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 – MD5

版本 1.0　2010 年 6 月 10 日

标题：文件完整性 - MD5

日期：2010 年 6 月 10 日

背景：

三个 ICH 地区之间进行安全的电子监管信息交换在业界已成为共识。这种安全的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，用于检测在传输或存储期间可能产生的意外错误。数据的完整性可以随时通过重新计算“校验和”并将其与存储“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。

电子化提交应包括所传输的每个独立文件的“校验和”。建议将 MD5 消息摘要算法（MD5）用于此目的。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”和计算的“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）。

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：MD5 是由互联网工程任务组（IETF）RFC 1321 定义的开放标准。ICH M2 认识到 MD5 设计中存在有记录的缺陷，虽然密码学家已经开始建议使用其他算法， 但是，MD5 足以满足验证文件完整性的要求。