Report Published under Section 48(1) of the Personal Data (Privacy) Ordinance (Cap. 486)

根據《個人資料（私隱）條例》（第 486 章）第 48（1）條發表的報告

Report Number: R08-4232

報告編號：R08-4232

Date issued: 22 July 2008

發表日期：2008 年 7 月 22 日

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

醫院管理局病人資料系統的視察報告

本報告是本人根據《個人資料（私隱）條例》（第 486 章）（下稱「條例」）第 36 條對醫院管理局進行的視察，並根據條例第 VII 部行使本人獲賦予的權力而發表。

條例**第 36 條**訂明：

「在不損害第 38 條的概括性原則下，專員可對 —

(a) 資料使用者所使用的任何個人資料系統；或

(b) 屬於某資料使用者類別的資料使用者所使用的任何個人資料系統，

進行視察，目的在確定資訊以協助專員 —

(i) 在 —

(A) ...

(B) (b)段適用時，向有關的資料使用者所屬於的一個類別的資料使用者，

作出建議；及

(ii) 作出關於促進有關的資料使用者或有關的資料使用者所屬於的一個類別的資料使用者（視屬何情況而定）遵守本條例的條文（尤其是各保障資料原則）的建議。」

在條例第 2(1)條中，「**個人資料系統**」一詞是指*「全部或部分由資料使用者用作收集、持有、處理或使用個人資料的任何系統（不論該系統是否自動化的），並包括組成該系統一部分的任何文件及設備」*。

醫院管理局屬於提供醫療服務的資料使用者類別。

條例**第 48(1)條**訂明：*「在符合第(3)款的規定下，專員在第 36(b)條適用的情況下完成一項視察後，可 —*

(a) *發表列明由該項視察引致的、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）的任何建議的報告；及*

(b) *以他認爲合適的方式發表該報告。」*

第(3)款訂明：*「除第(4)款另有規定外，根據第(1)或(2)款發表的報告的擬訂形式，須以防止可從報告中確定任何個人的身分爲準」。*

第(4)款訂明：*「第(3)款不適用於屬以下人士的個人 —*

(a) *專員或訂明人員；*

(b) *有關資料使用者。」*

吳斌
個人資料私隱專員
香港特別行政區

（註：本報告乃翻譯本，一切以英文文本爲準。）

目錄

第一章

引言

1.1 本報告是個人資料私隱專員（下稱「專員」）依據《個人資料（私隱）條例》（第 486 章）（下稱「條例」）第 36 條就醫院管理局（下稱「醫管局」）轄下多間醫院最近發生多宗遺失病人個人資料的事件而進行視察的結果。專員非常關注醫管局的個人資料系統是否不足以確保病人資料的安全及遵從條例的規定。

1.2 與是次視察相關的規定是條例附表 1 的**保障資料第 4 原則**，該原則訂明：

「第 4 原則 — 個人資料的保安

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。」

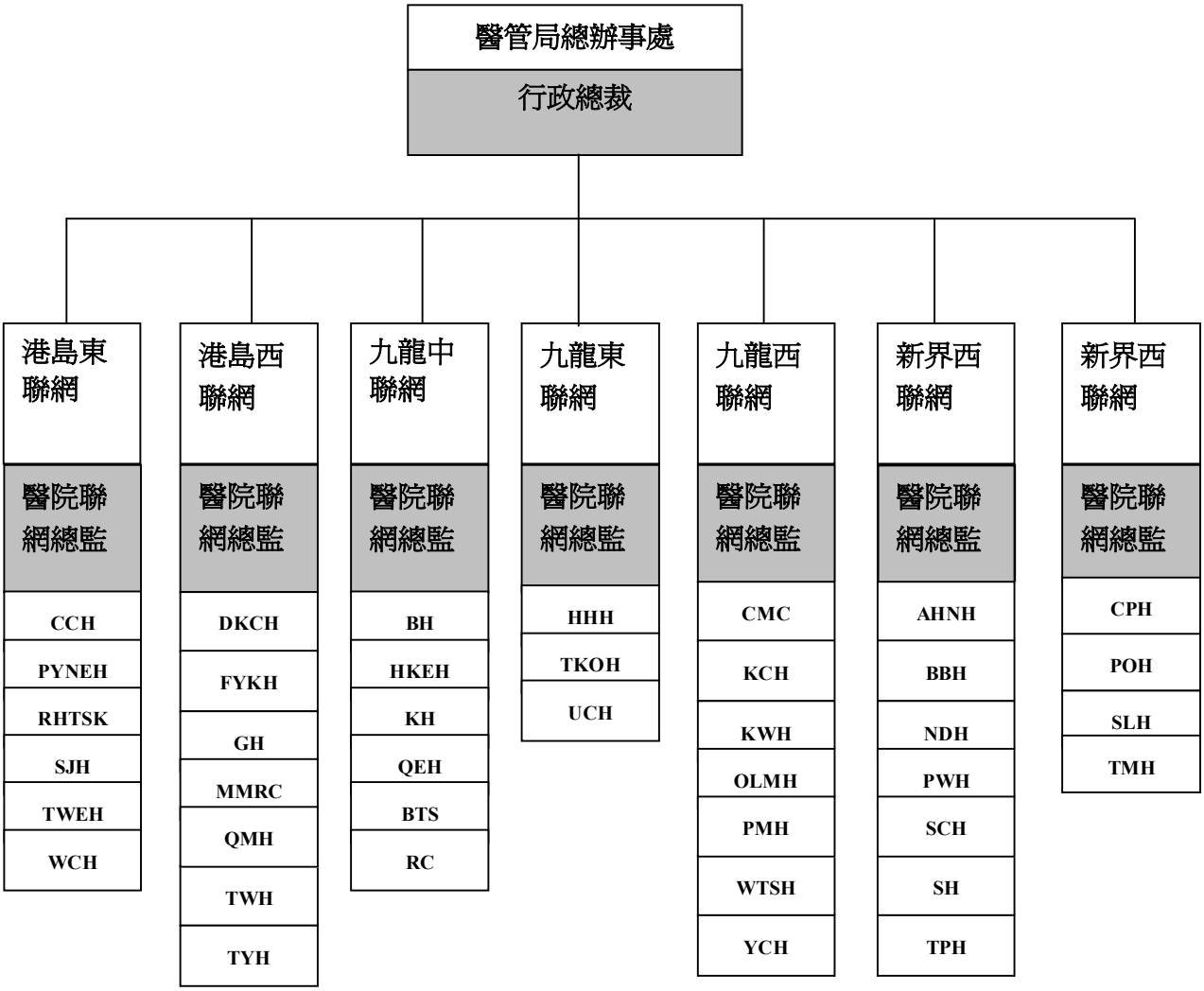
「切實可行」一詞在條例第 2(1)條是指「*合理地切實可行*」。

1.3 病人的醫療資料一般被視爲特別敏感，因此在處理該等資料時，資料使用者有責任份外小心，以確保該等資料的安全。尤其當資料使用者是屬於醫療服務提供者類別，其日常職能及責任涉及處理大量病人資料，資料的保安至爲重要。不當處理資料當事人（病人）的醫療資料，可以對他們造成嚴重及深遠的損失或損害。因此，醫管局應注意其持有的資料的敏感性及未獲准許而查閱資料的風險，確保所採取的保安預防措施是合理、合適及有效的，以遵從保障資料第 4 原則的資料保安規定。

1.4 醫管局是一個法定機構，根據《醫院管理局條例》（第 113 章）於 1990 年 12 月 1 日成立，負責管理香港特別行政區所有公立醫院提供的醫院服務。醫管局是一個獨立機構，惟須透過食物及□生局局長向政府負責。醫管局於 1991 年 12 月 1 日接管 38 間公立醫院及有關醫療機構，以及其屬下 37,000 名員工。目前，醫管局轄下有 41 間公立醫院及醫療機構、48 間專科門診診療所及 75 間普通科門診診療所。截至 2008 年 6 月 6 日，醫管局聘用了約 53,000 名員工。

1.5 醫療服務的管理是由醫管局行政總裁爲首的總辦事處（下稱「醫管局總辦事處」）負責，透過七個地區的區域聯網（或醫院群組），下達各醫院。每間醫院位於一個區域聯網內，區域聯網由醫院聯網總監管理。每間醫院亦有其管理隊伍，由醫院行政總監領導。下圖爲醫管局行政架構：

醫管局行政架構



醫院名稱代號詳情見**附件 I**。

視察起因

1.6 2008 年 3 月，公署接獲一宗投訴，指基督教聯合醫院一名僱員遺失一個載有病人資料的通用序列匯流排（「USB」）記憶體，導致投訴人的個人資料被錯置。

1.7 2008 年 4 月 26 日，傳媒報導上文第 1.6 段所述的基督教聯合醫院遺失病人資料事件。

1.8 2008 年 5 月 5 日，醫管局行政總裁公布，過往 12 個月內，共發生九宗遺失病人資料的事故（包括上文第 1.6 段所述的事件），涉及五間醫院[1]。事故涉及的病人數目約 6,000 名。

1.9 此外，2008 年 5 月 5 日，公署接獲威爾斯親王醫院的電話通知，表示遺失了一個載有 10,000 名病人個人資料的 USB 記憶體。故此，在過去 12 個月內，10 宗遺失手提電子儲存裝置的事件，共涉及遺失約 16,000 名病人的個人資料。

1.10 連串事故顯示，醫管局管理的個人資料系統存在不足之處。鑑於病人資料的敏感性質、受影響人數眾多，以及涉及病人資料的數量龐大，專員認爲，基於公眾利益，應審視其整套系統。爲緩和公眾的關注，醫管局應採取有效程序防止事故重演，並挽回公眾對醫管局的信心，讓公眾確信其有能力妥善保管接受醫療服務的病人所提供的個人資料。

1.11 專員認爲應採取三管齊下的措施，以釐定問題的嚴重程度，及建議如何防止事故再次發生。據此，專員決定：

(a) 根據條例第 38(a) 條，就公署接獲有關基督教聯合醫院遺失病人資料的投訴進行調查；

---

[1] 包括東區尤德夫人那打素醫院（4 宗）、屯門醫院（1 宗）、九龍醫院（2 宗）、基督教聯合醫院（1 宗，即第 1.6 段所述的事故）、西營盤賽馬會普通科門診診所（1 宗）。

(b) 根據條例第 38(b)條，就醫管局行政總裁所公布及上文第 1.8 和 1.9 段所述已知會公署的九宗遺失病人資料事故（沒有接獲投訴），主動進行調查；及

(c) 根據條例第 36 條，就病人資料的保安問題展開對醫管局個人資料系統的視察，以期向醫管局提出建議，促進有關方面遵守條例所訂明的保障資料原則，特別是保障資料第 4 原則。

1.12 視察的目的是透過查詢醫管局經聯網到轄下醫院實施的個人資料系統在保護病人個人資料方面的效能，藉以審視醫管局的個人資料系統是否妥善。由於專員的經費及資源有限，故必須將視察醫管局個人資料系統的實際運作範圍收窄至一間醫院，作爲醫管局轄下所有醫院運作的一個例證。

