



Data Transfer Options and Requirements

Original date 25 Jan 2005
Revision date 21 Aug 2018

Proprietary and Confidential

Summary of changes

Date	Short description of changes
September 2016	Updated name of submission tool to SDSS.
August 2018	Rebranded.

Contacting support

Support is available through the following link:

https://www.ibm.com/software/support/watsonhealth/truven_support.html

Contents

Summary of changes	2
Contacting support	2
Contents	3
Overview	5
Electronic data transfer methods	5
Data suppliers	5
Data recipients	5
Physical media options (for data suppliers and recipients)	5
Data suppliers: sending data to IBM Watson Health	6
Methods for submitting electronic data to IBM Watson Health	6
File naming conventions for submitting electronic data to IBM Watson Health	9
IBM Watson Health file naming requirements	9
SFTP and HTTPS push with PGP-encrypted files	9
Header/trailer and tag identifier character	10
Multiple files	10
Supplier-selected file naming requirements	10
SFTP pulls/pushes and HTTPS push	10
Control information for submitting electronic data to IBM Watson Health	11
Embedded header or trailer record	11
Tag file	11
Supported compression and encryption methods for submitting electronic data to IBM Watson Health	14
Physical media submission	14
Physical media format options	14
Media types	14
Compression	14

Parsing files prohibited	14
Media contents	15
Data security	15
Physical media labeling and documentation requirements	15
Physical media identification	15
Proper identification of the media	15
Unidentified physical media retention policy	15
Data recipients: receiving data from IBM Watson Health	16
Methods for receiving electronic data transmissions from IBM Watson Health	16
Appendix A: sample Media Submission Form	18

Overview

This document is designed to provide data suppliers and data recipients with information about the different data transfer methods supported by IBM Watson Health as well as their requirements. Although physical and electronic media submissions are both accepted, IBM Watson Health encourages electronic data transfers (EDT).

Electronic data transfer methods

Data suppliers

Several methods can be used to submit data to IBM Watson Health over the internet, and this document provides information about each of them. See page 6 for details about method, setup, and requirements for sending data via:

- Secure FTP (SFTP) – push and pull
- HTTPS - push
- Interactive web submission

Data recipients

IBM Watson Health offers five different setup methods for transmitting data to data recipients. See page 16 for details about methods, setup, and requirements for receiving data from IBM Watson Health via:

- Standard FTP over VPN – push only
- FTP push and pull
- HTTPS pull
- SFTP push and pull

Physical media options (for data suppliers and recipients)

IBM Watson Health accepts data submission in a variety of physical media options. See page 14 for details about format options and requirements for:

- External USB hard drives
- CDs and DVDs

Data suppliers: sending data to IBM Watson Health

Electronic data transfers (EDT) rely on standard Internet protocols to transfer data to and from IBM Watson Health for processing. This service has several options you can use to submit data to IBM Watson Health. Acceptable file types include .txt, .dat, and .csv. Do not send proprietary-format file types (such as .xls, .doc, and so on). IBM Watson Health adheres to HIPAA (Health Insurance Portability and Accountability Act) standards regarding the transmission of medical data, including authenticating users and encrypting transmissions.

Note

All electronic data submission methods require the submission of control information in specified formats and may require files to be named according to IBM Watson Health file naming convention. Please see page 9 for information about file names. **Data will not be processed without control information.** Please see page 11 for information about control totals. For additional information about control information requirements, contact your IBM Watson Health Account Team Representative.

Methods for submitting electronic data to IBM Watson Health

The methods listed below can be used to send data to IBM Watson Health.

- **Secure FTP (SFTP) – push and pull**

This option uses an encrypted SSH (Secure Shell) channel to pull data from supplier sites. It also uses Secure FTP on port 22 to accomplish the data transfer. Zipped files may be transmitted using this method. Please see “Supported compression and encryption methods for submitting electronic data to h” on page 14 for more information about zipped files. PGP encryption is supported but not required.

Note

SSL on port 21 (FTPS) is not supported by IBM Watson Health.

IBM Watson Health supports SSH key authentication as well as username/password authentication. SFTP Push users with username/password authentication will be issued a temporary password, which must be changed upon successful login. Data suppliers using key authentication are required to provide IP addresses for filtering purposes. If you are using SSH key authentication, you will not be prompted for a password.

