根據《個人資料（私隱）條例》（第 486 章）第 48（2）條發表的報告

報告編號：R08-1935

發表日期：**2008** 年 **12** 月 **24** 日

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

基督教聯合醫院遺失病人的個人資料事件

個案編號：200801935

本報告乃有關本人根據《個人資料（私隱）條例》（第 486 章）（下稱「條例」）第 38(a)條對醫院管理局（下稱「醫管局」）轄下的基督教聯合醫院（下稱「聯合醫院」）進行的調查，並根據條例第 VII 部行使本人獲賦予的權力而發表。條例第 48(2)條訂明*「專員在完成一項調查後，如認爲如此行事是符合公眾利益的，可－*

(a)　發表列明以下事項的報告－

(i)　該項調查的結果；

(ii)　由該項調查引致的、專員認爲是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及

(iii)　由該項調查引致的、專員認爲適合作出的任何其他評論；及

(b)　以他認爲合適的方式發表該報告。」

吳斌
個人資料私隱專員

個案情況

投訴人表示她曾於2007年8月24日於牛頭角母嬰健康院接受精神科治療，並向一位精神科護士X姑娘提供其個人資料。其後，投訴人於2008年1月25日收到聯合醫院一位Z姑娘的電話，表示聯合醫院於2008年1月17日發現遺失了儲存其個人資料（當中包括姓名、身份證號碼、住址及聯絡電話號碼）的電腦USB閃存驅動器（下稱「USB」）。Z姑娘並向投訴人表示同時遺失了合共23名女士的個人資料，而聯合醫院已於2008年1月18日向警方報案。

2. 就此，投訴人投訴聯合醫院遺失了其個人資料。

條例的相關條文

3. 與本個案直接有關的是條例附表1的保障資料第4原則的規定：－

> *「須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料（包括採用不能切實可行地予以查閱或處理的形式的資料）受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響，尤其須考慮——*
>
> *(a) 該等資料的種類及如該等事情發生便能造成的損害；*
> *(b) 儲存該等資料的地點；*
> *(c) 儲存該等資料的設備所包含(不論是藉自動化方法或其他方法)的保安措施；*
> *(d) 爲確保能查閱該等資料的人的良好操守、審慎態度及辦事能力而採取的措施；及*
> *(e) 爲確保在保安良好的情況下傳送該等資料而採取的措施。」*

4. 根據條例第2(1)條的釋義，*「切實可行」*是指*「合理地切實可行」*。

調查所得資料

5. 在本個案的調查過程中，本公署會見了 X 姑娘及聯合醫院的醫院行政總監 Y 醫生，並爲他們錄取口供。此外，本公署亦取得聯合醫院就本個案的書面回覆及有關資料文件。至此，本公署搜集到下列與本案有關的資料。

個案背景

6. 醫管局自 2006 年 2 月聯同衞生署向公眾提供兒童身心全面發展服務。而由於該服務包括向產後婦女提供精神健康服務，故此，聯合醫院的精神科護士會被派駐衞生署轄下三間九龍東（即牛頭角、藍田及將軍澳）的母嬰健康院、聯合醫院的婦產科門診診所或容鳳書紀念中心精神科（下稱「容鳳書」）提供有關服務。

7. X 姑娘於 2007 年 7 月 24 日被調派到聯合醫院的兒童身心全面發展服務工作，她的主要辦事處位於容鳳書，她亦需被派駐牛頭角母嬰健康院及其他地點爲懷孕及產後婦女提供精神健康服務。

8. 在 X 姑娘的日常工作中，她需要會見病人。在會見過程中 X 姑娘需收集病人的登記資料(registration data)（包括姓名、出生日期、身分證號碼、地址及電話號碼等）和醫療資料(clinical consultation notes)。由 X 姑娘處理的病人大致可分爲兩類，第一類是曾經於容鳳書或聯合醫院登記的病人（下稱「第一類病人」），第二類是從未於容鳳書或聯合醫院登記的病人（下稱「第二類病人」）。由於第一類病人曾經接受過容鳳書或聯合醫院的服務，所以 X 姑娘需要將第一類病人的醫療資料輸入醫管局的電腦系統 Clinical Management System（下稱「CMS」）內作醫療用途。至於第二類病人，則由於醫管局的醫護人員不曾向該些病人提供醫療服務，他們只屬於兒童身心全面發展服務的病人，故此無須將該類病人的任何資料輸入醫管局的 CMS 內。但由於兩類病人均屬兒童身心全面發展服務的病人，故仍需將他們的登記資料儲存於容鳳書的兒童身心全面發展服務的總登記資料電腦檔案中，並將他們的醫療資料文件存檔。

