

Welcome to the first quarterly electronic New Hampshire Comprehensive Health Care Information System Newsletter. You will be notified through e-mail each time the newsletter is posted to www.nhchis.org. It will contain articles such as Current Processing Center Status, Data Collection Rule Clarifications and Processing Center Change Notifications.

GENERAL DATA RULE NOTES

Rule Differences

A number of differences between the NH and ME data collection rules have been identified and posted on the web site. One additional difference has been identified since the posting of those changes: **MC022A – Discharge Date** – is collected in the NH medical claims file. It is not collected in Maine.

Signs

We would like to draw your attention to formatting modifications that have been in the ME rule that do not appear in the NH Rule. The main example of this is the reference in the NH Rule to use both the + and – signs on all INT or Decimal fields.

First: The + sign is not required in any field that contains a positive number, using this value may actually cause issues if it is added to certain fields. Only the – (negative) sign is required on any field where a negative value is being reported.

Second: The only fields that contain true quantity values or dollar values need to have a sign applied. Report only the – (negative) sign. **Positive values must not contain a sign.**

Clarifications

We have received questions regarding the population of Bill Type (MC036) and Facility Type (MC037) fields. **Bill Type and Facility Type are mutually exclusive.** The Bill Type field should only be populated on facility claims (to refer to a paper claim, anything submitted on a UB-92 claim form). The Facility Type field should only be populated on Non-Facility Claims, primarily Professional claims (again, relative to a paper claim, anything

submitted on a HCFA-1500 claim form).

The Record Type (ME020, HD004, TR004) for Eligibility files should all be coded as ME. There is conflicting information in different parts of the rule. The correct value is ME. This is the primary reason eligibility files are failing the encryption process.

PHARMACY CLAIMS

Claims for prescriptions that are dispensed by a pharmacy or mail order facility and paid in part or in total by the carrier must be reported in the pharmacy claims submission.

There have been several questions about how to handle certain types of Pharmacy claims that may be processed in a Medical claim processing system when a member paying totally for the prescription and seeking reimbursement or because the drug was administered in a clinical setting. Below is a Rule Clarification with examples to guide you. If you have any questions, please contact us directly.

1. A prescription is purchased by the member at a Pharmacy and the member pays only the member liability. That claim should be sent in the Pharmacy claims submission regardless if the claim was processed by the PBM or by the carrier as a Medical Claim.
2. A prescription is purchased by the member at a Pharmacy and the member pays full price. Later the member sends the receipt to the carrier for reimbursement. If this claim is processed as a Medical claim and reimbursement is made directly to the member, the claim should be reported in the

(Continued on page 2)

In This Issue

Page 1 – General Data Rule Notes

Page 1 - Pharmacy Data Clarification

Page 2 – Data Submission Requirements – Examples

Page 3 – NCDMS – Current System Status

Page 4 - Web Encryption Information and Tips

Page 5 - Web Uploader Concerns; Key E-mail Addresses

(Continued from page 1)

Medical claims submission. Report the value "MEMREB" (without quotations) in the Provider fields (Number (MC024), TaxID (MC025), and Last Name (MC030)) and "DRUG" (without quotations) in the Principal Diagnosis (MC041) and Procedure Code (MC055) fields.

- 3) If a prescription drug was administered at a physician's office or Home Health Agency or similar clinical setting (usually these are injectable drugs identified with a HCPC beginning with the letter J) and the carrier processes these claims as medical claims, they should be reported in the medical claims file and the procedure code should be reported as the appropriate HCPC J-code. If these codes are being converted to a local carrier code then the local code should be reported in the procedure code field.

The basic rule to remember is that if the pharmacy or mail order facility is the recipient of the carrier's reimbursement then the claim should be reported in the Pharmacy Claims submission. If the member, a physician's office or other non-pharmacy agency is the recipient of the carrier's reimbursement then the claim should be reported in the Medical Claims submission.

NHCHIS INCLUSION DATA SUBMISSION REQUIREMENT CLARIFICATION

The MHIC has received many questions regarding what data should actually be included or excluded under the provisions of the New Hampshire Rule Chapter INS 4000. Follow the guidelines below to determine what data you should include and what data should be excluded from your data submission.

