

Health Card Validation

Reference Manual

Health Card Validation Reference Manual

All possible measures are exerted to ensure accuracy of the contents of this manual; however, the manual may contain typographical or printing errors. The public is cautioned against complete reliance upon the contents hereof without confirming the accuracy and currency of the information contained herein. The Crown in Right of Ontario, as represented by the Ministry of Health and Long-Term Care, assumes no responsibility for any person's use of the material herein or any costs or damages associated with such use.

Ministry of Health and Long-Term Care
Registration and Claims Branch

January 2006

TABLE OF CONTENTS

SECTION 1:	INTRODUCTION
About This Manual	1-1
Health Card	1-2
Version Code	1-3
Health Card Validation	1-3
Benefits of HCV	1-3
Validation Process	1-4
Validating for Specific Services	1-4
Access Options.....	1-5
Interactive Voice Response.....	1-6
Overnight Batch Eligibility Check.....	1-7
Health Card Reader.....	1-7
Health Number Release	1-9
SECTION 2:	TECHNICAL
Specifications	2-1
General Message Formats.....	2-1
IVR Technical Requirements.....	2-2
OBEC Technical Requirements.....	2-2
OBEC Input Transaction.....	2-2
OBEC Output Transaction.....	2-4
Datapac Technical Requirements	2-5
Datapac Procedures.....	2-6
Data Specification Input Transaction.....	2-10
Data Specification Output Transaction.....	2-11
TCP/IP Technical Requirements.....	2-12
TCP/IP Data Specifications	2-13
TCP/IP Socket Troubleshooting.....	2-14
IMS Connect Information	2-15
TCP/IP Input Transaction	2-20
TCP/IP Output Transaction.....	2-21

SECTION 3:

HELP

Help Desk..... 3-1
 Resources Access Control Facility - Password..... 3-2
 Password Guidelines 3-2
 Datapac Password Help 3-3
 Testing with the Ministry 3-4

SECTION 4:

APPENDICES

Appendix A – Response Codes 4-1
 Appendix B – IVR Operating Instructions..... 4-11
 Appendix C – Magnetic Strip..... 4-26
 Appendix D – Frequently Asked Questions 4-29
 Appendix E – Glossary 4-31

INTRODUCTION

1

SECTION 1

INTRODUCTION

About This Manual

The Ministry of Health and Long-Term Care (MOHLTC) Health Card Validation (HCV) system allows health care providers to validate the eligibility of the cardholder and the status of his or her health card and version code.

This manual is intended to provide the user with adequate information to select, develop and use the system including:

- an overview of HCV
- an overview of current HCV options
- technical specifications and data specifications/file layout
- user information

Section 1 – Introduction provides:

- an understanding of HCV, the benefits and the process
- a non-technical overview and description of the HCV options currently available

NOTE: *Each option should be reviewed and considered in context with the health provider or facility's business needs. Once an option is chosen, the reader should move to the appropriate sub-section in Section 2 – Technical to review the technical requirements and file layouts.*

Section 2 – Technical provides:

- technical information
- data specifications/file layout

Section 3 – Help provides:

- how to access help
- password information
- user ID information

Section 4 – Appendices provides:

- response codes
- Interactive Voice Response (IVR) operating instructions
- frequently asked questions
- glossary of terms

Health Card

Each eligible resident in the province of Ontario is registered for the Ontario Health Insurance Plan (OHIP) and is provided with a 10-digit health number and version code. A health card is provided to the insured person for the purpose of obtaining insured health services in Ontario. An insured person presents their health card at each visit to a health care provider.

There are 4 variations of the Ontario health card in circulation. All magnetic striped health cards contain the unique 10-digit lifetime identification number assigned to all eligible Ontario residents. It should be noted that all of the following health card types are acceptable.



Photo Health Card:

A plasticized green health card depicting a Trillium and bearing the insured person's name, 10-digit personal health number, version code, date of birth, gender and card's issue and expiry date. This card displays the person's photo and signature unless a photo and signature exemption has been granted or the person is under 16 years of age.



Original Red and White Health Card:

A plasticized red and white health card displaying the insured person's name, 10-digit personal health number and version code if applicable.



Health Card 65:

A plasticized red and white health card for persons 65 years or older, displaying the insured person's name, 10-digit personal health number and version code if applicable. The number 65 is displayed on the card beside the words Health Santé.

Version Code

Some original red and white health cards do not have a version code. Version codes were introduced to uniquely identify a health card and allow the ministry to verify the status of a health card, thus reducing fraud opportunities. When a new health card is required, a replacement card is issued to the insured person with the same health number and a new version code. A different version code will be assigned for any subsequent card issued.

Health Card Validation

The Health Card Validation (HCV) system enables hospitals, physicians or other health care providers to validate a health card when presented at the time or point of service. The validation transaction checks the status and validity of the 10-digit health number presented and the individual's eligibility for health care coverage. This service is available 24 hours a day, 7 days a week with scheduled downtime for maintenance every second Sunday of the month between 5:00 am and 8:00 am.

Benefits of HCV

Validation responses provide decision-making information at the time of service and allow a health care provider to:

- reduce claim rejects by ensuring a client is eligible for service prior to service delivery
- reduce claim rejects associated with incorrect version codes
- reduce administrative costs by allowing health care providers to bill clients at the time of service where applicable
- reduce health care fraud by eliminating service to ineligible clients and by visually confirming HCV response information with client at the point of service (e.g., gender, date of birth)

Health Card Validation (Continued)

Validation Process

Health number identification information is transmitted to the ministry when an HCV service is accessed at the point of service. The health card number or the information contained on the magnetic stripe on a health card are transmitted to the ministry mainframe via an approved and authorized HCV method. Additional information sent in the registration identifies the sender and the sender's physical location.

The validation process consists of edit checks to ensure:

- a valid health card
- a valid 10-digit health number that has been issued by the ministry
- the health number presented belongs to a registrant who is eligible for health care in the province of Ontario
- the card is current by checking the version code

If the number is determined to be invalid or the registrant is not eligible, appropriate response codes will be returned indicating the reason why the card/number has been rejected (refer to *Appendix A – Response Codes*).

NOTE: *Validation checks eligibility and validates the health card/number but does not guarantee payment of the claim.*

Validating for Specific Services

Specific regulations and limits apply to some services such as oculo-visual assessments. Validating for these services must be performed through Interactive Voice Response (IVR). The response returned will include date-of-service (DOS) information (refer to *Appendix B – IVR Operating Instructions*).

Access Options

Currently, there are three options available for accessing HCV – Interactive Voice Response (IVR), Overnight Batch Eligibility Check (OBEC) and Health Card Reader (HCR). Health care providers may review each of the options to determine the most appropriate option to meet their needs based on current business practices and technical capability.

NOTE: *In addition to the HCV options as noted above, the ministry provides a Health Number Release option for situations where a client has forgotten to bring their health card to their appointment or have misplaced their card. Details regarding Health Number Release are included following the HCV options in this section of the manual.*

The ministry strongly recommends that all HCV users register for IVR along with any other HCV access method. IVR will act as a backup method for HCV in the event the chosen access method is unavailable.

Along with HCV service the IVR method also has a Bulletin Board service available. The Bulletin Board provides information to registered IVR users regarding scheduled system downtime, and/or periodic updates in the event of prolonged periods of unavailability (refer to *Appendix B – IVR Operating Instructions*).

Each of the HCV options has a corresponding communication determining how it connects with the ministry mainframe to complete a transaction (refer to *Section 2 – Technical* for data specifications), such as:

- IVR uses a telephone line
- OBEC uses Electronic Data Transfer (EDT) protocol via a long-distance direct dial telephone call or through a Bell Canada Datapac line or TCP/IP
- HCR Software Application Solution uses Bell Datapac or TCP/IP
- HCR Point of Service option uses a Bell Datapac line

EDT/HCV Help Desk staff are available to answer questions regarding HCV options and any other information contained in this manual.

To contact the EDT/HCV Help Desk, call 1 800 262-6524.

Access Options (Continued)

1. Interactive Voice Response

The Interactive Voice Response (IVR) HCV method allows registered health care providers and facilities to validate health cards in real-time by using a touch-tone telephone and the ministry toll-free service. Real-time interaction allows validation of health cards with appropriate ministry databases. An eligible health care provider or facility may register to become an authorized user of IVR by contacting the EDT/HCV Help Desk (1 800 262-6524).

The following information is returned:

- response code
- gender
- date of birth
- first 3 characters of the last name
- fee schedule code service response code (if applicable)
- date of service (if applicable)

IVR is well suited for low-volume users (less than 40 transactions per day) or remote locations/clinics.

The ministry strongly recommends that all health care providers register for IVR along with other HCV access options to ensure a backup validation method is available (refer to *Appendix B – IVR Operating Instructions*).

Access Options (Continued)

2. Overnight Batch Eligibility Check

The Overnight Batch Eligibility Check (OBEC) method allows registered health care providers and facilities to validate health cards by collecting and batching health numbers in a formatted file prior to service delivery. Batches are electronically transmitted over a ministry approved Electronic Data Transfer (EDT) protocol to the ministry.

Batches submitted by 4:00 pm each day and the resulting validation information is returned electronically by 7:00 am the following day. The following information is provided in the return response:

- response code
- gender
- date of birth
- up to 20 characters of the first name
- up to 30 characters of the last name

A health care provider or facility may register to become an authorized user of EDT and OBEC by contacting the EDT/HCV Help Desk (1 800 262-6524).

OBEC is well suited in clinics to check the next day's scheduled appointments where patients are referred, are coming from out-of-town, or for a patient who has had claims rejected in the past.

The ministry recommends that all health care providers register for IVR along with OBEC to ensure a backup validation method is available (refer to *Section 2 – Technical*).

3. Health Card Reader

There are two Health Card Reader (HCR) methods currently available – Software Application Solution or Point of Service Device (POS).

