EWG M2 给 ICH 指导委员会的建议
监管信息电子传输标准（ESTRI）
文件完整性建议 - SHA-256

版本 1.0-2015 年 6 月 11 日

标题：SHA-256

背景：

ICH 地区之间需要进行安全的电子监管信息交换在业界已成为共识。这种安全信息交换的关键在于确保接收者能够准确地收到发送者想要发送的信息的方法 。

建议：

建议使用“校验和”来确保文件的完整性。“校验和”或“哈希和”是由任意数字数据块计算的固定大小的数据，用于检测文件传输或存储期间可能引入的错误。数据的完整性可以随时通过重新计算文件的“校验和”并将其与存储的“校验和”进行比较来检查。如果“校验和”不匹配，基本可以确定数据被（有意或无意地）更改了。

将“校验和”用于传输文件有很多优点，包括：

- 可以通过比较与文件一起提交的“校验和”以及收到文件后计算的“校验和”来验证每个文件的完整性。
- 可以使用“校验和”来验证文件在监管部门的历史归档中未被更改。尤其是当文件从一个存储介质迁移到另一个存储介质时（例如，当文件备份到磁带存储器时）。

电子提交应包括所传输的每个独立文件的“校验和”。建议将 SHA-256 消息摘要算法用于此目的。

在 ESTRI 规范中将对交换消息的准确实施加以规定（例如，ESTRI eCTD 规范定义了包括“校验和”在内的精确实施方法）。监管部门的内部安全和访问控制流程应维护所提交文件的完整性。

条件：

无

备注：

- 2007 年，ICH 指导委员会一致通过 ICH 不会成为数据标准制定组织，而是与 Health Level 7（HL7）和 ISO 等成熟的数据标准开发组织（SDO）合作，开发、测试和采用基于 ICH 要求的新数据标准。根据这一决定，ICH 必须采用 HL7 信息弧下的一系列技术标准。ICH 建议采用 SHA-256 消息摘要算法，因为它已被 HL7 确立为确保文件完整性的首选安全标准。
- 安全哈希算法（SHA）由 NIST（美国国家标准技术研究所）与美国国家安全局（US National Security Agency, NSA）联合开发，并于 1993 年 5 月首次发布为安全哈希标准（此后称为 SHA-0）。由于（在 SHA-0 中）发现了一个未发布的缺陷，在 1995 年发表了该算法的第一次修订，该修订被称为 SHA-1。除了 SHA-1 哈希，NIST 还发布了一组更复杂的哈希函数，其输出

范围从 224 位到 512 位。SHA-2 是这四个哈希函数的通用名称，也称为 SHA-224、SHA-256、SHA-384 和 SHA-512。 它们的后缀源自它们产生的消息摘要的位长度。

- 用于实施 SHA 的源代码样例能够以 IETF RFC 4634 的形式获得。
- ICH 以前发布的 “文件完整性-MD5” 建议将一直有效直至被撤销。针对监管信息传输，ICH 建议未来所有发布的实施指南和规范遵循 SHA-256 标准。