Note

Passwords will expire every 90 days; users will receive a reminder **only** if they have requested an automated e-mail to notify them when their password is about to expire.

- **HTTPS – Push**

This option uses an encrypted SSL channel to push data to IBM Watson Health. It utilizes Internet standard port 443 to accomplish the data transfer. Zipped files may be transmitted using this method. Please see “Supported compression and encryption methods for submitting electronic data to h” on page 14 for more information about zipped files.

Note

HTTPS Push users will be issued a temporary password, which must be changed upon successful login. Passwords will expire every 90 days; users will receive a reminder **only** if they have requested an automated e-mail to notify them when their password is about to expire.

- **Interactive Web Submission**

The Secure Data Submission System (SDSS) is a web-based software application that allows a data supplier to validate the structure of a file and send it electronically to IBM Watson Health over the internet. A small Java applet guides the user through the data submission process. In this process, data is validated against the agreed-upon data format. This method cannot be automated. Zipped files may not be sent using this method.

Table 1: Electronic data submission method features

Feature	Interactive web	HTTPS	SFTP
Compression	✓		
File encryption			✓ Supported
Transfer method encryption	✓	✓	✓
User authentication	✓	✓	✓ Supported
Key authentication		✓	✓ Supported
Data pushed to IBM Watson Health	✓	✓	✓ Supported
Data pulled by IBM Watson Health			✓ Supported
Can be automated		✓	✓

Table 2: Electronic data submission method requirements

Requirement	Submitting data via Interactive Web	Submitting data via HTTPS	Submitting data via SFTP
Software	Java Run-time 1.5 or greater (installed during first SDSS login, if not present)	SSH client or web browser	Pull SSH Server responding on port 22 Push SSH client or web browser
Hardware	PC with Windows 2000 or Windows XP workstation, with latest Windows updates 56Kb modem or better (broadband Internet connection preferred) 128MB RAM or better Pentium 200Mh processor or better	N/A	N/A
Web Browser	Internet Explorer 6 or Internet Explorer 7	IE 6 or IE 7	Pull N/A Push IE 6 or IE 7
File Size Limit	2GB	15GB	Pull 15GB Push 10GB (file or batch)
Control Information	Entered on Web Interface	Header/Trailer or Tag File	Header/Trailer or Tag File
File Names	N/A	File names supplied by IBM Watson Health unless otherwise specified by supplier.	File names supplied by IBM Watson Health unless otherwise specified by supplier.
Permissions	Administrator access on workstation to install Java Run-time		Permission to delete files from remote server

File naming conventions for submitting electronic data to IBM Watson Health

When submitting files by FTP Pull or SFTP, the file names should follow the IBM Watson Health naming convention, unless otherwise specified by the data supplier.

IBM Watson Health file naming requirements

SFTP and HTTPS push with PGP-encrypted files

Format ONLY for 4-digit customer/data supplier identification numbers with 5-digit layout identification numbers

This format is to be used **only** when both the customer and the data supplier have a 4-digit identification number and when the layout has a 5-digit identification number. It cannot be used if either the customer or the data supplier has a 5-digit identification number or if the layout identification number is longer than 5 digits.

In the template shown below, the italicized text represents variable information. The angle brackets (< >) must **not** be included in the file name; they are used only for clarity's sake.

In this file naming format, the customer number is 4 bytes, the data supplier number is 4 bytes, the header/trailer identifier is 1 byte, and the layout group number is 5 bytes, for a 14-byte length. Starting at byte 15 and before the file extension, an underscore followed by optional text may be entered in the file name. Although the underscore is optional, IBM Watson Health suggests that it be included before the optional text. See "Control information for submitting electronic data to IBM Watson Health" on page 11 for additional details about the header/trailer identifier located at byte 9.

Note

PGP is optional. If using PGP, the file extension must be added at the end of the file name, as shown in the example below.

<Customer#><Supplier#><Header/TrailerID><LayoutGroup#>_<OptionalText>.<FileExtension> pgp
Optional

If you send the control information in a separate tag file, the file name for the tag file and **must** match the file name for the data file up to the file extension. In the example below, the two file names match except for the .txt and .mms file extensions.

Example 17460770E10356_1Q11.txt.pgp and 17460770E10356_1Q11.mms.pgp

Format for 4- or 5-digit customer/data supplier identification numbers

This format includes a delimiter, so it can be used for all customers and data suppliers and with all layouts. In the template shown below, the italicized text represents variable information. The delimiter we use between sections takes the form of a hyphen-underscore-hyphen (-_-), and it must be inserted where indicated. The angle brackets (> <) must **not** be included in the file name; they are used only for clarity's sake.