1.13 專員選取了律敦治醫院及鄧肇堅醫院（下文統稱「有關醫院」）進行調查，原因包括以下多項因素：有關醫院屬中等規模，而現時並非專員調查對象之一。此外，直至 1998 年，有關醫院是兩間獨立醫院，同屬歷史悠久的社區醫院。其中較大的律敦治醫院在 1842 年成立，當時是一間海員醫院（在灣仔道山坡西面，仍然豎立著當年由海港碼頭直接運送海員到醫院使用的閘門）。該醫院舊名爲律敦治療養院，多年來由香港防癆心臟及胸病協會營運，直至 1991 年才由醫管局接管。該醫院有約 572 張急症及全科病床，並提供 24 小時急症服務。鄧肇堅醫院在 1969 年成立，以其捐款人已故的鄧肇堅爵士命名，取代了當時的東區公立醫局。其急症科在 2002 年 9 月遷往律敦治醫院，而該院現已成爲社區日間醫療中心。專員認爲有關醫院的個人資料系統已運作多年，足以作爲引證醫管局在管理個人資料系統方面的實際例子。有關醫院屬港島東聯網，向醫院聯網總監負責，並最終向醫管局行政總裁負責。

1.14 2008 年 5 月 8 日，專員根據條例第 41 條向醫管局送達通知書，表示他擬根據條例第 36 條，就病人個人資料的處理事宜，對醫管局的個

人資料系統進行視察，以期就促進條例（特別是保障資料第 4 原則）的遵守提出建議。

1.15 2008 年 5 月 9 日，專員率領其職員出席與醫管局行政總裁預先約定的會議。會議目的是就近期發生連串遺失資料（特別是遺失多個載有大量病人資料的 USB 記憶體）事故表達對私隱問題的關注。醫管局行政總裁向專員簡報已即時採取的行動，以應付使用手提電子儲存器材儲存病人資料的保安風險，包括限制員工使用私人的手提電子儲存器材儲存有關資料，以及採取行動知會受遺失資料事故影響的人士。專員告知醫管局行政總裁，他已行使權力調查已知悉的遺失病人資料的各個個案，並擬對醫管局的個人資料系統進行視察，以及將在合適時就保障病人資料的措施提出建議，以供醫管局參考。專員通知醫管局行政總裁，他會透過視察鄧肇堅醫院及律敦治醫院（醫管局行政總裁建議的）來視察醫管局的個人資料系統。醫管局行政總裁承諾將與醫管局員工及有關醫院充分配合這次視察。應專員的要求，醫管局行政總裁亦同意向專員提供醫管局、聯網及有關醫院所發布有關病人資料保安的一切相關政策及實務文件。在醫管局行政總裁的建議下，專員同意他和公署人員會於 2008 年 5 月 16 日的一周內到有關醫院作視察前的到訪，初步了解有關醫院所實行的醫管局的個人資料系統、電腦系統及工作環境。

視察範圍

1.16 視察的重點針對以下各項：

(a) 醫管局收集的病人資料；特別是 —

(b) 以電子方式儲存及處理病人資料的程序；及

(c) 對於保障轄下醫院所收集的病人資料，醫管局所採取的保安措施是否足以符合保障資料第 4 原則的規定。

視察小組

1.17 視察小組（下稱「小組」）由專員吳斌先生領導，並由副專員關綺蘿女士協助。小組成員包括公署審查部、執行部及法律部的人員，以及四名顧問（下稱「顧問」）。小組的成員名單載於**附件 II**。顧問團的成員是專員因應他們在醫療、資訊科技、私隱及法律範疇的專業知識而邀請他們提供協助，包括協助專員達致持平觀點，及向醫管局提出有建設性的實用建議。

第二章

事件時序

2.1 條例並沒有訂明根據條例第 36 條進行視察的方法。爲了進行視察，小組參考條例下資料使用者須遵從的法定要求。小組爲了評估醫管局在遵從保障資料第 4 原則所採取的保障病人資料措施的實施程度，審閱了醫管局的政策及措施、實地視察有關醫院實施的醫管局資料保安系統、會見有關醫院及醫管局負責資訊科技保安、培訓及教育、循規監督及保安審核的職員。小組亦設計了問卷，並會見隨機選擇的有關醫院員工，以了解員工的私隱意識水平。

2.2 在 2008 年 5 月 9 日的會議（第 1.15 段）上，專員要求索取而醫管局同意向小組提供有關文件，包括保障資料政策的手冊、指引及實務文件，以及其總辦事處、聯網及分區醫院的架構圖。醫管局提交了大量文件，包括下列各項：

(a) *《個人資料（私隱）條 例 》手冊*（1996 年 12 月修訂版）；
(b) *臨床資料政策手冊*（0609 版，2006 年 9 月發布並於 2008 年 5 月作最新修訂）；
(c) *優良醫療紀錄管理手冊*（2001 年 1 月）；
(d) *資訊保安政策，程序及指引*（於 2008 年 5 月修訂）；
(e) *醫院管理局職員資訊科技保安實用守則*（2008 年 5 月）；
(f) *電子通訊政策*（1.0 版，2005 年 1 月）；
(g) *醫管局員工申請查閱臨床資料通知書；*
(h) *透露病人資料守則的草擬文件*（1999 年 5 月）；
(i) 醫院管理局總辦事處資訊科技通告第 1/2008 號*《加強個人資料保安措施》*（2008 年 5 月 14 日發出）（下稱「該資訊科技通告」）；
(j) 醫院管理局總辦事處運作通告第 9/2008 號*《處理遺失載有可識別個人資料電子儲存媒體的政策》*（2008 年 5 月 18 日發布）；*及*
(k) 醫院管理局總辦事處制定的*《行爲守則》*。

2.3 小組成員自始即經常舉行會議，並花了大量時間審閱醫管局提交的文件，研讀了多項政策文件、指引及實務聲明，以充分了解醫管局的個

人資料保安系統的運作。透過醫管局所提交的文件或與有關醫院高級職員面談，小組評估了各項文件的相關程度，並就此編製了多份審視項目的清單，以供視察時使用。

2.4 在醫管局建議下，小組於 2008 年 5 月 16 日下午到訪有關醫院，與有關醫院的高層（包括有關醫院的行政總裁）及數名醫管局總辦事處的代表進行視察前會議。根據專員所定的議程，小組花了數小時聽取報告，了解醫管局的個人資料保安系統如何於有關醫院運作。小組成員還參觀了有關醫院的不同地方，以了解有關醫院各系統的實際運作模式。有關醫院的職員亦應要求向小組解答了不同提問。在討論過程中，專員要求有關醫院的高級職員提交文件，陳述有關醫院如何執行醫管局制定的保障資料政策及措施。

2.5 首次拜訪有關醫院後，小組進行深入討論並設計了一份問卷，以供有關醫院的職員在視察期間填寫。問卷的目的是確定員工對醫管局有關資料保安政策的認知程度、醫護人員在有關醫院工作時如何應用此等政策、員工認爲值得關注的地方，以及測量他們遵守醫管局政策及保障資料第 4 原則規定的程度。

2.6 2008 年 5 月 20 日，有關醫院應專員要求提交題爲「*醫院管理局香港東聯網律敦治醫院及鄧肇堅醫院在保障病人資料私隱方面的政策*」的文件。

2.7 2008 年 5 月 21 日，公署人員在有關醫院與該院的資料管控員(Data Controller) 面談。

2.8 實地視察有關醫院如何實施醫管局制定的個人資料系統的工作，在 2008 年 5 月 23 日（星期五）開始，並在 2008 年 5 月 26 日（星期一）繼續進行。

2.9 在 2008 年 5 月 23 日視察期間，公署人員隨機選擇了約 100 名員工進行面談，就問卷中所列的問題收集答案。有關醫院的內聯網亦在 2008 年 5 月 27 日應專員要求呼籲有關醫院全體員工就醫管局個人資料系統的保安事宜直接向公署表達意見。

2.10 公署人員在 2008 年 5 月 26 日至本報告撰寫期間，多次以書面及口頭

通訊方式向醫管局及有關醫院提出了跟進問題及澄清要求。

2.11 2008 年 6 月 12 日，小組會見醫管局行政總裁及其職員，澄清一些視察期間有待答覆的事項，並向醫管局提出可能建議，讓醫管局作出回應。視察報告的草擬本亦於 2008 年 6 月 18 日交予醫管局，由醫管局核實內載的事實。小組已小心考慮醫管局的回應及意見，並在適合的情況下納入報告的最後版本中。

醫管局行政總裁蘇利民先生、專員及小組成員於 2008 年 6 月 12 日舉行會議。

第三章

醫管局的個人資料系統

醫管局持有的個人資料

3.1 醫管局持有的個人資料分爲三大類[2]：

(a) 人事記錄，包括個人資料、工作詳情、工資、酬金、福利、培訓、資歷、紀律事宜及表現評估；

(b) 醫療記錄，包括載有關於個別病人生理及／或心理健康資料的記錄；

(c) 其他記錄，包括訂立合約、頒發獎學金、醫管局大會及各醫院管治委員會的委任、行政檔案、薄紙副本檔案、公眾投訴、個人簡介等；

小組此次的視察的目的只專注於病人的醫療記錄。

病人資料

3.2 醫管局的《*臨床資料政策手冊*》（下稱「該手冊」）界定「病人」爲任何正接受／已接受醫管局服務的人士。

[2] 請參閱醫管局《個人資料（私隱）條例手冊》D 部。

3.3 條例**第 2 條**界定「**個人資料**」爲「*任何資料：*

(a) 直接或間接與一名在世的個人有關的；

(b) 從該等資料直接或間接地確定有關的個人的身分是切實可行的；及

(c) 該等資料的存在形式令予以查閱及處理均是切實可行的。」

3.4 根據醫管局於各手冊及指引內就「病人資料」所作的定義，其意思指在臨床護理過程中收集得到的病人資料，包括人口、行政及臨床資料，不論有關資料是以電子方式（例如臨床管理系統（Clinical Management System，下稱「CMS」））儲存或是以印刷本方式儲存。至於「臨床資料」一詞，醫管局則定義爲與個別人士的生理或心理健康有關的個人資料，及／或與個別人士所接受健康護理有關的資料。

3.5 病人資料中的醫療記錄可以印刷本、電子或圖像（例如 X 光片）形式儲存。小組獲悉，有關醫院的往來資料有 66%以電子形式記錄，餘下則以書面形式記錄。

3.6 只要病人爲在世人士，且醫管局所收集資料的記錄形式足以直接或間接確定其身份，則有關資料符合條例下「個人資料」的定義。

醫管局的病人資料系統

3.7 醫管局用以處理病人資料的個人資料系統每日約有三百萬個登入記錄，爲香港特別行政區最龐大的系統之一。醫管局處理病人資料的臨床資訊科技系統是由內部的資訊科技部研發的，使用者（即醫生、護士、綜合保健專業代表）亦有參與。醫管局轄下的公立醫院均使用此

