

## 美國衛生部門公布個人健康資訊外洩責任實施綱領



美國健康與人類服務部（Secretary of Health and Human Services；以下簡稱HHS），於2009年4月17日公布「個人健康資訊外洩通知責任實施綱領」（Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information；以下簡稱本綱領）。本綱領為美國迄今唯一聯盟層級之資料外洩通知責任實施細則，並可望對美國迄今四十餘州之個資外洩通知責任法制，產生重大影響。

本綱領之訂定法源，係依據美國國會於2009年2月17日通過之經濟與臨床健康資訊科技法（Health Information Technology for Economic and Clinical Health Act；以下簡稱HITECH），HITECH並屬於2009年「美國經濟復甦暨再投資法」（America Recovery and Reinvestment Act；簡稱ARRA）之部分內容。

HITECH將個人健康資訊外洩通知責任的適用主體，從「擁有」健康資訊之機構或組織，進一步擴大至任何「接觸、維護、保留、修改、紀錄、儲存、消除，或以其他任何形式持有、使用或揭露安全性不足之健康資訊」的機構或組織。此外，HITECH並規定具體之資料外洩通知方法，即必需向當事人（資訊主體）以「即時」（獲知外洩事件後60天內）、「適當」（書面、或輔以電話、網站公告形式）之方式通知。不過，由於通知之範圍僅限於發生「安全性不足之健康資訊」外洩，故對於「安全性不足」之定義，HITECH即交由HHS制定相關施行細則規範。

HHS本次通過之實施辦法，將「安全」之資料定義「無法為第三人使用或辨識」，至於何謂無法使用或辨識，本綱領明定有兩種情形，一是資料透過適當之加密，使其即使外洩亦無法為他人辨識，另一則是該外洩資訊之儲存媒介（書面或電子形式）已被收回銷毀，故他人無法再辨識內容。

值得注意的是，有異於美國各州法對於加密標準之不明確態度，本綱領已指明特定之技術標準，方為其認可之「經適當加密」，其認可清單包含國家標準與技術研究院（National Institute of Standards and Technology）公布之Special Publication 800-111，與聯邦資訊處理標準140-2。換言之，此次加密標準之公布，已為相關業者提供一可能之「安全港」保護，使業者尚不幸遭遇資料外洩事件，得主張資料已施行適當之加密保護，即無需承擔龐大外洩通知成本之衡平規定。

本文為「經濟部產業技術司科技專案成果」

### 相關附件

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf> [pdf]

[American Recovery and Reinvestment Act](#) [pdf]

鄭菀瓊 編譯整理

上稿時間：2009年05月

**資料來源：**

American Recovery and Reinvestment Act，2009年02月18日，[http://www.hipaa.com/documents/arra\\_2009.pdf](http://www.hipaa.com/documents/arra_2009.pdf)，最後瀏覽日：2009年06月08日

Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements，2009年04月17

日，<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/hitechrfi.pdf>，最後瀏覽日：2009年06月08日

**延伸閱讀：**

張乃文，美國「2009年經濟復甦暨再投資法」大幅度修正HIPAA隱私權條款，載於資策會科技法律中心網站-資訊通信法制-資訊安全-法律要聞，2009年04月，<http://stlc.iii.org.tw/ContentPage.aspx?i=3018>

推薦文章