NATIONAL PRACTITIONER DATA BANK - HEALTHCARE INTEGRITY AND PROTECTION DATA BANK (NPDB-HIPDB)

ICD TRANSFER PROGRAM (ITP) INSTALLATION INSTRUCTIONS

Version 1.12

January 2009

National Practitioner Data Bank
Healthcare Integrity and Protection Data Bank
P.O. Box 10832
Chantilly, VA 20153-0832

U.S. Department of Health and Human Services
Health Resources & Services Administration
Bureau of Health Professions
Division of Practitioner Data Banks
Parklawn Building, Room 8-103
5600 Fishers Lane
Rockville, Maryland 20857

DOCUMENT CHANGE HISTORY

The table below identifies changes that have been incorporated into each baseline of this document.

Date	Version #	Change Description
10/17/2005	1.04	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.04. Effective October 17, 2005, this document version 1.04 replaces version 1.03. The changes in this version are indicated below: • Updated installation instructions. See Sections 2.2 and 2.3. • Added guidance for configuring the ITP client program for use with a proxy server. Users who have a previous version of the software and wish to take advantage of this additional functionality must install the latest version of the ITP software. Users do not need to reinstall ITP if they do not wish to take advantage of the additional functionality. See Section 4.4. • Removed unused Status Codes. See Section 3.3.
10/17/2005	1.05	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.05. Effective October 17, 2005, this document version 1.05 replaces version 1.04. The changes in this version are indicated below: • Updated the list of .jar files provided in the itp.zip file. See Sections 2.2 and 2.3.
5/8/2006	1.06	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.06. Effective May 8, 2006, this document version 1.06 replaces version 1.05. The changes in this version are indicated below: • The Data Banks' Web site is now located at www.npdb-hipdb.hrsa.gov. The Data Banks are using a .gov domain name to help prevent fraud by showing Data Banks' users that the NPDB-HIPDB Web site is under the Government-run domain. Please update your Internet bookmarks to reference the .gov address for the Data Banks' Web site. NPDB-HIPDB Web site references in this document now refer to the new Web site address. • Due to the NPDB-HIPDB Web site address change, all ITP and QRXS client programs must be upgraded to a new version.

Date	Version #	Change Description
		Updated client programs are now available on the NPDB-HIPDB Web site. While the current versions of the ITP and Querying and Reporting XML Service (QRXS) client programs will continue to function for a limited time, all ITP and QRXS users must upgrade their client program to the new version no later than September 18, 2006. • Updated the commons-fileupload jar to version 1.1
7/31/2006	1.07	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.07. Effective July 31, 2006, this document version 1.07 replaces version 1.06. The changes in this version are indicated below: • Updated installation instructions. See Sections 2.2 and 2.3. • Added the limitation note of the submission file name length. See Section 3.5.
6/18/2007	1.08	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.08. Effective June 18, 2007, this document version 1.08 replaces version 1.07. For transaction submissions prior to June 18, 2007, readers should refer to version 1.07 of the ICD Transfer Program (ITP) Installation Instructions available at *http://www.npdb-hipdb.hrsa.gov*. The changes in this version are indicated below: • Added consent to monitoring notice paragraph. See Section 1.1. • Added Section 1.2, User Account Security. • Added Section 1.3, Contact Information. • Updated software requirements. See Section 2.2. • Added field UserId to the initialization file. See Section 3.2. • Updated and changed the format of the status codes. See Section 3.3. • Removed submission file name length limitation of 30 characters. See Section 3.5. • Added Section 3.8, Password Changes. • Updated sample configuration with new initialization parameters. See Section 4.