系統。

3.8 小組獲告知醫管局有兩個主要的臨床資訊科技系統。其中一個以局部區域網絡爲基礎的系統（即 CMS），而另一個則是以網絡爲基礎的病人電子記錄系統。其他部門如化驗室及配藥部均有各自的系統，並會將資料輸入上述兩個主要系統中。大部分的工作站皆爲「封閉」性質，即無 USB 接口，並只准使用內聯網溝通。病人資料的書面記錄在無需使用時則儲存於有關醫院的醫療記錄儲存室內。

3.9 小組獲悉，病人資料的查閱權限取決於職員的級別及職務，規限查閱的原則必須符合兩項使用目的，分別爲「**負責醫護**」和「**按職能需要知道**」。除此兩項原則外，醫管局嚴禁查閱病人的資料。醫管局先後在多份文件及政策手冊中重申此限制。

3.10 根據該手冊，「負責醫護」所指的情況是專業醫護人員有權查閱其護理病人的臨床資料，而所查閱的資料須與其護理有關。「按職能需要知道」一詞於該手冊內的定義，概括指病人護理範圍以外有需要查閱病人資料的情況，例如用作臨床審核、臨床研究、教學用途、管理層審核及內部調查等。

3.11 醫管局的職員須申請成爲 CMS 帳戶，方可查閱病人資料。申請的方法有兩種：(i) 電子形式；或(ii) 書面形式。申請人須於申請表格內註明符合上述其中一項原則。

3.12 爲落實執行查閱病人資料前須符合其中一項原則的規定，根據醫管局提供的文件，它在審核查閱權限上採用了一套以保安風險程度作區別的制度，防止系統遭到濫用。據該手冊第 3.3 節所載，制度共設有三個權限審核保安區，分別以紅、黃、綠色代表查閱病人資料所涉保安風險的不同級別。**「綠色保安區」**指*「爲向病人提供醫護服務的目的*

而查閱其資料，或者在病人求診或入院的合理期間內查閱其資料」。小組獲悉，爲方便資訊科技系統建立適當的程式，該段「*合理期間*」初始設定爲病人求診前後的 365 日，但此項資料並無載於該手冊內。綠色保安區代表的是最低程度的保安風險。相反，「**紅色保安區**」代表的風險程度最高，包括涉查閱醫院職員的病歷資料的情況，有關的查閱並不符上文第 3.9 段所載兩項大原則。該手冊建議每月審核紅色保安區的查閱資料申請，且每當有人經紅色保安區查閱資料時，應即啓動通報機制。「**黃色保安區**」在文件中的定義較爲模糊，泛指「*紅、綠色保安區以外的一切病人資料查閱*」申請。然而，一如下文第 3.24 段所述，文件所定的區域與現實並不相符。醫管局聲稱，這是因爲落實三個保安區的概念是循序漸進地進行，以減低對病人護理的干擾。醫管局預期會在 2008 年全面實行。不過，小組看不到任何明確書面政策，支持醫管局所說。

3.13 所有員工開始在醫管局服務時，均須簽署一份承諾書，承諾遵守條例及履行病人資料的保密責任。根據醫管局發出的《*醫管局員工申請查閱臨床資料通知書*》，任何員工如欲查閱醫管局臨床系統內的電子臨床資料，均須填寫一份申請表格，當中列明需要查閱資料的理由及需要取用資料的期間，並須獲得申請人主管及醫管局執事人員的支持，方可進行。個別醫院各有自行設計的 CMS 使用者名稱申請表格及進行醫學研究目的的 CDARS[3] 使用者申請表格，格式各有不同。不過，醫管局總辦事處認爲所有醫院在制定表格時，均已遵從《*醫管局員工申請查閱臨床資料通知書*》的規定。

資料保安管治

3.14 醫管局總辦事處負責監督資料保安的一切管治事宜，並制訂有關病人資料收集、使用及保安的政策、指引及指示。在聯網層面上，不同的

[3] 臨床資料分析及報告系統(Clinical Data Analysis and Reporting System)，內容與進行醫學研究有關。

委員會負責處理各自權限內的特定事項。

3.15 2006 年 10 月，醫管局轄下的港島東聯網成立了一個**聯網資料私隱委員會**（下稱「CDPC」），負責管理私隱及保安事宜。委員會的工作範圍是「*根據醫管局的臨床資料政策及其他相關政策及條例，制定在香港東聯網實施的資料私隱及保安政策及指引，並監察情況。範圍包括：(i)管理查閱資料權限，(ii)審批查閱資料的要求，(iii)執行查閱審核制度，及(iv)調查可能違規的情況。*」CDPC 的職權範圍載於**附件 III**。小組認爲觀其工作範圍，醫院職員提出的查閱病人資料要求理應由 CDPC 處理。但醫管局表示，有關要求查實是由有關醫院的**資訊科技發展委員會**（下稱「資訊科技委員會」）處理，而 CDPC 只處理對資訊科技委員會決定所提出的上訴。

3.16 2000 年，**聯網資訊科技督導委員會**成立，監控聯網的資訊科技事宜，當中包括監督有關資料保障的一切事宜。醫管局解釋，CDPC 於 2006 年成立後，監管及制定政策的職責已交予 CDPC。

3.17 2002 年，**聯網倫理委員會**（下稱「CEC」）成立，職權範圍包括臨床及研究方面的倫理規範，以及就使用可識別身份的病人資料作研究及分析用途提供建議。其職權範圍載於**附件 IV**。

3.18 **聯網醫療記錄委員會**亦已於 2008 年成立，以就各聯網醫院的醫療記錄服務，制訂、檢討及更新聯網政策、策略、標準及工作程序。

3.19 在醫院層面上，資訊科技委員會在 1996 年成立，每半年召開一次會議，專注處理病人私隱事宜。小組獲悉該委員會亦處理有關醫院職員查閱病人資料的要求，而 CDPC 則負責處理有關上訴事宜。

3.20 病人資料保安是有關醫院***「週年工作計劃第 3 節：標準 53」***所列的檢討項目之一。該項目規定所有醫管局轄下的醫院進行自我評估，確

保在醫療記錄、健康資料及查閱病人臨床資料方面均已具備保安及保密指引。遺失的記錄須予加註，並在全面搜尋後向有關醫院管理層匯報。醫管局向專員進一步闡釋，各醫院必須向醫院管治委員會及醫管局總辦事處匯報自我評估的結果，而*第 3 節標準*的遵行情況會根據風險爲本的評估原則進行機構審核。醫管局沒有提供證據，證明醫管局總辦事處現時有對所有醫院進行按原則及有系統的私隱風險審核。

3.21 有關醫院每半年實行一次保障資料原則的循規審核，最近一次審核日期爲 2007 年 9 月 25 日。

3.22 有關醫院內部的資訊科技支援小組[4]亦會對公開的 CMS 電腦工作站進行年度審核，確保須輸入密碼方可進入 CMS 系統，以及設有自動登出功能。這項審核是有關醫院管理層主動提出並在有關醫院進行的。

3.23 有關醫院亦編製了本身的*病人資料私隱核對表*，每年分發各部門填寫。有關醫院管理層會審閱所得結果，以改善運作質素。醫管局解釋，這核對表亦有透過醫管局的網絡安排，與其他醫院共用。不過，沒有指定政策及措施顯示這是醫管局轄下所有醫院必須遵行的訂明程序。

3.24 上文第 3.12 段提及該手冊設置了紅、黃及綠色三個權限審核制度保安區，但紅色保安區實際並不存在。根據醫管局提供的資料，紅色保安區未有實行，是由於此舉須將醫管局職員的個人資料資料庫與 CMS 收集的病人資料資料庫自動配對，始可確定哪些身爲職員的病人資料被擅自查閱。這樣配對可能違反條例的規定，因爲醫管局收集職員的個人資料是爲了人事用途，不應用作其他不相關的目的，例如用作配對以醫療目的收集的資料。因此，並無實施紅色保安區權限審核制度。此外，黃色保安區亦未有按照文件規定執行。因此，實際上

[4] 根據有關醫院提供的資料，支援小組共有三名資訊科技職員，包括一名電腦操作員、一名技術服務助理及一名總務助理，由一名醫院經理管轄。該審核由醫院經理、電腦操作員及一名醫生進行。

有關醫院只實行**「綠色」**及**「非綠色」**保安區權限審核制度。對大多數醫管局員工而言，「綠色保安區」的定義較「負責醫護」的定義爲廣，這是由於綠色保安區資料並不限於病人於接受醫療期間其病人資料可被查閱，還包括該病人住院或接受治療前後 365 日期間其資料亦可被查閱。

3.25 由於並無使用紅色保安區，亦無妥善執行黃色保安區權限審核，所有審核均重新分類，撥入**「非綠色」**保安區，以分析審核追蹤記錄方式進行。該手冊第 3.3 條解釋了**「審核追蹤」**的重要性：*「所有查閱病人資料的記錄須予保存。審核追蹤可能成爲法律訴訟的理據，因此不應刪除、覆蓋或修改。審核追蹤須予保留，與病人檔案同時留存」*。有關醫院確認，2001 年至 2006 年期間，曾就正確使用 CMS 進行最少 15 次審核，隨機選取電腦系統內達百分之五的職員審核追蹤記錄進行分析。自 2006 年 CDPC 成立並議決制訂指引及準則將審核標準化以來，有關醫院只審核了一次審核追蹤記錄，時爲 2008 年 5 月。

3.26 醫管局的紀律政策及程序列明，任何職員未經授權擅自查閱病人的機密或受限制資料（包括病人檔案），可構成重大行爲失當事故，並可能須接受紀律處分，包括視乎每宗個案的情況而發出警告、停職、革職或其他適當行動。

職員培訓

3.27 所有新入職員工開始在醫管局服務時，均須參加一項迎新計劃，內容包括一個資料私隱的課程。有關醫院曾籌辦多次講座，並在 2005 年至 2008 年期間，三度邀請公署人員爲其員工講解資料私隱事宜。醫管局證實曾透過不同方式宣揚資料私隱的重要性，包括聯網通訊《東協》內的訊息傳播及在內聯網設立的「常見問題」一欄內發放等。

第四章

視察

導言

4.1 經過內部討論，審閱醫管局的文件及在有關醫院管理層的協助下，專員決定視察應集中於有關醫院如何執行醫管局制定的個人資料系統，主要範疇如下：

(a) 醫管局制定的有關病人資料保安的政策及行事方式；

(b) 醫管局資訊科技系統保安的充足程度；

(c) 監督、培訓及教育醫管局員工處理病人資料保安事宜；及

(d) 病人資料保安的審核制度，以及發生違規事故時的應變計劃。

4.2 2008 年 5 月 16 日，小組與有關醫院的高層及醫管局總辦事處的相關人員舉行視察前會議，並實地視察了有關醫院資料保安系統的運作情況（見第 2.4 段）。

2008 年 5 月 21 日：與有關醫院的資料管控員[5]面談

4.3 有關醫院的資料管控員身兼其他職務。2008 年 5 月 21 日，他在有關醫院與公署職員面談。面談期間，他被要求提交述明其職務範圍的文件，但他表示並無有關文件。他在 2002 年獲有關醫院委任爲資料管控員，作爲主要職務以外的兼任職位。他表示資料管控員無需特別必

