MedInsight New Hampshire Comprehensive Health Care Information System

Encryption/Hashing Methodology

April 12th, 2017

1301 Fifth Avenue, Suite 3800
Seattle, WA 98101 USA
Tel +1 206 624 7940 Fax +1 206 447 6909

milliman.com

Table of Contents

I. Purpose

The purpose of this document is to provide an overview of the process that data suppliers follow to submit data to Milliman for NH APCD and to provide insight regarding encrypted data elements in the NH APCD specification. With the support of the following specifications and the NH Pre-processor User Guide, any new data supplier entering the APCD will have the ability to encrypt personal health identifiers and securely transmit data to the APCD. Prior to reading this document the audience should have a basic understanding of the State's APCD rules and regulations, file formats, file types and element naming conventions.

II. Process of file submissions and processing

When a data supplier gets registered with NH APCD in order to start submitting data, they are provided with the NH Pre-processor tool/application. This application is used by all data suppliers to process their files before submitting them to Milliman. The application allows data suppliers to hash personal health identifiers contained in the file and securely transmit to Milliman and the APCD. Hashing details can be found in further sections of the document. Because data is hashed using the .NET version of SHA-512 hash algorithm and PHI fields are converted to a 128 character alpha-numeric sequence, there is no way for anyone at Milliman or the State to unhash this data. These hashed files that Milliman receives are then further encrypted before they are sent to the State as extracts. The following additional hashing and hiding of data is done for the Extracts:

1. For Consolidated, Limited Use, and Public Use Extracts: Member_ID is encrypted a second time.
2. For Consolidated, Limited Use, and Public Use Extracts: On claims where an abortion was performed, the Attending Provider and Billing Provider are set to NULL.
3. For Limited Use and Public Use Extracts: Group ID is encrypted so it cannot be used to identify individual patients.
4. For Public Use Extracts: The names of Provider who are Individuals are set to 'Provider Name Restricted'.
5. Certain Payers are excluded from Limited Use and/or Public Use Extracts (based upon a specific list of payers provided by NH DHHS: they are Medicare, Medicaid (including Managed Care/ MCO payers).

III. Encryption/Hashing methodology

The NH Pre-processor is used to hash ASCII files that contain health care claims data that are submitted to the state of New Hampshire, Department of Health and Human Services (DHHS). The utility encrypts the specified ASCII files, creating an output ASCII file and a zip file. Non-ASCII files are not supported.

The following section will describe the common fields to which the .NET version of SHA-512 hash algorithm is applied, the changes aligned to the file specifications, and the way in which each element is cleansed before applying the hash.

To clarify further, hashing is a form of cryptographic security which differs from encryption. Whereas encryption is a two-step process used to first encrypt and then decrypt a message, hashing condenses a message into an irreversible fixed-length value, or hash. Since the re-processor utility is hashing the data (not encrypting) the data cannot be un-hashed by anyone.

IV. Encrypted/Hashed Elements

Elements that require encryption are located within delimited positions in each file type laid out by the APCD rule. This requires each file to be parsed based on the state specification. The file specification for NH can be found here: http://www.gencourt.state.nh.us/rules/state_agencies/ins4000.html

Table 1. Encrypted APCD Field Names by File Type and Field Name

FIELD NAME	ELEMENTS BY FILE TYPE			
	ELIGIBILITY	MEDICAL CLAIMS	PHARMACY CLAIMS	DENTAL CLAIMS
Encrypted Subscriber Social Security Number	ME008	MC007	PC007	DC007
Encrypted Plan Specific Contract Number	ME009	MC008	PC008	DC008
Encrypted Member Suffix or Sequence Number	ME010	MC009	PC009	DC009
Encrypted Member Social Security Number	ME011	MC010	PC010	DC010
Encrypted Subscriber Last Name	ME101	MC101	PC101	DC101
Encrypted Subscriber First Name	ME102	MC102	PC102	DC102
Encrypted Subscriber Middle Initial	ME103	MC103	PC103	DC103
Encrypted Member Last Name	ME104	MC104	PC104	DC104
Encrypted Member First Name	ME105	MC105	PC105	DC105
Encrypted Member Middle Initial	ME106	MC106	PC106	DC106
Encrypted Carrier Plan Specific Contract Number or Subscriber/Member Social Security Number	NA	MC208	PC204	DC202

ME201 (Member Street Address) field is returned as blank or made null by the pre-processor irrespective of whether the field is populated or not.

In addition to this, the NH pre-processor performs the following validations when processing each data file:

- Files must be ASCII, text files, with * (asterisk) delimiters.
- Total records in trailer must match actual records submitted.
- Required fields must be submitted.
- Header and trailer records must be submitted.
- Header and trailer records must have correct values and correct number of fields.
- Payer code in header record must match payer code in trailer record.
- Reporting period in header and trailer records must match.
- Eligibility year/month value in data must fall within reporting period provided in header.
- Paid Date year/month value in data must fall within reporting period provided in header.
- Eligibility year/month value in data must fall within reporting period provided in trailer.
- Paid Date year/month value in data must fall within reporting period provided in trailer.
- Data records must have the correct number of fields.

- Social Security Numbers cannot be ‘999999999’ or ‘111111111’ or ‘222222222’ or ‘333333333’ or so forth.
- The first three digits of the social security number cannot be all zeroes.
- The data can be any ASCII character, with the following exceptions:
    - A field that contains one or more asterisks must be surrounded by double quotes.
    - Double quotes are not allowed in the data.

V. Encryption Technical Specifications

Once all the data elements have been cleansed and converted to uppercase as described in the previous section, the elements are then hashed using the .NET version of the SHA-512 hashing algorithm. Technical details regarding hash are as follows:

- Conversion – HEX (128)
- Storage – Hashed value is stored in uppercase.

A. Production Support

For support, please email NHCHISsupport@milliman.com