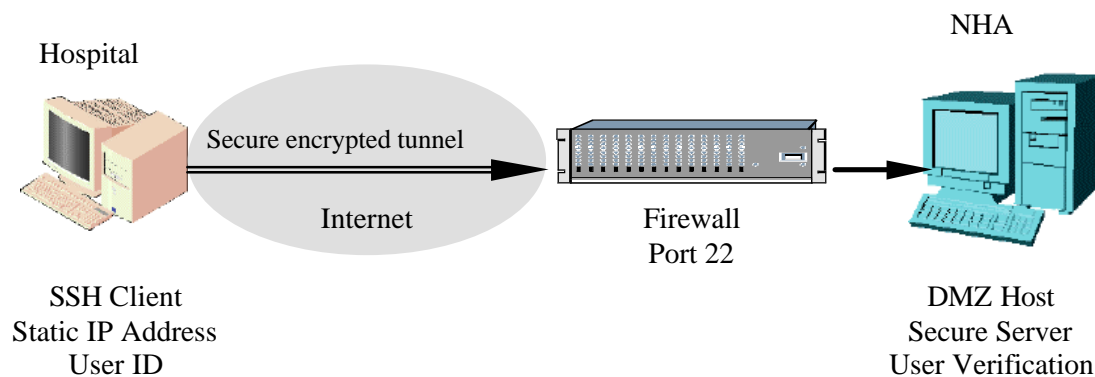
Nebraska Hospital Association Nebraska Hospital Information System

Internet Data Transmission

The Internet data transmission process utilizes a Secure Shell Version 2 (SSH) connection and Secure File Transfer Protocol (SFTP) to transmit claims. The SSH protocol creates a “tunnel” over the Internet for exchange of information encrypting data, user names and passwords. SSH uses port 22 of an IP address. The NHA firewall has been configured to allow inbound files over port 22 from known external IP addresses. Prior to transmitting, NHA will need to verify your IP address and add it to the list of approved addresses.

As an added layer of security, each hospital will be assigned a unique user ID and strong password. The hospital User ID will allow the transmission of files to a secure “DMZ” SFTP server located behind the NHA firewall. After files are received on the NHA server, they will be moved to another protected drive. The combination of SSH, passwords and secure server will meet the HIPAA security requirements.

Secure Data Transmission



Secure Shell File Transfer

A Secure Shell (SSH) connection is one of the safest ways to make specific data available to partners without exposing critical information to the public network. Using SSH on your remote machines effectively restricts access to authorized users and encrypts user names, passwords and files sent to the secure server.

Secure File Transfer Protocol (SFTP) is a subsystem of the Secure Shell protocol. In essence, it is a separate protocol layered over the Secure Shell protocol to handle file transfers. SFTP has several advantages over non-secure FTP. First, SFTP encrypts both the user name/password and the data being transferred. Second, it uses the same port as the Secure Shell server, eliminating the need to open another port on the firewall or router.

The Secure Shell protocol provides four basic security benefits:

User Authentication

Authentication, also referred to as user identity, is the means by which a system verifies that access is only given to intended users and denied to anyone else.

Host Authentication

A host key is used by a server to prove its identity to a client and by a client to verify a “known” host.

Data Encryption

Encryption, sometimes referred to as privacy, means that your data is protected from disclosure to a would-be attacker “sniffing” or *eavesdropping* on the wire.

Data Integrity

Data integrity guarantees that data sent from one end of a transaction arrives unaltered at the other end. SSH uses Message Authentication Code (MAC) algorithms for data integrity checking.

SSH Remote Client

NHA will distribute SSH remote software at no cost for hospitals to use. If your facility is already using a SFTP product, that product may also work with the NHA SFTP server. The SSH remote software (called pspc.exe) is a command line utility that can be part of a batch file, run from a command prompt, or Window shortcut. The pspc.exe software is available for download at various web sites. NHA will include the software on the installation CD.

To automate the process, NHA will also distribute a free utility titled Log Monitor. Log Monitor runs in the background of your Windows computer and waits for a specified file to be created. Once the file is created, Log Monitor can call the SSH program and automate the file transfer. Hospitals would not need to use Log Monitor, but it does automate the process. If desired, the SSH client can be run from an existing hospital process.