防疫也須防弊！美國加州檢察總長針對醫療照護機構遭受勒索軟體攻擊提出適當措施與事故通報指引

由於近日頻傳醫院遭受勒索軟體攻擊（ransomware attacks），美國加州檢察總長於2021年8月24日發布官方公告（bulletin）：在加州州法「醫療資訊保密法」（Confidentiality of Medical Information Act, CMIA）與聯邦法「健康保險可攜與責任法」（Health Insurance Portability and Accountability Act of 1996, HIPAA）規範下，蒐集、處理和利用醫療健康資料的醫療照護機構，有採取適當措施與事故通報的義務，以維護醫療健康資料保密性。

針對「採取適當措施」的內容，美國加州檢察總長於本次官方公告中，提出明確指引（guidance）：醫療照護機構須至少採取下列5項防範措施（preventive measures），以避免勒索軟體威脅：

1. 確保所有存取醫療健康資料的作業系統與軟體，均升級至最新版本；
2. 安裝防毒軟體，並維護其運作；
3. 定期為員工舉辦教育訓練，包含教導員工不要點擊可疑網址和防範釣魚電子郵件（phishing email）；
4. 限制員工下載、安裝和運作未經批准的軟體；
5. 維護和定期測試資料備份與救援計畫，以便於事故發生時，控制對資料和系統的影響範圍及程度。

此外，針對「資料外洩事故通報義務」（breach notification obligations），美國加州檢察總長指出：依據「加州民法」（California Civil Code）第1798.82條，擁有或經授權使用含有個人資料的「電腦化資料」（computerized data）的醫療照護機構，於發生，或可合理確信發生，影響超過500位加州居民的資料外洩事故時，即負有將該事故通報檢察總長辦公室的義務。

相關連結

- Attorney General Rob Bonta Calls for Full Compliance with State Health Data Privacy Laws
- CA Attorney General Calls Out Unreported Healthcare Data Breaches
- Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector
- 加州消費者隱私保護法修正法案重點說明
- 美國衛生暨福利部於09年8月公布關於醫療資訊外洩通知義務之暫行最終規則

相關附件

- BULLETIN: Obligation to Proactively Reduce Vulnerabilities to Ransomware Attacks and Requirements Regarding Health Data Breach Reporting [pdf]

你可能會想參加

→ 【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
→ 【2023科技法制變革論壇】 高齡科技發展與法制策略論壇
→ 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
→ 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

李宗儒
副法律研究員 編譯整理

上稿時間：2021年10月

資料來源：

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE OFFICE OF THE ATTORNEY GENERAL, *Attorney General Rob Bonta Calls for Full Compliance with State Health Data Privacy Laws*, Aug. 24, 2021, https://oag.ca.gov/news/press-releases/attorney-general-rob-bonta-calls-full-compliance-state-health-data-privacy-laws (last visited Sep. 16, 2021).
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE OFFICE OF THE ATTORNEY GENERAL, *BULLETIN: Obligation to Proactively Reduce Vulnerabilities to Ransomware Attacks and Requirements Regarding Health Data Breach Reporting*, Aug. 24, 2021, https://oag.ca.gov/system/files/attachments/press-docs/2021AUG24%20Ransomware%20Bulletin.pdf (last visited Sep. 16, 2021).
Jill McKeon, *CA Attorney General Calls Out Unreported Healthcare Data Breaches*, HEALTHITSECURITY, Aug. 27, 2021, https://healthitsecurity.com/news/ca-attorney-general-calls-out-unreported-healthcare-data-breaches (last visited Sep. 16, 2021).

延伸閱讀：

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY [CISA], *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector*, Oct. 28, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-302a (last visited Sep. 16, 2021).
邱曉麗，〈加州消費者隱私保護法修正法案重點說明〉，資策會科技法律研究所，2021/03，https://stli.iii.org.tw/article-detail.aspx?tp=1&i=180&d=8630&no=64（最後瀏覽日：2021/09/16）。
詹世榕，〈美國衛生暨福利部於09年8月公布關於醫療資訊外洩通知義務之暫行最終規則〉，資策會科技法律研究所，2009/11，https://stli.iii.org.tw/article-detail.aspx?tp=1&i=40&d=3167&no=64（最後瀏覽日：2021/09/16）。

文章標籤

個資管理制度 智慧醫療 隱私保護 數位健康

推薦文章