[5] 根據《*個人資料（私隱）條例手冊*》，這是由醫院自行任命，負責確保醫院遵從條例規定的人士。

要技能，資料管控員通常由有經驗的行政職員擔任，但有少數是醫生。他表示，身爲資料管控員，他的主要職責是處理及監督員工處理由資料當事人提出的查閱資料要求[6]，這些要求所涉及的記錄包括員工記錄、病人記錄及投訴人記錄。他無須向醫管局總辦事處的資料管控員負責。當被問及資料管控員會否進行審核工作時，他表示他每年須向聯網行政總監提交一份題爲「*律敦治醫院及鄧肇堅醫院病人資料私隱核對表*」的審核核對表。醫管局總辦事處會對有關醫院進行審核，而資料保障是其中一項審核項目。他亦會定期到訪資料收集中心，及隨機抽查其他資料工作站。

4.4 在培訓方面，他表示聯網人力資源部(HR)每年會爲新入職員工籌辦數次迎新課程，課程包括一些個人資料管理的培訓。聯網近年亦籌辦了多次有關資料保障的講座。他表示他並無責任確保有關醫院爲職員提供個人資料保障的培訓，但他會應要求提供協助或參與這些活動。

4.5 在發放資料保障的信息方面，他表示有關醫院管理層會以電郵方式向有關職員發放醫管局總辦事處及聯網的有關政策及指引，亦有向無權使用電腦工作站的員工派發印刷本。有關醫院管理層亦有向員工提供最新的資料保障訊息，這些訊息會被本位化，以便更適用於有關醫院，但他強調，有關的更新資料必須符合醫管局指引的核心要求。

2008 年 5 月 23 日至 2008 年 5 月 26 日：實地視察

4.6 小組首先邀請醫管局總辦事處及有關醫院的代表講述處理病人資料保安的各個範疇（見下文分項），然後進行問答環節，當中小組成員可以自由提問，由有關醫院給予進一步詳情、解釋或闡述。整個視察活動都是以這個形式進行。此外，有關醫院管理層亦引領小組成員巡視有關醫院的不同部門。

---

[6] 根據條例第 18 條，資料當事人有權向資料使用者提出查閱資料要求。

視察保安政策及做法

4.7 在這個環節裡，有關醫院的代表向小組演示了有關醫院及聯網各個委員會在監督資料私隱方面的職能。醫院委員會的職權範圍僅限於所屬醫院，而聯網委員會則可在其權限內監督聯網醫院一切事宜。聯網 CMS 工作組集中管理 CMS 所載的臨床電子資料，而 CDPC 則專注於以電子及書面形式儲存的病人資料私隱事宜。聯網醫療記錄委員會監督有關病人臨床記錄（特別是文書記錄）的一切管理事宜。CEC 主要負責處理臨床研究的申請，並提醒研究的申請人嚴格遵守尊重資料私隱的規範。

4.8 聯網委員會由不同醫院的職員組成，當中部分職員是跨會成員。

4.9 有關醫院的代表告知小組，有關醫院的資料管控員的主要職責爲處理行政工作，而他獲委任爲資料管控員，只是在其主要職責以外的兼任職務。他並非 CEC 或 CDPC 的成員。小組問及資料管控員的職責範圍，其後獲得的答覆是小組可參閱營運通告第 13/2007 號《*遵守醫管局有關條例*》，當中載有負責人員名單。此外，《*個人資料（私隱）條例手冊*》規定，資料管控員由醫院自行提名，負責確保醫院遵從條例規定。除所提及的*「確保遵從條例規定」*外，小組發現並無文件說明資料管控員須履行的特定職責及角色。

4.10 有關醫院的代表接著向小組成員描述一個典型以研究用途爲由，申請查閱 CEC 所管理的一名病人的資料的過程。申請人須先填妥一份申請表格，列明一切必要詳情，並聲明申請理由，始將申請表格提交 CEC 秘書處。申請表格將轉交 CEC 主席，如主席認爲申請查閱的敏感資料並無臨床或私隱風險時（但使用香港身份證號碼則不屬任何風險評估範圍），他可本人予加快批准。但如他持保留意見，他可將申請表格退回申請人，要求提供更具體資料，或將申請轉交 CEC 以待全體委員批准。有關醫院的代表出示了一份標準的 CDARS 使用者申請表格，以供小組審閱。

4.11 有關醫院的代表演示的另一個管制範疇是 CDPC 的管制範疇。除了決定申請人能否查閱紅色保安區內的資料外，CDPC 還負責批准病人資料查閱級別的一般提升程序，包括查閱紅色保安區資料及查閱附有香港身份證號碼的病人資料的申請。CDPC 是根據醫管局總辦事處的指令及個別醫院的特殊情況作出決定。CDPC 還會按個別情況處理特殊要求，事後再交由聯網管理層副署同意。應小組要求，有關醫院同意提供 CDPC 會議記錄的副本[7]。

4.12 有關醫院的代表接著闡述另一個範疇，這個範疇正導致針對基督教聯合醫院的投訴，即遺失載於手提電子儲存裝置的資料。小組成員參閱了醫管局在轄下若干醫院遺失資料事故後於 2008 年 5 月 14 日發出的資訊科技通告。該資訊科技通告就使用 USB 記憶體下載資料及其保安問題發出了明確指示，包括規定所使用的 USB 記憶體必須支援加密功能及配備密碼鎖定裝置，並須集中由醫管局供應。

4.13 在該資訊科技通告發出後，各員工須先獲得聯網管理層批准，方可下載病人資料。該資訊科技通告亦指定，除「*對病人護理有絕對需要*」外，一概不得下載病人資料。資料只可在遵照該資訊科技通告的規定下，經聯網管理層同意，及必須經過加密及以密碼保護的情況下才可下載。有關醫院的代表向小組出示了最近制定的《*加密 USB 記憶體使用者申請表格*》，當中載有申請人提交申請時須就資訊科技保安、保密及版權作出的聲明。

4.14 小組獲告知在 2008 年 5 月 15 日發出的新政策，題為《*處理遺失載有病人的可識別個人資料電子儲存媒體的政策*》[8]，內容指已實施一套有系統的申報制度，而員工、主管、部門主管及醫院管理層均有責任申報。醫管局亦將按醫事匯報系統(Advanced Incident Reporting System)（下稱「AIRS」）要求提交報告，並作出補救行動，例如向警

---

7 有關醫院其後提交了 CDPC 三次會議的會議記錄副本，以供小組審閱。

8 醫管局總辦事處營運通告第 9/2008 號。

方報案、通知病人及專員，以及發出新聞稿。

問答

4.15 小組詢問 CEC 在加快批准查閱病人資料作研究用途的申請時，有否作出任何風險評估。有關醫院的代表回應指，CEC 將考慮多項因素，例如：會否增加對臨床治療的干擾；會否涉及敏感的私隱問題（如已識別爲愛滋病(AIDS)病人的個人資料）；擬進行的研究是否涉及易受損害的人士；以及是否已獲得其他聯網有關委員會的事先批准。對於 CEC 主席給予的加快批准，CEC 並無要求在批准查閱資料後的會議上須列作跟進及追認的事項。小組對 CEC 及 CDPC 若干角色重疊的情況表示關注，例如處理查閱載有識別資料的病人資料。

4.16 對於審批查閱病人資料級別的申請，現時的審批標準是按個別情況考慮，小組詢問這方面有沒有審批指引。小組獲告知，審批查閱權限乃基於兩項原則決定，即「負責醫護」及「按職能需要知道」（見第 3.9 段）。例如，註冊護士獲授權查閱其任職病房內病人的資料，而部門營運經理有權查閱其部門內所有病房病人的資料。另一方面，有特別職責的職員，例如感染控制組成員及病人關係主任，根據「按職能需要知道」的原則獲授權查閱有關醫院所有病人的資料。除了根據以職位爲本的原則下限制查閱權限外，他們沒有訂明的指引，在審批查閱病人資料的申請時作爲依據。

4.17 小組問及綠色保安區與紅色保安區在查閱權限上的分別，得到的回覆是只會就紅色保安區的查閱權限進行事後審核（每週一次）。在處理查閱資料申請的過程中，系統只會在發現申請並無填報所需資料時，才會自動發出審核提示。醫管局並無規定轄下醫院須就此作出匯報，但仍有部分醫院選擇這樣做。根據有關醫院的資料，紅色保安區的審核制度自 2007 年 9 月起停止執行，原因是醫管局早前曾致函公署，詢問關於人力資源部的員工檔案與 CMS 內收集的員工病歷檔案的配

對問題，而當時醫管局收到了公署的回覆。由於配對的結果不會使資料被配對的資料當事人遭受「不利行動」，因此並不構成條例下的「核對程序」，故有關申請無須專員批准。但爲恐有關的配對作爲會違反條例其他條文，因此他們一直未有復行上述審核制度。

4.18 有關醫院應要求作出澄清，指有關醫院在將醫管局的政策及措施「本位化」、並自行發出關於處理病人資料的內部通告或指引前，無須先經醫管局總辦事處批准。有關醫院的代表解釋，該等通告及指引所規定的標準不得低於醫管局的總政策及行事方式，但有關醫院可按照本身情況作出輕微修訂。

4.19 小組留意到各醫院所使用的申請表格存在若干不一致及錯誤之處[9]，但其基本精神則屬一致。

4.20 被問及如何向員工有效傳達醫管局的資料保安政策及做法時，有關醫院回應指，員工通常會參閱內聯網上的《*資訊科技保安手冊*》及《*臨床資料政策手冊*》。此外，有關醫院亦會定期向員工發出通告及電郵。小組獲提供由有關醫院管理層發出的通告副本，內容是提醒員工有責任將病人資料保密，以及如何正確使用 CMS。醫管局提供的進一步資料亦確認，在履行職務時，前線員工會參閱政策及措施的簡易版[10]；臨床管理職員會參閱手冊及政策的全文[11]；資訊科技人員則會參閱相關的資訊科技手冊[12]。

---

9 如：CMS 使用者申請表格、CDARS 使用者申請表格及資訊科技承諾書。看來每間醫院自行設計其 CMS 申請表，有些醫院更以該表格用於其他申請，例如 CDARS，而且表格內所註明的使用規則詳情亦各有不同。《加密 USB 記憶體使用者表格》中亦有些錯字。

10 題爲《*醫院管理局職員資訊科技保安實用守則*》、《*保障病人機密資料*》及《*臨床資料政策常見問題*》的刊物。

11 《*臨床資料政策手冊*》、《*個人資料（私隱）條例手冊*》及《*披露病人資料守則*》。

12 《*資訊保安政策，程序及指引*》及《*電子通訊政策*》。

視察資訊科技保安系統

4.21 醫管局總辦事處的代表用電腦簡報了醫管局轄下各個臨床系統，概要圖表載於**附件 V**。醫管局設計了機構臨床系統，因應不同的組成系統而具備不同的功能，例如：病人登記、病人治療、X 光檢查、病理測試或配藥。使用前述功能的人士無法查閱工作所需以外的其他資料。各醫院網絡以廣域網絡連接醫管局總辦事處的網絡系統。