The following information is provided in the return response for either validation method:

- response code
- gender
- date of birth
- up to 20 characters of the first name
- up to 30 characters of the last name
- other information as defined in the software application

Access Options (Continued)

HCR – Option 1

Software Application Solution

Software Application Solutions can be purchased from an HCV solution developer or an application may be developed within your organization. The application is installed onto a computer and a card-swipe wedge may be attached to the computer. At the point of service, the health card is swiped/keyed using the wedge and a real-time transaction is performed over an approved telecommunication protocol to validate a health card against appropriate ministry databases.

An eligible health care provider or facility may register with the ministry for access to HCV via a Software Application Solution by contacting the EDT/HCV Help Desk (1 800 262-6524). The Software Application Solution is well suited for high-volume users.

The ministry strongly recommends that all health care providers register for IVR along with the HCR Software Application Solution to ensure a backup validation method is available.

HCR – Option 2

Point of Service Device

A Point of Service (POS) device is a stand-alone machine similar to those used by retail stores for Interac and credit card transactions. At the point of service, the health card is swiped/keyed using the device and a real-time transaction is performed over Bell Datapac to validate a health card against appropriate ministry databases.

An eligible health care provider or facility may register to become an authorized user of POS by contacting the EDT/HCV Help Desk (1 800 262-6524).

POS devices connect to HCV services via Datapac (refer to *Section 2 – Technical* for specific Datapac technical information). The ministry does not supply POS devices. The EDT/HCV Help Desk staff can provide information regarding POS device vendors. POS is well suited for moderate-volume users (more than 40 and less than 80 transactions per day).

The ministry strongly recommends that all health care providers register for IVR along with POS to ensure a backup validation method is available.

Health Number Release

The Health Number Release (form 1265-84) allows registered health care providers and facilities access to a client's health number and version code if a client cannot produce a health card. In most cases, the client has forgotten to bring their health card to their appointment or has misplaced their card.

In order for the ministry to release health card information, to the provider or facility, the client must provide consent. Consent is obtained through the Health Number Release form.

The Health Number Release form must be completed by the health care provider or facility providing the service and must be signed by the client. When completed and signed, the form provides consent to the ministry to release the health card number and version code to the health care provider or facility that has completed the form.

The completed form must be mailed or delivered in person to your local ministry office for processing. Faxes **are not** accepted. Once processed, the response is mailed back to the health care provider or facility.

Copies of the *Health Number Release* form may be obtained from your local ministry office or printed via the ministry website at:

http://www.health.gov.on.ca/english/public/forms/form_menus/ohip_fm.html

An accelerated process for the release of a health number/version code is also available. Only authorized and specified emergency services and departments have access to this service. Please refer to your organization's policy and/or administration to determine if this service is available in your organization and to obtain the procedure and Personal Identification Number (PIN).

TECHNICAL

2

SECTION 2:

TECHNICAL

Specifications

Data specifications describe the way in which information **must** be presented in order for collected data to be used to verify health number information contained on the ministry mainframe. Data specifications are very technical and are intended to be used by a computer programmer to develop a user-friendly application to allow the logon, password and data collection required for the HCV process.

The ministry does not develop or support HCV applications. Data specifications are provided for a programmer to develop an application that meets the data specification requirements. A user instruction manual may be written by the software developer to describe the application and provide step-by-step user instructions.

Vendors and/or other health care providers and facilities may have developed applications for the HCV process. New HCV users may wish to use an application that has been developed, tested and in use by another health care provider. In this instance, new HCV users are encouraged to contact colleagues, professional associations or other health care providers regarding vendors and/or applications available for HCV.

The following technical specifications, with the exception of IVR, are intended to be used by a computer programmer to develop a compatible HCV application.

General Message Formats

- Both keyed and swiped transactions are supported.
- Health number/version code fields must be blank for card swipe transactions.
- Magnetic stripe fields must be blank for keyed transactions.
- All fields must be transmitted to the host.
- All fields are considered MANDATORY unless noted to be OPTIONAL.
- MANDATORY fields are subject to audit.
- Fields marked as OPTIONAL are not required for successful processing and must contain spaces if the desired information is unavailable.
- Date format is always YYYYMMDD.
- All data must be left justified.
- Input message character data may be either upper or lower case.
- Output message character data is returned in upper case only.

IVR Technical Requirements

The following equipment and service are required to participate in IVR:

- standard residential or business telephone line
- touch tone service
- touch tone telephone
- cellular telephones are **not** permitted for use with IVR for security reasons

IVR is provided through toll-free telephone access.

OBEC Technical Requirements

Electronic Data Transfer (EDT) service is a vehicle for the electronic transmission of OBEC files from your computer to the ministry's mainframe computer.

EDT has specific technical requirements and is accessed either via a long distance direct dial telephone call, through Bell Canada Datapac lines, or TCP/IP. EDT uses a private network.

Further EDT information is available on the ministry website at: www.health.gov.on.ca.

OBEC Input Transaction

Input Filenames

OBEC filenames should follow the standard DOS filename conventions, of one-to-eight characters followed by a file type of one-to-three characters. Naming standards for OBEC submissions are listed below and are recommendations only. Other naming conventions will be accepted and processed.

- OBECzxxx.ttt
- Where "OBEC" is a constant to identify the file as an OBEC request
- Where "z" is A or E as follows:
 - To receive a response file containing one record for each record submitted, files submitted should be named OBEC A xxx.ttt (**A for All**)
 - To receive a response containing only those Health Number/version codes that generate a response code other than "50" (Card Passed Validation), files submitted should be named OBEC E xxx.ttt (**E for Exceptions**)
- Where "xxx" is any valid alphabetic or numeric characters or can be omitted
- Where "ttt" is DAT or TXT for normal text (ASCII) files

OBEC Technical Requirements (Continued)

OBEC Input Transaction (Continued)

*Optional Fields

Description	Start	End	Length	Notes
Transaction Code	01	06	06	Must be OBEC01
Health Number	07	16	10	
Version Code	17	18	02	Where there is no version code, spaces should occupy this field
Submission Identifier *	19	22	04	<p>Provided to allow submission records to be identified by information meaningful to the submitter (e.g., department, physician, day, and am/pm)</p> <p>Can be padded with spaces or the record can end after column 18</p>
Postal Code *	23	28	06	User can choose to send the ministry the verified address that it has for the patient, etc.
Municipality*	29	58	30	<p>NOTE: Currently, this information is only stored. At some later date the ministry will use this information to initiate the address change process.</p>
Street Address line 1 *	59	90	32	
Street Address line 2 *	91	122	32	Can be padded with spaces or the record can end after column 18

Processing Rules

- There must be a carriage return/line feed indicator at the end of each record. Also the end of a file must be indicated by CTRL Z (i.e., hex value of 1A).
- If a health number appears more than once in a submission file, only the first occurrence will be processed.
- Invalid transaction codes and non-numeric health numbers will not be processed and will not generate a response record.
- Submission files with no valid records will generate a response file containing no records.

OBEC Technical Requirements (Continued)

OBEC Output Transaction

Output Filenames

The OBEC response file is sent to the EDT INBOX of the user ID who submitted the OBEC request. The file name for this file is RESPONSE.TXT.

The file subjects are: IN: nnnn CHECKED: nnnn OK: nnnn

- “IN” represents the number of records in the submission file
- “CHECKED” represents the number of records processed based on the processing rules
- “OK” represents the number of records resulting in a response code of “50” (Card Passed Validation)

Response files not downloaded expire in 7 days from the date sent and will be deleted.

Description	Start	End	Length	Notes
Health Number	01	10	10	Output as received on input
Version Code	11	12	02	Output as received on input
Response code	13	14	02	Values found in <i>Appendix A–Response Codes</i> At a minimum, the Response Code numbers provided in Appendix A must be echoed to the client for troubleshooting purposes.
Submission Identifier	15	18	04	As provided in the submission
Gender Code	19	19	01	Values are M or F Values represent the data as retained on the MOH database and are provided only when response codes are 50 – 59 inclusive
Birth Date	20	27	08	Values represent the data as retained on the ministry database and are provided only when response codes are 50 – 59 inclusive
Expiry Date	28	35	08	
Last Name	36	65	30	
First Name	66	85	20	
Second Name	86	105	20	
Reserved for MOH use	106	207	102	Reserved for MOH use

Datapac Technical Requirements - for use with HCR Option 1

Datapac is a public data communications network offered through Bell Datapac. It is similar to the long distance telephone network used for voice calls but is designed specifically for data communications. The HCR Software Application Solution and Point of Service options can utilize Datapac for HCV access.

Access to the network is on a “dial-up” basis using your regular telephone line and modem for communication needs that are occasional or intermittent.

Datapac is a usage-sensitive network with two basic billing components – time and data usage. Time is billed by the minute for dial-up access. Data usage is billed by mileage and is based on the amount of data transmitted.

There is a one-time service charge for the installation of new access lines or changes to existing lines.

Please contact a Bell Datapac sales representative for more information or call toll-free 1 800 267-6574.

NOTE: *The ministry is not responsible for Bell Datapac services, costs, changes or discontinuance of any service. Arrangements and/or contracts for Bell Datapac are directly between the user and Bell Datapac.*

Datapac Procedures

The following instructions are for use in developing the client access portion of the application used to access HCV over Datapac and are valid for Datapac only.

Conventions used in these instructions:

Terminal Attribute	Terminal Action/Output
<u>Underline</u>	<u>Computer input</u>
<CR>	Terminal carriage return
Bold	Computer output
Lower case alpha	Variable data

Instructions

Communication parameters are asynchronous half duplex, 7 data bits, 1 stop bit, even or odd parity.