9. 故此，X 姑娘在日常工作中需要將在她的其中一處工作地點牛頭角母嬰健康院收集所得的病人登記資料，帶回並儲存至

在容鳳書的兒童身心全面發展服務總登記資料電腦檔案中，以及將病人的醫療資料帶回容鳳書加以印製及存檔，作爲開會時討論病人個案之用。但在 2007 年 10 月 10 日以前，牛頭角母嬰健康院仍未設有能連接醫管局或容鳳書的電腦系統。即使在 2007 年 10 月 10 日以後，牛頭角母嬰健康院開始設有 CMS，但在牛頭角母嬰健康院設立 CMS 的目的只爲處理醫管局的病人資料及其他有關用途，並非作爲儲存兒童身心全面發展服務的病人資料之用。故此，聯合醫院於 X 姑娘首天在兒童身心全面發展服務上班當日（即 2007 年 7 月 24 日）向她發放了一支 USB（下稱「該 USB」），作爲她在工作中儲存病人的醫療資料，及傳送病人登記資料至容鳳書並輸入兒童身心全面發展服務的總登記資料電腦檔案之用。X 姑娘表示，聯合醫院在發放該 USB 給她時有口頭向她講解有關使用 USB 以收集、儲存及刪除病人個人資料的程序及要求（詳情如下）。

10. 在 2007 年 10 月 10 日以前，當 X 姑娘在牛頭角母嬰健康院接見病人後，會將上述兩類病人的登記資料及第二類病人的醫療資料儲存在該 USB 的密碼保護區內，而第一類病人的醫療資料則會被記錄在紙張上，待返回容鳳書工作時，才分別將兩類病人的登記資料輸入兒童身心全面發展服務的總登記資料電腦檔案中，並將第一類病人的醫療資料從記錄紙上輸入醫管局的 CMS 內。當召開每星期會議討論病人個案時，X 姑娘需要從 CMS 及該 USB 分別印製有關第一及第二類病人的醫療資料作開會及存檔之用。

11. 有關刪除資料方面，X 姑娘獲告知她需要在每個星期的內部會議上討論病人個案，以及在正式終止向病人提供服務後，立即從該 USB 內刪除有關病人的醫療資料。至於病人的登記資料，則仍會被保留在該 USB 的密碼保護區內，目的是讓 X 姑娘日後如收到醫管局或兒童身心全面發展服務其他醫護人員向她查詢有關病人的情況時，可根據仍儲存於該 USB 內的登記資料作出解答。

12. 自 2007 年 10 月 10 日起，牛頭角母嬰健康院開始設有能連接醫管局的 CMS，故此 X 姑娘只需將所收集得的第一類病人的醫療資料直接在牛頭角母嬰健康院輸入 CMS 內，但她仍需將上述兩類病人的登記資料及第二類病人的醫療資料儲存在該 USB 的密碼保護區內，以帶回容鳳書將登記資料輸入兒童身心全面發展服務的總登記資料電腦檔案中，及解答其他醫護人員的

查詢之用。

13. X 姑娘因每天需到不同的地點工作，故她會將該 USB 帶往工作地點，下班後再將它帶回家中，直至 X 姑娘需要返回容鳳書工作，才將病人的登記資料輸入總登記資料電腦檔案中，而仍未被終止處理的第二類病人的醫療資料，則繼續儲存在該 USB 內。

遺失投訴人個人資料的經過

14. X 姑娘於 2007 年 8 月 24 日接見經牛頭角母嬰健康院轉介接受有關精神健康服務的投訴人。投訴人屬第一類病人，所以 X 姑娘只將投訴人的登記資料儲存在該 USB 的密碼保護區內。同日的稍後時間，X 姑娘亦終止繼續向投訴人提供服務，但如上文第 11 段所述，投訴人的登記資料仍被保存於該 USB 的密碼保護區內。

15. 2007 年 10 月中旬，X 姑娘發現該 USB 的密碼保護區損壞了，使她無法於該區存取資料，惟 X 姑娘未有即時向上級作出報告。爲了繼續執行職務，X 姑娘將她自 2007 年 7 月 27 日開始處理過的全部 26 位病人（包括投訴人）的登記資料，從儲存在容鳳書的總登記資料電腦檔案內複製至該 USB 的非密碼保護區內。X 姑娘於發現該 USB 的密碼保護區損壞了至遺失該 USB 期間，沒有於該 USB 內加入新病人的資料。即是說，本個案中所遺失的個人資料包括該 26 位病人（包括投訴人）的登記資料及仍儲存在該 USB 的密碼保護區內部份病人的醫療資料。