A payer (defined as Carrier and TPA) that does not meet the requirements for submission exclusion as defined in the New Hampshire Rule - Chapter Ins 4000 by premium level or membership level is required to submit data to the contracted entity. The requirement for exclusion for Carriers is less than \$250,000 in accident and health insurance premiums in New Hampshire on an annual basis and for TPA's is administrators of health insurance plans covering fewer than 200 New Hampshire lives in total.

Regardless of payer type (Carrier or TPA) the requirement for reporting data for both self-insured and fully insured business is based on the location of the policyholder. If the policyholder is a New Hampshire business or resident then the claims data must be reported for all persons covered under that policy, regardless of the residency of those persons.

In this case policyholder is considered to be the employer/business or individual that contracts directly with the payer to obtain Health Coverage Services.

Under this definition the following examples lists situations where the data would or would not be required in a data submission.

1. A local non-National NH employer contracts with a payer for Health benefits, but does have a few employees living in border states of ME and MA. All of the data for this employer's data must be submitted, including those employees and dependents living in ME and MA.
2. A National business headquarters is located in NH and contracts Health benefits/policies for all of its employees nationwide through the main office in NH. Again, all of this employer's data is required to be submitted, even for members living in CA, TX, AZ, etc. However, if sending in all of the data for these members is problematic for a payer (based on multiple processing systems/locations, etc), please contact us at nhinfo@ncdms.org with the details of your concerns.
3. A payer offers individual Health benefits to residents of NH and their families and/or directly to small businesses. All of the data for individuals and small businesses under the policy is required to be submitted.
4. Company A with its headquarters located in another state, (e.g. ME, AK) has chain stores/operations/employees in NH. Company A issues Health Care benefits/policies out of a location outside of NH. Under the current rule structure Company A's data is NOT required to be submitted for any of the covered lives including those with residency in NH.
5. Company B with its headquarters located in another state, (e.g. ME, AK) has chain stores/operations/employees in NH. Company B contracts for health benefits for its employees located in NH and/or other states. Any covered lives under such a policyholder are required to be submitted under the rule.

(Continued on page 3)

(Continued from page 2)

The above definition and examples are the same for both fully funded business and self-funded business at a payer. If you, as a payer, have a scenario with a policyholder that does not fit within one of the five examples above please contact us at: nhinfo@ncdms.org and we will determine if the data for said policyholder is required or exempt. We will also continue to add examples of new scenarios to this list over time.

NHCHIS CURRENT SYSTEM STATUS

For those of you that have been submitting data to the Maine Health Data Processing System you will find a different look and feel for this Web Site, but the functionality, except for the encryption program, is very similar. For those of you not familiar with the ME system, welcome aboard. In this article we will explore some of the enhancements that have been made and give you an idea of where we are in terms of Current Data Processing Center Status.

CURRENT CENTER STATUS:

- ◆ All who have registered and are required to submit data received a Welcome Email that contained your secure web site login and password and indicated that the first version of the new and improved web start encryption application was ready to be installed and tested.
- ◆ On Aug. 22nd the Center was open for testing and accepting test files from all of you. **Remember your test files should be a full three months of what would be normal production Data.** This gives us the ability to fully test the system with “live” data. If, at the end of testing, your data is verified as accepted/passed, we can mark this data as production data instead of test. This will reduce the volume and timeframe of data that you will need to submit starting October 1st.
- ◆ Also on Aug. 22nd for those of you that have this requirement your HEDIS and CAHPS production data was due to the Center. We have received and are reviewing with the State of New Hampshire these data sets for all of the payers that indicated they produce this data for NCQA.
- ◆ Overall we have registered over 70 payers, about half of which are currently required to submit data under the provisions of the rule.
- ◆ We will be open to receive “production” data for the first 8 months of 2005 on Oct 1st and will be continuing to shake down the system during the month of October while we process your files.

WHAT ARE SOME OF THE DIFFERENCES BETWEEN THE NH AND ME WEB PROCESSES?