Date	Version #	Change Description
6/18/2007	1.09	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.09. Effective June 18, 2007, this document version 1.09 replaces version 1.08, which provided six months advance notice for functionality changes that also became effective June 18, 2007. • Updated Section 1.2, User Account Security. • Added status codes. See Section 3.3. • Updated notes in Section 3.8, Password Changes.
6/18/2007	1.10	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.10. Effective June 18, 2007, this document version 1.10 replaces version 1.09. The changes in this version are indicated below: • Updated mailing list instructions in Section 1.3, Contact Information. • Updated notes in Section 3.5, Upload File. • Updated notes in Section 3.8, Password Changes. • Modified descriptions to status codes C62, C63, C64, and C65. Added new status code C66. See Section 3.3.
1/14/2008	1.11	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.11. Effective January 14, 2008, this document version 1.11 replaces version 1.10. The changes in this version are indicated below: • Added new status code C67. See Section 3.3.
1/26/2009	1.12	Below is a summary of changes to the ICD Transfer Program (ITP) Installation Instructions version 1.12. Effective January 26, 2009, this document version 1.12 replaces version 1.11. The changes in this version are indicated below: • Updated the e-mail address for the NPDB-HIPDB Customer Service Center to help@npdb-hipdb.hrsa.gov. See Sections 1.1 and 1.3. • Added note 4 in Section 3.6, Download Directory and Download List File.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Scope

The National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB) provides the Interface Control Document Transfer Program (ITP) to users who wish to receive machine-readable responses. The ITP Service is an alternative to the Integrated Querying and Reporting Service (IQRS) and is ideal for large volume queriers and reporters who wish to use their own transaction processing systems and want to interface those systems with the NPDB-HIPDB.

The ITP Service is a stand-alone program that transmits ASCII text files containing transaction data to the NPDB-HIPDB and receives ASCII text file responses from the NPDB-HIPDB. These transactions can be a query, a report, or a password change request. For security, data is transmitted over a Secure Socket Layer (SSL) connection. This program can be executed as a stand-alone program, or it can be executed under the control of other programs.

Submission and response file formats are defined in interface control documents (ICD) published by the Data Banks, available on-line at *http://www.npdb-hipdb.hrsa.gov/itp.html*. The Data Banks make an effort to notify clients at least one month in advance of an update to code lists. Users should expect code lists to be updated quarterly. Additional updates to the file formats are required periodically. Users will be notified six months in advance of updates to ITP file formats. To receive e-mail notification of upcoming improvements, contact the Customer Service Center by e-mail at *help@npdb-hipdb.hrsa.gov* or by phone at 1-800-767-6732 (TDD 703-802-9395).

New users are strongly encouraged to contact the Customer Service Center regarding their use of the ITP Service. Test submission files may be sent to the Customer Service Center for validation. The Data Banks will process your test file and return a response via e-mail. If you are using the ITP Service to submit queries, be aware that the ITP test database does contain several test reports. You may query on subjects identified in these reports and receive a matched query response to test your system. Copies of test reports are available on-line at *http://www.npdb-hipdb.hrsa.gov/itp.html*.

When using the ITP Service, you are accessing a U.S. Government information system. System usage may be monitored, recorded, and subject to audit. Unauthorized use of this system is prohibited and subject to criminal and civil penalties. Use of this system indicates consent to monitoring and recording. Should you have questions concerning your responsibilities, please contact the Customer Service Center immediately as specified in Section 1.3 (Contact Information).

1.2 User Account Security

1.2.1 User Accounts

Each entity has two types of accounts to access the Data Banks, the administrator account and user accounts. The administrator account is used to create and manage the user accounts. User accounts are used to submit transactions and retrieve responses from the Data Banks. The Data Banks have established security policies in order to reduce the risk of unauthorized access to user accounts and protect the confidentiality of practitioner reports.

1.2.2 New Entity Registration Passwords

New entities that register with the Data Banks will receive registration information via U.S. mail providing them with a Data Bank Identification Number (DBID), the administrator account User ID, and a temporary administrator account password. A newly registered entity is required to log in to the IQRS or ITP Service and change the administrator account password within 30 calendar days of the registration verification mailing date. If an entity does not log in to the IQRS or ITP Service within 30 calendar days of the registration verification mailing date, the registration password will expire, the account is automatically locked, and the administrator must contact the Data Banks to reset the password.

1.2.3 User Account Password Policies

A user must provide their organization's DBID, their user ID, and user account password each time they access the IQRS or ITP Service. If a valid password is not provided after five consecutive attempts, the user account is locked and the user must contact the entity administrator to submit a user account password reset request.

