

# 馬偕醫學院 個資即時防護 稽核符合規定

## 採用 IBM Guardium 全面保護個資安全



2009年創校的馬偕醫學院，目前共有醫學系、護理學系、聽力暨語言學系與生物醫學研究所等四大系所。馬偕醫學院資訊中心楊明正主任指出，醫學院與一般大專院校有許多差異，資安防護也需考量更多。

### 醫學院資安考量多，個資防護成焦點

首要差異來自複雜學制與課程。醫學院學制共七年，涵蓋一般課程、整合型課程、PBL 小組專案課程、實習課程等。許多課程會長期累積圖檔、研究內容、動態模擬紀錄等異質資料，導致資料複雜度高，資安規劃與管理也更為複雜。

其次，醫學院有許多研究個資。這些研究資料未來可能成為學校與研究團隊的專利及智慧財產，其重要性可見一斑。

因此，即便2009年創校時個資法尚未三讀通過、詳細規範內容未知，許多學校還採取觀望姿態，馬偕醫學院資訊團隊就當機立斷、決定要以最新觀念及最高標準來規劃個資防護。

「研究指出，有80%的資料外洩是來自資料庫伺服器，但是網路安全卻佔去80%預算與人力，資料庫安全只能分到20%資源；」楊明正說明，「我們是全新學校，沒有舊包袱，所以決定一開始就把資料庫安全做好。」

**馬**偕紀念醫是北台灣最古老的西式醫院，100多年來從事醫療傳道，造福無數病患。但近年來醫療生技快速進步，深切體驗到基礎研究與教學的重要性，自1995年開始籌備、於2009年申請通過馬偕醫學院。

馬偕醫學院目前共有醫學系、護理學系、聽力暨語言學系與生物醫學研究所等四大系所。以一流之教學資源、最佳的課程規劃、最人性化的建築設計、最合理的生師比例、加上豐富的學習資源等，提供學生「身、心、靈完整醫治」的全人醫學教育訓練。

據統計，80%的資料外洩事件來自資料庫伺服器。當個資法上路，每一所大專院校與企業都必做好完善資料防護與內稽內控，才能避免因個資外洩而蒙受損失。馬偕醫學院資訊團隊不僅要管理師生個資，還有來自各項研究計畫的敏感性資料，必須以高標準來規劃資料庫安全解決方案，才能確保個資安全、達到符規免責的要求。

## 一步到位，選擇 Guardium

在楊明正的規畫中，個資安全防護分為四個階段：資料庫稽核、資料遮罩、資料遺失防範、內控稽核資訊化與結構化。第一階段—資料庫稽核能夠完整紀錄資料庫的所有行為，即時監控異常存取，同時若未來被控資料外洩時可舉證自保。

楊明正認為，資料庫稽核好比買保險，既然已經決定要投資，就要做到一勞永逸、無後顧之憂。因此，馬偕醫學院決定採用領導品牌 IBM Guardium。

「當需要舉證時，如何讓法院相信稽核紀錄的公信力？如果是業界普遍使用的解決方案，可信度當然比較高。」楊明正直指選擇 Guardium 主因。

當時 IT 團隊評比市面上各廠牌解決方案、也在業界詢問風評，得知多數金融業者都選擇 Guardium，顯見其個資防護能力備受肯定。且在研究機構 Forrester 的「The Forrester Wave™：資料庫稽核與即時防護」報告中指出，IBM Guardium 亦是該領域中的領導者，在產品面、策略面、市場面共17項指標全部高居榜首。

## 完整證據力，確保符規免責

IBM 軟體事業處協理胡育銘指出，即時防護是資料庫安全預警的第一道防線、而稽核報表則是企業組織自保的最後一道防線。為確保報表具有完美證據力，Guardium 提供多重防護機制：

- 具「不可否認性」的稽核資料：職權分立機制，將稽核資料儲存於多個不同的實體與虛擬裝置中，任何人均無權篡改。
- 三層式架構的使用者追蹤：完全對應應用伺服器使用者資料與 database session 及 SQL 資訊，為全球唯一100%完全正確追蹤使用者的解決方案。
- 資料完整性設計：Buffer 機制在網路忙碌或中斷時可先暫存交易資料，網路恢復後立即續傳到稽核資料庫，不漏失封包，確保稽核資料完整。
- 高可用性與附載平衡設計：無論發生天災人禍、或資料庫交易附載過大，都能夠透過備援或分散式收錄來確保稽核資料完整無缺。

馬偕醫學院稽核重點聚焦於內稽內控。透過 Guardium 的自訂功能，可以輕鬆客製化專屬的內控報表，協助強化內部管理。

## 獨家 Agent 技術，即時監控效能好

此外，Guardium 的效能也顯著優於其他解決方案，原因在於採用了獨步全球的 Agent 技術。相較於以封包為基礎的技術，Agent 採取非侵入性即時監控，在影響系統日常運作，也不須改變資料庫或應用程式配置，可隨系統架構靈活配置與擴充。

比較個平台的效能，即可看出 Guardium 的優勢。他廠解決方案動輒占用10%-15%系統效能，而 Guardium 在 UNIX 平台上僅需3%、Windows 平台上低於5%效能，對於經常吞吐大量資料的資料庫系統，效能差異將直接影響業務運作穩定性與使用者體驗。

馬偕醫學院 IT 團隊成員、負責資料庫管理的林紫晴指出，導入兩年多期間，其系統運作一直十分穩定，期間也曾遇到颱風停電導致空調停機，機房溫度飆高，但 Guardium 還是穩健運作，即時防護與稽核未曾中斷，完美發揮其功能，值得稱許。

此外，林紫晴還發現了一項意想不到的便利功能：Guardium 內建的資料庫效能監控紀錄。「今年初曾遇到資料庫效能很慢，這項功能可以看到那些指令的效能異常、回應延遲，後來就常用效能監控報表來改進資料庫效能。」林紫晴分享這個預期之外的小驚喜。

## IBM 專業服務，個資防護與時俱進

個資防護是一項與時俱進、永無止境的艱鉅任務。個資法三讀通過後，有了更明確的法令遵循方向，馬偕醫學院也規畫繼續採用 IBM 的維護服務合約，由 IBM 專業團隊來協助馬偕醫學院實現符規的個資防護。