16. 2007 年 10 月 20 日，當 X 姑娘返回容鳳書後，她發現遺失了該 USB，但她未能確定何時、在何種情況及如何遺失該 USB。在回應本公署的查詢時，X 姑娘表示她最後使用該 USB 的日期是 2007 年 10 月 17 日，記憶中她曾於 2007 年 10 月 18 日到過容鳳書、聯合醫院婦產科門診及牛頭角母嬰健康院工作，但她忘記了 2007 年 10 月 19 日（公眾假期）的工作地點。在發現遺失該 USB 後，X 姑娘曾作出搜尋但未能尋獲，故於 2008 年 1 月 17 日向上級報告有關遺失。聯合醫院於翌日向警方報案。自從發現遺失該 USB 後，X 姑娘便停止使用 USB 處理或儲存病人的個人資料，並改爲親自携帶或傳真病人的登記資料文件回容鳳書，以及以醫管局提供給她的內聯網的電子郵件帳戶儲存病人的醫療資料。

聯合醫院有關使用 USB 的內部指引或程序

17. 聯合醫院向本公署提供下列的文件副本以表示他們就有關 USB 的使用有既定的內部指引：

(a) 《Clinical Data Policy Manual – Section 3.5》
(b) 《Information Security Policy and Procedure – Section 6.6.1 – 6.6.2》
(c) 《A Practical Guide to IT Security for Everyone Working in HA – P.9》
(d) 《Protect Patient Confidentiality》小冊子

18. 此外，Y 醫生表示聯合醫院除不時向職員提供培訓及安排專題講座讓職員了解該院的政策及指引外，每當聯合醫院發出新的或修訂版的政策、內部指引及/或通告，院方一般會採用下列四種方式通知院內各職員：

(1) 電郵
在本案發生前，聯合醫院的管理人員、醫生、護士（包括 X 姑娘）、專職醫療人員及部份其他職員都獲發一個由院方提供的電郵賬戶，以接收院方的政策、內部指引及通告。

(2) 拷貝文件
聯合醫院會將新發出的或修訂版的政策、內部指引及/或通告以拷貝方式在院內各部門傳閱。院方各部門可自行決定是否需要員工在閱後簽署作實。

(3) 內聯網
院方亦會將新發出的或修訂版的政策、內部指引及/或通告儲存在院方的內聯網供各職員以無需使用密碼的方式隨時登入閱讀或下載有關政策、內部指引及/或通告。

(4) 屏幕保護功能
聯合醫院會透過院方電腦的屏幕保護功能，提示員工有關新發出的或修訂版的政策、內部指引及/或通告。

19. 不過，X 姑娘表示聯合醫院除了以口頭通知她有關使用

USB 於收集、儲存及刪除病人個人資料的程序及要求外，並無向她提供任何有關使用 USB 或其他可携式電子儲存儀器處理病人個人資料方面的培訓、通告或指引。直至 2008 年 5 月，聯合醫院才向她提供有關的培訓、講座及內部通告。

20. 此外，Y 醫生表示聯合醫院沒有針對性規定當職員遺失了病人的個人資料時，該於何時向院方作出報告，但院方設有「早期事故通報系統」，讓職員可隨時透過此系統作出各類事故的匯報。而 X 姑娘於 2008 年 1 月 18 日亦有透過此系統報告遺失該 USB 一事。

21. Y 醫生確認聯合醫院沒有定期跟進檢查職員使用 USB 處理病人個人資料的情況。但自本案後，聯合醫院已禁止所有職員使用 USB 處理病人的個人資料，除非事前向他本人申請並獲得批准。不過，他未有收過員工使用 USB 的申請。

聯合醫院就事件所採取的補救措施

22. 就是次事件，聯合醫院採取了一系列的補救行動，當中包括：

(1) 由 2008 年 1 月 19 日起，聯合醫院已收回向兒童身心全面發展服務的護士發放的所有 USB 並刪除內存的所有病人資料。

(2) 兒童身心全面發展辦事處的主管護士由 2008 年 1 月 23 日至 1 月 28 日致電事件中涉及的病人以解釋事件的經過及致歉，並於 2008 年 1 月 30 日與投訴人面談。

