Nebraska Hospital Association

Nebraska Hospital Information System

The NHA Nebraska Hospital Information System (NHIS) collects data in a non-proprietary design that allows a hospital choice in how to submit copies of their claims data. Under this process, a hospital may use any software or clearinghouse of their choice. The process allows for the following formats to submit claims data. It is possible to use a combination of the formats.

NHIS Claims Data Formats

The claims data collection process is a non-proprietary design that will allow a hospital to submit copies of their claims data directly to the NHA. 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. The process allows the hospital to choose the above formats to submit your claims data. It is possible to use a combination of the formats but the preferred inbound claim format is an 837i.

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 837i 5010A2 compliant transaction, or
  - File extract matching NHA 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. Allow outbound communication through port 22 on the firewall and proxy servers.

- Use remote client software. NHA will supply software utility to perform the transmission of claims information over the Internet if necessary. If the hospital already uses a similar SSH utility, it may work with the NHA system. The hospital should contact the NHA to verify their process for new submissions or changes.

- If the hospital's clearinghouse partner participates with the NHA, the hospital my elect to have the clearinghouse submit their claims data files to the NHIS on behalf of the hospital.

HIPAA 837i transaction with clearinghouses or direct submission

The NHA is set to receive copies of compliant 837i transactions files as part of the data collection. The 837i files can be created for any clearinghouse. 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.

NHA File Extract

In place of an 837i file and if the hospital is able, they can create a file extract using an NHA pre-defined record layout. The NHA can process this proprietary file structure along with 837i claims data files. Documentation on the predefined flat file format is available on request. The NHA would prefer weekly or monthly submission of 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 claims data file. Mailing the file on a CD or USB is not an option to be compliant with HIPAA breach notification requirements.

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 combination of the methods outlined above allows your hospital to continue sending claims data to the NHA. There is no need for the hospital to select bill types. The NHA accepts all claims data and processes by UB-04 bill type. If you desire to limit bill types, below are the bill types required for complete reporting of patient data:

0111-0118: Hospital Inpatient
0121-0128: Hospital Part B bills
0131-0138: Hospital Outpatient
0141-0148: Hospital Outpatient Special
0831-0838: Ambulatory Surgery
0841-0848: Free Standing Birthing Center
0851-0858: CAH Outpatient

File Name

The file naming convention is to facilitate processing of claims data. Variations are acceptable, but please contact Kevin Conway at 402-742-8150 to discuss options.

- Prefix: File prefix should be SSH account. ie. h045t or c207h. The NHA supplied utilities will append the prefix to the file during the file transmission.
- Date/time stamp: File name should include date time stamp to keep each unique. The common format being used is ccyymmddhhmm (200505251152).
- Spaces or non-alpha/numeric characters are not allowed. Dash and underscore are acceptable.
- Sample valid file names are:
    - h045t_200505251152_nha.837
    - h056k.200505160953.IPUB.nha.837
    - c206h-oct06-ip-nhav02.dat

If the hospital makes the file available to download on a SFTP site, the account prefix should not be added.

Nebraska Hospital Association

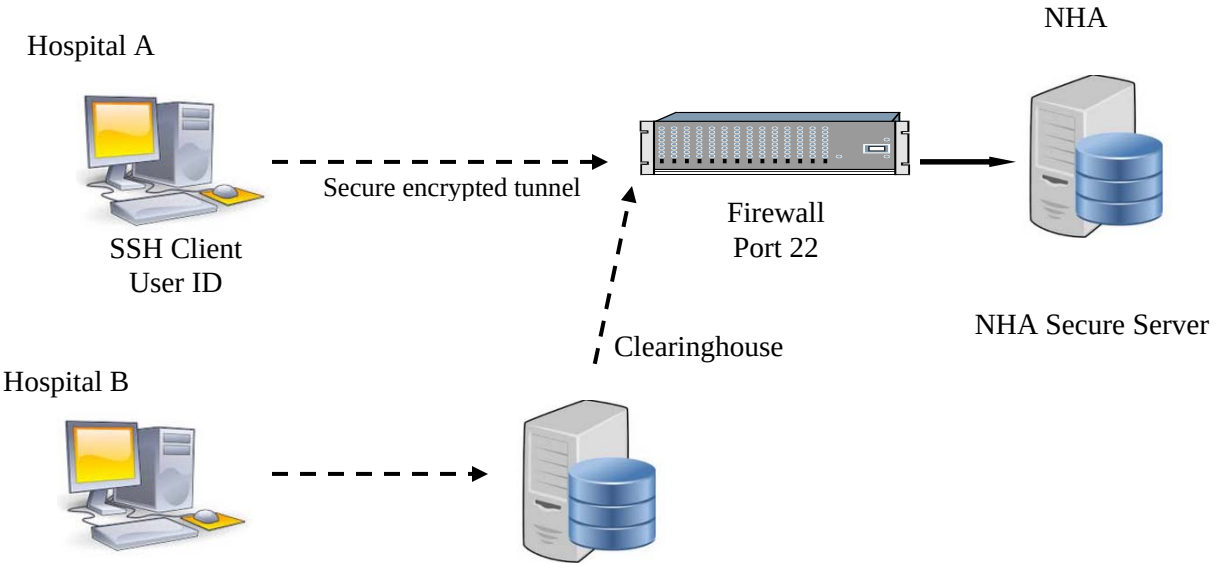
Nebraska Hospital Information System

SSH 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 external IP addresses. Prior to transmitting, NHA will need to verify your account and add it to the list of approved senders.

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 SFTP server located behind the NHA firewall. After files are received on the NHA server, they will be moved to an internal protected server. The combination of SSH, passwords and secure server assist in meeting 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 client software at no cost for hospitals to there use. If your facility is already using a SFTP product, that product may also work with the NHA SFTP server. The SSH client software is a command line utility that can be part of a batch file, run from a command prompt, or Window shortcut. The PuTTY open source software is available for download at various web sites. NHA will include the software on the installation CD.

Log Monitor

To automate the process, NHA will also distribute a 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.