Step 1

- Dial or connect to Datapac
- **Key two periods .. followed by <CR>**
e.g., ..<CR>

Response screen will display:

DATAPAC:nnn nnn

(nnn nnn will be eight digits), followed by the hexadecimal string:
2020 0D0A 0000

Step 2

- **Key word NUI <space>**
- **Key your Datapac Network User Identifier (NUI) followed by <CR>**
e.g., NUI ididid<CR>

Response screen will display:

Datapac Password
XXXXXXXX

Datapac Procedures (Continued)

Instructions (Continued)

Step 3

- **Key your NUI Password followed by <CR>**

Response Screen will display:

Datapac: Network User Identifier ididid Active

(If you do not receive this message, repeat steps 2 and 3.)

Step 4

- **Key the network address: 25900365 followed by <CR>**

Response screen will display:

**MANAGEMENT BOARD SECRETARIAT ONTARIO
GOVERNMENT NETWORK**

FOR NETWORK INFORMATION CALL:

CTS SERVICE DESK

(416)327-3900

ENTER APPLICATION LOGON –

NOTE: *The final hyphen(-) is followed by an ASCII space (0x20).*

Step 5

- **Key the application logon string**
 - **for production environment: KIMS followed by <CR>**
 - **for test environment: IMSDVH followed by <CR>**

Response screen will display:

DFS20002 HH:MM:SS TERMINAL

CONNECTED TO IMS IMSP 2020 2020 200A

(2020 2020 200A represents the hexadecimal string that represents
5 ASCII spaces and a line feed)

Datapac Procedures (Continued)

Instructions (Continued)**Step 6**

- **Key your ID and password followed by <CR>**
e.g., /SIGN idxxxx password <CR>

Response screen will display:

DFS058I 10:01:19 SIGN

COMMAND COMPLETED

(will be followed by an ASCII online feed of 0X0A:)

Transactions may now be entered in accordance with the Datapac data specification contained on the following pages. All validation responses are terminated by an ASCII carriage return (0x0D).

Step 7

If a new password is either desired or mandated by the Host, the following command must be sent at the /SIGN screen prompt:

- **Key your userid password NEWPW new password followed by <CR>**

You may encounter the following messages. Call the EDT/HCV Help Desk for assistance, if necessary.

Message	Definition
DFS2470/SIGN COMMAND	Sign command required
DFS2467I/SIGN COMMAND REJECTED SYNTAX ERROR	Syntax error
DFS2467I/SIGN COMMAND REJECTED NEWPWD INVALID	Invalid New Password
DFS2467I/SIGN COMMAND REJECTED PASSWRD NOT DEF	Password Invalid
DFS2467I/SIGN COMMAND REJECTED PASSWRD EXPIRED	Password Modification Prompt

Datapac Procedures (Continued)

Instructions (Continued)

Step 8

To disconnect: /RCL

- **<CR>**

Response screen will display:

**DFS0581 11:19:40 RCLSDST
COMMAND COMPLETED**

Followed by:

**CALL CLEARED:DTE-Cleared by
other end:0 - No more information**

NOTE: *Disconnect from Datapac as necessary.*

Data Specification Input Transaction

*Optional fields

Description	Start	End	Length	Notes
Transaction Code	01	09	09	Enter RPVR0300 followed by a space
Health Number	10	19	10	Must be provided for a keyed transaction and omitted for a swiped transaction
Version Code	20	21	02	Must be provided for a keyed transaction and omitted for a swiped transaction
MOH User ID	22	29	08	Authorization ID (HECSnnnn) issued by the ministry In the case of a network host, this will be the same for all of the networked sites
EITHER MOH Facility ID	30	36	07	Represents the ministry issued facility or provider number At least one of these fields must be present on all transactions
OR MOH Provider ID	37	46	10	Data must be left justified and, if necessary, padded with spaces
Local User ID	47	54	08	In the case where a client is routing through another facility, the ministry assigned ID # to the client will be used (HCNP # # # #) For a single hospital or provider, this will be the ID assigned by the ministry (HECS # # # #)
Local Device ID*	55	62	08	May identify where the transaction came from within a facility (e.g., Emergency Department)
Client Text*	63	82	20	Echoed back unedited and unchanged Recommended that the field include a unique identifier assigned to each transaction to facilitate message sequencing
<i>Magnetic Stripe</i> (refer to Appendix C – Magnetic Stripe)				
Track 1	83	161	79	Mandatory for a card swipe transaction
Track 2	162	201	40	Ontario health cards conform to ISO 7811/12 Data must be left justified and, if necessary, padded with spaces

Data Specification Output Transaction

Description	Start	End	Length	Notes
Transaction Code	01	09	09	Copied from input transaction
Local User ID	10	17	08	Copied from input transaction
Local Device ID	18	25	08	Copied from input transaction
Health Number	26	35	10	Output as received on input If magnetic stripes are submitted, the health number and version codes are extracted therefrom
Version Code	36	37	02	Output as received on input. If magnetic stripes are submitted, the health number and version codes are extracted therefrom
Response Code	38	39	02	Values may be found in <i>Appendix A – Response Codes</i> At a minimum, the Response Code numbers provided in Appendix A must be echoed to the client for troubleshooting purposes
Gender Code	40	40	01	Values are M or F Values represent the data as retained on the ministry database
Birth Date	41	48	08	Values represent the data as retained on the ministry database
Expiry Date	49	56	08	Values represent the data as retained on the ministry database
Client Text	57	76	20	Output as received on input
Last Name	77	106	30	
First Name	107	126	20	
Second Name	127	146	20	
Redundant Response Code	147	148	02	Available for message delivery verification
Carriage Return	149	149	01	Indicates the end of the output message

TCP/IP Technical Requirements - for use with HCR Option 1

Note to Programmers

IMS Connect vs. IMS Listener

Previous versions of the HCV Technical Specification have included instructions for connection to ministry applications through IMS Listener. The ministry has upgraded the connection software to IMS Connect. All new developments are to be written to the IMS Connect technical specification as included in this manual.

It is recommended that existing applications be upgraded to conform to the IMS Connect technical specifications as the IMS Listener technology will be phased out.

The primary differences between IMS Connect and Listener are in throughput and security. The benefits of IMS Connect are:

- Faster throughput
- Enhanced security

From the client point of view, the main differences are:

- IRM header vs. TRM header
- Reading the response should begin at a different offset than the Listener specification
- Response information unchanged

Overall, program changes are minimal and straightforward.

Password Information

Client systems should not perform edits on input passwords that are sensitive to the published rules (e.g., minimum length), and must provide a facility for manually entering any arbitrary password value. Failure to do so will likely render a client system unusable at some point in time.

For further information on User IDs and Passwords, refer to *Section 3 – Help*.

TCP/IP Data Specifications

The following instructions are for use in developing the client access portion of the application used to access the HCV service using TCP/IP over the integrated network.

TCP/IP Client Access Instructions for IMS Connect

NOTE: *To be used in conjunction with the TCP/IP Data Specifications on the following pages.*

Every transaction message begins with an IRM header segment and ends with an EOM segment.

The validation message includes the Input Transaction, whereas the other two (User ID/Password Authentication and Password Change) do not.

Step		Description
1	Socket	Obtain a socket descriptor
2	Connect	Request connection to host address Specific host name/URL to be provided during conformance testing process
3	Write	Fill a character buffer with (in sequence): <ol style="list-style-type: none"> 1. the appropriate IRM header¹, 2. the input transaction record (if required)²; 3. the EOM segment. Send the contents of the buffer <i>as a single write</i> .
4	Read	Receive response: <ul style="list-style-type: none"> ▪ If a Request Status Message (RSM) is returned it means the submission was rejected, or you have used Data Specification 1 or 2, which only return RSM responses (refer to <i>Appendix A – Response Codes</i>) ▪ If an HCV Output Transaction is returned, process as you desire ▪ If a CSM message is received, all available output has been received ▪ If an EOM message is received, output may have been discarded - go to step 8
5	Repeat	IDENTIFIED VOLUME USERS <i>ONLY</i> : repeat process starting at step 3
6	Close	Terminate connection and release socket resources

¹ "Check the Validity of the User ID" "Change the Password of the User ID" or "send a Regular Validation Transaction".

² Input transactions required only when a Validation request is being submitted.

TCP/IP Socket Troubleshooting

Refer to the steps below before contacting EDT/HCV Help Desk for assistance.

The first troubleshooting step should always be to ensure that the transaction data has been assembled correctly by referring to the IRM Header and Input Data Specification – ensure all fields are of correct width and are correctly ordered. Some troubleshooting steps are outlined below for steps 1, 2, and 4 of the TCP/IP Client Access for IMS Connect Data Specification.

Step	Symptom	Items to Check	Follow-up
1. Socket	Unable to initialize socket	Ensure: <ul style="list-style-type: none"> ▪ development environment supports sockets ▪ required libraries and modules are available in your runtime environment 	<ul style="list-style-type: none"> ▪ Address further questions to vendor of development environment
2. Connect	Host connection fails	Ensure: <ul style="list-style-type: none"> ▪ client machine has active network connection ▪ host address and port are correctly set ▪ host is responding (<i>ping</i>) 	<ul style="list-style-type: none"> ▪ Contact your local system administrator ▪ If client machine has active connection, and host parameters are correctly set, but <i>ping</i> still fails, call 10.5 ▪ Help Desk
	Host connection rejected ¹	Ensure: <ul style="list-style-type: none"> ▪ user ID and password entered correctly, and that password has not expired² 	<ul style="list-style-type: none"> ▪ Change password, continue ▪ If problem persists call EDT/HCV Help Desk
4. Read	Return message appears to be nonsense	Ensure: <ul style="list-style-type: none"> ▪ output record is being parsed correctly ▪ correct character set is being used (IMS Connect sends and receives ASCII characters) ▪ read buffer correctly initialized between read calls 	<ul style="list-style-type: none"> ▪ Ensure that client application always tests type of return record
	Validation returns a response code greater than 90 indicating system problems	<ul style="list-style-type: none"> ▪ refer to description in <i>Appendix A – Response Codes</i> 	

¹ If connection is rejected, host returns a 20-byte Request Status Message (RSM), documenting the source of failure. Ensure that RSMRetCode is set to “8” then evaluate the RSMReasCode to determine the source of the error.

