

保護電子病歷資料，遵循 HIPAA 要求

以業界最佳範例建立堅實的電子病歷資料與應用程式保護機制

從紙本作業走向電子化應用程式處理電子病歷資料的過程中，如何讓這些資料以更安全的方式儲存與處理，成為政府機關與業界一個重要的課題。美國健康保險可攜性與責任法案(Health Insurance Portability & Accountability Act, HIPAA)原本是在紙本病歷資料的處理環境下通過，對於電子病歷資料(ePHI)的管理、使用技術、與實體資料的保護反而成為難題。在 HIPAA 規範下，健康照護業者與醫療資訊交換中心(health care clearing houses)必須謹慎處理個人資料，像是姓名、住所、聯絡方式、身份證字號等。這些機構必須在資料儲存時期、傳輸過程、使用過程中謹慎盡到保護的義務。

主要優點

- 提供完整解決方案，並可降低遵循成本與複雜度
- 遵循HIPAA法規的最安全解決方案
- 完整的稽核記錄
- 不影響作業流程
- 可針對特定法規遵循進行模組化支援

SafeNet 符合 HIPAA 要求	
要求	SafeNet 解決方案
164.308 (a)(1) 安全管理流程：建立規則與作業程序，以避免、偵測、控制、與矯正安全問題。	二維認證(Two-Factor Authentication) 檔案加密(File Encryption) 磁碟加密(Disk Encryption) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.308 (a)(3) 受雇成員之安全要求：建立規則與作業程序，確保所有受雇成員對電子病歷資料有適當的存取權限，避免沒有授權的成員接觸電子病歷資料。	二維認證(Two-Factor Authentication) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.308 (a)(4)資料存取管理：建立規則與作業程序，經過申請方可授權存取電子病歷資料。	二維認證(Two-Factor Authentication) 磁碟加密(Disk Encryption) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.308 (a)(7) 意外事件應變計畫：建立規則	二維認證(Two-Factor Authentication)

與作業程序，對於緊急事件或突發事件有完整的應變計畫。	檔案加密(File Encryption) 磁碟加密(Disk Encryption) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module) 網路加密(Network Encryption)
164.310 (a)(1) 設備存取控制：建立規則與作業程序，限制實體的資訊系統與設備存取，確保適當的存取授權。	二維認證(Two-Factor Authentication) 硬體加密模組(Hardware Security Module)
164.310 (c) 工作站安全：建立規則與作業程序，建立工作站實體安全，確保授權使用者存取電子病歷資料。	二維認證(Two-Factor Authentication) 磁碟加密(Disk Encryption) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.310 (d)(1) 設備與媒體控制：建立規則與作業程序，由設備取出之硬體、設備送出之電子資料不含電子病歷內容。	二維認證(Two-Factor Authentication) 磁碟加密(Disk Encryption) 網路加密(Network Encryption)
164.312 (a)(1) 存取控制：建立規則與作業程序，資訊系統只允許授權人員或應用程式進行存取。	二維認證(Two-Factor Authentication) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.312 (c)(1) 完整性：建立規則與作業程序，保護電子病歷資料不受竄改、損毀。	磁碟加密(Disk Encryption) 二維認證(Two-Factor Authentication) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.312 (d) 人員或實體認證：建立規則與作業程序，檢驗人員或實體存取電子病歷資料之認證。	磁碟加密(Disk Encryption) 二維認證(Two-Factor Authentication) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module)
164.312 (e)(1) 通訊安全：建立技術評量方法，保護電子病歷資料不受未經授權的通訊網路傳輸。	二維認證(Two-Factor Authentication) 檔案加密(File Encryption) 磁碟加密(Disk Encryption) 資料庫加密(Database Encryption) 硬體加密模組(Hardware Security Module) 網路加密(Network Encryption)

HIPAA 法規遵循

SafeNet以最完整、最易於管理的資料保護解決方案，大幅縮減企業遵循HIPAA的成本與複雜度。SafeNet的EDP(Enterprise Data Protection)能協助必須遵循HIPAA法規的健康相關機構，得到最先進的加密與金鑰管理技術。其他單獨效果的解決方案只強調單一需求的支援，SafeNet是唯一可從資料庫、應用程式、網路、端點設備等，全面性的保護企業資料，並減少遵循成本與複雜度。

Safe 企業資料保護

SafeNet企業資料保護(Enterprise Data Protection、EDP)是目前市面上唯一由內而外的資料保護解決方案，從儲存中的資料、傳輸中資料、使用中的資料，SafeNet的EDP解決方案可減少法規遵循、資料隱私、與資料風險管理之成本，並降低建置複雜度。不若其他不同廠牌拼湊出來只有「單獨效果」的方案，SafeNet EDP解決方案提供完整、集中控管的資安政策與報表的資安平台，可全面管理資料庫內資料、應用程式資料、網路傳輸資料與端點資料。想獲得更多SafeNet EDP資訊，請瀏覽www.safenet-inc.com/EDP。

關於 SafeNet

SafeNet是全球知名的資安廠商，成立超過 25 年，以加密技術提供完整的資安需求，從資料傳輸、智慧財產、到數位身份識別(digital identities)，全系列產品線包括硬體、軟體與加密晶片組。我們的客戶包括ARM、美國銀行、思科、美國國防部與國土安全部、微軟、三星、德州儀器、美國國稅局等等客戶都將他們的安全交付給SafeNet。想獲得更多資訊，請瀏覽www.safenet-inc.com網站。