

## Refuah公司與紐約總檢察長達成和解並投資120萬美元保護病人資料



紐約州總檢察長Letitia James於2024年1月5日與健康照護服務業者Refuah Health Center, Inc.（下稱Refuah公司）達成和解，主因為該公司遭受勒索軟體攻擊（ransomware attack），約25萬紐約州民個資遭到洩漏。和解協議要求Refuah公司支付共計45萬美元之民事懲罰金及費用（penalties and costs），且應投資120萬美元加強網路安全（cybersecurity）。

Refuah公司主要業務為經營三家醫療機構和五輛行動醫療車（mobile medical vans）。2021年5月，Refuah公司遭到勒索軟體攻擊，網路攻擊者得以近用數千名病人的資料，取得了包含姓名、地址、電話號碼、社會保險號碼、駕照號碼、出生日期、金融帳號、醫療保險號碼等資料。

依據檢察長辦公室的調查顯示，攻擊者之所以得近用這些資料，原因為Refuah公司未採取適當安全維護措施，包括：未停用不活躍之使用者帳號（inactive user accounts）；未定期更換使用者帳號憑證（user account credentials）；未限制員工僅得近用其業務所必需之資源和資料；未使用多重要素驗證（multi-factor authentication）以及未加密病人資料。

依據協議內容，Refuah公司同意投資120萬美元，用於開發和維護更強大的資訊安全計畫（information security programs），以更妥適地保護病人資料。該協議還要求Refuah公司應：

1. 維護全面的資訊安全計畫，以保護消費者資料的安全性、機密性和完整性；
2. 實施並持續更新消費者資料近用限制相關政策和程序；
3. 遠端近用資源和資料應使用多重要素驗證；
4. 定期更新近用資源和資料的憑證；
5. 至少每半年進行一次稽核，確保使用者僅近用其業務所必需之資源和資料；
6. 對所有儲存或傳輸的消費者資料進行加密；
7. 實施控制措施，監控和記錄公司網路和系統的所有安全和操作活動；以及
8. 制定、實施和持續更新全面的事務應變計畫。

Refuah公司還須向州政府支付共計45萬美元之民事懲罰金及費用，其中10萬美元將在該公司投入120萬美元開發和維護其資訊安全計畫後，得暫緩支付。

### 相關連結

[Office of the New York State Attorney General\[NYAG\], Attorney General James Reaches Agreement with Hudson Valley Health Care Provider to Invest \\$1.2 Million to Protect Patient Data \(2024\)](#)

### 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
- 112年度「領航臺灣數位轉型」國際研討會-實體場
- 112年度「領航臺灣數位轉型」國際研討會-直播場
- 新創採購-政府新創應用分享會
- 【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管理常見問題說明會



## 謝滄婷

法律研究員 編譯整理

上稿時間：2024年05月

### 資料來源：

Office of the New York State Attorney General[NYAG], Attorney General James Reaches Agreement with Hudson Valley Health Care Provider to Invest \$1.2 Million to Protect Patient Data (2024), <https://ag.ny.gov/press-release/2024/attorney-general-james-reaches-agreement-hudson-valley-health-care-provider> (last visited Mar.20, 2024).

### 延伸閱讀：

阮韻蓀，〈美國公布實施零信任架構相關資安實務指引〉，資策會科法所法律要聞，<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=8885&no=64>（最後瀏覽日：2024/03/20）。

陳政陽，〈新加坡物聯網產品網路安全防護之初探〉，資策會科法所法律要聞，<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=9061&no=64>（最後瀏覽日：2024/03/20）。

劉宥好，〈歐盟推出給在中華區企業參考之網路犯罪與營業秘密保護指南〉，資策會科法所法律要聞，<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=8929&no=64>，（最後瀏覽日：2024/03/20）。

### 文章標籤

個資管理制度

物聯網

個人資料

資訊安全

隱私保護

## 推薦文章