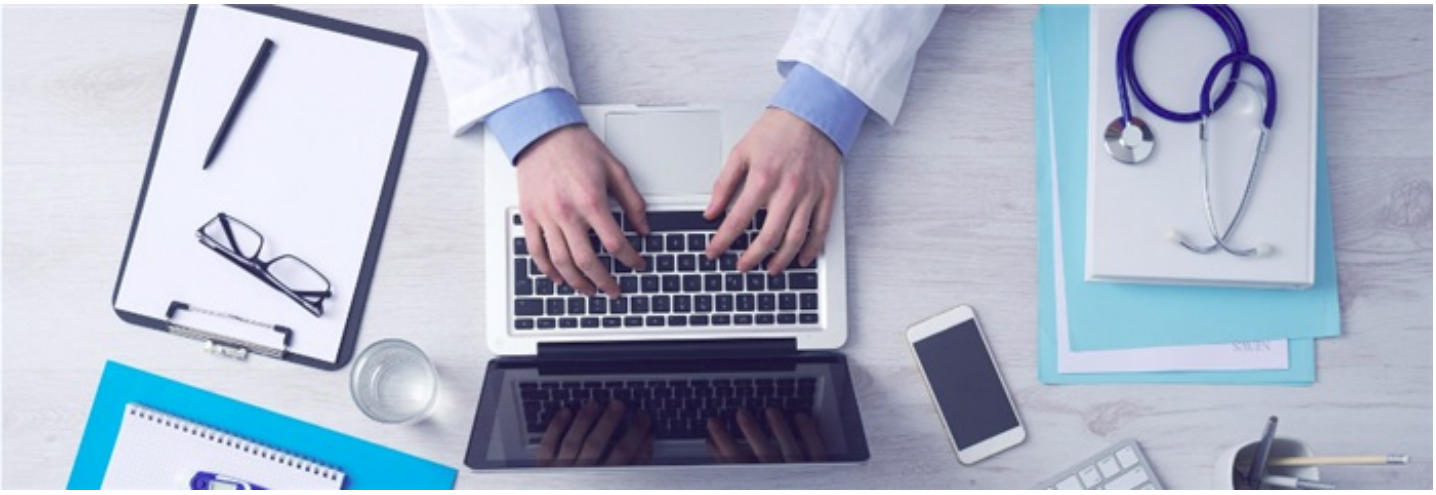
美國公民權利辦公室就Sentara醫療機構違反個資外洩通知義務予以重罰



美國衛生及公共服務部（Department of Health and Human Services, 下稱HHS）轄下的公民權利辦公室（Office for Civil Right, 下稱OCR）在2019年11月27日，正式對Sentara醫療機構處以217萬美元行政罰，主因該機構違反《健康保險可攜與責任法》（Health Insurance Portability and Accountability Act, 下稱HIPAA）的醫療個資外洩通知義務。

HIPAA是美國有關醫療個資管理的主要規範，依據HIPAA第164.400條以下「違反通知規則」（Breach Notification Rule）規定，當超過500位病患的「受保護健康資訊」（Protected Health Information, 下稱PHI）遭受不當使用或被外洩時，除應通知受害人外，還必須立即告知HHS以及在當地知名媒體發布新聞。而OCR主要負責檢查受規範機構，是否確實執行HIPAA隱私、安全和違反通知規則。

而在2017年4月，HHS收到指控Sentara將含有病患姓名、帳號、就診日期等涉及PHI的帳單發送到錯誤地址，造成557名病患個資外洩。Sentara卻認為該帳單內容未含有病患病歷、治療資訊或其他診斷紀錄，且僅有8人被影響，並非HIPAA應進行個資外洩通知義務之範疇，故不依規定程序通報HHS。不過OCR認為依HIPAA第160.103條規定，PHI包含病史、保險資訊、就醫紀錄（含日期）、身心健康狀態等可識別個人之健康資訊。因此認為Sentara確實違反個資外洩通知義務，予以罰款並命檢討改善。

Sentara醫療機構服務範圍橫跨美國維吉尼亞州（Virginia）和北卡羅來納州（North Carolina），共有12家急性照護醫院、10家護理中心和3家照護機構，為美國最具知名的大型非營利醫療機構之一。這次重罰也告誡國內醫療機構當發生敏感性醫療個資外洩時應從嚴判斷，以避免民眾對醫療照護單位失去信任，確保國內醫療機構體系應恪遵HIPAA規範。

相關連結

- 1. OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information
- About Us
- Breach Notification Rule

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
- → 【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
→ 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

吳昌鴻
法律研究員 編譯整理

上稿時間：2020年02月

資料來源：

1. OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information, HHS, https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html (last visited Dec. 3, 2019).
2. About Us, OCR, https://www.hhs.gov/ocr/about-us/index.html (last visited Dec. 3, 2019).
3. Breach Notification Rule, OCR, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Dec. 4, 2019).

文章標籤

個人資料 隱私保護

推薦文章