Note

PGP is optional. If using PGP, the file extension must be added at the end of the file name, as shown in the example below.

<Customer#>-_-<Supplier#><Header/TrailerID><LayoutGroup#>-_-<OptionalText>.<FileExtension> pgp
Optional

See “Control information for submitting electronic data to IBM Watson Health” on page 11 for additional details about the header/trailer identifier.

Examples

1746-__-0770E10356-__-Nov2010.txt.pgp and 1746-__-0770E10356-__-Nov2010.mms.pgp
 14325-__-0631T5113.txt
 09989-__-16723T22048-__-3Q2010.txt

Note

If you send the control information in a separate tag file, the file name for the tag file and **must** match the file name for the data file up to the file extension. In the first example above, the two file names match except for the .txt and .mms file extensions.

Header/trailer and tag identifier character

The header/trailer and tag identifier character indicates the location of the control information.

- **E** indicates a separate tag file with an .mms extension
- **T** indicates an embedded header/trailer record

Examples

7705-__-0770E10356.TXT.PGP and 7705-__-0770E10356.MMS.PGP
 7705-__-0770T10356.TXT.PGP

See “Control information for submitting electronic data to IBM Watson Health” on page 11 for additional details about the header/trailer identifier.

Multiple files

To push multiple files at one time, a unique identifier can be inserted into the file name after the layout group number and before the .txt or .mms extension.

Examples

7705-__-0770E10356-__-4Q10.TXT.PGP and 7705-__-0770E10356-__-4Q10.MMS.PGP
 7705-__-0770E10356-__-1Q11.TXT.PGP and 7705-__-0770E10356-__-1Q11.MMS.PGP

Supplier-selected file naming requirements

SFTP pulls/pushes and HTTPS push

In almost all cases, IBM Watson Health requires the use of our file naming conventions when submitting via FTP with PGP encryption, FTP over VPN, or SFTP. If you are unable to comply with this requirement, then the file names you use **must** contain a static component from submission to submission.

Examples Customer_medclaims_Jun2011.txt (Data file name)
 Customer_medclaims_Jun2011.mms (Tag file name)

In the examples above, “Customer_medclaims_” remains the same for each submission, but the time period is updated with each submission. File names for data and tag files should be identical except for the file extension. Remember that our file system is case sensitive.

Note

Do not use spaces, periods (.) except immediately before the txt and pgp extensions (if applicable), or special characters: !, #, or @ in file names.

Control information for submitting electronic data to IBM Watson Health

Files submitted electronically to IBM Watson Health must contain information about the data contents. This information can be provided in one of two ways:

- Embedded header or trailer record
- Tag file

Embedded header or trailer record

If the data format contains layouts for a header or trailer record that contain control total information about the file, these records can be appended to the data detail.

Note

If you are adding headers and/or trailers that have not been previously discussed, contact your IBM Watson Health Account Team Representative first.

The header/trailer record must be the same length as other layout(s) in the group when using fixed-width formats. At a minimum, the header/trailer record must contain the following information:

- Total file record count including header and/or trailer
- Dollar totals (such as net payments), if applicable
- Start time period (dates must be in the same format as dates in the data detail)
- End time period (dates must be in the same format as dates in the data detail)

Tag file

A tag file, in the context of the automated EDT process developed by IBM Watson Health, is a small text file that contains information about a specific data file. Each data file transmitted to IBM Watson Health must be accompanied by a tag file or must have a header/trailer. A tag file or a header/trailer is required with each file submitted so that IBM Watson Health can properly catalogue and process the data content included in the submission.

IBM Watson Health only processes data files and tag files in pairs. Orphaned data files or tag files will not be processed. Except for the file extensions, data file and tag file pairs must also have identical file names to process:

Example

Customer_medclaims_Jun2006.txt	(Data file name)
Customer_medclaims_Jun2006.mms	(Tag file name)

The first 25 bytes of each required line (or record) will comprise the literal label used in the example below. The data corresponding to the label will begin in column 26 and end in column 80 for that respective line (or record).

The data supplier should provide in the tag files the content shown in the table below.