Users are required to change their account password **every 90 calendar days.** A password change request can be submitted at any time to change an account's password. Once a password expires, a **30 calendar day** grace login period is available to allow the account password to be changed. Once a password has expired, the NPDB-HIPDB will not accept submissions and access will not be permitted to response files from that account until the account password is successfully changed. Once the grace login period is expired, the account is automatically locked and the user must contact the entity administrator to reset the user's password.

To ensure the security and privacy of user account passwords when using the ITP Service, the response to a password change request transaction can only be downloaded by the same user account that submitted the transaction.

1.2.4 Resetting Passwords

When a user forgets his or her password, or is locked out of the IQRS or ITP Service, the entity administrator is responsible for providing a new Data Banks-generated temporary password to the user. A Data Banks-generated temporary password is valid for three calendar days and must be changed by the user before the user can submit transactions or retrieve response files. Only the administrator can submit and download transactions to reset user passwords using the ITP

Service. The administrator cannot reset his or her own password. A password change transaction should be submitted instead of a password reset transaction.

To ensure that the current administrator is correctly identified in the Data Banks, he or she must log in to the IQRS and update the administrator's user account by entering the administrator's Name, Title, and Telephone Number in the appropriate fields on the User Account Information screen.

If the entity's administrator forgets his or her password, or is locked out of the IQRS or ITP Service, the administrator must call the NPDB-HIPDB Customer Service Center to receive a Data Banks-generated temporary password. If the administrator's name is not maintained in the administrator's IQRS user account, the company's certifying official will be required to submit a signed, faxed request for the change on company letterhead. The Customer Service Center will respond by immediately changing the old administrator password and contacting the new administrator with a Data Banks-generated temporary password and instructions for updating the administrator's user account. These temporary passwords (user and administrator) will only be valid for three calendar days. The user/administrator should change his or her password immediately; and no grace login period will be permitted.

1.2.5 Password Restrictions

The Data Banks also prohibit the use of common or easily guessed passwords by applying the following password restrictions:

- Passwords must be from 8 to 14 characters.
- Passwords must have at least one alphabetic and one numeric character.
- Passwords may not be the same as the User ID.
- Passwords may not be the same as any of the last four passwords.
- Passwords may not contain a word found in the dictionary.
- Passwords may not be a common Data Bank word (e.g., NPDB, IQRS).
- Passwords may not be a simplistic or systematic sequence (e.g., abcd1234).

1.3 Contact Information

The ITP Service is updated periodically by the Data Banks. It is strongly recommended that users join the ITP Mailing List at *http://www.npdb-hipdb.hrsa.gov/MailingListReg.html* to receive notice of updates.

The Data Banks make an effort to notify users at least one month in advance of an update to code lists. Users should expect code lists to be updated quarterly. Additional updates to the ITP file formats are required periodically. Users will be notified six months in advance of updates to the ITP file formats. If you are already registered for the ITP Mailing List and would like to be removed, contact the Customer Service Center.

For additional information, visit the NPDB-HIPDB Web site at
http://www.npdb-hipdb.hrsa.gov/itp.html. If you need assistance, contact NPDB-HIPDB
Customer Service Center by e-mail at *help@npdb-hipdb.hrsa.gov* or by phone at
1-800-767-6732 (TDD 703-802-9395). Information Specialists are available to speak with you
weekdays from 8:30a.m. to 6:00p.m. (5:30p.m. on Fridays) Eastern Time. The NPDB-HIPDB
Customer Service Center is closed on all Federal holidays.

1.4 Conventions

Names of files, URLs, parameters, example DBIDs, example passwords, or documents, are
presented in italics.

   http://java.sun.com/

Data that must be entered into the computer, commands you must enter, contents of files, and
contents of directories, are presented in "Courier New."

```
java Itp send
```

Where the explicit use of upper or lower case letters are necessary due to the system interpreting
upper and lower case letters as distinct characters, the text will clearly identify the command as
"case sensitive."

