Health Canada Santé Canada

Final Audit Report

Audit of Data Integrity

The Health Information Claims Processing System (HICPS)

October 2008

Table of Contents

Executive Summary

The Health Information Claims Processing System (HICPS) is used to process claims relating to the Non-Insured Health Benefits Program (NIHB). It is one of several systems that provide data to SAP, the Department's financial system. Since 1990, Health Canada has engaged a contractor, to provide Health Information and Claims Processing Services for the drug, medical supplies and equipment, and dental benefit components of the NIHB Program. In turn, the contractor has subcontracted with a third party to process a large proportion of the claims associated with these components. In 2006-2007, these claims amounted to about $545 million.

The objectives of the audit were to:

a) determine the completeness and accuracy of the HICPS data that is uploaded to Health Canada's financial system; and

b) provide an overall assessment of the internal control environment for the Health Information Claims Processing System.

The Audit and Accountability Bureau conducted the audit in accordance with the *Government of Canada's Policy on Internal Audit.*

We did not find any major problems with the accuracy and completeness of data during this audit. However, we did note that the design of HICPS made it possible for NIHB employees who are authorized to enter and update data, to enter a fee for dental services that could exceed the maximum allowed amount. Should this occur, an overpayment to a dental practitioner could result.

The control environment for HICPS is generally satisfactory. However, the activities of end users is not monitored at either the application or database level. We also found that documentation relating to the granting of access privileges to HICPS for NIHB staff was incomplete. These findings indicate a risk of unauthorized access to the HICPS application or the database.

Introduction

Background

The Non-Insured Health Benefits (NIHB) Program of the First Nations and Inuit Health Branch (FNIHB) is Health Canada's largest program, representing about 29 percent of Health Canada's total budget. It provides a range of medically necessary health-related goods and services to about 780,000 eligible registered First Nations people and recognized Inuit. The goods and services that NIHB provides are those not provided either through private insurance plans, provincial or territorial insured health and social programs, or by other publicly funded programs.

Since 1990, Health Canada has contracted out the Health Information and Claims Processing Services to handle claims for the drug, medical supplies and equipment, and dental benefit components of the NIHB Program. In turn, the contractor has subcontracted a third party to operate the Health Information Claims Processing (HICPS), the system that processes claims associated with these components. The HICPS is one of several systems that feed data into the Department's financial system (SAP). In Fiscal Year 2006-2007, HICPS processed claims amounting to about $545 million.

The subcontractor's key HICPS-related responsibilities include—but are not limited to:

- processing claims for drugs, medical supplies and equipment, and dental treatment; and
- providing, operating and modifying the HICPS and maintaining its database.

The HICPS includes all services and systems for processing NIHB claims; processing and settling claims from service providers; and ensuring compliance with NIHB's policies—including those relating to audit, reporting and financial control practices.

At the time of the audit, service providers were submitting about 99% of the pharmacy claims and 44% of the dental claims electronically over an Electronic Data Interchange (EDI) network. All claims for medical supplies and equipment were submitted manually. The contractor processes all claims that require manual input.

Appendix A provides an overview of the architecture of HICPS that supports electronic processing of claims.

The audit was undertaken by the Audit and Accountability Bureau in accordance with Health Canada's Risk-Based Audit Plan, which was approved by the Departmental Audit and Evaluation Committee on October 4, 2006. The audit was conducted in accordance with the *Government of Canada's Policy on Internal Audit*.

Objective(s)

The two objectives of the audit were to:

- determine the completeness and accuracy of the HCIPS data that is uploaded to Health Canada's financial system; and
- provide an overall assessment of the internal control environment for the Health Information Claims Processing System.

The two lines of enquiry (LOEs) for this audit were:

- **The completeness and accuracy of the claims data**

  This LOE covered:

  - the controls to ensure that transactions are completely and accurately processed
  - segregation of duties with respect to transaction processing;
  - the accuracy and completeness of claims data uploaded to SAP; and
  - the process for identifying and correcting, in a timely manner, transactions that have been incorrectly processed (Error Processing).