4.22 職員申請 CMS 使用者賬戶時，有關申請須經其管理小組提交。系統管理員會提供一個新的使用者名稱及密碼，從而開設使用者賬戶。職員須按要求填妥使用者賬戶申請表及簽署保密承諾書。病人資料按職級實行查閱權限管制，例如：醫生級別可獲授權查閱其身爲臨床醫生所需的資料，如處方、一般臨床要求等。護士級別職員則獲授權查閱病人出院、病床分配等資料。

4.23 每當登入 CMS 系統時，屏幕均會彈出一段重要訊息，提醒員工有責任將病人資料保密。系統會保存所有使用者的登入登出記錄，包括其身份、登入時間、取用的病歷種類及性質。該等審核記錄可供醫院進行調查、隨機檢查及審核等用途。

4.24 醫管局總辦事處的代表就醫管局實施的權限審核制度進行了個案分析簡報。資料先按有關風險分爲紅色（即高風險，例如員工檔案、涉及公眾利益的病人資料）、黃色（即中風險）及綠色（即低風險，例如病人求診記錄）。基於上文第 4.17 段所載原因，紅色保安區的權限審核已在 2007 年 9 月停止執行。有關方面曾嘗試使用其他方法執行審核，但該等方法並無成效。因此，現時只按審核追蹤及查閱理由，進行「非綠色保安區」權限審核。然而，至今並未全面制訂一套審核準則，以識別不正常的查閱情況。一經發現違規，當局會視乎違規情況輕重即時展開紀律行動[13]，包括給予輔導、發出警告信及向警方報

[13] 醫管局的紀律政策及程序，所有僱員必須遵從醫管局不時制定或公布的規則及規例。違反醫管局規則及規例的僱員可處政策所定的紀律處分。未獲授權查閱有關病人的機密或限閱資料，包括病人記錄，被視爲重大行政失當。

案等。2008 年 5 月，有關醫院根據編製給其覆核及研究的「非綠色保安區」查閱資料記錄表，進行了一次「非綠色保安區」權限審核，而據醫管局表示，該次審核是根據聯網一般的共同看法及覆核人的專業判斷進行。不過，小組對於該次審核不是根據指定的審核方法進行表示關注。會上亦向小組演示了有關醫院各部門的工作流程，藉此解釋各系統的相互關係。

問答

4.25 被問及有關醫院的病人資料由誰擔任資訊科技保安負責人時，醫管局總辦事處的代表回應指負責人是資訊科技委員會。他補充指，在有關醫院的 172 部終端機中，只有 10 部配備可使用的 USB 連接埠，其餘工作站均以「封閉」方式運作，並無連接視窗作業系統。

4.26 小組詢問系統登入密碼的使用期限。小組留意到雖然有關醫院定期提示員工應更改密碼，但並無就密碼設定使用期限。有關醫院的代表解釋，有關醫院曾嘗試執行更改密碼的措施，但此舉引起混亂，其後再無執行。然而，在開設賬戶後，員工須在首次登入系統時更改密碼。員工亦不得與其他使用者共用密碼。系統並不容許使用者下載或列印有關醫院系統內所儲存一名病人的全部檔案。

4.27 被問及使用手提電子儲存裝置下載病人資料的情況時，醫管局總辦事處的代表回應指，不論採用何種器材（不論是筆記本電腦或 USB 記憶體），有關資料均須至少以 128 位元 RC4 標準加密[14]。醫管局早前發出規管使用手提電子儲存裝置的資訊科技通告，規定員工須經批准，方可使用該等裝置，有關醫院隨即提醒員工刪除載於其私人器材內的所有病人資料。有關醫院員工無需使用其私人電子儲存裝置於其工作上，但如欲使用，須先把有關裝置向有關醫院登記。有關醫院並無 Wi-Fi 設備。

[14] 微軟辦公室軟件所實施的標準，其保安成效備受質疑。

4.28 被問及遙距登入醫管局系統的情況時，醫管局總辦事處的代表回應指，除非經指定的遙距電腦，否則不能以遙距方式登入系統，而無支援此項功能（即並無安裝視窗作業系統）的工作站亦不能下載資料。就使用電子通訊設備而言，醫管局的《*電子通訊政策*》訂明使用電郵及互聯網等電子通訊設備的規定，禁止以電子郵件傳送機密資料（雖然在技術上接駁了互聯網的電腦可以做到）。關於愛滋病、精神病病人的敏感資料一律加上特殊標記並獨立存檔，以加強保障。

4.29 被問及資訊科技承辦商在測試系統時會否使用真實的病人資料，醫管局總辦事處的代表回應指，承辦商一般不會使用真實資料。相反，所使用的資料是假資料，而資訊科技承辦商只准實地工作，並須簽署保密承諾書。小組要求醫管局總辦事處的代表提供標準的資訊科技合約及保密承諾書，以供審閱[15]。

4.30 小組問到，下載病人資料（包括病人的身份證號碼）作研究用途是否須獲得批准，以及使用者有權查閱資料是否自動等同有權下載病人資料。回應指，任何研究報告的終稿均不含身份證號碼，因此，員工在研究期間可查閱及下載該等號碼，並無重大影響。小組關注此舉忽視了資料原始檔案的私隱風險。醫管局總辦事處的代表亦澄清，申請系統配備功能，可就每名員工的個別申請授予指定的查閱權限（例如限於開設賬戶、查詢、打印、下載資料等個別使用要求）。因此，系統管理員可根據員工的權限及需要授予查閱權限，換言之，有權查閱病人資料，並不自動等同有權下載資料。

4.31 在保安問題上，醫管局總辦事處的代表回應指，資料下載功能加入了密碼保護及資料加密兩項特點。所有有權下載資料的員工在下載資料時，必須使用密碼保護及檔案加密的功能。

---

[15] 有關文件其後由醫管局提交。

視察員工的循規監管、培訓及教育

4.32 有關醫院的代表簡報了監管員工遵從資料保安政策及措施方面的情況，以及爲員工提供保障病人私隱資料培訓及教育的情況。

4.33 有關醫院的代表確認，有關醫院定期向員工發出及傳閱有關於對病人資料保密及正確使用 CMS 的通告。員工須逐一簽署，確認已閱讀有關通告。在使用電子通訊的適當行爲上，醫管局在 2005 年 1 月 19 日發出了一份題爲《*電子通訊政策*》的資訊科技通告，並在 2008 年 5 月 14 日再發出另一份題爲《*加強個人資料保安措施*》的資訊科技通告。一旦發現以不當登入行爲及重大行爲失當，有關醫院將採取紀律行動，包括給予輔導、發出警告信、解僱或向警方或執法機關報案。員工均須遵守受聘時獲發的醫管局行爲守則手冊。保障病人資料的規定亦曾在 2008 年 2 月份的聯網通訊《*東協*》內公布。

4.34 港島東聯網的人力資源部爲各醫院員工開辦個人資料私隱的培訓計劃，包括綜合保健／管理及行政員工迎新計劃（每年一次）、醫務人員迎新計劃（每年兩次）、護理人員迎新計劃（每年兩次）、後勤員工迎新計劃（每年三至四次），亦曾舉辦個人資料私隱的研討會及講座，並邀請公署人員主持講座（2005 年至 2008 年間合共三次）。2006 年 12 月 13 日，CDPC 亦爲各聯網醫院舉辦了關於查閱臨床資料及臨床資料政策的研討會。據有關醫院提供的統計數字顯示，參與上述研討會及講座的員工比例偏低。關於這個現象，醫管局表示這是所有醫院都知道的問題，這是因爲輪班制及需要照顧病人所致。醫管局預期那些參加者擔當有計劃的角色，透過小組會議等，將所學的知識傳給同事。但醫管局沒有提供政策或實務文件，證明該有計劃角色的存在。

4.35 最近期的「個人資料私隱」研討會是由有關醫院及醫管局總辦事處合辦，於 2008 年 5 月 20 日舉行，即專員向醫管局送達視察通知後不久。

問答

4.36 小組詢問，對於醫管局委任承辦商提供的碎紙服務，有否執行適當的監察措施，另對於醫療記錄辦事處存置的不同類型資料，有否監察其有否遵守規定的保留期限。有關醫院的代表回應指，由於醫療記錄辦事處的儲存空間有限，有關醫院定必銷毀不必要的書面資料。該代表示意小組可聯絡醫管局，索取與碎紙服務承辦商訂立的標準服務合約副本[16]。

4.37 小組獲告知，有關醫院每年均會進行一次審核，確保在公眾地方的工作站設有保護密碼及適當的自動登出功能。

4.38 小組詢問有關醫院在使用 USB 記憶體方面如何執行資訊科技通告的規定。有關醫院的代表回答稱，有關醫院會保留使用記錄，員工如需使用 USB 記憶體，須先提出申請，院方會視乎運作需要決定是否批准。目前，醫管局總辦事處合共分配了五個附設加密及密碼保護功能的 USB 記憶體，以供有關醫院使用。使用登記冊則由醫管局總辦事處保存。

4.39 小組又問到，如何向員工有效傳達內聯網上數量如此龐大的政策、資訊及資料。有關醫院的代表確認，聯網內聯網上的資料的確愈來愈多，但他不認爲員工只傾向查閱有關醫院層面的訊息。

4.40 被問及聯網之間會否分享培訓資料時，有關醫院的代表回應指，大部分培訓資料均由醫管局總辦事處的負責人員編製，他注意到所有聯網使用的培訓資料基本相同。

4.41 被問及員工的資料保安知識會否反映於其年度表現評核時，有關醫院的代表承認，對於員工的個人資料私隱的培訓，監管水平等常識及遵守程度並未如員工須對傳染病及職業安全常識認知般嚴格，故並無硬性規定員工出席培訓及達至所需標準。

---

[16] 服務合約副本已於其後提交專員審閱。

視察資料保安審核系統及資料保安違規的應變計劃

4.42 有關醫院的代表簡報了資料保安審核及應變計劃的內容。據他表示，有關醫院的*「週年工作計劃第 3 節： 標準 53」*約於十年前實施，各醫院須進行自我評估，確保在醫療記錄、健康資料及查閱病人臨床資料方面均已具備保安及保密指引。遺失的記錄須予加註，並向醫院管理層匯報。審核結果必須向醫院管治委員會及醫管局總辦事處匯報。有關醫院的代表確認，有關醫院已全面遵守病人資料保安及保障的訂明標準。

4.43 有關醫院就條例的循規審核，每半年進行一次，上次審核於 2007 年 9 月完成。有關醫院的資訊科技部員工亦對密碼監控及自動登出功能進行年度資訊科技審核。有關醫院最近編製了一份*私隱事項核對表*，以供有關醫院各部門使用。醫管局向小組確認，有些醫院已透過醫管局的網絡安排，分享使用該核對表。

4.44 有關醫院的代表表示，在 2002 至 2006 年間共進行了約十五次審核，憑審核人員的經驗及判斷，審視病人資料有否被異常查閱。有關醫院以隨機抽樣方式，抽查多達百分之五員工於電腦系統內的審核追蹤記錄。其後因 CDPC 決定接手審核工作並制訂系統性指引，有關醫院內部進行的審核工作便於 2006 年底停止。然而，CDPC 至今尚未制訂出審核準則，以供開展系統性的審核工作。