² An expired password causes RSMReasCode “105”.

IMS Connect Information

1. Check the Validity of the User ID: Information Management System (IMS) Request Message (IRM)

Description	Length	Notes
IRMLLLL	4 Bytes	Set to x'00000034' (decimal 52)
IRMLen	2 Bytes	Set to x'002C' (decimal 44)
IRMRsv	2 Bytes	Set to x'0000' (decimal zero)
IRMIId	8 Bytes	*HCVREQ*
IRMTrnCod	8 Bytes	&&PWDCHK
IRMUsrID	8 Bytes	User ID assigned by Ministry of Health and Long-Term Care
IRMRsv2	8 Bytes	' ' (8 blanks)
IRMPassw	8 Bytes	Password for the User ID above

IMS Connect Information (Continued)

2. Change the Password of the User ID: IMS Request Message (IRM)

Description	Length	Notes
IRMLLLL	4 Bytes	Set to x'00000044' (decimal 68)
IRMLen	2 Bytes	Set to x'003C' (decimal 60)
IRMRsv	2 Bytes	Set to x'0000' (decimal zero)
IRMIId	8 Bytes	*HCVREQ*
IRMTrnCod	8 Bytes	&&PWDCHG
IRMUsrID	8 Bytes	User ID assigned by ministry
IRMRsv2	8 Bytes	' ' (8 blanks)
IRMPassw	8 Bytes	Password for the User ID above
IRMNewPW	8 Bytes	A new password that is either desired or mandated by the host
IRMNwPwC	8 Bytes	A confirmation of the new password

NOTE: For information on User IDs and Passwords refer to Section 3 – Help.

IMS Connect Information (Continued)

3. Send a Regular Validation Transaction: IMS Request Message (IRM)

Description	Length	Notes
IRMLLLL	4 Bytes	Set to x'00000101' (decimal 257)
IRMLen	2 Bytes	Set to x'002C' (decimal 44)
IRMRsv	2 Bytes	Set to x'0000' (decimal zero)
IRMId	8 Bytes	*HCVREQ*
IRMTrnCod	8 Bytes	RPVR0300
IRMUsrID	8 Bytes	User ID assigned by Ministry of Health and Long-Term Care
IRMRsv2	8 Bytes	' ' (8 blanks)
IRMPassw	8 Bytes	Password for the User ID above

IMS Connect Information (Continued)

4. End of Message Segment (EOM):

Description	Length	Notes
EOMLen	2 Bytes	Set to x'0004' decimal 4
EOMRsv	2 Bytes	Reserved (x'0000')

5. Completion Status Message (CSM):

Description	Length	Notes
CSMLen	2 Bytes	Will be x'000C' decimal 12
CSMRsv	2 Bytes	Reserved (x'0000')
CSMId	8 Bytes	'*CSMOKY*'

6. Request-Status Message (RSM):

Description	Length	Notes
RSMLen	2 Bytes	Will be x'0014' decimal 20
RSMRsv	2 Bytes	Reserved (x'0000')
RSMId	8 Bytes	'*REQSTS*'
RSMRetCod	4 Bytes	RSM Return Code*
RSMRsnCod	4 Bytes	RSM Reason Code*

If RSMRetCod has been set to 4, the RSMRsnCod may have the following values:

Info #200 The password has been successfully changed. This is only returned in response to a transaction of "&&PWDCHG".

Info #201 Successful sign-on (User ID and password are good). This is only returned in response to a transaction of "&&PWDCHK".

IMS Connect Information (Continued)

If RSMRetCod has been set to 8, the RSMRsnCod may have the following values:

Error #1	The transaction was not defined to IMS Connect.
Error #2	An IMS error occurred and the transaction was unable to be started.
Error #3	The transaction failed to perform TAKESOCKET call within the 3-minute timeframe.
Error #4	The input buffer is full, as the client has sent more than 32KB of data for an implicit transaction.
Error #5	An AIB error occurred when the IMS Connect tried to confirm if the transaction was available to be started.
Error #6	The transaction is not defined to IMS or is unavailable to be started.
Error #7	The IMS-request message (IRM) segment not in correct format.
Error #101	User ID/Password is missing.
Error #102	Invalid length of User ID/Group/Password data.
Error #103	User ID not defined to the system.
Error #104	Invalid password for this User ID.
Error #105	Password has expired.
Error #106	New password supplied is not a valid one.
Error #107	User ID does not belong to Group.
Error #108	User ID has been revoked – call the EDT/HCV Help Desk.
Error #109	Access to Group is revoked – call the EDT/HCV Help Desk.
Error #110	Authorization error.
Error #111	Internal error.
Error #112	Some other error.
Error #114	New password and confirmation of new password do not match.
Error #115	Internal error.

TCP/IP Input Transaction

*Optional fields

Description	Start	End	Length	Notes
Length	01	02	02	Set to x'00CD' (205)
Reserved	03	04	02	Set to x'0000' (0)
Transaction Code	05	13	09	RPVR0300 (followed by 1 blank)
Health Number	14	23	10	Must be provided for a keyed transaction and omitted for a swiped transaction
Version Code	24	25	02	
MOH User ID	26	33	08	Authorization ID (HECSnnnn) issued by the ministry In the case of a network host, this will be the same for all of the networked sites
EITHER MOH Facility ID	34	40	07	Represents the ministry issued facility or provider number At least one of these fields must be present on all transactions
OR MOH Provider ID	41	50	10	
Local User ID	51	58	08	In the case where a client is routing through another facility, the ministry assigned ID # to the client will be used (HCNP # # # #) For a single hospital or provider, this will be the ID assigned by the ministry (HECS # # # #)
Local Device ID*	59	66	08	Optionally, Local Device ID may identify where the transaction came from within a facility (e.g., Emergency Department)
Client Text*	67	86	20	Optionally, Client Text is echoed back unedited and unchanged Recommended that the field include a unique identifier assigned to each transaction to facilitate message sequencing
Magnetic Stripe (refer to Appendix C–Magnetic Stripe)				
Track 1	87	165	79	Mandatory for a card swipe transaction Ontario health cards conform to ISO 7811/12
Track 2	166	205	40	Data must be left justified and if necessary, padded with spaces

TCP/IP Output Transaction

Description	Start	End	Length	Notes
Length	01	02	02	x'0099' (153)
Reserved	03	04	02	x'0000' (0)
Transaction Code	05	13	09	RPVR0300 followed by 1 space
Local User ID	14	21	08	
Local Device ID	22	29	08	
Health Number	30	39	10	
Version Code	40	41	02	
Response Code	42	43	02	Values may be found in Appendix A – <i>Response Codes</i> At a minimum, the Response Code numbers provided in Appendix A must be echoed to the client for troubleshooting purposes
Gender Code	44	44	01	Values are M or F Values represent the data as retained on the ministry database
Birth Date	45	52	08	Values represent the data as retained on the ministry database
Expiry Date	53	60	08	Values represent the data as retained on the ministry database
Client Text	61	80	20	Output as received on input
Last Name	81	110	30	
First Name	111	130	20	
Second Name	131	150	20	
Redundant Response Code	151	152	02	Available for message delivery verification
Carriage Return	153	153	01	Indicates the end of the output message

HELP

3

SECTION 3:**HELP**

Help Desk

All requests for registration, questions, concerns and inquiries regarding HCV should be directed to the EDT/HCV Help Desk. The EDT/HCV Help Desk staff will record contact information in the EDT/HCV Help Desk software application and provide assistance where applicable. If the problem cannot be resolved, the call is escalated to an on-call ministry staff member who will return the call as soon as possible and provide assistance to resolve issues quickly.

The ministry maintains 24 hour, 7 days of the week technical help to support health card validation users. The EDT/HCV Help Desk is staffed from 8:00 am until 5:00 pm Monday through Friday. After these hours, on weekends and holidays, messages may be left in the EDT/HCV Help Desk voicemail box. Messages left in the EDT/HCV Help Desk voicemail box are dispatched to an on-call staff member. Urgent calls such as HCV service unavailable are returned immediately and every effort is made to resolve problems as quickly as possible. Non-urgent calls are returned on the next business day.

In order to assist with problem resolution, please be prepared to provide the following information to the EDT/HCV Help Desk when calling for assistance:

- Ministry ID number
- Name and telephone number of the person placing the call
- Name and telephone number of the contact person
- E-mail of contact person
- Full address of where the problem is occurring including postal code
- Description of the problem
- IP address and port number if possible

The following site-specific information will also be required if different from the above:

- Name of the contact person for the site
- Name and telephone number of the person who can let the vendor into the site
- Name of the person who can identify where the problem is
- Name of the person who has the problem
- Name of the person who has a key to the wiring closet

EDT/HCV Help Desk Telephone Number: 1 800 262-6524

Resource Access Control Facility – Password

The Resource Access Control Facility (RACF) is a software security program that resides on the MOHLTC mainframe computer and limits a user's access to specific areas of the ministry systems and transactions. RACF limits access to the system as well as to various levels of information on the system based on a user's need.

Password Guidelines

- Organization and/or each user registered and authorized for HCV are assigned a RACF ID and an initial password by the ministry.
- Initial passwords may be up to 8 characters long.
- An initial password is issued in an expired state and clients are required to change initial passwords prior to processing any HCV transactions.
- Subsequent passwords must be 6 to 8 characters long.
- Password changes resulting from ministry reset or revocation will be up to 8 characters long.
- Passwords must be changed every 35 days.
- The system maintains a history of the last 12 passwords and these passwords will not be permitted for re-use during the next 12 password changes.
- Passwords cannot contain your RACF ID.
- If your RACF ID is HEZZXX then these letters cannot be present in your password (e.g., HEZZXX, HEZZXX01, 01HEZZXX).
- These common 3 character abbreviations cannot appear anywhere in the password (e.g., GOV, ONT, JAN, FEB).
- The first 4 characters of the new password cannot match the first 4 characters of the current password.
- The 4th – 8th characters of the new password cannot match the 4th – 8th characters of the old password (e.g., OLDPASSWORD: SPSTST NEWPASSWORD: CONTST).
- Passwords will be checked against a confidential list of passwords commonly used by computer hackers. Passwords found on the list will not be permitted.