Table 3: Tag file fields

Label	Format	Description
Number of Records	Numeric, left justified, no commas	Identifies the number of records included in the data content file.
Record Length	Numeric, In bytes at source, left justified, no commas	Identifies the number of bytes per record (excluding the record terminator).
Start Paid Date	Date: MM/DD/CCYY with "/" delimiter and leading zeros as needed for single-digit months and days	Identifies the starting date for the period included in the data submission.
End Paid Date	Date: MM/DD/CCYY with "/" delimiter and leading zeros as needed for single-digit months and days	Identifies the ending date for the period included in the data submission.
Dollar Totals	Numeric, left justified, no commas or dollar sign (\$), negatives should be signed on the far left, two explicit decimal places to the right of the included decimal point	Provides a control total for dollar amounts for files that include dollar amounts in the record layout. Note If a record layout does not include a dollar amount, the label must remain in place, while the remainder of the line is left blank.
Contact Name and Phone	Text, First (space " ") Last ###.###.#### (X##### for extension)	Provides contact information that can be used for follow-up in the event of problems reading or interpreting the data content file.
Comments	Text, columns 26 through 80, one comment per line with a maximum of four lines.	Provides space for comments regarding the data content, such as data type, or special instructions, and so on.

Example tag file

```

1-----26-----40-----60-----80
Number of Records:      105623
Record Length:         450
Start Paid Date:       01/01/2010
End Paid Date:         01/31/2010
Dollar Totals:         2356497.88
Contact Name and Phone: Joyce Welch-Smith 734.555.9876X4321
Comments:              Claims Data
Comments:              Replacement file

```

Note

The dashed line with numbers in the example above indicates the relative positions in the record layout – it must not be included in the text of the tag file.

Example tag file

```

1-----26-----40-----60-----80
Number of Records:      265884
Record Length:         353
Start Paid Date:       03/01/2010
End Paid Date:         03/31/2010
Dollar Totals:
Contact Name and Phone: Franklin Haskel 734.555.9876X4321
Comments:              Eligibility Data
Comments:              Replacement file

```

Notes

If you are submitting a tag file for data that has no financial information included, the "Dollar Totals:" label must remain in place but leave the rest of the line blank.

The dashed line with numbers in the example above indicates the relative positions in the record layout – it must not be included in the text of the tag file.

Supported compression and encryption methods for submitting electronic data to IBM Watson Health

The only encryption method supported by IBM Watson Health is PGP. Files sent to IBM Watson Health using the PGP encryption method should be encrypted using the IBM Watson Health Analytics Public Key (`IBM_Watson_Health_Analytics.asc`). The public key will be provided during the data transmission setup process.

IBM Watson Health can accept zipped files via most electronic transmission methods. However, specific naming conventions must be followed:

- Files may be zipped using Winzip, pkzip, or gzip.
- Files may have either a `.zip` or a `.gz` extension.
- Files with `.tar`, `.tgz` and `.rar` extensions will not be processed.
- If files are to be PGP encrypted, zipping should be done before encryption.
- All zipped files must be named according to the transmission method's file naming requirements, with the `.txt` or `.mms` extension replaced by the `.zip` or `.gz` extension.
- All files in archives must follow the file naming convention set by IBM Watson Health, regardless of transmission method. See page 9 for file naming requirements for each data transfer method.

Examples

`1055-__-0770E12345.ZIP` (Contains `1055-__-0770E12345.TXT` and `1055-__-0770E12345.MMS`)

`Customer_claims.zip` (Contains `10550770T12345.TXT`)

Note

Zipped files are not supported for Interactive Web Submission.

Physical media submission

Although IBM Watson Health encourages the use of electronic data submission, physical media submission is also available. The media format options, which are described below pertain to media to be received by IBM Watson Health. However, the same media formats and requirements are also used to send data files externally (originating from IBM Watson Health). If you receive data files on physical media from IBM Watson Health and have other requirements, please notify your IBM Watson Health account representative.

Physical media format options

Media types

- CD-ROM – 700MB
- DVD – 4.3GB single layer or 8.5GB dual layer
- External hard drive with USB 2.0 or USB 3.0 (recommended) connection formatted for Windows

Compression

Data files may be compressed using WinZip Self-Decrypting Archive format.

Parsing files prohibited

Data files should not span multiple media. Please choose a type of media that will accommodate the entire data volume or limit the file size appropriately.