2. INSTALLATION

2.1 System Requirements

1. Supported Microsoft Windows versions: Windows 98, Windows NT 4.0, Windows 2000, and Windows XP.

2. Access to the Internet and SSL port (443).

2.2 Software Requirements

1. JRE version JRE 1.5.0 or higher.

    The JRE can be downloaded from Sun's JRE download page:

    http://java.sun.com/javase/downloads

    Follow the instructions provided on the web page to download and install the JRE. Only the JRE is required; the JDK is not needed. If the default installation is followed, the JRE will install to a directory specific to the exact release number of Java. For example, if the release is at version 1.5.0_06, the default installation will create a directory named \Program Files\Java\j2re1.5.0_06.

2. The following files are provided in the *itp.zip* file available at *http://www.npdb-hipdb.hrsa.gov/itp.html*.

    commons-codec-1.3.jar
    commons-fileupload-1.1.jar
    commons-httpclient-2.0.jar
    commons-logging.jar
    itp.jar
    itp.ini
    ITP_Installation_Instructions.pdf

2.3 Software Installation

1. Install the JRE. Instructions are provided at Sun's JRE download page, referenced above.

2. Install the JAR files from the *itp.zip* distribution. Copy the .jar files (*itp.jar, commons-codec-1.3.jar, commons-fileupload-1.1.jar, commons-httpclient-2.0.jar,* and *commons-logging.jar)* to the JRE's library extension directory. For example:

    ```
    C:\Program Files\Java\j2re1.5.0_06\lib\ext
    ```

3. Install the ITP initialization file. Copy the file *itp.ini* to the directory from which the ITP executes (your working directory, e.g., `c:\Itp`).

3. ITP CONFIGURATION AND EXECUTION

3.1 Executing the ITP Client Program

The ITP client program takes one command-line parameter. The parameter determines if submission files are sent or response files are downloaded from the Data Bank(s). The parameter values are "send" or "receive." The following are the only supported ITP commands:

```
java Itp send      (for sending submission files); or
java Itp receive (for receiving response files).
```

Note: The program name and the command-line parameter values are case sensitive.

3.2 Preparing the Initialization File

On startup, the ITP client program reads *itp.ini* for initialization information. The *itp.ini* file resides in the working directory as described in Section 2.3 (Software Installation), Step 3. A sample *itp.ini* file is provided in the zip file. All the required information in the initialization file must be complete and valid. If the information is missing or invalid, the program terminates. Users may configure their own *itp.ini* files to reflect their desired log file location, upload/download directory locations, upload/download list file locations, and to specify use of a proxy server.

Certain characters such as spaces and slashes may be interpreted as instructions by the user's operating system or by the ITP client program. For this reason, the *itp.ini* file must be written in such a way that each character is interpreted literally, and not as an instruction. In order to accomplish this, characters that may be interpreted as instructions must be escaped; i.e., a backslash ("\") character is placed in front of the character that may be interpreted as an instruction. If you are unsure as to whether a character will be interpreted as an instruction by the operating system, use the escape character. In general, escaping characters which do not need to be escaped will not affect program execution; however, do not escape the equal sign which separates the parameter names from the parameter values.

The following is a sample *itp.ini* file:

```
DataBankIdNbr=123400000000123
UserId=smithj
Password=UuhUh5owKFEeue
DownloadDir=c:\\Itp\\download
UploadFile=upload.lst
TempDir=c:\\temp
ItpLogFile=itpinfo.log
DownloadListFile=icdfiles.lst
UserName=John\ Smith
```

Notes:
1. The parameters are case sensitive.

2. The password is encoded and must be set using a separate program included in the download. Instructions on setting the password are in Section 3.7 (Encode Password).

3. The backslash character itself must be escaped, because in this case it must be interpreted literally; this is the reason for the two backslashes in the directory values.

4. The parameters within the file may appear in any order. Some parameters are required while others are optional as shown in the table below. Users are encouraged to set all parameters to user-specific values.

The following parameters are allowed. Users must enter any parameters that they do not wish to use the default values for:

Parameters	Required?	Descriptions
DataBankIdNbr	Yes	The Data Bank Identification Number (DBID).
UserId	Yes	The user account established for use with the Data Bank Identification Number (DBID).
Password	Yes	Encoded Data Bank password (also known as the IQRS password).
DownloadDir	Yes	Directory to hold the downloaded ICD response files.
UploadFile	Yes	Name of the file containing one or more names of ICD submission files.
TempDir	No	Temporary work directory; defaults to the working directory if not set.
ItpLogFile	No	Program log file; defaults to *itp.log* if not set.
DownloadListFile	No	File containing names of the ICD response files downloaded; defaults to *download.lst.*
UserName	No	Unique name indicating the person operating the software.
ProxyHostName	No	Name of the proxy host (usually an IP Address). Only required when using a proxy server (see Section 4.4, Proxy Server for more information).
ProxyPort	No	Port number of the proxy server. Only required when using a proxy server (see Section 4.4, Proxy Server for more information).

