OHIP Technical Bulletin

Claims Services Branch

Ensuring excellence in claims service delivery for Ontarians

To: **OHIP Billing Software Vendors**

Date Issued: **August 12, 2016** **Bulletin #: 16-001**

Re: **MCEDT and HCV Web Service Security Certificate and Cryptography Protocol Upgrade**

The ministry will be updating its security certificates and cryptography protocol to be in line with industry standards. This Technical Bulletin is intended to provide details on the upgrade and the procedures required by vendors. It also serves as notification of changes to the Technical Specification for the Medical Claims Electronic Data Transfer (MCEDT) Service via Electronic Business Services (EBS) and Technical Specification for Health Card Validation (HCV) Service via Electronic Business Services (EBS). This upgrade will require all vendors to successfully demonstrate compliance by **undergoing modified conformance testing by October 31st, 2016**. The current URLs for the MC EDT and HCV Web Services will be **decommissioned December 9th, 2016**.

Background

Certificate Update

Secure Hash Algorithm (SHA) is a cryptographic hash function used by web applications in order to encrypt data. SHA-1 was introduced in 1995. In 2001, SHA-2 was introduced; strengthening the encryption process from SHA-1.

Ontario

During this time, web applications and web servers were able to process security certificates using either SHA-1 or SHA-2. In 2005, many organizations suggested that SHA-1 was not secure enough for ongoing use. In 2014, many browser developers (Microsoft, Google, Mozilla) announced that their browsers would stop accepting SHA-1 security certificates by 2017. In response to the support for SHA-1 ending, the ministry will update all its security certificates to SHA-2 by January 1st, 2017.

Internet Cryptography Protocol Update

Secure Sockets Layer (SSL) is a cryptography protocol for establishing an encrypted link between 2 machines, for example a browser and web server. In response to vulnerabilities in this protocol, the ministry is discontinuing support for SSL v3 and TLS 1.0. The MC EDT and HCV Web Services will restrict all connections to Transport Layer Security (TLS) protocols TLS 1.1 and TLS 1.2.

Security Update Procedures

In order to manage a smooth transition to the new security certificates and updated cryptography, the ministry will migrate all MC EDT and HCV clients to new URLs. The ministry will provide new production and conformance URLs.

All vendors will be required to successfully complete conformance testing before October 31st, 2016. Vendors are highly encouraged to begin conformance testing as soon as possible to prevent backlogs due to volume before the deadline. Upon successful completion of conformance testing, an updated URL will be provided for the new production environment. The current URLs for the EDT Web Service and HCV Web Service will be decommissioned December 9th, 2016, so all vendors are required to complete conformance testing and start using the new environments prior to that date or risk a disruption in services to their customers.

The process for beginning conformance testing is as follows:

1. Submit Acceptable Use Policy (AUP) to the Service Support Contact Centre (SSCC) for conformance specifying you are retesting for SHA-2 compliance;

2. SSCC will provide the updated Technical Specifications and the new root certificates required for conformance testing and the new production environment;

3. MOHLTC test teams will contact you with credentials and the modified test scenarios; and

4. Upon successful completion of conformance you will be provided with the new production URL. You will continue to use your existing production key.