- **The general control environment for limiting access to the system**

  This LOE covered:

  - management's review of user accounts;
  - access to HICPS by NIHB employees;
  - access to the system by Database Administrators (DBAs);
  - problem management; and
  - back-up and recovery procedures

Scope and Approach

The scope of the audit focused on the accuracy and completeness of the HICPS data relating to processing claims for drugs, medical supplies and equipment, and dental benefits. The fieldwork was conducted at NIHB operations in the National Capital Region, at First Canadian Health in Toronto, and at the subcontractor's operations in Mississauga.

We did not examine the validity of claims processed over the Electronic Data Interchange (EDI) network. This would have involved examining the network, which is outside the scope of this audit.

The audit was conducted using criteria based on Information Systems Audit and Control Association's (ISACA) IT governance model - Control Objectives for Information and Related Technology (COBIT); departmental Administration Procedures Manuals (APMs); and Health Canada's IT Security Policy.

Interviews were conducted with functional experts from NIHB, the contractor and the subcontractor, and we reviewed documents relating to the HICPS. These documents included the Detail Design Documents, Administration Procedural Manuals, and training and other technical manuals. We also tested HICPS' general computer and application controls and carried out detailed tests of the pharmacy, medical supplies and equipment, and dental benefit databases for the months of April, July and October 2006 and April 2007. The audit included verifying the accuracy of data inputs, access controls, authorization and exception handling and logging, and backup and restoration procedures.

Findings, Recommendations and Management Responses

Completeness and accuracy of the data

Input Processing and Output

Best practice requires that data for processing be subject to a variety of controls to check for accuracy, completeness and validity. Procedures should exist to correct any errors that are detected as early in the process as possible. Output should be routinely reviewed to ensure that it reflects the original data.

We examined a sample of 26 claims that had been entered into the HICPS to assess their validity, accuracy and completeness. We also reviewed the documentation of procedures to ensure that it included key controls such as segregation of duties, and data input controls (controls to ensure that only valid data are processed). The audit team also looked at the extent to which segregation of duties existed, and the process for inputting data associated with benefit claims.

We found that the Pharmacy, Medical Supplies and Equipment, and Dental Benefit databases showed no discrepancies between the databases and the source documents that we reviewed. Audit testing of the reconciliation process was conducted for the months of April, July, October 2006 and April 2007 to determine the accuracy and completeness of the data uploaded to Health Canada's financial system. No major discrepancies were found.

We noted that the HICPS has numerous features to ensure that claims data are processed completely and accurately. However, our detailed testing of dental claims data identified

150 transactions for the months of September and December 2006 where the Approved Professional Fee field had been modified by an NIHB employees to reflect applicable Professional Fees at the time of payment. The rationale for the override of the Approved Professional Fees, as described by NIHB is:

i. to address circumstances such as unexpected delays in updating professional service fees; or
ii. where the dental practitioner has discovered that the dental procedure is more complex than originally anticipated and therefore has submitted a claim that is above the maximum Dental Fee Allowed.

The fact that the system allows NIHB employees to override the "Approved Professional Fee" field and enter a different fee creates a risk that inappropriate fees could be recorded and paid and would thereby need to be closely monitored. At the time of our audit, NIHB had not been monitoring these override transactions.

Recommendation No. 1

It is recommended that the Assistant Deputy Minister, First Nations and Inuit Health Branch, ensure that a senior NIHB officer reviews and approves all transactions where the Approved Professional Fee exceeds the maximum Dental Fee Allowed in the HICPS.

Management Response

The functionality that allows officers to adjust fees to be paid over the amount normally allowable is related to an operational requirement. The Non-Insured Health Benefits Directorate agrees that the controls are not sufficient around this functionality and will implement measures that allow proper oversight in instances where approved professional fees are being increased by Health Canada officers to address situations where defined NIHB allowable fees cannot cover the actual professional costs due to specific client needs.

General Control Environment

We expected that management would have a process for reviewing, confirming and monitoring all users' access rights to the system, and that management would periodically review who has accessed the system and what transactions have occurred. Best practice also requires that passwords be properly managed to control access to the system.

