美國NIST發布更新《網路安全資源指南》提升醫療領域的網路安全及隱私風險管理

美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）於2022年7月21日發布更新《網路安全資源指南》（A Cybersecurity Resource Guide, NIST SP 800-66r2 ipd）。本指南源自於1996年美國《健康保險流通與責任法》（Health Insurance Portability and Accountability Act, HIPAA）旨在避免未經患者同意或不知情下揭露患者之敏感健康資料，並側重於保護由健康照護組織所建立、接收、維護或傳輸之受保護電子健康資訊（electronic protected health information, ePHI），包括就診紀錄、疫苗接種紀錄、處方箋、實驗室結果等患者資料之機密性、完整性及可用性。其適用對象包含健康照護提供者（Covered Healthcare Providers）、使用電子方式傳送任何健康資料的醫療計畫（Health Plans）、健康照護資料交換機構（Healthcare Clearinghouses）及為協助上述對象提供健康照護服務之業務夥伴（Business Associate）均應遵守。

本指南最初於2005年發布並經2008年修訂（NIST SP 800-66r1 ipd），而本次更新主要為整合其他網路安全相關指南，使本指南與《網路安全框架》（Cybersecurity Framework, NIST SP 800-53）之控制措施等規範保持一致性。具體更新重點包括：（1）簡要概述HIPAA安全規則；（2）為受監管實體在ePHI風險評估與管理上提供指導；（3）確定受監管實體可能考慮作為資訊安全計畫的一部分所實施的典型活動；（4）列出受監管實體在實施HIPAA安全規則之注意事項及其他可用資源，如操作模板、工具等。特別在本指南第三章風險評估與第四章風險管理提供組織處理之流程及控制措施，包括安全管理流程、指定安全責任、員工安全、資訊近用管理、安全意識與培訓、應變計畫、評估及業務夥伴契約等。而在管理方面包括設施權限控管、工作站使用及安全、設備媒體控制；技術方面則包含近用與審計控管、完整性、個人或實體身分驗證及傳輸安全。上述組織要求得由政策、程序規範、業務夥伴契約、團體健康計畫所組成，以助於改善醫療領域的網路安全及隱私保護風險管理。預計本指南更新將徵求公眾意見至2022年9月21日止。

相關連結

- NIST Updates Guidance for Health Care Cybersecurity, National Institute of Standards and Technology, July 21, 2022
- Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (NIST Special Publication 800-66, Revision 2), National Institute of Standards and Technology, July 21, 2022

你可能會想參加

- → 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- → 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
- → 供應鏈資安國際法制與政策趨勢分享會
- → 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 數位發展部數位產業署113年資訊服務業安維計畫常見問題分享說明會
- → 商業服務業個資保護宣導說明會
- → 個人資料保護新思維企業法遵論壇
- → 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座

→ 中部場–商業服務業個資保護工作坊
→ 南部場–商業服務業個資保護工作坊
→ 北部場–商業服務業個資保護工作坊
→ 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會
→ 電商零售業法制宣導說明會暨產學研座談會
→ 數位海盜時代來臨–抵禦海上資安威脅的實踐與挑戰
→ 零售業個資保護宣導暨座談會
→ 零售業個資保護及資訊安全教育講習
→ 零售業個資保護及資訊安全教育講習

盧秉羲
副法律研究員 編譯整理

上稿時間：2022年09月

資料來源：

NIST Updates Guidance for Health Care Cybersecurity, National Institute of Standards and Technology, July 21, 2022, https://www.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity（last visited Sept. 2, 2022）.

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (NIST Special Publication 800-66, Revision 2), National Institute of Standards and Technology, July 21, 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf（last visited Sept. 2, 2022）.

延伸閱讀：

施雅薰，〈歐盟執委會發布「歐洲健康資料空間」規則提案，旨在克服健康資料利用之障礙〉，資訊工業策進會科技法律研究所，2022/6，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8858（最後瀏覽日：2022/9/2）。

邱美蘅，〈美國21世紀醫療法最終規則下之資訊封鎖條文生效，患者健康資料進用權利獲保障〉，資訊工業策進會科技法律研究所，2021/6，https://stli.iii.org.tw/article-detail.aspx?tp=1&d=8679&no=64（最後瀏覽日：2022/9/2）。

文章標籤

TPIPAS　個資管理制度　個人資料　智慧醫療　資訊安全　隱私保護

科法觀點

保護隱私！資策會成APEC跨境隱私規則當責機構

推薦文章