Media contents

Media should only contain data files. No other files should be present on the disk, including third party software (for example, applications that can be used to view/edit data files).

Data security

Due to HIPAA privacy and security regulations and increased data breach sanctions under the American Recovery and Reinvestment Act of 2009 (ARRA) and HIPAA HITECH act, IBM Watson Health strongly recommends protecting data containing PHI that is placed on physical media and shipped to IBM Watson Health. Protection can be achieved by using encrypted FIPS 140-2 certified USB external hard drives which ensure safe harbor for data under the final rule of the HIPAA HITECH act. PGP encryption or password protected WinZip (preferably using 256-bit AES encryption) or any WinZip compatible application for CD-ROM or DVD. Passwords should not be shipped in the same package as the media. This will help protect the data from unauthorized access.

Physical media labeling and documentation requirements

External media label and documentation requirements apply to all physical media types.

Physical media identification

IBM Watson Health can provide an electronic Media Submission Form for data suppliers that submit data via physical media. The forms provide data security and privacy while expediting processing upon receipt at the IBM Watson Health data center. Appendix A contains a sample of the Media Submission Form. Please notify your contact at IBM Watson Health if you require a Media Submission Form.

Proper identification of the media

1. When using an electronic form create a unique id/serial number and write it on both the form and media so they can be matched together at our data center.
2. If you place multiple files on the same media, list the files on the Media Submission Form by file name or volume serial number. For each file, indicate the record count, net payments (if applicable), and time period.
3. To protect the media from unauthorized access we recommend that you e-mail the media submission form to mediamanagement@us.ibm.com when you ship the media.

Note

Never combine files for multiple customers on a single item of media. For example, if you use CDs and you have files for three customers, you would send three CDs (there would be one set of customer files per CD).

Unidentified physical media retention policy

Physical media sent to IBM Watson Health for processing, but which doesn't have supporting documentation (that is, there is no password, no identifiable customer or supplier, etc.), will be retained for a period of two weeks while we work to obtain the necessary information needed to process the media. If, after two weeks, we are still unable to identify or process the media, it will be destroyed.

Data recipients: receiving data from IBM Watson Health

Electronic data transfers (EDT) rely on standard Internet protocols to transfer data to and from IBM Watson Health for processing. This service has several options by which you can receive data from IBM Watson Health.

IBM Watson Health adheres to HIPAA (Health Insurance Portability and Accountability Act) standards regarding the transmission of medical data, including authenticating users and encrypting transmissions.

Methods for receiving electronic data transmissions from IBM Watson Health

The methods listed below are used by IBM Watson Health to transmit data to a data recipient:

- **FTP Pull**
The FTP Pull option allows data recipients to pull PGP Encrypted data from an external IBM Watson Health server. Data recipients can retrieve files non-interactively through automated scripts via FTP, SFTP (SSH), and HTTPS. This process requires a data recipient user name and password to access ftp2.medstat.com. User accounts on ftp2.medstat.com have passwords that expire every 90 days.
- **FTP Push**
The FTP Push option transmits unencrypted and PGP-encrypted data from an internal IBM Watson Health server to the data recipient server. FTP Push uses Rebex on port 21 to accomplish the data transfer. This process may require changing the settings for the data recipient's firewall.
- **HTTPS Pull**
The HTTPS Pull option transmits data to a IBM Watson Health external server. This process requires a data recipient user name and password to access ftp2.medstat.com to retrieve the data via HTTPS through a web browser or a client. IBM Watson Health can supply MOVEit® Xfer to complete non-interactive HTTPS transfers. User accounts on ftp2.medstat.com have passwords that expire every 90 days.
- **SFTP Push**
The SFTP Push option transmits data from an internal IBM Watson Health server to the data recipient server. SFTP Push transfers use Rebex on port 22 to accomplish the data transfer (data recipient specific ports can also be specified). This process requires access to the recipient server for the IBM Watson Health internal FTP server.
- **SFTP Pull**
The SFTP Pull option allows data recipients to pull data from an external IBM Watson Health server. Data recipients can retrieve files non-interactively through automated scripts. This process requires a data recipient user name and password to access ftp2.medstat.com through a web browser or a client. IBM Watson Health supports SSH key authentication as well as username/password authentication. SFTP Push users with username/password authentication will be issued a temporary password, which must be changed upon successful login. Data suppliers using key authentication are required to provide IP addresses for filtering purposes, and they will **not** have passwords associated with their accounts.