We found that the control environment for the HICPS is generally satisfactory. However, we had two concerns. First, there is no monitoring of user activity of the HICPS including activity at the database level. We also noted that documentation relating to the granting of

the HICPS access privileges to NIHB staff was incomplete. Such documentation is central to ensuring that only authorized personnel can access the data in the HICPS.

Management Review of User Activity

We found no documented evidence that management routinely tracks and monitors which NIHB staff have accessed the HICPS application. Management does not monitor user activity to HICPS including access to the database by the Data Base Administrators (DBAs) working at the subcontractor's facility. This is of concern because DBAs, unlike other users, have unlimited access to the database, including the ability to make changes to it.

We note that reports for tracking and monitoring purposes could be available to management. The system does have the capability to generate logs that can provide an audit trail which records transactions and tracks who has accessed the system. However, at the time of the audit, the subcontractor had not turned on the audit-trail feature because it consumes large amounts of computing resources and affects the performance of the system.

Because this feature had not been activated, no monitoring takes place of any activity on HICPS. Accordingly, management had no way of knowing if there has been any irregular activity or potentially inappropriate access to the database.

Not using available information to periodically review the system-related activities of all users, including DBAs, exposes the Department to the risk that someone could access or make unauthorized changes to the HICPS data (thus compromising its accuracy and completeness), and that the Department would not be able to determine who was responsible.

We also noted that Data Base Administrators at the subcontractor's facility could make unlimited unsuccessful attempts to log into the system without being locked out. Therefore, there is a risk that anyone from this group could, through a process of trial and error, find a password that would give him or her access to the system without proper authorization.

Recommendation No. 2

It is recommended that the Assistant Deputy Minister, First Nations and Inuit Health Branch, ensure that the activities of all users who have access to the Health Information Claims Processing System, including access to the database, are periodically monitored. Monitoring should include the activities of NIHB staff at the application level, and of the subcontractor's Database Administrators at the database level.

Management Response

The Non-Insured Health Benefits Directorate agrees with the recommendation. This issue has been previously identified by the Program and for which new requirements have been built into the Statement of Work (SOW) for the new HICPS currently under development.

Administering Access to HICPS

Best practice and the Department's security policy require that the rights of users to access any system should be documented. We expected to find an up-to-date record of all NIHB employees who are authorized to access the system, what operations they are allowed to perform on it, and who has authorized them to do so. This information should be recorded on "Security Request Forms" (SRFs), which should be retained for at least three years, as required by the government's Policy on Information Holdings.

We found that a number of SRFs in our sample were incomplete. For example, some did not indicate who had requested the authorization for particular employees to access the system, or who had ultimately granted it. Other SRFs had been discarded by the sub-contractor after one year.

Recommendation No. 3

It is recommended that the Assistant Deputy Minister, First Nations and Inuit Health Branch, ensure:

(a) that all Security Forms are retained at least 3 years (i.e. Policy on Information Management);
(b) that all Security Request Forms are approved by only authorized staff; and
(c) that all Security Request Forms contain approval signatures of authorized management.

Management Response

The Non-Insured Health Benefit Directorate agrees with this recommendation and has already taken measures to resolve the problem. A full reconciliation of Health Canada users has been conducted in response to a Privacy Impact Assessment completed by the Program in June 2006. The reconciliation ensures that only authorized users have access to the current HICPS.

Problem Management

We expected NIHB management to have implemented a system for ensuring that all operational incidents, problems and errors are recorded, analyzed and resolved in a timely manner.

The HICPS-related problems are designated as "Critical", "High", "Medium" or "Low", and are prioritized accordingly. For the purposes of this audit, we focussed on "Critical" problems in four problem logs maintained by the contractor and the subcontractor in order to provide assurance that they were being resolved without undue delay. Critical problems are defined as **"**A system problem impeding service delivery for which there is

no reasonable system or manual work around (the work around would be time intensive, require high human interaction, or be open to repeated human error), and/or is a risk to client health and safety, and/or increases program cost, and/or compromises client, financial and/or provider data integrity, and/or impedes 5+ users or one entire office/region, and/or compromises system security**"**.