4.45 「紅色保安區」的審核工作因第 4.17 段所述理由停止。

4.46 至於應變計劃，現時具備一套系統，通過 AIRS 通報載有病人資料的電子儲存裝置的遺失事故。醫管局於 2008 年 5 月 15 日發出的*營運通告第 9/2008 號*載有各級通報方式。一旦發生任何資料遺失事故，員工須通知主管或部門首長，並通過 AIRS 提交報告，而警方亦會收到報告。主管或部門首長亦必須向醫院的行政總監及／或聯網行政總監報告事故，後者將於 48 小時內上報醫管局總辦事處。

4.47 當發生遺失載有個人資料的電子儲存裝置時，醫管局須通知受影響病人及公署，並撰寫新聞稿公布事故。

問答

4.48 小組獲告知，查驗審核追蹤記錄被認爲是有效的方法。雖然小組成員讚賞有關醫院透過一名醫生所做的工作及成績，但成員同時質疑過份依賴一個人的專業判斷，而沒有制定按原則或客觀的準則的方法以供依從，是否明智。

4.49 小組讚揚醫管局以高度透明手法處理資料保安違規事故，在發生資料遺失事件後，盡快通知當事人，有助減輕對他們造成的私隱損失。同時作爲良好的行事方式，小組亦鼓勵醫管局採取積極措施，主動通知執法機關及公署。

實地巡視

律敦治醫院

4.50 經過簡報及問答環節後，小組於 2008 年 5 月 23 日下午前往律敦治醫院的急症科、醫療記錄儲存室、病理科、病房及物理治療部視察。

4.51 視察過程中，小組的成員注意到下列情況：

急症科

(a) 以中、英文撰寫的《*病人通告*》張貼於當眼處，告知病人於登記時需要收集個人資料。病人提供個人資料時，院方亦會出示類似的通告；

(b) 病人需要出示身份證以便核實身份；

(c) 在病情評估分流區，病人的醫療記錄暫時擺放在一個文件盤上，並以印有「機密」及註明「*根據個人資料（私隱）條例，未經授權查閱本文件夾內的資料即屬違法*」字句的警告告示覆蓋；

(d) 所有電腦系統只可連接至臨床管理系統，但不得連接互聯網；

(e) 放有書面病人醫療記錄的文件盤一律以印有「機密」的綠色封面覆蓋；

(f) 當螢幕顯示病人的籌號時，病人需要前往櫃檯付款及登記。會見醫生時，職員會講出病人的名稱；

<u>醫療記錄儲存室</u>

(g) 所有書面病人醫療記錄（不包括 X 光片）均存放在上鎖的文件櫃內；

(h) 對於超過六年並無再次求診的病人，院方會每年利用碎紙機將這些病人的醫療記錄銷毀，只有未經使用的非機密紙張會循環再用。碎紙工作會交由醫管局委聘的指定承辦商負責，紙張會存放在密封的不透明膠袋內，等待每星期收集；

(i) 用作運送醫療記錄進出儲存室的手推車以特製的布套遮蓋；

(j) 法醫醫療記錄存放在儲存室另一個上鎖的房間內；

<u>病理科</u>

(k) 載有病人血型及身份證號碼的檔案會每月下載至一個獨立系統，以便一旦主系統停止運作時可以將檔案復原。檔案以 128 位元 RC4 加密方法加密，而獨立系統不會連接互聯網；

九樓病房（名稱爲「A9」）

(l) 巡房過後，所有無需使用的醫療記錄及文件會妥爲收集及放置於護理站前的手推車上；

物理治療部

(m) 病人每次應診時，職員會在病人的物理治療咭上註明病人的姓名、床位編號及將要進行的物理治療項目；

(n) 完成物理治療後，物理治療師或護理人員會即時在病人的書面醫療記錄中記下日期及所進行的物理治療項目。

鄧肇堅醫院[17]

4.52 小組其後前往鄧肇堅醫院視察以下部門，而鄧肇堅醫院並無提供病人住院服務：

登記及付款櫃檯

(a) 接待處亦有張貼與律敦治醫院展示的類似通告；

(b) 所有電腦並無連接互聯網；

(c) 每位首次求診的病人均會獲發一張覆診咭，其上印有病人姓名及指定的病人編號（並非身份證號碼）。病人下次需要帶同覆診咭覆診；

[17] 這座建築物與律敦治醫院大樓分開，相距約 10 分鐘的路程。

醫療記錄儲存室

(d) 所有書面病人醫療記錄均妥善存放在上鎖的文件櫃內；

(e) 放有書面病人醫療記錄的手推車均以印有「機密」的綠色封面覆蓋；

(f) 只有未經使用的非機密文件會用作循環再用紙；

(g) 未經使用的機密文件會放置於密封的不透明膠袋內，然後轉交醫管局指定的承辦商負責碎紙；

活動室

(h) 所有位於公眾地方的電腦系統並無連接互聯網；

(i) 由於部分電腦螢幕面向公眾地方，電腦的自動登出時間由一般的 10 分鐘改爲 1 分鐘；

家庭醫學專科診所

(j) 以《*收集個人資料聲明*》爲標題的通告（備有中、英文版本）張貼於登記處，而通告副本亦可供病人索取；

(k) 可登入 CMS 的工作站並無連接互聯網；

(l) 所有病人的醫療記錄均以印有「機密」的綠色封面覆蓋；

(m) 每位首次求診的病人均會獲發一張印有「*家庭醫學診所／一般門診醫療記錄*」字樣的醫療記錄咭，其上貼有病人識別標貼，載有病人姓名、身份證號碼、性別及出生日期。每次求診時，醫護人員或護理人員會將病人的診斷結果及其他醫療詳情記錄在咭上，作爲病人記錄及保管之用。

專員及小組成員於有關醫院的急症科觀看臨床管理系統的操作。

有關醫院的代表於 2008 年 5 月 23 日向小組講述情況。

第五章

問卷

5.1 小組進行視察前，有機會審閱醫管局提供的大量文件，內容關於保障病人資料的政策、已發出的通告及委員會會議記錄。因此，小組可藉有關文件及有關醫院職員在會面中提供的資料，確定醫管局資料系統中哪些範疇有待進一步詳細查詢，以便評估有關醫院的員工對私隱的認知程度。

5.2 2008 年 5 月 23 日，公署人員隨機選出約 100 名有關醫院的員工面談。由於面談可能會對員工的日常工作造成不便，有關醫院事前獲告知有關面談。公署人員向他們派發一份英文問卷，但告知他們如在理解問題方面遇到任何困難，可索取問卷的中文版本。若干問題的結果出現差異，因爲部分員工選擇不回答個別問題，又或堅持填寫多於一個回應欄[18]。問卷副本及問卷結果分析，連同下文第 5.7 (o)段所述的改善建議概要載於**附件 VI**。

5.3 儘管部分回應引起上述關注，問卷得出的結論屬意料之內。須要指出的是，公署人員認爲有關醫院在視察前曾爲員工提供協助[19]，估計員工會被問及的問題。支持以上觀點的理據包括，部分員工回答若干較深入的問題時，他們的回應似乎未如回答問卷問題般準確。雖然公署人員認爲回應大致正確，但對整體回應結果某程度上存保留態度。

5.4 儘管如此，對於用作諮詢員工意見的開放式問題，他們都率直坦誠地回應，員工多表示需要安排更多培訓，藉以提高對私隱的認知程度。

5.5 2008 年 5 月 23 日進行問卷調查後，公署向有關醫院員工發出一份邀請書，邀請員工就病人資料保安方面，直接向公署表達意見及評語。

---

[18] 參閱附件 VI 的問卷部分問題的回應統計撮要。

[19] 舉例來說，有關醫院於 2008 年 5 月 20 日（剛好在視察進行之前）舉辦了一個有關個人資料私隱的研討會。正面來看，專員認爲視察的進行，有利讓員工溫故知新，讓醫院提醒他們各手冊、政策及措施中有關保障個人資料私隱的規則及規例，提升員工的私隱意識。

可惜截至本報告撰寫當日仍未收到任何回應，專員對此表示遺憾。

5.6 小組關注的具體事項載列如下，當中反映在醫管局資料保安政策及存檔、銷毀檔案、監督、教育及培訓等相關事宜方面員工的認知情況。

5.7 小組希望從前線使用者當中，就以下範疇收集更多有關醫院在資料處理實務方面的資料。對收回的問卷進行分析後，小組亦提出以下評語：

(a) 有關醫院的員工有否接獲指示，得知在查閱病人資料前，須事先取得批准？（問題 6）

相當數目的員工(34%)表示，他們從未接獲任何有關指示。結果顯示員工並不知悉取得醫管局系統的密碼，是獲准在日常工作中查閱病人資料的標準程序。

(b) 有否指示員工僅可在符合「負責醫護」或「按職能需要知道」兩項條件之一的情況下，方可查閱病人資料？（問題 8）

正面回應的百分率相當高(93%)，表現理想。

(c) 員工有否在查閱資料後自行登出系統，還是待工作站處於休止狀態 10 分鐘後自動登出？（問題 10）

依據系統自動登出的做法(10%)應受阻止。

(d) 員工有否共用系統密碼？（問題 11）

此舉屬瀆職行爲(3%)，應予以禁止。

(e) 員工有否匯入病人資料？如有，以甚麼方式匯入？（問題 12／13）

有關回應有助評估工作實務。

(f) 員工有否下載或匯出病人資料？如有，資料是否設有密碼保護或

加密？（問題 14）

有使用加密／密碼(83%)，部分原因可能是醫管局總辦事處近期發出的資訊科技通告所致。

(g) 有否獲授權下載資料？如有，由誰人授權？（問題 15）

近 20%員工顯然在未獲授權的情況下擅自下載資料。雖然這明顯是嚴重的違規行爲，但小組相信，較可能的是員工誤解了問題，因爲小組認爲員工下載資料確需要獲授權。

(h) 匯出的資料在匯出前是否已除去可辨識身份的資料？（問題 18）

半數回應者（11 人答「有」；11 人答「沒有」）並無除去可辨識身份的資料，而他們不除去有關資料可能有合理原因，小組對此並不表示反對。小組得到的解釋是，沒有身份證號碼會難以重新配對 CDARS 資料，這可能是合理原因，但仍然會有私隱風險。

(i) 員工可否獲准將病人資料帶離工作場所？如是，則是在甚麼情況、基於甚麼理由及由誰人授權下才可同意批準？（問題 27）

可能員工對「工作場所」一詞有混淆，以致數據可能有誤導成份。

(j) 員工有否將病人資料儲存在其私人器材內？（問題 29）

大多數人對問題(a)及(b)回應「沒有」；這可能是近期發出該資訊科技通告禁止員工使用私人電子儲存裝置所致。

(k) 員工是否知悉爲了規管處理病人資料而發出的政策及指引？如是，則有多了解有關政策及指引？（問題 31）

對問題兩部分的正面回應達 98%，高於小組預期。

(l) 員工是否知悉關於通報任何遺失病人資料事故的政策或指引？（問題 34）

回應率同樣較高。

(m) 員工有否接受任何病人資料保安培訓？如有，培訓是否足以使他們明白資料保安的相關事宜？（問題 35／36）

「不關心」的回應達 3%，結果令人失望。

(n) 員工是否知悉有關醫院一直存在的問題，即共用密碼、查閱資料後未有登出系統、廣泛使用手提電子裝置及在無人看管下放置載有資料的手提電子裝置？（問題 42）

電腦在使用後沒有被登出有較高的回應率，反映小組在有關醫院某部門所見的情況。

(o) 員工亦獲邀概括評論如何改善有關醫院現行的個人資料系統，藉以加強保障病人資料。（問題 44）

收集的觀點有助小組制訂建議。

第六章

觀察所得及建議

保障資料第 4 原則的應用

6.1 在進行視察及向醫管局作出建議時，專員必須評估醫管局是否已採取保障資料第 4 原則所規定的「切實可行的步驟」，保障病人的資料。醫療服務提供者所採取的保障病人資料措施，應該與收集、持有、處理及使用該等資料的私隱風險相稱。尤其應考慮：

