EWG M2 Recommendation to the ICH Steering Committee
Electronic Standards for the Transfer of Regulatory Information (ESTRI)
File Integrity Recommendation - SHA-256

Version 1.0 - 11JUNE2015

Title: SHA-256

Background:
It is recognized that there is a need for secure electronic regulatory information exchange among the ICH regions. Critical to this secure information exchange is a method to ensure that the recipient has received exactly what the sender intended.

Recommendation:
It is recommended that a "checksum" be utilized to ensure file integrity. A checksum or hash sum is a fixed-size datum computed from an arbitrary block of digital data for the purpose of detecting errors that may have been introduced during a file's transmission or storage. The integrity of the data can be checked at any later time by recomputing the checksum for the file and comparing it with the stored checksum value. If the checksum values do not match, the data was almost certainly altered (either intentionally or unintentionally).

The use of a checksum for transmitting files provides a number of benefits including:

- The integrity of each file can be verified by comparing the checksum submitted with the file and the computed checksum calculated upon receipt.
- The checksum can be used to verify that the file has not been altered in the historical archive of the regulatory authority. This is particularly useful as files are migrated from one storage medium to another (e.g., when files are backed up to magnetic tape storage).

Electronic submissions should contain checksums for each individual file transmitted. It is recommended that the SHA-256 Message-Digest Algorithm be used for this purpose.

The exact implementation will be defined in ESTRI specifications for the exchange message (e.g., the ESTRI eCTD specification defines the precise way in which checksums are included). Internal security and access control processes in the regulatory authority should maintain the integrity of the submitted files.

Conditions:
None

Remarks:

- In 2007 it was agreed by the ICH Steering Committee that ICH not become a data standards development organization but rather work with established data standards development organizations (SDOs), like Health Level 7 (HL7) and ISO, in order to develop, test and adopt new data standards based on ICH requirements. In keeping with this decision there are a number of technical standards under the arc of HL7 that ICH must adopt. The SHA-256 Message-Digest Algorithm is recommended as it has been established by HL7 as the preferred security standard to ensure file integrity.
- The Secure Hash Algorithm (SHA) was developed by the NIST (National Institute of Standards and Technology) in association with the NSA (U.S. National Security Agency) and first published in May 1993 as the Secure Hash Standard (later known as SHA-0). The first

revision to this algorithm was published in 1995 due to an unpublished flaw found (in SHA-0), and was called SHA-1. In addition to the SHA-1 hash, the NIST also published a set of more complex hash functions for which the output ranges from 224 bit to 512 bit. SHA-2 is a common name for these four hash functions also referred to as SHA- 224, SHA-256, SHA-384 and SHA-512. Their suffix originates from the bit length of the message digest they produce.

- Sample source code for the implementation of SHA is available as IETF RFC 4634.
- The previously issued ICH recommendation entitled “File Integrity – MD5” will remain in effect until withdrawn. However it is recommended that all future ICH-issued implementation guides and specifications for the transfer of regulatory information implement the SHA-256 standard.