(3) 聯合醫院的精神科部門主管及兒童身心全面發展服務護士於 2008 年 1 月 22 日開會討論改善措施，當中通過利用護士的內聯網電郵及傳真以儲存及傳送病人在母嬰健康院的個人資料，取替以 USB 儲存及傳送病人資料的方法。

(4) 聯合醫院於 2008 年 4 月 25 日成立調查小組，以找出發生問題的原因及可改善的地方。爲確保調查公正及透明度，聯合醫院邀請了該院的醫院管治委員

會一名成員及醫管局總部的醫療訊息部的職員參與調查。

(5) 醫管局行政總裁於 2008 年 5 月 7 日向醫管局所有職員發出電郵，要求他們將所有載有病人個人資料的儀器儲存在安全地方、將所有載有病人個人資料的檔案加密並以密碼保護，以及除非獲醫院行政總監的書面批准，否則員工不可將載有病人個人資料的 USB 帶離醫管局範圍。

(6) 醫管局亦於 2008 年 5 月 14 日發出內部通告《Hospital Authority Head Office Information Technology Circular No. 1/2008 – Enhanced Measures on Enforcing Personal Data Security》，就加強病人的個人資料的保安措施方面發出有關守則。

(7) 醫管局於 2008 年 5 月 15 日發出另一份內部通告《Hospital Authority Head Office Operation Circular No. 9/2008 – Policy on the Management of Loss of Electronic Devices Concerning Patient Identifiable Personal Data》，指示職員當發現遺失載有病人個人資料的電子儲存儀器時，必須立即報告，並列出報告的流程。

調查結果

23. 本個案涉及有關處理病人個人資料的程序問題，聯合醫院作爲公營醫療服務提供者，所處理的病人個人資料的數量十分龐大，而有關資料亦屬高敏感度，故此就病人個人資料的保安問題上，理應採取更嚴謹的保障個人資料措施，以確保病人的個人資料得到保護。

24. 就本個案的情況而言，聯合醫院須按照保障資料第 4 原則的規定，採取所有切實可行的步驟以確保由該院持有的病人（包括投訴人）的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除或其他使用所影響。本個案的調查重點是聯合醫院在提供 USB 予其職員使用以處理及儲存病人個人資料的情況下，所採取的保護措施是否足夠。本投訴引申的相關問題是聯合醫院讓職員採用 USB 處理及儲存病人的個人資料時，該院是否已有合適的政策及指引通知其職員以保障病人的個人資料，以及

是否已有相應措施確保有關職員遵守有關的政策及指引。

25. 根據聯合醫院及 Y 醫生所述，該院有向所有職員提供培訓及安排專題講座讓職員了解該院的政策及內部指引，而每當聯合醫院發出新的或修訂版的政策、內部指引及/或通告，院方一般會採用不同方式通知院內各職員。故此，聯合醫院向本公署所提供的上文第 17 段的文件副本理應已供包括 X 姑娘在內的職員參閱。惟根據 X 姑娘所述，聯合醫院只曾以口頭方式通知她有關以 USB 收集、儲存及刪除病人的個人資料的程序及要求，在本案發生前卻從未見過聯合醫院所提供的有關保障病人的個人資料私隱的指引或接受過由聯合醫院所提供與使用 USB 或其他可携式電子儲存儀器有關的培訓。如聯合醫院確曾以上述的傳達機制向 X 姑娘提供有關的政策、指引及/或通告，從 X 姑娘的供詞可見該機制在下達資訊方面實在存在問題。

26. 再者，即使如聯合醫院及 Y 醫生所述，該院已制訂有關使用 USB 或其他可携式的電子儲存儀器的政策或內部指引，及向包括 X 姑娘在內的職員提供了有關的政策或內部指引，但本人在細閱有關的文件內容後，認爲有關的政策或內部指引只是概括提醒職員應小心使用電子儲存儀器處理病人的個人資料，舉例說：－

> 《Clinical Data Policy Manual – Section 3.5》
>
> *"Guidelines*
>
> *Since exporting patient data may increase the possibility of breach of confidentiality, intentionally or inadvertently, data exports should be avoided as far as possible"*
>
> 《Information Security Policy and Procedure － Section 6.6.1》
>
> "***Removable computer media should be controlled.***
>
> …
>
> *4. Store all media in a safe, secure environment, in accordance with manufacturers' specifications."*
>
> 《Protect Patient Confidentiality》小冊子－Section IV

"General Principle

All stored personal information, whether in hard copy, any types of computers, laptop, home-based PC or any other medium, should be protected from unauthorized or accidental access, processing, erasure or other use through the use of appropriate security devices and functions.