(a) 該等資料的種類及如未經准許的查閱等事情發生所能造成的損害；

(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步驟。

6.2 保障資料第 4 原則並沒有規定資料使用者有絕對責任保證所持有的個人資料的安全。保障資料第 4 原則只是要求資料使用者採取**「合理地切實可行」**的步驟，保護資料免受未經准許的或意外的查閱、處理、刪除或其他使用所影響。「合理地切實可行」一詞經常在法律的條文中出現。專員參考了有關判例 [20]，在審研資料使用者是否已證實採取合理地切實可行的步驟時，它必須顯示：

(a) 有存在風險的意識（就本個案而言，該風險涉及出現未經准許的或意外的查閱、處理或刪除病人資料的情況）；

[20] Edwards v. National Coal Board [1949] 1 AER 743 及 Marshall v. Gotham Co. Ltd. [1954] AC 360。

(b) 已確定有關風險；及

(c) 資料使用者（在本個案指醫管局及有關醫院）在衡量現時實務中採取保障該等資料的步驟與是否須付出超乎比例的「時間、金錢或麻煩」以執行該些步驟之間，作出有意識的決定或連串決定。

6.3 在衡量醫管局是否已採取**「合理地切實可行」**的步驟時，專員知道醫院的首要職責是拯救生命，這個職責是對公眾非常重要的。專員亦明白現今並無任何政策、指引或手冊，能夠完全防止人爲錯誤的發生。不過，藉著較佳的資料保障系統和對受託處理病人資料的人加以適當的監督、培訓及教育，應可以大爲降低人爲錯誤的發生。資料使用者不能貿然以採取這些保安措施所花費或招致的「時間、金錢或麻煩」作爲理由或藉口，延遲或逃避實行足夠的保安措施，保障其持有的個人資料。鑑於公立醫院系統是由醫管局管理、涉及的病人數目龐大，以及由他們處理的敏感資料數量繁多，他們的處理手法對病人資料的保安至爲重要。醫管局如能對病人資料保安系統作詳細檢討及改進，不單可以恢復公眾信心，長遠來說，還會對建議推行的電子醫療平台有著利好的影響。因此，爲了公眾利益，醫管局應採取高水準的保安措施。

6.4 小組承認醫管局已作出重大努力，制定一個病人資料保安系統，在提供醫療服務之餘，亦保障資料的安全。小組的整體印象是，醫管局確有制定良好及詳細的政策和措施，保障病人資料的安全；由醫管局總辦事處經聯網到醫院，在實施該等政策和措施上的水準和協調程度，介乎尚可至滿意。不過，他們須在監察條例的遵從及保安審核方面作出更多努力，設立有效有系統的方法以偵測任何洩漏資料或不遵從條例規定的癥兆。最後，員工的一般私隱意識程度，顯示有迫切需要作出提升，因爲很多資料洩漏事件都是由人爲錯誤造成的。總而言之，醫管局必須作出更多努力，尤其在儲存及使用電子形式的病人資料方面，提供足夠的安全保障。

6.5 小組在是次視察中確定了不同的關注範圍，並向醫管局作出了相應的建議，促進他們遵從條例的保安規定。專員在作出這些建議時，知道他不應取代醫管局管理層的角色，代爲決定哪是最佳的做法。正如其他資料使用者一樣，這個決定留待醫管局作出。因此，有關建議在執

行上是具彈性的，醫管局可以因應特定的運作需要或情況而施行，以遵從條例的規定。有關建議現分別載列如下。

I 保安政策及措施

關注範圍：

6.6 醫管局制定的處理病人資料的保安及保密的政策方面，文件數量繁多，而且內容重疊，令職員在遵從方面存在困難。醫管局沒有定期和有系統的更新及檢討程序，例如：根據其提供的資料，*《個人資料（私隱）條例手冊》*的最近更新日期爲 2007 年 8 月，是透過補充及取代形式在內聯網上作出的；*《透露病人資料守則的文件》*仍然是草擬本階段，沒有確定的完成日期。不同的手冊的部分章節均有講述如何處理以電子形式儲存的資料，但就沒有完整及統一的版本，方便閱覽。儘管醫管局有相關的政策及指引，規管處理電子或紙張形式的病人資料，但在處理紙張記錄時，職員似乎傾向只參考*《優良醫療紀錄管理手冊》*；在處理電子資料時，他們則多依賴簡易版的*《資訊科技保安實務指引》*。醫管局在政策及措施的修訂，亦只是零碎地作出。

6.7 醫管局容許個別醫院把醫管局的政策及措施就實際須要作出「本位化」的改動，卻沒有系統性的監察，確保其政策不會因改動而減低效力。他們似乎沒有進行定期的循規審核及監察，確保醫院所採用的 CMS 使用者申請表、CDARS 使用者申請表，及資訊科技承諾表格等，與醫管局的總政策及措施相符。

6.8 政策上的溝通及現行措施都有改善空間。問題的核心是如何將這些大量的政策、指引及措施有效地傳遞予忙碌的醫護人員，尤其是有關使用手提電子儲存裝置的保安問題。有關醫院發出的通告主要是關於「未經准許查閱病人資料」及「病人的機密」的事宜，但沒有就活動式電子儲存裝置的使用及保管給予明確的提示通知[21]。

[21] 醫管局在 2008 年 5 月 14 日才向全體員工發出加強個人資料保安的資訊科技通告。

下述建議的目的：

有系統地制定、檢討及更新資料保安政策和措施，以及適時和有效地向員工傳遞。

建議

1. 指派一個醫管局總辦事處的專責委員會或指定人士，清楚訂明其職權及職能，制定、更新、檢討及統一所有關於病人資料保安的手冊、政策及措施。

2. 被指派的醫管局總辦事處專責委員會或指定人士，同時應負責引領、協調及監察所有聯網及醫院遵從這些政策及措施的情況，例如：制定標準的 CMS 使用者申請表、CDARS 使用者申請表，及資訊科技承諾表格，供所有醫院統一使用。

3. 在聯網及醫院層面，聯網委員會及醫院委員會應負上明文責任：

(i) 實行醫管局總辦事處的政策及程序；
(ii) 在適當時向醫管局報告進展（及統計數字）；
(iii) 指出在實行上遇到的困難；及
(iv) 就有關問題向醫管局總辦事處作出檢討建議。

4. 考慮及檢討現時所有手冊、政策、措施及文件，確保有關處理病人資料的資訊是最新的，並著重有關使用以電子形式儲存的病人資料的私隱風險及適當的處理方法。

5. 雖然個別醫院可能有需要把醫管局的總政策及措施「本位化」來配合其運作需要，但醫管局應進行定期審核，確保經改動的政策及措施與醫管局的總政策及措施吻合。

6. 採取步驟，更有效地把保安政策及措施內容傳遞予員工，讓他們可以透過容易使用及透明度高的途徑，快捷地找到正確資料（例如向指定職員查詢或從內聯網閱覽有關文件）。爲了令有關政策易於閱覽，並顧及員工的不同職級和工作要求，可以考慮採用

分層通知的方法，首先透過第一層的資訊，以簡潔的語言向全體員工傳達基本的保安要求，然後進展至第二層的資訊，發放特定的規則及政策，例如下述使用規則：(i)醫管局的手提電子儲存裝置的使用限制；(ii)提出 CMS 使用者申請或 CDARS 的申請時須注意的事項；(iii)將病人資料帶離工作地點處理時須遵守的規定等。

II 聯網委員會及資料管控員

關注範圍：

6.9 聯網委員會的實際職能有時會重疊，致令這些委員會在保障病人資料私隱的角色上可能產生混淆。例如：CDPC 成立於 2006 年，其職權範圍是負責資料私隱及保安事宜，包括管理查閱資料的限制、處理查閱資料要求及進行資料查閱審核。不過在實際上，申請查閱病人資料作研究用途是由 CEC 處理的，該委員會的職權範圍並沒有規定他們在給予批准之前進行任何資料私隱風險評估。CDPC 自成立以來，從沒有處理過任何提升使用者查閱權限的申請，因爲在實際上，這項工作是由資訊科技委員會負責，而 CDPC 只是處理員工就資訊科技委員會的決定而提出的上訴。

6.10 有關醫院的資訊科技委員會進行的醫院內部的審核追蹤記錄檢討，完全是出於有關醫院管理層的判斷及決定，醫管局總辦事處並無設立定期和有系統的政策及方法，亦沒有硬性規定醫院作出報告，此外，亦沒有跟進行動。

6.11 資料管控員的角色模糊。根據與有關醫院的資料管控員的會面，他主要是負責處理病人的查閱資料要求，及每年向醫院聯網總監提交有關病人資料的私隱審核核對表。進行有關事宜是沒有指定的方法。醫院沒有清楚指明他有責任爲員工安排私隱培訓，他亦不是 CDPC 的成員。

<u>下述建議的目的</u>：

清楚界定聯網委員會的職能，並加強資料管控員的職能，以保障病人資料的安全。

建議

7. 檢討各聯網及醫院委員會的角色，清晰界定職權範圍，以免職能重疊。處理查閱病人資料及進行私隱審核的工作，應該清楚地根據相關委員會的權限來委派。在批准查閱病人資料之前，應進行私隱風險評估，考慮及平衡不同風險因素，並記錄存檔。爲確保委員會之間的協調，主要人員可同時擔任多個委員會的成員。

8. 檢討及加強資料管控員的角色，並考慮委任他爲 CDPC 的成員，有效發揮其職能。

9. 考慮通知員工，有關醫院內的個人資料保障事宜的查詢，應向資料管控員或其他指定人士作出。

10. 爲了問責性及透明度，考慮委任獨立第三者成爲這些委員會的成員，參與決策過程。

III 保安措施

關注範圍：

6.12 雖然小組認爲準確鑑定病人身份以減少醫療失誤是非常重要，但在非爲鑑定病人身份的目的的情況下，不必要地以病人的身份證號碼作配對用途，會令病人資料承受不必要的私隱風險。觀察所得，病人的身份證號碼及個人資料被使用於貼紙及預約便條上，而這些貼紙及預約便條的使用情況並不一定涉及鑑定病人身份，由於該貼紙已附加電腦條碼，如果醫院確有需要核實病人的身份，可以輕易地透過掃描條碼，將系統內儲存的病人的身份證號碼與醫管局存有關於他的資料紀錄作對比。此外，病人的身份證號碼有時會因醫學研究用途而被披露，以便作出研究人員可藉此配對系統內關於該病人的記錄，但做法引起私隱的關注，因爲採用其他對私隱侵犯程度較低的方法，例如醫院號碼或病人號碼，亦同樣能夠達到某些醫學研究的目的。