In analyzing the problem logs, we found a total of 176 critical problems. Of these, 24% critical problems had been resolved within 48 hours. We found that it took more than 2 months to resolve 38% of the critical problems.

Although there is a Performance Incentive Program (PIP) implemented in the 2007 contract year we noted that there is no formal agreement between the contractor and its subcontractor that sets reasonable standards for the time to resolve ***critical*** problems (as defined above). The PIP provides incentives for resolving critical problems within between one and twelve months.

Taking a long time to resolve critical problems is of concern, given the risks of impeding service delivery, the risks of increases in program costs, and/or the risk of compromising client, financial and/or provider data integrity that continues while these problems remain unresolved is a concern.

Recommendation No. 4

It is recommended that the Assistant Deputy Minister, First Nations and Inuit Health Branch, ensure that there are shorter agreed- upon standards with the contractor/sub-contractor required to resolve critical problems.

Management Response

The Non-Insured Health Benefits Directorate agrees that the timely resolution of adjudication system problems deserves continuous attention. Through negotiations, NIHB has made significant progress in reducing the problem log list and improving the management and resolution of problems under the terms of the contract. The Non-Insured Health Benefits Directorate is not in a position under the terms of the contract established in 1997 to further incite the contractor, and has decided to impose new requirements on the new contractor to implement problem resolution standards. The contractor also has an obligation under the terms of the new contract to ensure these requirements apply to any sub-contractor. To make real progress in the short-term NIHB Directorate has enhanced its efforts at the system-testing stage to reduce the occurrence of error, as well as to continually work with the contractor/prime contractor to identify effective and timely solutions and work-arounds, and to prioritize work according to risk. None of the problems currently being addressed are creating health or financial risks for the department and the log is subject to regular joint review process to prioritize according to risks. Measures have been taken to refine the incident management process and standards under the new HICPS contract and ensure these requirements will apply to any sub contractors

Backup and Recovery

There should be documented procedures used to define and implement the backup and restoration of system and data as part of a business continuity and disaster recovery plan. There should also be adequate safeguards in place to protect the data. We verified and tested for compliance to the procedures and to best practices needed to ensure that the system and its data was adequately backed up and if necessary restored. We found that the subcontractor was complying with the procedures required to backup, restore and safeguard the system and its data.

Appendices

Appendix A: Lines of Enquiry and Audit Criteria

LINES OF ENQUIRY	AUDIT CRITERIA
A. The completeness and accuracy of the claims data	
The controls to ensure that transactions are completely and accurately processed	• Procedures ensure that all authorized source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry. • Transaction data entered for processing people generated, system-generated or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness and validity.
Segregation of duties with respect to transaction processing;	• Authorized personnel who are acting within their authority properly prepare source documents and an adequate segregation of duties is in place regarding the origination and approval of source documents.
The accuracy and completeness of claims data uploaded to SAP.	• Output is routinely balanced to the relevant control totals. Audit trails facilitate the tracing of transaction processing and the reconciliation of disrupted data.
The process for identifying and correcting, in a timely manner, transactions that have been incorrectly processed (Error Processing).	• Procedures for the correction and re-submission of data that were erroneously input are in place and followed. • Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.
B. The general control environment for limiting access to the system	
Management reviews user accounts.	• Management should have a control process in place to review and confirm access rights periodically.
Access to HICPS by NIHB employees is controlled and monitored.	• User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person.
Access to the system by Database Administrators (DBAs) is controlled and periodically reviewed.	• Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external
There is a problem management system in place and problems are resolved in a timely manner.	• The organisation should establish data processing error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruption of the processing of other valid transactions.
Back-up and recovery procedures are in place.	• Define and implement procedures for backup and restoration of systems, data and documentation in line with business requirements and the continuity plan. Verify compliance with the backup procedures, and verify the ability to and time required for successful and complete restoration. Test backup media and the restoration process.

Audit criteria have been summarized for presentation purposes.

Appendix B: System Architecture