Notes:
1. For parameter *DataBankIdNbr*, enter a Data Bank Identification Number (DBID). An entity would enter the entity's DBID. An agent would enter the agent's DBID whether it is representing itself or another entity.

2. For parameter *UserId*, enter the name of a user or the administrator account that has previously been established for the DBID.

3. For parameter *Password*, enter the password for the user ID specified for *UserId*. Passwords are not displayed as regular text but are encoded. Refer to Section 3.7 (Encode Password) for more information on how to set *Password* in the *itp.ini* file. Passwords expire every 90 days and may be changed by submitting a password change transaction via the ITP Service or by

accessing the Integrated Querying and Reporting Service (IQRS) at
http://www.npdb-hipdb.hrsa.gov. The IQRS password is the same as the ITP password.

4. For parameters *UploadFile*, *ItpLogFile,* and *DownloadListFile*, acceptable values of the
    parameters include the file name only, or a path name and the file name. If the value is the
    file name only, then the file is assumed to be located in the working directory.

5. For parameters *DownloadDir* and *TempDir*, enter a directory path name for each, either a
    relative path to the working directory or a full path.

6. For parameter *UserName*, remember to include a backslash ("\") in front of a character that
    may be interpreted as an instruction.

7. For parameter *ItpLogFile*, this file contains program execution warnings and errors. To
    determine whether the send or receive operation was successful, the *itpstat.dat* file contains
    this information, refer to the Section 3.4 (ITP Status File).

3.3 Status Codes

The ITP Service provides status in two ways. First, an exit code is always returned; second, a
file called *itpstat.dat*, which contains the status code, is created. This file is created in the
program's working directory. Status code "C00" indicates that the transaction was successful,
and any other status code indicates that the transaction failed.

The following status codes are returned:

Status Code	Description
C00	Success, no errors.
C01	Error on NPDB-HIPDB server, reattempt transfer.
C04	Database error on NPDB-HIPDB server, reattempt transfer.
C06	Database connection error on NPDB-HIPDB server, reattempt transfer.
C08	Communication error with NPDB-HIPDB ICD server during response retrieval, reattempt transfer.
C18	Error in downloaded response files, reattempt transfer.
C19	Error in getting information from the downloaded file, reattempt transfer.
C20	Unable to open downloaded file, check if sufficient disk space is available to download file and reattempt transfer.
C21	Generic error code; used for failures not yet categorized.
C22	Usage error, check command-line parameter.
C23	Error in reading Initialization file *itp.ini*, check that *itp.ini* file is in working directory.
C24	Unable to open program log file, check that disk space is available.
C25	Error in user ID and password validation, check that the DBID and password are correct.