Unsuccessful attempts to log on with a RACF ID will result in a “lock-out” from the system. A call to the EDT/HCV Help Desk at 1 800 262-6524 is required for a “reset”.

NOTE: *A password reset occurs when the ministry reverts a password back to the system default password (e.g., a user forgets the current password or when a RACF ID has been revoked and then re-issued).*

Datapac Password Help

Bell Datapac will provide the initial assignment of Network User Identification (NUI) and password along with password rules and other associated information. Questions regarding Datapac passwords should be directed to Bell Datapac at 1 800 267-6574.

Guidelines for Choosing a Good Password

Use care when choosing your password. You are responsible for all transactions associated with the RACF ID assigned to you. Ministry staff cannot see your password and cannot look it up.

Password guidelines are provided to assist in the selection and maintenance of a secure password:

- select something easy for you to remember
- don't write your password down
- don't share your password
- form a compound word from two smaller words, for example:
SOURTEA
- mix upper and lowercase letters, for example:
sOuRtEa
- remove all vowels from a common word, for example:
MANHATTAN=MNHTTN
- use the first or last letters from each word of a phrase, for example:
TO BE OR NOT TO BE=TBRNTB
- incorporate special characters, for example
any&DAY
- combine letters and numbers such as the name and birth date of a friend, for example:
JOE1064

Testing with the Ministry

All vendors, registered providers and facilities are required to complete a connectivity and conformance test with the ministry prior to the implementation of access to HCV. Any environment change, including protocol or software changes are also subject to connectivity and conformance testing. Information on how to connect to the ministry test environment will be provided following HCV registration.

All testing is done on the ministry's User Acceptance Testing platform. Specified HCV transactions are provided for the testing. When testing is complete, the ministry will review the results and if the input data is in compliance with the technical specifications the client will be moved to the production platform.

NOTE: *Client using Datapac dial-up connection will test by substituting "IMSDVH" for "KIMS" in the application.*

To begin testing:

Call the EDT/HCV Help Desk at 1 800 262-6524 to advise of intention to begin testing. Instructions regarding connectivity and conformance testing will be provided.

The ministry will revoke access to any vendor that provides access to a client who has not been registered for Health Card Validation by the ministry.

APPENDICES

4

SECTION 4

APPENDICES

Appendix A

Response Codes

A response code is a number generated by the ministry mainframe in the HCV process. The response code corresponds to a message that describes the status of a health card.

NOTE: *If the user, (health care provider) is not authorized to access health card validation, a response code will be returned indicating an unauthorized user. Please refer to the following page for a list of Response Codes.*

Along with the health card check and response code, a health care provider is also expected to review the health card including the individual's photo, date of birth and gender. If a discrepancy is apparent, additional information and identification should be requested.

In the event of suspected fraud the health care provider must contact the MOHLTC Fraud Line at:

1 800 265-4230

Response Codes - Quick Reference

The following is an overview of valid response codes:

- between 0 and 25 indicates the health card is invalid; cardholder not eligible
- between 50 and 55 indicates a valid health card; cardholder is eligible
- between 60 and 83 indicates health card is invalid; cardholder is eligible
- between 90 – 99 indicates HCV system information
- between 9A – 9M indicates an unauthorized HCV user

Appendix A – Response Codes (Continued)

Health Card Validation Response Codes¹

Code	Response
05	Incorrect health number – The HN is not 10 numeric digits
10	Incorrect health number – The HN was not found on RPDB
15	Pre-assigned newborn health number
20	Eligibility does not exist for this health number
25	Unknown card; Invalid stripe
50	Card passed validation
51	Card passed validation
52	Card passed validation; No response to ‘notice to register’
53	Card passed validation; Card is expired
54	Card passed validation; Card is future dated
55	Card passed validation; returned mail indicator on inactive card
60	Inactive card
65	Invalid version code
70	Stolen card
75	Cancelled or voided card
80	Damaged card
83	Lost card

¹ Note: English descriptions below are from the development Db2 tables and may differ from production.

Appendix A – Response Codes (Continued)

Health Card Validation Response Codes (Continued)

Code	Response
90	Information not available
99	System not available
9A	Health care provider/facility not authorized for HCV
9B	Health care provider/facility not authorized for HCV
9C	Health care provider/facility not authorized for HCV
9D	Health care provider/facility not authorized for HCV
9E	Health care provider/facility not authorized for HCV
9F	Health care provider/facility not authorized for HCV
9G	Health care provider/facility not authorized for HCV
9H	Health care provider/facility not authorized for HCV
9I	Health care provider/facility not authorized for HCV
9J	Health care provider/facility not authorized for HCV
9K	Health care provider/facility not authorized for HCV
9L	Health care provider facility not authorized for HCV
9M	Health care provider facility not authorized for HCV

Appendix A – Response Codes (Continued)

Response Codes – Explanation and Recommended Action

A list of response codes, explanations and recommended actions has been compiled to assist HCV users in determining appropriate action upon receipt of a response code. The recommended actions are intended to be suggestions – one or a combination of choices may be appropriate. Each health care provider should establish an appropriate level of action for each response code.

Code	Response	Provider Action Including Message to Patient
5	<p>Incorrect health number</p> <p>Health number is not 10 numeric digits (may be keying error or the card may be damaged).</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm number and version code ▪ Confirm cardholder identity ▪ Request surrender of health card - return it to MOHLTC ▪ Notify the fraud line where applicable 1 800 265-4230 ▪ No payment for services, bill the cardholder directly ▪ <i>Ask the cardholder to contact the local MOHLTC office</i>
10	<p>Incorrect health number</p> <p>The health number was not found on the ministry's Registered Persons Database.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code ▪ Confirm cardholder identity ▪ Request surrender of health card - return it to MOHLTC ▪ Notify the fraud line where applicable 1 800 265-4230 ▪ No payment for services, bill the cardholder directly ▪ <i>Ask the cardholder to contact the local MOHLTC office</i>
15	<p>Pre-assigned new-born health number - parent/guardian must complete registration</p> <p>Health number was released as a pre-assigned health number for new-borns. The registration process is incomplete.</p>	<ul style="list-style-type: none"> ▪ <u>Patient less than 3 months old:</u> ▪ Advise parent/guardian health number registration is incomplete ▪ Infant registration may be in process - request supporting evidence of Ontario residency (e.g., parent's health card, driver's licence) ▪ Advise client direct billing may result if registration not completed within 90 days of date of birth ▪ No payment will be made for services until registration is completed. ▪ <i>Ask the cardholder to contact the local MOHLTC office</i>

Code	Response	Provider Action Including Message to Patient
20	<p>Not eligible</p> <p>There is no eligibility for this health number on the ministry database.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code. ▪ Confirm cardholder identity ▪ Request surrender of health card - return it to MOHLTC ▪ Notify the fraud line where applicable at 1 800 265-4230 ▪ No payment for services, bill the cardholder directly ▪ <i>Ask the cardholder to contact the local MOHLTC office</i>
25	<p>Unknown health card</p> <p>Health card swipe does not have proper Issuer Identification.</p>	<ul style="list-style-type: none"> ▪ Verify health card appears to be ministry-issued health card and not a hospital card ▪ Check for keying errors ▪ Confirm health number and version code. ▪ Confirm cardholder identity ▪ Request surrender of health card - return it to MOHLTC ▪ Notify the fraud line where applicable at 1 800 265-4230 ▪ No payment for services, bill the cardholder directly ▪ <i>Ask the cardholder to contact the local MOHLTC office</i>
50	<p>Card passed validation</p> <p>This indicates a valid health card with current eligibility.</p>	<ul style="list-style-type: none"> ▪ No action required ▪ Request additional identification if it is suspected that the health cardholder is not the person to whom the health card was issued ▪ You will receive payment for billable services rendered on this day.
51	<p>Health card passed validation</p> <p>This indicates a valid health card with current eligibility.</p>	<ul style="list-style-type: none"> ▪ No action required ▪ Request additional identification if it is suspected that the health cardholder is not the person to whom the health card was issued ▪ You will receive payment for billable services rendered on this day.
52	<p>Health card passed validation</p> <p>Holder must contact ministry to ensure continued validity.</p>	<ul style="list-style-type: none"> ▪ Advise the cardholder to contact the ministry INFOLINE at 1 800 268-1154 ▪ Request additional identification if it is suspected that the cardholder is not the person to whom the health card was issued. ▪ You will receive payment for billable services rendered on this day. Registrant needs to contact the ministry to maintain coverage into the future.

Code	Response	Provider Action Including Message to Patient
53	<p>Health card passed validation</p> <p>Health Card ID expired. A renewal notification has been sent to the registrant.</p>	<ul style="list-style-type: none"> ▪ Advise the cardholder to contact the ministry on the INFOline at 1 800 268-1154 ▪ Request additional identification if it is suspected that the cardholder is not the person to whom the health card was issued ▪ You will receive payment for billable services rendered on this day. Registrant needs to contact the ministry to maintain coverage into the future.
54	<p>Health card passed validation</p> <p>Health card is future dated. The cardholder was issued this health card upon renewal or as a replacement.</p>	<ul style="list-style-type: none"> ▪ No action required ▪ Request additional identification if it is suspected that the cardholder is not the person to whom the card was issued ▪ You will receive payment for billable services rendered on this day.
55	<p>Health card passed validation</p> <p>The cardholder needs to update their address on file with the ministry.</p>	<ul style="list-style-type: none"> ▪ Advise the cardholder to contact the ministry on the INFOline at 1 800 268-1154 ▪ Request additional identification if it is suspected that the card holder is not the person to whom the health card was issued. ▪ You will receive payment for billable services rendered on this day. Registrant needs to contact the ministry to maintain coverage into the future.
60	<p>Expired health card</p> <p>If the cardholder has a new health card, they need to use the new health card. Otherwise the cardholder needs to contact the ministry to obtain a new health card.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code. ▪ Confirm cardholder identity ▪ Ask if cardholder has another health card ▪ Ask the cardholder to contact the local MOHLTC office ▪ Have cardholder complete a Health Number Release form ▪ No payment for services on this Health Number and Version Code combination. Use the health number and version code obtained through the Health Number Release form process to bill for services rendered.