…

What you shouldn't do:

…

✗ leave floppy discs, tapes, CD Roms and other types of media lying around unattended in a non-secure place"

但本人並無發現聯合醫院在 2008 年 5 月 14 日之前就如何使用 USB 等電子儲存儀器（包括在遺失有關儀器時的應對措施）備有詳細的指示及應用程序予職員跟從。

27. 此外，由於 CMS 及兒童身心全面發展服務已存有病人的登記及醫療資料，如有醫護人員向 X 姑娘查詢有關病人的病歷，X 姑娘理應可直接參考已存於 CMS 或兒童身心全面發展服務的檔案，以回答查詢。再者，相比 X 姑娘只靠病人的登記資料以記憶病人的病況，從 CMS 或兒童身心全面發展服務的檔案直接查閱有關病人的資料更爲準確。故此，本人認爲 X 姑娘無需仍保留已傳輸至兒童身心全面發展服務電腦檔案的病人登記資料於該 USB 內。如 X 姑娘爲了方便工作而保留該些病人登記資料於該 USB 內，這種做法相比保障病人個人資料私隱方面無疑並不對稱。

28. 至此，基於聯合醫院並無合適地制定有關使用 USB 的政策或內部指引，以致 X 姑娘在沒有實際需要的情況下，仍然將病人的登記資料存於該 USB 內，而當她發現該 USB 的密碼保護區損壞後，不但沒有即時向上級報告，還繼續使用該 USB，將病人的個人資料儲存在非密碼保護區內。而在 2007 年 10 月 20 日發現遺失該 USB 後，X 姑娘亦非即時向院方作出報告。

結論

29. 基於以上所述，本人認爲聯合醫院在本個案中並未有採取所有切實可行的步驟保障有關個人資料，導致遺失該 26 名病

人（包括投訴人）的個人資料，因而違反保障資料第 4 原則的規定。

執行通知

30. 根據條例第 50 條，如本人認爲醫管局已違反了條例的保障資料第 4 原則的規定，而違反情況令到違反行爲將持續或重複發生是相當可能的，則本人可向醫管局送達執行通知。不過，基於聯合醫院的職員已停止使用 USB 儲存及傳送有關病人資料，因此沒有資料顯示聯合醫院的違反行爲將持續或重複發生是相當可能的。故此，本人沒有因應此項調查向醫管局送達執行通知。

建議及其他評論

31. 本人得悉聯合醫院在本案發生後已禁止職員繼續使用 USB 處理及儲存病人的個人資料（除非有關做法事前獲醫院行政總監的批准）；即使職員可繼續使用 USB 處理及儲存病人的個人資料，醫管局已向聯合醫院職員提供有關的內部指引及使用程序。

32. 另外，本公署已於 2008 年 7 月 22 日就醫管局轄下醫院進行視察後所發表的視察報告中，作出了保障病人個人資料相關的建議，以協助醫院在處理病人的個人資料方面作出改善。

33. 隨着科技的發展，電腦儲存裝置的體積日趨細小，但儲存容量則越趨增大，以致遺失的風險及由遺失所導致受影響的人數均相應增加。科技的進步無疑能爲工作帶來方便，但資料使用者在使用科技提高工作效率的同時，亦需要相應地提高職員對個人資料保障方面的意識及要求，以及改進既有的政策及內部指引，達致所採取的保障個人資料措施能與時並進。

34. USB 的用途十分廣泛，且方便攜帶，本人相信數目不少的醫護人員都會使用 USB 儲存病人的個人資料。但在使用 USB 之前，醫護人員應該先考慮是否真正有需要使用 USB、是否有其他方法代替使用 USB，以及小心衡量使用 USB 的潛在風險。正如在本個案中，有關的醫護人員其實可以用內聯網代替 USB，而又可減低遺失病人個人資料的風險及影響。當然，在使用電子形式傳送資料前，亦須考慮安全性的問題。如醫護人員經審慎考慮

後，認爲使用 USB 儲存病人個人資料是必須的，則須採取有效的保障個人資料措施，以避免所儲存的個人資料受到未經准許的或意外的查閱、處理、刪除或其他使用所影響。例如，儲存於 USB 的病人個人資料應被加密處理、如發現 USB 的加密功能失效時應該立即停止使用有關的 USB、當使用完病人的個人資料後立即將之從 USB 中刪除，以及當醫護人員發現遺失儲存了病人個人資料的 USB 時，應該立即向有關方面作出報告等。