Status Code	Description
C30	Error validating parameter in *itp.ini*, a parameter is missing or value is invalid.
C31	Error validating *UploadFile*, upload file missing or a file listed in the upload file does not exist.
C32	Error validating *DownloadDir*, directory does not exist.
C40	Error opening connection to NPDB-HIPDB server, check internet connection and reattempt transfer.
C41	Error getting input stream to NPDB-HIPDB server, check internet connection and reattempt transfer.
C42	Error getting output stream from NPDB-HIPDB server, check internet connection and reattempt transfer.
C50	Error reading status response from NPDB-HIPDB server, reattempt transfer.
C51	Error processing web request, reattempt transfer.
C52	Error getting status code, reattempt transfer.
C53	Error sending submission files, reattempt transfer.
C54	Error downloading response files, reattempt transfer.
C55	Error moving response files to the download directory, no permission to write to the directory or the device has run out of space.
C56	Your password change request could not be successfully processed. Download the response file for further details.
C57	Your account has been locked out. Contact your entity administrator to reset the password. If you are using an administrator account, contact the NPDB-HIPDB Customer Service Center to reset the password.
C58	Your account has been locked out. The number of invalid login attempts has exceeded the allowable login limit. Contact your entity administrator to reset the password. If you are using an administrator account, contact the NPDB-HIPDB Customer Service Center to reset the password.
C59	Your account password has expired. Contact your entity administrator to reset the password. If you are using an administrator account, contact the NPDB-HIPDB Customer Service Center to reset the password.
C60	Unable to process submission files. The files are not in the appropriate format. Check to ensure that the files are not zipped or in a binary format prior to resubmission.
C61	Your password must be changed before other transactions can be submitted.
C62	The entity identified by the DBID in itp.ini does not have active status.
C63	The entity identified by the DBID in itp.ini does not match the DBID in the submission file.
C64	No more than one password change transaction can be listed in the upload file *UploadFile* at any time. Modify *UploadFile* to include only one password change transaction, reattempt transfer.
C65	Password change transaction processing was successful but an error occurred sending the other transaction files. Re-encode new password if necessary, remove password change transactions from the upload file *UploadFile*, and reattempt transfer of other transaction files.

Status Code	Description
C66	Password change transaction processing failed but the other transaction files were sent successfully. Modify the upload file *UploadFile* to include only one password change transaction, reattempt transfer.
C67	Your password has expired. You may login to the IQRS to reset your password or contact your administrator or the NPDB-HIPDB Customer Service Center.

3.4 ITP Status File

The *itpstat.dat* file contains the final status of the ITP client program execution. This file is
created in the working directory immediately upon program completion. The file contains two
lines. The first line indicates the overall status of "Done" or "Not Done." The second line
contains a status code of "C00" or another status code indicating an error (see Section 3.3, Status
Codes, for error codes that may be returned).

Sample *itpstat.dat* file for a successful execution:

```
Overall status          = Done
StatusCode=C00
```

Sample *itpstat.dat* file for an unsuccessful execution:

```
Overall status          = Not Done
StatusCode=C22
```

The *itpstat.dat* file is not referenced by a parameter in the *itp.ini* file. The name of this status file
cannot be configured. However, the file can be removed or renamed anytime after the
completion of the ITP client program and will get re-created with each completion of subsequent
ITP client program executions.

3.5 Upload File

The upload file contains the names (including the full or relative path) of the submission files
that are sent to the Data Bank(s). The name of the upload file must be specified in the *itp.ini* file,
parameter *UploadFile*.

A sample upload file with four submission files to upload, using a full path:

```
c:\Itp\upload\icd0001.dat
c:\Itp\upload\icd0002.dat
c:\Itp\upload\icd0004.dat
c:\Itp\upload\icd0005.dat
```

A sample upload file with three submission files to upload, using a relative path:

```
upload\file001.dat
upload\file002.dat
upload\file003.dat
```

Notes:
1. In the upload file, the backslash is not escaped.

2. A file name can be specified with a relative or full path as noted above. Each set of files
    above is specified differently, but all the files are located in `c:\Itp\upload`, and the

working directory is `c:\Itp`. Relative paths are specified in relation to the directory in which the ITP client program executes; this is also referred to as the working directory.

3. Each submission file name must not exceed 256 characters in length. This limitation only applies to the file name itself and not the path.

4. A submission file listed in the upload file may be a report, a query, or a password change transaction. No more than one password change transaction can be included at any time.

5. The Data Banks do not recommend submitting files that are larger than 1MB.

3.6 Download Directory and Download List File

Response files are stored in the download directory after being successfully downloaded from the Data Bank(s). The names of the files are in the following format: *msg#####.csm* (i.e., *msg00000.csm*, *msg00001.csm*). In addition to the data files, a separate file is provided that lists each file included in the download. By default, this file is named *download.lst*. Users may set the name of this file in the initialization file (*itp.ini*) using the parameter *DownloadListFile*.