Code	Response	Provider Action Including Message to Patient
65	<p>Incorrect version code</p> <p>If the cardholder has another health card, they need to use the other health card. Otherwise, the cardholder needs to contact the ministry to obtain a new health card.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code. ▪ Confirm cardholder identity ▪ Ask if cardholder has another health card ▪ Ask the cardholder to contact the local MOHLTC office ▪ Have cardholder complete a Health Number Release form ▪ No payment for services on this health number and version code combination. Use the health number and version code obtained through the Health Number Release form process to bill for services rendered.
70	<p>Stolen health card</p> <p>The health card has been reported as stolen. Card is no longer valid.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm number and version code. ▪ Ask if cardholder has another health card ▪ Request additional identification supporting Ontario residency (driver's licence) - cardholder may have recovered the health card but neglected to advise MOHLTC ▪ If unable to confirm the photo on the card bill the cardholder directly and notify the fraud line where applicable at 1 800 265-4230 ▪ Ask the cardholder to contact the local MOHLTC office ▪ Have cardholder complete a Health Number Release form ▪ No payment for services on this Health Number and Version Code combination. Use the Health Number and Version Code obtained through the Health Number Release Form process to bill for services rendered.
75	<p>Cancelled health card</p> <p>Health card cancelled by MOHLTC - replacement may have been issued</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code. ▪ Confirm cardholder identity ▪ Ask if cardholder has another health card ▪ Ask the cardholder to contact the local MOHLTC office ▪ Have cardholder complete a Health Number Release form ▪ No payment for services on this health number and version code combination. Use the health number and version code obtained through the Health Number Release form process to bill for services rendered.

Code	Response	Provider Action Including Message to Patient
80	<p>Damaged health card</p> <p>Health card cancelled by MOHLTC. A replacement may have been issued.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code ▪ Confirm cardholder identity ▪ Ask if cardholder has another health card ▪ Ask the cardholder to contact the local MOHLTC office ▪ Have cardholder complete a Health Number Release form. ▪ No payment for services on this health number and version code combination. Use the health number and version code obtained through the Health Number Release form process to bill for services rendered.
83	<p>Lost health card</p> <p>The health card has been reported as lost. The card is no longer valid.</p> <p>A replacement may have been issued.</p>	<ul style="list-style-type: none"> ▪ Check for keying errors ▪ Confirm health number and version code. ▪ Confirm cardholder identity ▪ Ask if cardholder has another health card ▪ Ask the cardholder to contact the local MOHLTC office ▪ Have cardholder complete a Health Number Release form ▪ No payment for services on this health number and version code combination. Use the health number and version code obtained through the Health Number Release form process to bill for services rendered.
90	<p>Information not available</p> <p>The MOHLTC system may be undergoing maintenance.</p>	<ul style="list-style-type: none"> ▪ Try the scan again ▪ Use Interactive Voice Response to validate the health card ▪ Access IVR Bulletin Board to obtain system maintenance, downtime information and periodic status updates ▪ Call the MOHLTC Help Desk at 1 800 262-6524 and report the problem.
99	<p>System not available</p> <p>Cannot access the MOHLTC database</p>	<ul style="list-style-type: none"> ▪ Try the scan again ▪ Use Interactive Voice Response to validate the health card ▪ Access IVR Bulletin Board to obtain system maintenance, downtime information and periodic status updates. ▪ Call the MOHLTC Help Desk at 1 800 262-6524 and report the problem.

Code	Response	Provider Action Including Message to Patient
9A	<p>Not authorized for HCV</p> <p>MOHLTC Provider ID is either missing on the input transaction record, or is not numeric or not left justified.</p>	<ul style="list-style-type: none"> ▪ Call 1-800-262-6524 and provide response code to Help Desk Agent
9B	<p>Not authorized for HCV</p> <p>The Facility ID is either missing on the input transaction record or not alphanumeric or not left justified or not 4 characters in length.</p>	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9C	<p>Provider ID does not match the data contained on the ministry's HCV Registration Table.</p>	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9D	<p>Facility ID does not match the data contained on the ministry's HCV Registration Table.</p>	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9E	<p>The MOHLTC User ID is either missing on the input transaction record or is not alphanumeric or not left justified.</p>	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent

Code	Response	Provider Action Including Message to Patient
9F	Provider # is not a valid status on ministry database.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9G	The Group # is not a valid status on ministry database.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9H	Organization Status is closed or Facility MNI not found on ministry database.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9I	User's Host ID (HECSxxxx) does not match ministry database.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9J	IVR PIN is not numeric or is equal to spaces.	<ul style="list-style-type: none"> ▪ Provider to re-try with correct PIN ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9K	Local User ID is not alphanumeric or is equal to spaces.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9L	User not found/authorized.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent
9M	Client of the Network Provider is not authorized.	<ul style="list-style-type: none"> ▪ Call 1 800 262-6524 and provide response code to Help Desk Agent

Appendix B

IVR OPERATING INSTRUCTIONS

NOTE: *The IVR system must be accessed by telephone only. The telephone must be a TOUCH-TONE telephone and you will need your Personal Identification Number (PIN).*

Verifying a Health Number and/or Oculo-Visual Service Date

1. From Metro Toronto call **416 326-6666**; otherwise call **1 800 265-6860**
2. Enter your 8-digit PIN to access the Main Menu
3. Press 1 from the Main Menu to verify a health number
4. Enter the 10-digit health number
5. Enter the version code if applicable
6. Enter Fee Schedule Code if applicable
7. Press 1 to verify another health number (maximum of 5 health numbers)
8. Press 7 to exit

Appendix B – IVR Operating Instructions (Continued)

Accessing the Bulletin Board

1. From Metro Toronto call **416 326-6666**; otherwise call **1 800 265-6860**
2. Enter your 8-digit PIN
3. Press 4 from the Main Menu to access the Bulletin Board

Accessing the Help Line

1. From Metro Toronto call **416 326-6666**; otherwise call **1 800 265-6860**
2. Enter your 8-digit PIN
3. Press 4 from the Main Menu to access the Bulletin Board
4. Press 3 from the Bulletin Board Menu to access the IVR Help Line

Calling In

The IVR System is accessed by keying the IVR phone number.

1. From Metro Toronto call **416 326-6666**; otherwise call **1 800 265-6860**

The system will respond as follows:

“Welcome to the Ministry of Health IVR system.” (Repeated in French)

If for any reason the IVR system is down, you will hear the following message and the call will be terminated:

“The system is unavailable, please try again later.” (Repeated in French)

Appendix B – IVR Operating Instructions (Continued)

Entering Your Personal Identification Number (PIN)

The system will prompt you to enter your Personal Identification Number.

“Please enter your Personal Identification Number.” (Repeated in French)

After the 8-digit PIN has been entered the system will validate the PIN and select your language preference (English or French) on file. The call will then proceed in your chosen language.

Keying Tips

- If you do not start to enter your PIN **within 5 seconds**, the system will repeat the message:

“Please enter your Personal Identification Number.” (Repeated in French)

- If there is a 5 second gap between keyed characters, the system will state:

“Incorrect, please repeat your Personal Identification Number.” (Repeated in French)

On a new attempt, the PIN must be re-entered from the beginning.

- After 3 invalid attempts, the call will be terminated.
- If the PIN is not valid the system will prompt you to try again with the message:
“Incorrect number, please try again.” (Repeated in French)
- If the PIN that is re-entered is also invalid the call will be terminated.

Appendix B – IVR Operating Instructions (Continued)

Accessing the Main Menu

Now that you have entered your valid PIN you will be given the following choices from the Main Menu:

- *“To verify a health number, press 1.”*
 - *“To access the ministry Bulletin Board, press 4.”*
 - *“To exit, press 7.”*
1. Press 1 to verify a health number
 2. Press 4 to access the ministry Bulletin Board
 3. Press 7 to exit

Keying Tips

- If any key other than 1, 4 or 7 is pressed, you will get the following message:
“Incorrect option, please try again”
- After 3 invalid attempts, the call will be terminated.
- If you access the ministry Bulletin Board, you will not be able to return to the main menu to verify additional numbers.

Appendix B – IVR Operating Instructions (Continued)

Entering the Health Number

- To verify a health number, press 1 from the Main Menu. The system will prompt you with the following:

“Enter the health number.”

- Key the 10-digit health number.

Keying Tips

- If you do not start to enter the health number **within 5 seconds**, the system will repeat the message:

“Enter the health number.”

- If there is a 5 second gap between keyed characters, the system will state:

“Please re-enter the health number.”

On a new attempt, the health number must be re-entered from the beginning.

- After 3 invalid attempts, the call will be terminated.

Appendix B – IVR Operating Instructions (Continued)

Entering the Version Code

- After you have entered the health number, you will be asked to enter the version code:

“Enter the version code.”

Each alpha character of the version code is represented by 2 numbers:

A=21	J=51	S=73
B=22	K=52	T=81
C=23	L=53	U=82
D=31	M=61	V=83
E=32	N=62	W=91
F=33	P=71	X=92
G=41	Q=11	Y=93
H=42	R=72	Z=12

If there is no version code, key #.