- ◆ The major change that has been made in the Data Processing Center is that the encryption application is now a Web Start application instead of a Desktop application. There is an article in this newsletter that goes into much more detail about this new Web Start application.
- ◆ We have also made some changes to the different processing stages. Once a file has been uploaded to our system the PRELIM and LOAD processes are the same. We have moved and renamed the COMPLIANCE stage to DATA ANALYSIS and now this stage looks at every field within the record layout and calculates a rate for valid, invalid & missing. We have also added functionality to this section to account for payer specific data exemptions. The TRANSFORM stage (where we create value added information) has remained the same except some of the simpler functions (creating an AGE value from DOB) has been moved to the LOAD process. Finally, the EDITS process has been renamed to the DQ (Data Quality) process. The process itself remains very similar to the ME system (there are some checks that only apply to one state or another), we just felt the new stage name better identified what was actually being done during this step.
- ◆ Another change is that you will have Web access to not only a final error report for a file, but also to the Data Analysis process Frequency Report and the final DQ process Data Quality Report. **All of these reports will be viewable through our Report Viewer software. However, for the software to work properly across the Internet you MUST have the pop-up blocker option turned off in your web browser.**
- ◆ Also, for any given file, unless there is a system error that prevents the file from completely processing in a stage, we will process the entire file through the stage and will produce a final error report that will list the first 25 unique errors that are encountered in any one file. This will hopefully reduce some of the re-submissions that occur in the ME system because the processing within a stage is halted after an error is encountered in most cases.
- ◆ Lastly, as you have seen we have created a new higher Web level over the state Web Sites named www.ncdms.org. This stands for National Claims Data Management System as we have heard from other states that they are interested in also gathering this type of payer claims data.

NHCHIS WEB-START ENCRYPTION INFORMATION & TIPS

The encryption software is a Java Web-start application that uses one of the larger and stronger NIST (National Institute of Standards and Technology) cryptographic hash functions (SHA-512 algorithm). The application was created by the Maine Health Information Center (MHIC) specifically for the New Hampshire Comprehensive Health Information System (NHCHIS). It uses a one way hash on Subscriber SSN (ME008, MC007, PC007), Contract ID (ME009, MC008, PC008) and Member SSN (ME011, MC010, PC010) to protect a member's identity. In addition to encrypting, the Encryption software also performs rudimentary checks on the data such as number of fields in a record, number of records in the file (as identified in the header record), data within date range specified (also in header record) and the presence of the required data items.

What exactly will happen when you press the "Launch Encryption" button for the first time may vary depending on whether you have installed Sun's Java Runtime Environment (JRE) on your PC. If you have not, the application will first prepare the Java environment on your PC and then install. It may appear that the installer is done but nothing is happening after a few moments. If this happens check the task bar on your PC to see if a web-start button has appeared and a Java warning message is there. The Java warning message pertains to the signed jar that contains the encryption application. Clicking YES at this point will allow you to proceed with encryption but you will receive the same prompt each time the encryption software is run. Clicking NO will prevent the installation of the encryption software. By clicking ALWAYS you will be able to proceed with encryption and will not be prompted again.

[NHCHIS Encryption software Installation Instructions:](#)

1. From the secure NHCHIS page select "Encryption Software"
2. Click "Launch Encryption" (located below the NHCHIS logo)
3. Depending on how your browser handles Java Web-start .JNLP files you may get a message saying: "You have chosen to open encrypter.jnlp." Choose to open with JNLPFile (default).
4. You will get a security warning stating that the "... application is requesting unrestricted access to your local machine...Do you want to install and run: NCDMS Encryption Utility..." Click START to complete installation and run the encryptor.

5. After the second time the encryption software is run, you may be asked if you would like a desktop shortcut. You can do this if you wish.
6. Each time the encryptor is run, it will check automatically for updates.