The following is the content of a download list file that might be created:

```
c:\Itp\download\msg00000.csm
c:\Itp\download\msg00001.csm
c:\Itp\download\msg00002.csm
c:\Itp\download\msg00003.csm
```

Notes:
1. The files in the download directory are not overwritten. If files from a previous download exist, then the names of the files start after the last increment name (i.e., if *msg00054.csm* is the last increment, then the name of the new file starts with *msg00055.csm*).

2. The download list file is recreated on every successful download of response files. The download list file is not created if there are no response files to download or if there was an error downloading response files.

3. Report responses will always be returned in a single response file. Responses for query submissions containing multiple subjects may be returned in multiple response files if the response will exceed 1MB. Responses that are larger than 1MB are separated into 1MB portions. Responses for a password change request will always be returned in a single response file. Users should read response files in numerical order.

4. No more than 1,000 non-password change response files may be downloaded at one time. Password change responses may be included in the download, but do not count toward this limit. Multiple download requests may be necessary to download all response files.

5. Responses to report and query submissions are available for download within an average of two to four hours after submission. Under certain circumstances, additional processing time may be required. Please do not re-submit your query or report on the subject in question,

since this will result in duplicate transactions and duplicate fees. If your submission file is not formatted properly, the Data Banks may not be able to process the file. If you do not receive your response within 2 to 3 business days of submission, please call the NPDB-HIPDB Customer Service Center.

6. Responses to password change request submissions are generally available for download immediately.

3.7 Encode Password

The password is encoded in the initialization file by executing the Encode program included in the download, and providing the password as a command-line parameter. The password is encoded and written to *itp.ini*; it is not displayed on the screen. The following is an example of how to execute the Encode program:

```
java Encode MyNewPasw0rd
```

Notes:
1. The command and the password are case sensitive.

2. Encode may cause some characters to be escaped; this is denoted by a backslash in front of the escaped characters. This will not affect the functionality of the ITP Service.

3.8 Password Changes

As explained in Section 1.2.3, *User Account Password Policies*, a valid password is required to submit transactions to and download responses from the Data Banks. This includes password change request transactions. To successfully change your password, a password change request must be submitted using your current password. Status code "C00" indicates that the password change request transaction was successful. Any other status code indicates an error.

Notes:
1. If status code "C00" is indicated after submitting a password change request transaction, the password for the specified DBID/user ID was changed successfully. The new password must be encoded into the *itp.ini* file in order to download the password change response, submit additional transactions and download responses. For that process, follow the instructions specified in Section 3.7 (Encode Password).

2. If status code "C00" is **not** indicated after submitting a password change request transaction, the password change request for the specified DBID/user ID was unsuccessful. The encoded password in the itp.ini file must remain unchanged in order to download the password change response file, which describes the reason(s) why the password change was rejected. Refer to the appropriate ICD specifications for rejections codes.

3. No more than one password change transaction can be included in the upload file at any time.

4. It is recommended that a password change request be submitted separately from report and query submissions in order to avoid confusion in regards to password status.

5. A response to a password change request transaction can only be downloaded by the same user account that submitted the transaction.

6. Only the administrator can submit and download transactions to reset user passwords using the ITP Service.

7. The administrator cannot reset his or her own password. A password change transaction should be submitted instead of a password reset transaction.

8. After a password is reset for a user or administrator, the system-generated password must be changed by submitting a password change transaction before other transactions can be submitted by that user or administrator.

4. SAMPLE CONFIGURATION AND EXECUTION

The following sections guide you through a sample configuration and use of the ITP Service. This is only a sample configuration and may be changed if desired.

4.1 Configuration

The ITP client program is installed in the directory `c:\Itp` for entity DBID *399700000000123* (parameter *DataBankIdNbr*) and user ID *jonesb* (parameter *UserId*), with password *MyNewPasw0rd* (parameter *Password*). The ITP initialization file is configured for the remaining parameters using:

- the download directory `c:\Itp\download` (parameter *DownloadDir*),
- temporary directory `c:\Itp\temp` (parameter *TempDir*),
- upload file *upldlist.fil* (parameter *UploadFile*),
- ITP log file *itperror.log* (parameter *ItpLogFile*),
- download list file *icdresp.fil* (parameter *DownloadListFile*), and
- the username *Bob Jones* (parameter *UserName*).