If there is a one-letter version code, you will need to key 2 numbers, followed by # (e.g., Version Code Q = 11#).

If there is a two-letter version code, you will need to key 4 numbers (e.g., Version Code JK = 5152).

Keying Tips

- If you do not start to enter the version code **within 5 seconds**, the system will repeat the message:

“Enter the version code.”

- If there is a 5 second gap between keyed characters, the system will state:

“Please re-enter the version code.”

On a new attempt, the version code must be re-entered from the beginning.

- After 3 invalid attempts, the call will be terminated.

Appendix B – IVR Operating Instructions (Continued)

Entering the Fee Schedule Code

- After you have entered the version code, you will be asked to enter the fee schedule code:
“Enter the fee schedule code.”
- Each alpha-character of the fee schedule code is represented by 2 numbers:
A=21 V=83

(e.g., V401 would be keyed as 83401)

If there is no fee schedule code, key #.

Keying Tips

- If you do not start to enter the fee schedule code **within 5 seconds**, the system will repeat the message:

“Enter the fee schedule code.”
- If there is a 5 second gap between keyed characters, the system will state:

“Please re-enter the fee schedule code.”

On a new attempt, the fee schedule code must be re-entered from the beginning.

- After 3 invalid attempts, the call will be terminated.

Appendix B – IVR Operating Instructions (Continued)

Validation Response Codes

After you have entered the health number and version code, the system will repeat the health number and version code which you entered and provide a response code, sex, date of birth and first three characters of the last name. The message will say, "*health number NNNNNNNNNN version code MM has a code of XX*" where:

NNNNNNNNNN	=	Health Number
MM	=	Version Code
XX	=	Response Code
NNNNNNNN	=	Date of Birth
M/F	=	Sex
MMM	=	Surname
MNNN	=	Fee Schedule Code (FSC)
NNN	=	Service Response Code
NNNNNNNN	=	Date of Service for Oculo-Visual Assessment

Please ensure that the health number and version code repeated to you are those that appear on the health card.

Appendix B – IVR Operating Instructions (Continued)

Oculo-Visual Assessment

The IVR system will issue either the Date of Service (DOS) of an oculo-visual assessment/major eye exam and a service response code, or just a service response code. This information will be in addition to the validation return code. The search of the data source will be based on the HN, version code and Fee Schedule Code (FSC) entered by the provider. If a DOS is returned to the provider it will **always** be the DOS for the most recent oculo-visual assessment or major eye exam. The service response code will indicate whether or not there is an additional oculo-visual assessment or a major eye exam present or not. The four service response codes are as follows:

- No FSC information is currently available for this patient – service response code 101
- FSC entered by provider invalid – service response code 102
- Oculo-visual assessment or major eye exam present – service response code 201 and oculo-visual assessment/major eye exam date of service (DOS)
- Additional oculo-visual assessment or a major eye exam present – service response code 202 and oculo-visual assessment/major eye exam DOS

Appendix B – IVR Operating Instructions (Continued)

Return of Surrendered Health Cards

Specific codes (*refer to Appendix A – Response Codes*) request the voluntary surrender of health cards. Please return **surrendered health cards** to the Ministry of Health and Long-Term Care, Verification Services, 49 Place d’Armes, 3rd Floor, Kingston, Ontario K7L 5J3. The returned health cards will be investigated and resolved.

Verifying Additional Health Numbers

At this point you have the option to verify additional health numbers (**maximum of 5 inquiries per call**). The system will prompt with the following choices:

- “To verify another health number, press 1.”
- “To repeat this information, press 2.”
- “To exit, press 7.”
- “To return to the main menu, press 9.”

If you press option 1, you may verify another health number (*refer to Entering the Health Number* to repeat the process).

1. Press 7 to exit
2. Press 9 to return to the Main Menu

Keying Tips

- If any key other than 1, 2, 7 or 9 is pressed, you will hear the following message:
“*Incorrect option, please try again.*”
- After 3 invalid attempts, the call will be terminated.
- A **maximum of 5 health numbers** may be verified during each call. To verify additional health numbers, please call again.

Appendix B – IVR Operating Instructions (Continued)

Accessing the IVR Bulletin Board

To access the ministry Bulletin Board from the Main Menu, press 4. The system will prompt with the following choices:

- *“For information on system availability, press 1.”*
- *“To access help, press 3.”*
- *“To exit, press 7.”*

Press 1 to receive information on system availability (e.g., messages relating to planned system downtime).

1. Press 3 to access the IVR Help Line
2. Press 7 to exit

Keying Tips

- If any key other than 1, 3 or 7 is pressed, you will hear the following message:
“Incorrect option, please try again.”
- After 3 invalid attempts, the call will be terminated.

Appendix B – IVR Operating Instructions (Continued)

Accessing the IVR Help Line

- To access the IVR Help Line, press 3 from the IVR Bulletin Board menu. The system will prompt with the following:

“Please hold, your call is being transferred.”

- If you press 3 between 8:00 am and 5:00 pm on regular ministry business days, you will reach a Help Desk operator.
- If you press 3 between 5:00 pm and 8:00 am, the system will respond as follows:

“You have reached the Ministry of Health and Long-Term Care Help Desk. Agents are not available to take your call. If you have a question about Health Card Validation, press 1 now.”

- If you press 1, the system will respond as follows:

“You have reached voice messaging for Health Card Validation. Please leave your name, telephone number and a brief description of your problem. Your call will be returned as soon as possible.”

Keying Tips

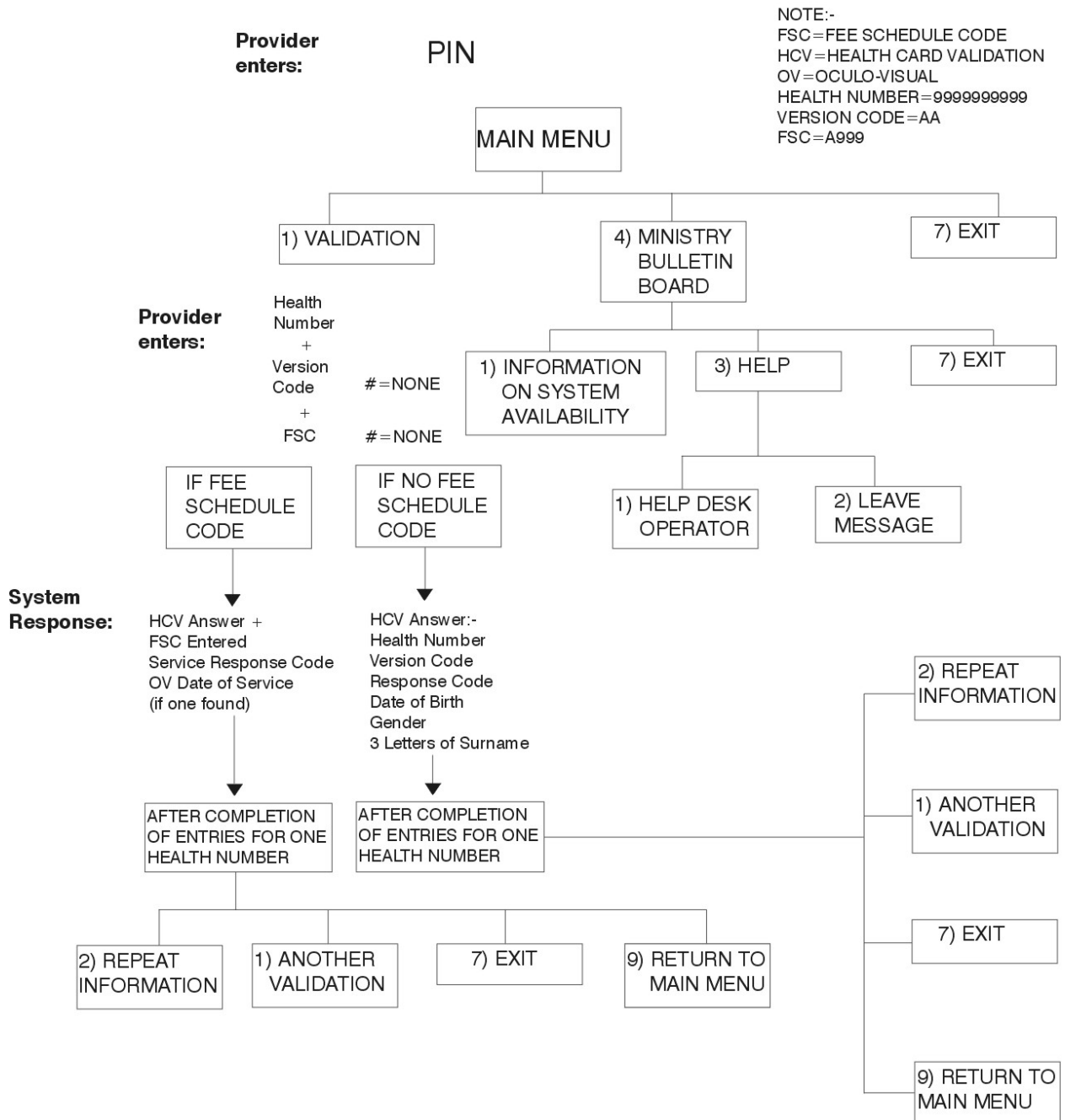
- If any key other than 1, 2, or 7 is pressed, you will hear the following message:

“Incorrect choice, please try again.”

- After 3 invalid attempts, the call will be terminated.