[Running the NHCHIS Encryption Software:](#)

1. From the secure NHCHIS page select "Encryption Software"
2. Click "Launch Encryption" (located below the NHCHIS logo) Note that this is the same procedure for installation. If there is a new version of the encryption software OR a new version of Sun's JRE is needed, running the software will automatically handle these updates.
3. If you have not previously opted to always accept signed applications from the Maine Health Information Center (MHIC), you will be prompted by a security warning asking you if you'd like to do so. Clicking NO at this point will abort the encryption process. Clicking YES will accept the certificate and run this time (you will be prompted again next time). By clicking ALWAYS, you accept the certificate permanently and will not be asked again.
4. Once the NCDMS Encryption application is running, you will:
 - select the source file to encrypt.
 - select the destination directory for the encrypted file.
 - click the encrypt button

[Encryption Tips & Notes:](#)

1. One of the most important things to remember about the encryption software is that you MUST have write permissions to the directory that you have selected as your destination directory.
2. With the encryption software being a Web-start application with the ability to auto install/update to new versions we may be making modifications to the software over time. If you ever run the software and it notifies you that a newer version exists please make sure you accept the updates. Any updates on this nature will be tested and approved for release to either enhance the existing software or fix a newer diagnosed bug. One such enhancement that will be released shortly is the addition of a Web Browser Launch Button that will take you directly to the login page for the secure NHCHIS Web Page.

NHCHIS UPLOAD CONCERNS

We are sensitive to the privacy and security of your data files during the transfer process. If you are not comfortable using the Secure Web Upload process, you have the option of submitting data on a standard physical media type (CD/DVD). However, it would be more convenient for you and for us to receive these files electronically.

The secure web upload is currently the only electronic data transfer option that is offered. Without going into a long discussion, the SSL protocol that MHIC uses is the same one that banks and online vendors are using to safely transfer sensitive bank account and credit card information across the Internet. Your original delimited text file is compressed into a binary archive file by the same utility that encodes the sensitive fields (Employee SSN, Contract ID and Member SSN). It is then broken up into hundreds or thousands of packets which are encrypted and sent across the Internet by the Web file transfer application. Intercepting and decrypting a single packet would not yield readable text. In order to get readable text, it would be necessary to somehow intercept and decrypt all of the packets that make up the file, assemble them back into a complete compressed binary archive file, then bypass the password protection on the archive file to restore the original text file.

While no method of transferring data is completely safe, we feel that the risk of data being intercepted during the Secure Web transfer is no greater than the risk of it being intercepted during shipping or being intercepted from computer systems either before you send it or after we have received it.

If you are interested in using the Web file transfer, there are two things that you can/should do to make the transfer as secure as possible:

1. **Use the SSL certificate** to help you insure that the Web site you are connecting to is, in fact, the Web site that you are supposed to be connecting to. When connecting to the secure portion of the NCDMS web site (user services including encryption utility software download, data file upload, and data submission reports), you should see an icon of a locked golden padlock along the bottom of your browser window. By clicking on this icon, the certificate can be seen. Examine the certificate to make sure that the certified network address, organization name, and organization location are what they should be (secure.mhic.org, Maine Health Information Center Inc, Manchester, Maine, US) and that the certificate date range is valid. If this information is not valid, or if you see the icon of an unlocked

golden padlock along the bottom of your browser window, you should contact us before proceeding.

2. **Use the highest supported level of encryption.** There are two levels of encryption that are supported by the SSL standard (50-bit and 128-bit). Some Web browsers support only the lower level of encryption (50-bit). Our Web server supports higher level 128-bit encryption but will negotiate with the Web browser that is asking for a connection and will drop down to the lower level 50-bit encryption if that is all that your browser can support. The 128-bit encryption is significantly harder to crack than the 50-bit encryption. You can check this by clicking on the help option in Internet Explorer and going to the "about Internet Explorer" drop-down menu option. On the popup screen, there will be an entry titled "cipher strength" which will say either 50-bit or 128-bit. If your browser is using 50-bit encryption, you can download the 128-bit version of Internet Explorer for free from Microsoft.

KEY DATES:

- **OCTOBER 1—JANUARY-AUGUST 2005
DATA DUE**
- **OCTOBER 31—SEPTEMBER 2005
DATA DUE**

KEY E-MAIL ADDRESSES

- nhinfo@ncdms.org for general questions.
- WebAdmin@ncdms.org for questions or issues regarding the web site, including the data upload process and encryption software.
- nhdata@ncdms.org for questions, issues or the status of a data submission. This includes questions about submitting data via the web.

Editor: Adam J. Thebeau
Director of Health Information Systems
Maine Health Information Center