Note

Passwords will expire every 90 days; users will receive a reminder **only** if they have requested an automated e-mail to notify them when their password is about to expire.

Table 4: Electronic data transmission method features

Feature	FTP Pull	FTP Push	HTTPS Pull	SFTP Push	SFTP Pull
File Encryption	✓ Required if protected health information is being transmitted	✓ Required if protected health information is being transmitted	✓ Supported	✓ Supported	✓ Supported
Transfer Method Encryption			✓	✓	✓
User Authentication	✓	✓	✓	✓	✓ Supported
Key Authentication					✓ Supported

Table 5: Electronic data transmission requirements

Requirement	Receiving data via FTP Pull	Receiving data via FTP Push	Receiving data via HTTPS Pull	Receiving data via SFTP Push	Receiving Data via SFTP Pull
Software	Standard FTP Client or Web Browser	Standard FTP Server	Web Browser or MOVEit® Xfer* with any HTTPS Client	Standard SFTP Server	Standard SFTP Client Browser
Hardware	N/A	N/A		N/A	N/A
Web Browser	Internet Explorer 6 or greater	N/A	Internet Explorer 6 or greater	N/A	N/A
File Size Limit	40 GB	40 GB	40 GB	40 GB	40 GB
Permissions	IBM Watson Health user account	IBM Watson Health write permissions on recipient server	IBM Watson Health user account	IBM Watson Health write permissions on recipient server	IBM Watson Health user account

* IBM Watson Health can supply MOVEit® Xfer to complete non-interactive HTTPS transfers.

Table 6: Physical media features and requirements

Feature	CD-ROM	DVD	USB External Hard Drive
Capacity	700 MB	4.3GB single layer or 8.5GB dual layer	500 GB up to 1.5 TB
Encryption Method	WinZip SDA	WinZip SDA	FIPS 140-2 certified encrypted drive
OS/Format	Windows, Mac	Windows, Mac	Any OS

Appendix A: sample Media Submission Form

No.

ID1 (Customer)

ID2 (Data Supplier)

Date Created

Tape # of

This form can be e-mailed. See instructions below.

Senders Name:

Senders Phone:

Senders Email:

IBM Watson Health Contact:

Media Submission Form

No.

Type of Media (select one or specify)

Select one... Specify:

Please ship media separate from submission form.

Your Company Name:

Who Data Belongs to:

Date Created:

Courier:

Tracking #:

File Information	File #1	File #2	File #3
Character Set (Select one)	Select one... <input type="text"/>	Select one... <input type="text"/>	Select one... <input type="text"/>
Encryption (Select one)	Select one... <input type="text"/>	Select one... <input type="text"/>	Select one... <input type="text"/>
*Password	<input type="text"/>	<input type="text"/>	<input type="text"/>
Dataset Name	<input type="text"/>	<input type="text"/>	<input type="text"/>
VOL-SER Number	<input type="text"/>	<input type="text"/>	<input type="text"/>
*Data Type (Select one, or specify)	Other (specify below) <input type="text"/>	Select one... <input type="text"/>	Select one... <input type="text"/>
Record Format (Select one)	Select one... <input type="text"/>	Select one... <input type="text"/>	Select one... <input type="text"/>
Record Length	<input type="text"/>	<input type="text"/>	<input type="text"/>
Total Record Count	<input type="text"/>	<input type="text"/>	<input type="text"/>
Total Net Payments	<input type="text"/>	<input type="text"/>	<input type="text"/>
*Time Period	<input type="text"/>	<input type="text"/>	<input type="text"/>

Instructions:

1. Use one form per media (Only one customer's data per media)
2. Use additional forms if media contains more than three files
3. Fill in information inside dotted line, cut out, and affix to media.
4. Address packaging and ship separate from media submission form
5. Complete remainder of media submission form
6. e-mail media submission form

Ship Media to:

Century Link

Attn. IBM Watson Health – MMT

14901 FAA Blvd.

Ft. Worth, TX 76155

Property of IBM

© Copyright IBM Corporation 2018

IBM Corporation
Software Group
Route 100
Somers, NY 10589

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Produced in the United States of America August 2018

IBM, the IBM logo, ibm.com, and Watson Health are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at: <https://ibm.com/legal/copytrade.shtml>

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The information in this document is provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others.

No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.