Appendix B – IVR Operating Instructions (Continued)

IVR Application Flowchart



Appendix B – IVR Operating Instructions (Continued)

Fee Schedule Codes

Code	Description
General Practitioners	
A110	Periodic oculo-visual assessment, aged 19 and below
A112	Periodic oculo-visual assessment, aged 65 and above
A115	Major eye examination aged 20-64
K065	Periodic oculo-visual assessment, aged 20-64 (MCSS – ODSP)
K066	Periodic oculo-visual assessment, aged 20-64 (MCSS – OW)
Ophthalmologist	
A237	Periodic oculo-visual assessment, aged 19 and below
V239	Periodic oculo-visual assessment, aged 65 and above
Optometrists	
V404	Periodic oculo-visual assessment, aged 19 and below
V406	Periodic oculo-visual assessment, aged 65 and above
V409	Major eye examination, aged 20 - 64
V450	Periodic oculo-visual assessment, aged 20 – 64 (MCSS – ODSP)
V451	Periodic oculo-visual assessment, aged 20 – 64 (MCSS – OW)

Service Response Codes

Code	Response	Requirement or Explanation	Action
101	No information available	There is no FSC information currently available for this patient.	There is no FSC information available for this patient.
102	Invalid FSC	The FSC entered by the provider is not valid.	The FSC entered is invalid – retry or hang up.
DOS & 201	Oculo-visual assessment performed	An oculo-visual assessment has been performed on this patient within the permitted time frame.	The patient has had an oculo-visual assessment performed within the prescribed time frame.
DOS & 202	Additional oculo-visual assessment performed	An additional oculo-visual assessment has been performed on this patient within the permitted time frame.	The patient has had an additional oculo-visual assessment performed within the prescribed time frame.

Appendix C**MAGNETIC STRIPE**

Track I Recording density 210 bpi
 7 bits per character, 79 alphanumeric characters

Field	Field Name	Size	Comments/Values
1	Start Sentinel	1	Value = “%”
2	Format Code	1	Value = “b”
3	Issuer Identification	6	Value = “610054”
4	Health Number	10	
5	Field Separator	1	Value = “^”
6	Name	26	As per ISO standards. Separated by “/”
7	Field Separator	1	Value = “^”
8	Expiry Date	4	YYMM or zero filled
9	Interchange Code	1	7
10	Service Code	2	Value = “99”
11	Sex	1	1 = Male 2 = Female
12	Date of Birth	8	YYYYMMDD
13	Card Version Number	2	XX (may be blank)
14	First Name-Short	5	First 5 characters of first or middle name
15	Issue Date	6	YYMMDD
16	Language Preference	2	01=END 02=FR
17	End Sentinel	1	Value = “?”
18	Longitudinal Redundancy Check (Parity)	1	As per ISO standards

Appendix C – Magnetic Stripe (Continued)

Track II Recording density 75 bpi
 5 bits per character, 40 numeric characters

Field	Field Name	Size	Comments/Values
1	Start Sentinel	1	Value = “;”
2	Issuer Identification	6	Value = “610054”
3	Health Number	10	
4	Field Separator	1	Value = “=”
5	Expiry Date	4	YYMM or zero filled
6	Interchange Code	1	Value = “7”
7	Service Code	2	Value = “99”
8	Filler	4	Value = “0000”
9	Card Type	1	1 = REG 2 = 65
10	OHIP Number	8	Number or “00000000”
11	End Sentinel	1	Value = “?”
12	Longitudinal Redundancy Check (Parity)	1	As per ISO standards

For the Expiry Date on Track I and II and the Issue Date on Track I the year remains as a 2-digit character.

- if the year is 30 or less, then the century is “20”
- if the year is greater than 30, then the century is “19”

Example:

Expiry Date	3001	=	203001
Expiry Date	2901	=	202901
Expiry Date	3101	=	193101
Issue Date	000101	=	20000101
Issue Date	980101	=	19980101
Issue Date	890101	=	19890101

Appendix C – Magnetic Stripe (Continued)

Track III Recording density 210 bpi
5 bits per 980 character, 107 numeric characters

Field	Field Name	Size	Comments/Values
1	Start Sentinel	1	Value = “;”
2	Format Code	2	Value = “90”
3	Issuer Identification	6	Value = “610054”
4	Health Number	10	
5	Field Separator	1	Value = “=”
6	Filler	85	Value = “0”
7	End Sentinel	1	Value = “?”
8	Longitudinal redundancy Check (Parity)	1	As per ISO standards

NOTE: *Track III is reserved for possible future use.*

Appendix D FREQUENTLY ASKED QUESTIONS

Q 1: *Why should I use Health Card Validation?*

A 1: Validation responses provide decision-making information at the time of service and allow a health care provider to:

- reduce claim rejects by ensuring a client is eligible for service prior to service delivery
- reduce claim rejects associated with incorrect version codes
- reduce administrative costs by allowing health care providers to bill clients at the time of service where applicable
- reduce health care fraud by eliminating service to ineligible clients and by visually confirming HCV response information with client at the point of service (e.g., gender, date of birth)

Q 2: *I want to start using the Health Card Validation (HCV) service, how do I get started?*

A 2: Please *review Section 1–Introduction* to determine the best HCV access method to meet your needs. Once you have made a selection, contact the EDT/HCV Help Desk at **1 800 262-6524** to advise them of your choice. Your contact information will be recorded and the relevant documents and forms will be forwarded to you for completion.

Q 3: *Do you have a list of software vendors that offer HCV access software?*

A 3: The ministry does not provide or maintain a list of software vendors. You may contact your professional association for a list of vendors or a colleague who is currently registered as an HCV user.

Q 4: *Is there a cost associated with accessing HCV?*

A 4: The ministry does not charge for HCV access. However, there may be set-up and ongoing costs depending on the access method chosen. You will need to discuss set-up and ongoing costs with your software vendor or solution provider.

Appendix D – Frequently Asked Questions (Continued)

Q 5: *Do I need special equipment to access HCV services?*

A 5: Depending on the HCV option and corresponding communication protocol you choose, you will need associated equipment. Your vendor can provide you with information regarding any required equipment.

Q 6: *What level of help and service does ministry provide to registered HCV users?*

A 6: The ministry operates a Help Desk 24 hours of the day, 7 days a week. The EDT/HCV Help Desk can be reached by calling **1 800 262-6524**. Ministry Help Desk staff will assist you with your problem, or for after-hours service you can leave a message at this number. Ministry Help Desk staff will return your call. If the problem cannot be solved immediately, the call will be escalated and you will be kept informed of progress.

Q 7: *After I have selected an option and my equipment and protocol are in place, what is the process to begin using HCV?*

A 7: Once ready to begin using HCV, conformance and connectivity testing are required. Contact the EDT/HCV Help Desk at **1 800 262-6524** and you will be provided with information on how to connect to the ministry test lab. Specific health card numbers will be provided for testing HCV transactions in the test environment. Upon successful completion of testing you will be provided with information on how to connect to the production environment.

Appendix E**GLOSSARY**

Term	Definition
Card Status	Refers to the status of a health card such as issued, cancelled, lost, stolen
Conformance Testing	Performed by ministry staff to ensure that software and hardware “conforms” to the technical specifications that have been distributed and that the software/hardware can communicate with the ministry systems to retrieve accurate information
Connectivity Testing	Performed by ministry staff to ensure that protocols and connection methods can communicate with ministry systems appropriately
Datapac	Service offered by Bell Canada to provide secure communication lines on which HCV data is transmitted
Dialup	Telephone connection established via a modem and phone line and is maintained for a limited time for electronic transactions
EDT	Vehicle for electronic transmission of files from a PC to the ministry mainframe computer
Fee Schedule	List of physician fees
HCR	Device used to read the magnetic strip on a health card - POS devices and wedges are used as HCRs for HCV
HCV	Checks the status and validity of the 10-digit health number and version code presented and an individual’s eligibility for health care coverage
Health Care Provider	Individual, group or facility licensed to provide health care services
Health Number Release Form	Allows client’s health number and version to be checked if a client cannot produce a health card
HN	Health number

Appendix E – Glossary (Continued)

Term	Definition
IVR	Automated telecommunication system that allows authorized health care providers to connect to the RPDB and use a touch tone telephone to key health numbers version codes and receive validation responses
IVR Bulletin Board	Provides information to registered IVR users regarding scheduled system downtime, and/or periodic messages (refer to <i>Appendix B – IVR Operating Instructions</i>)
Keyed Transaction	Health card number and version code that is keyed into the computer via the keyboard instead of swiping a card
Mainframe	Large multi-functional computer
Ministry Help Desk	First line of contact (Tier 1) for client support for HCV (1 800 262-6524)
OBEC	Method of validating health cards prior to service delivery
On-Call	Help Desk after hours support
Password	Sequence of characters used to determine that a computer user requesting access to a system or data is really that particular user
PIN	Personal Identification Numbers are assigned to users to access IVR services
POS	Point of Service – actual time or point of service delivery (e.g., Doctor’s office, hospital)
POS Device	Point of Service Device – used to read health cards for real-time validation with ministry
Protocol	Set of standards for exchanging information between two computer systems
Real-time	Level of computer responsiveness that provides immediate access of information
Response Code	Code returned in an HCV process identifying the status of a health card

Appendix E – Glossary (Continued)

Term	Definition
RPDB	Registered Persons Database – all individuals registered for health care services in Ontario
Scheduled Downtime	System maintenance is performed to the systems that provide HCV service every second Sunday of the month between 5:00 am and 8:00 am
Software Application	Program designed to perform a specific function-in-house or vendor-developed applications are written to interact and interface with the ministry databases to validate health numbers
SSHA	Smart Systems for Health Agency–primary role is to provide foundations and infrastructure and a secure, standardized network connection to health care providers
Swiped Transaction	HCV transaction performed by swiping a health card through a POS device or wedge
TCP/IP	Transmission Control Protocol/Internet Protocol – an industry standard set of rules used to send data in the form of message units between computers over the Internet - ministry is moving toward TCP/IP as the standard communication protocol
Technical Specification	Document that describes a process in technical detail outlining the technical requirements of an application or process
Valid	Legitimate and assigned health number
Vendor	Company that has developed, tested and sells solutions that can interact with specific ministry applications
Wedge	Device that reads the information on the magnetic strip of a health card when connected to a computer with appropriate software