

二零零八年五月三十日

討論文件

立法會資訊科技及廣播事務委員會

醫院管理局遺失可攜電子儲存裝置事件

目的

本文件旨在向委員闡述醫院管理局(醫管局)轄下醫院近期遺失載有可識別病人身分資料的可攜電子儲存裝置的事件，並向委員提供醫管局處理病人電子資料的保安系統，以及已採取的有關改善措施的資料。

背景

2. 醫管局自一九九零年成立以來，已制定資訊科技系統的發展策略，推動業務流程自動化，以支援前線的醫護工作和後勤辦公室的行政工作。醫管局至今已在全部 41 間醫院／院舍和超過 100 間門診所設置各種資訊科技系統。現時每間醫院已在急症、住院、門診、化驗及藥房等多項服務上廣泛應用臨牀系統。

3. 有關的臨牀系統載存病人接受上述服務時的各項資料，並提供病人資料予其他醫護人員作醫療相關用途。醫管局對病人電子資料保密的工作非常重視，並為此制定各項政策、程序手冊、指引和其他

資料，就處理病人電子資料方面為員工提供清晰的指引，以保障這些資料的安全。

近期遺失載有病人資料的可攜電子儲存裝置的個案摘要

4. 自二零零七年四月一日，醫管局接獲十宗有關遺失載有或可能載有病人資料的電子器材的報告。有關個案與六間醫院／診所有關，包括東區尤德夫人那打素醫院(四宗)、九龍醫院(兩宗)、威爾斯親王醫院(一宗)、西營盤賽馬會普通科門診診所(一宗)、屯門醫院(一宗)及基督教聯合醫院(一宗)。在這十宗個案中，有八宗報稱發生於醫院／診所內，兩宗則發生於醫院／診所以外地方。遺失的電子器材包括五個便攜式電子儲存媒體(USB 電子儲存媒體)、一部電子手帳、一部數碼音訊處理器(MP3 player)、一部中央處理器、一部手提電腦及一部電子照相機。十宗個案中有七宗懷疑涉及盜竊，而其餘三宗則屬遺失個案。所有個案已向警方報告。

5. 估計這十宗個案共涉及 16 000 名病人，其中約 3 000 名病人的資料並不涉及個人資料，而另外約 2 000 名病人的資料受密碼保護。醫院已透過會晤、電話或信件通知受事件影響的病人。直至目前為止，並無收到這些病人資料外泄的報告。

醫管局現行有關保護資料的政策及指引

6. 過去數年，醫管局為保護病人資料制定了全面的政策及指引，以避免這些資料遭非法查閱。醫管局總辦事處的臨牀資料政策工

作小組，負責制定各項保護電子臨牀資料的政策及指引，而醫院聯網的臨牀資料私隱委員會則負責在聯網層面監督有關政策及指引的執行。

7. 這些政策及指引所涵蓋的範圍廣泛，包括收集、運用、查閱資料和保留資料，以及為保護資料所作的技術性及實際安排等各方面。根據其一貫政策，醫管局只容許基於以下原則查閱病人資料：

- (i) 只有負責向病人提供臨床護理的醫護人員才可以基於“病人接受治療中”的原則查閱病人資料；
- (ii) 對於非直接對病人提供護理服務的活動，例如擬備醫療報告、進行臨牀研究及臨牀審核等，醫護人員只能基於“確有需要”的原則下查閱病人資料；
- (iii) 醫管局規定員工在下載病人資料進行工作或學術研究時，應盡量以代號替代可辨認身分的病人及個人資料。如果下載的資料含有可辨認身分的病人及個人資料，則有關資料必須經加密程序處理；及
- (iv) 基於運作需要，醫管局會容許醫護人員在某些情況下(例如當醫管局醫生在安老院舍或社康護士在病人家中提供服務時)，在醫院/診所以外地方查閱病人資料。

醫管局資訊科技系統的保安及防止擅用措施

8. 在資訊科技的基礎設施方面，醫管局已設有一個包括防火牆、防止入侵保護及劃一資源位址過濾系統的安全網絡基礎設施，以免個人資料遭受他人在未獲授權情況下查閱及惡意入侵。

9. 只有在執行職務時有運作需要的員工才獲准進入系統。使用者進入系統受多項控制因素限制，包括只限於同一醫院的員工、員工的職位及職級、所屬專科及部門，以及工作性質，例如他們是否為該病人提供護理服務等。有關系統亦留有病人資料被查閱的記錄，以便追查使用資料的醫護人員，避免資料被非法查閱。員工在獲得批准進入臨床系統前，他們必須留意及承擔保密病人資料的責任，並簽署保密協議。使用者每次登入系統時，系統會展示訊息提醒他們須維護病人私隱和對病人資料保密。

公布指引及員工培訓

10. 醫管局早在發生相關事件前，已透過通告、內部通訊、小冊子、醫管局內聯網以及醫院員工的資訊科技研討會和簡報會等向前線員工公布上述政策及指引。

11. 醫管局亦透過員工培訓加強員工了解保護病人資料的重要性及這方面的意識。對於新入職員工，特別是臨牀人員，醫管局會在入職簡介中向他們介紹對病人資料保密的責任及資訊科技的保安事宜。

醫管局為實習醫生提供有關使用臨牀管理系統的培訓中，亦包括對病人資料保密的責任和資料查閱管制的課題。

改善措施

12. 對於近日發生遺失可攜電子儲存裝置的個案，醫管局已即時採取下列措施以加強保護病人資料：

- (i) 提升病人資訊系統，令下載的病人資料（包括姓名及身分證號碼）必須以加密程序保護；
- (ii) 強制員工使用備有加密和密碼“鎖定”功能的可攜電子儲存裝置(USB 電子儲存媒體)，以保護病人資料；
- (iii) 刊發有關加強執行個人資料保安措施的工作通告，提醒員工保障病人私隱的重要性，並為員工提供處理和保護病人資料的清晰指引；
- (iv) 推出保護病人資料的宣傳片及複修課程，以教育員工有關保護病人資料的知識；及
- (v) 改善內部的早期事故通報系統。自 2008 年 5 月 19 日起，如有病人資料外泄/遺失，有關員工必須透過醫管局內部的「早期事故通報系統」盡快向醫院報告，讓管理層可立即採取補救措施。而醫院當局則必須於事發 48 小時之內向醫管局總辦事處提交初步報告，並在兩星期內向受影響病人解釋情況。此外，醫管局在這方面亦已發出另一份工作通

告，闡述處理遺失載有可識別病人身分的個人資料的電子器材事件的政策。

13. 醫管局已成立了獨立的病人資料安全及私隱專責小組(專責小組)，檢討現時保護病人資料的政策和保安制度，並提出改善措施。專責小組將於三個月內完成檢討，並向醫管局行政總裁提交報告。

14. 我們會繼續加強保安措施以保護病人資料，同時亦會兼顧查閱該等資料的臨牀及工作需要。除了推行上文第 12 段所述的改善措施外，我們亦會在適用之處推行專責小組及個人資料私隱專員的建議。

徵詢意見

15. 請委員閱悉本文件的內容。

醫院管理局

二零零八年五月