The ICD submission files for upload are located in the `c:\Itp\upload` directory. The user creates the three new directories:

```
cd Itp
mkdir temp
mkdir download
mkdir upload
```

The following is a listing of files in directory `c:\Itp`:

```
itp.ini
<DIR>   temp
<DIR>   download
<DIR>   upload
```

The working directory is `c:\Itp`. Encode the password by executing the following command:

```
java Encode MyNewPasw0rd
```

The following is a printout of the *itp.ini* initialization file:

```
#Mon June 18 13:29:03 EDT 2007
DataBankIdNbr=399700000000123
UserId=jonesb
Password=2MhEB2Fsue1I7eqJLDyI
DownloadDir=download
UploadFile=upldlist.fil
TempDir=temp
ItpLogFile=itperror.log
DownloadListFile=icdresp.fil
UserName=Bob\ Jones
```

Notes:
1. The order of parameters may vary; this is normal.

2. The backslash in the username escapes the space character; this is also normal. The escape appears after executing the encoding program.

4.2 Upload Submission Files

The submission files must first be uploaded to the Data Bank(s). Submission files *icd0001.dat, icd0002.dat*, *icd0004.dat*, and *icd0005.dat* are placed in the upload directory c:\Itp\upload. The upload file, *upldlist.fil*, is placed in the working directory c:\Itp. The following is a printout of *upldlist.fil*:

```
c:\Itp\upload\icd0001.dat
c:\Itp\upload\icd0002.dat
c:\Itp\upload\icd0004.dat
c:\Itp\upload\icd0005.dat
```

Execute the following command, either from the DOS prompt or from a user application, to upload files to the Data Bank(s). This command is case sensitive and must be executed exactly as shown here:

```
java Itp send
```

After execution of this command, the submission files are uploaded to the Data Bank(s) successfully. Files *itperror.log* and *itpstat.dat* are created in the working directory c:\Itp. The *itperror.log* file is empty because no errors were generated upon a successful upload. The *itpstat.dat* file indicates a successful status code of 0. The following is a printout of the *itpstat.dat* file that is created:

```
Overall status        = Done
StatusCode=C00
```

4.3 Download Response Files

The response files may be downloaded after they have completed processing. To download response files, execute the ITP client program in receive mode:

```
java Itp receive
```

The response files are first downloaded to a temporary directory, `c:\Itp\temp`, and then moved to the download directory, `c:\Itp\download`. The temporary directory is specified by the parameter *TempDir* and the download directory is specified by parameter *DownloadDir*. There are four response files to download; thus, the directory `c:\Itp\download` contains the following files:

```
msg00001.csm
msg00002.csm
msg00003.csm
msg00004.csm
```

The download list file *icdresp.fil* is created in the directory `c:\Itp`. The following is a printout of the *icdresp.fil* file:

```
c:\Itp\download\msg00001.csm
c:\Itp\download\msg00002.csm
c:\Itp\download\msg00003.csm
c:\Itp\download\msg00004.csm
```

In `c:\Itp`, *itperror.log* is appended to. If the file does not exist, it is created. Since the download was successful, no messages are logged. The status file *itpstat.dat* is also created in the directory `c:\Itp`. The following is a printout of the *itpstat.dat* file that is created:

```
Overall status        = Done
StatusCode=C00
```

4.4 Proxy Server

A proxy server is a program that mediates requests between the local network and the workstations on them and the Internet beyond. Contact your network administrator for proxy server information. To enable the ITP client program to work with proxy servers, the *itp.ini* file needs the parameters *ProxyHostName* (specifies the host name of the proxy server; usually an IP Address), and *ProxyPort* (specifies the port number the proxy server connects to). Once these parameters are set, sending and receiving via the ITP Service proceeds as normal.

The following is a printout of the *itp.ini* initialization file for use with a Proxy Server:

```
DataBankIdNbr=123400000000123
UserId=smithj
Password=UuhUh5owKFEeue
DownloadDir=c:\\Itp\\download
TempDir=c:\\temp
UploadFile=upload.lst
ItpLogFile=itpinfo.log
DownloadListFile=icdfiles.lst
UserName=John\ Smith
ProxyHostName=111.111.111.111
ProxyPort=1000
```