6.13 小組留意到，在醫管局的兩個主要系統以外儲存的病人電子資料被長時間保存，醫管局沒有制定在考慮到有關使用目的及私隱風險後的保留資料的正式政策[22]。舉例來說，爲行政、配藥及化驗目的而保存的病人電子記錄不應過度保留。此外，根據該手冊第 3.25 條，每次查閱病人資料都會被記錄下來，只要該病人的記錄存在，審核追蹤亦會被保留。由於審核追蹤亦載有病人資料，病人資料有可能因此被保留至病人去世爲止。小組認爲，如審核或檢討程序已經完成，再將其繼續保留便屬於超乎適度。醫管局解釋，在實際上，他們完成審核或檢討程序後，便會刪掉抽取作審核用途的審核追蹤副本。但小組關心的是原本的審核追蹤仍然被無限期地保留。

6.14 由於密碼沒有設定使用期限，因此醫管局目前所採用的密碼控制及自動登出系統有待改善。

6.15 雖然有關使用手提電子儲存裝置的政策[23]現已實施，但有關政策不足以全面針對其他有關及基本的問題，例如：

(i) 有系統地檢討有合理原因使用有關裝置的需要；
(ii) 採取步驟，以繼續「清洗」手提電子儲存裝置內的資料；
(iii) 在達成使用目的之後，安全地刪除有關裝置內的資料；
(iv) 規管下載擬用作模板的文件內所載的病人資料的做法；
(v) 微軟視窗辦工室軟件使用者所建立的資料，可能載有病人資料(例如用作撰寫醫療筆記及關於病人的信件)，而員工可能把這些資料帶回家中以其個人電腦繼續工作等；及
(vi) 下載敏感個人資料（如病人的身份證號碼）時，使用標準的微軟辦公室軟件的加密功能是否足夠提供安全保障。

6.16 應採取更多步驟，確保負責醫院資訊科技保安的合約資訊科技員工具備「良好操守、審慎態度及辦事能力」[24]。從醫管局的「電腦人員服務合約」標準版本來看，內裡沒有明文條款，要求承辦商遵從條例規定[25]。

6.17 除了兩大原則之外，在編配不同職級員工的查閱權限時，沒有制定任

---

22 據醫管局表示，他們會按照運作指引定期刪除化驗及配藥系統內的一些資料。不過，他們並沒有編制系統性的資料保留政策。

23 資訊科技通告第 1/2008 號*《加強個人資料保安措施》*。

24 保障資料第 4 原則規定，資料使用者須採取切實可行的步驟，以確保能查閱個人資料的人的良好操守、審慎態度及辦事能力。

25 合約第 12 條。

何原則性的指引。除了一般的以職級及角色爲本的方法外，在編配、更改、檢討及取消查閱權限的過程時，應該按一套清楚訂明的詳細原則及方法進行。

下述建議的目的：

加強保安措施，以減低未經准許或意外查閱病人資料的風險。

建議

11. 研究下述可行性：使用獨特識別代號代替身份證號碼，作爲鑑定病人身份及處方藥物以外的用途(例如有關 CDARS 研究用途；以及透過對比醫院號碼或門診號碼，核對醫管局其他資料庫所保存的病人資料)。使用其他獨特識別代號，例如病人號碼或醫院號碼，或將病人的身份證號碼加密，令這些資料在被下載到手提電子儲存裝置後，亦只能在醫管局系統內識辨，進而減少人爲錯誤的私隱風險(例如員工不小心遺失載有該等資料的器材)。

12. 考慮進行保安風險評估，評估目前以身份證號碼作爲識別代號的做法，尤其是將身份證號碼使用在預約便條及貼紙上的做法，是否涉及披露太多具侵犯私隱性高的資料。

13. 考慮、檢討及制定臨床資料以外的電子資料的保留政策，以防止過度囤積不必要的資料，並考慮、檢討及制定有關在醫管局主要系統以外的部門（例如配藥部及化驗室）的保留資料政策。

14. 考慮及檢討有關使用手提電子儲存裝置的政策及措施，並透過下述方法，訂明批准及檢討持續需要的機制：(i)訂明批准的期間；(ii)規定在「按職能需要知道」這個寬廣的原則下列出明確的原因；(iii)訂明續期申請程序；及(iv)保存使用記錄，以作審核用途。

15. 檢討由員工建立的病人資料的下載及使用情況，例如將撰寫的醫療報告或信件儲存於微軟辦公室軟件並下載及帶回家中繼續工作。應制定政策及指引，規管將病人資料帶離工作地點的情況，

以確保(i)特別敏感的病人資料不獲准帶離工作地點；(ii) 病人資料應盡可能去除可識辨性，或使用醫管局分配的除身份證號碼以外的識別代號，例如病人號碼或醫院號碼，而這些代號只能在醫管局系統內識辨；(iii)使用者的個人電腦不應安裝間諜軟件及檔案分享軟件，例如 Foxy；(iv)工作完成後，應安全地刪除有關資料；及(v)處理敏感個人資料時，例如下載病人的身份證號碼時，所使用的加密方法須提供足夠的安全保障。

16. 考慮就批准及檢討員工查閱病人資料的權限上，進一步制定一套具備詳細批准原則的訂明程序，以確保有關查閱只按「負責醫護」及「按職能需要知道」兩大原則作出。

17. 考慮及檢討訂明查閱 CMS 的密碼有效期限的可行性，或規定雙重鑑定，例如使用密碼加代符，以增加保障。

18. 對受託處理病人資料的第三者(例如資訊科技承辦商及廢物處理承辦商)，施以更明確的合約責任，以確保資料安全地刪除，及禁止將資料作其他用途。應盡可能的話不讓資訊科技承辦商或員工將個人資料帶離醫院進行測試[26]。

IV 私隱審核

關注範圍：

6.18 爲了確保醫護服務的迅速提供不受影響，追溯式的檢討將是醫管局系統中重要及必要的一環。不過，這些檢討必須按照已標準化的程序，適時地（每日而非每季）及有系統地進行。但目前的情況並不如是。

6.19 醫管局沒有定期進行有系統的資訊科技審核。醫院沒有定期和有系統地監察資料的保安，醫管局亦沒有定期進行保安審核。雖然醫管局的「*週年工作計劃第 3 節： 標準 53 規定*」要求醫院必須具有醫療記錄及健康資料的保安及保密和查閱病人臨床資料的指引及規定須將遺失記錄加註及向醫院管理層匯報，但進行的形式只是由個別醫院進行

[26] 參閱專員在已發表的報告#R06-2599 中作出的建議，該報告是關於聘用外判承辦商及代理時應採取的措施。該報告可從 http://www.pcpd.org.hk/chinese/publications/files/IPCC_c.pdf 下載。

自我評估，醫管局並沒有適時及有系統地主動審核每間醫院的保安水準。

6.20 由資料管控員每年匯報的保障資料原則循規審核，似乎並不是根據訂明的方法進行。雖然有關醫院的管理層制定了一套病人資料私隱核對表，供有關醫院各部門每年按表完成，但這並不表示醫管局規定所有醫院採取畫一的訂明程序。

6.21 對開放的 CMS 電腦工作站的隨機審核（以確保需要以密碼進入系統及設有自動登出功能），只是由有關醫院的資訊科技員工每年一次進行。在視察當日，專員的其中一名人員觀察到律敦治醫院配藥部的一台電腦工作站插有有兩個類似 USB 記憶體的物件，無人看管，而該工作站當時是處於運作模式中（即沒有登出）。有關醫院在回應專員的疑問時指稱，該電腦是一台獨立電腦，沒有接駁醫管局的任何資訊科技系統，不過該電腦可以連上互聯網及內聯網，只供藥劑師使用。有關醫院證實該電腦從沒有儲存病人資料，該電腦主要是用來製作關於藥物問題的員工通訊、藥物期刊及有關藥物使用的報告。有關醫院解釋，他們一直裝有插入式的無線滑鼠感應器，並以照片向專員闡述有關裝置。配藥部職員向有關醫院證實，該部門從沒有使用任何私人擁有或醫院提供的 USB 記憶體。由於缺乏其他證據證明有不當使用 USB 記憶體，小組不能就此事作進一步行動。另一方面，有關醫院承認，有關的工作站是沒有自動登出功能，他們現正考慮在該台電腦安裝自動登出系統的可行性。此事顯示須更頻密和定期作出檢查。

6.22 醫管局已停止「紅色保安區」審核，原因是醫管局擔心將 CMS 內的職員病人記錄資料庫與職員的人事記錄資料庫作配對會違反保障資料第 3 原則的規定。醫管局似乎沒有適當考慮條例的其他條文，尤其是向資料當事人徵求同意及條例的豁免條文的適用性。

6.23 「非綠色保安區」的審核方法，是檢查審核追蹤記錄，偵查有沒有不尋常的查閱 CMS 的行爲，有關的審核是由個別醫院自行按其決定及判斷而進行的[27]。醫管局並沒有制定有系統的審核及「自動警報」準則，亦沒有進行定期監察。2006 年成立的 CDPC 已決定制定指引，進行有系統的審核，讓所有豁下醫院遵從。唯該委員會至今尚未制定有系統的審核方法，供所有醫院遵從。此外，由於對很多醫院員工來說，

[27] 有關醫院表示，由 2001 年至 2006 年間就 CMS 的適當使用進行了大約 15 次審核。此項工作自 CDPC 成立後便停止，該委員會決定接管審核工作，並制定一般指引。

綠色保安區的範圍包括查閱超越「負責醫護」[28] 的資料，這方面看來亦有審核的需要。

6.24 「自動警報」系統的準則應盡早敲定，以便開始落實。

<u>下述建議的目的</u>：

制定有系統的資料保安審核方法，由聯網及醫院遵行。

建議

19. 檢討及制定一個定期和有系統的循規審核系統，由醫管局總辦事處監管，在適時及定期的基礎下有效地進行，以確保保安政策及措施獲得遵從。醫管局總辦事處應該考慮委派一隊機構系統保安隊伍或向外聘用獨立人士進行審核工作。

20. 個別醫院進行的內部私隱審核，應該有系統地按照訂明程序進行。應該制定一套一致的核對表或「自我評估工具」，應用於所有醫院。

21. 考慮及檢討現時綠、黃及紅色保安區的定義，以便進行該手冊所規定的審核。

22. 考慮進行「綠色保安區」審核的需要；檢討「紅色保安區」進行審核的可行性，小心研究條例的法律規定，尤其是向資料當事人徵求訂明同意及豁免條文的適用性方面。

23. CDPC 加快制定「自動警報」的準則，以便有效及有系統地對審核追蹤記錄進行保安審核。

24. 考慮強制規定醫院在進行審核後，向聯網及醫管局總辦事處詳細報告結果，如要採取補救措施，醫管局總辦事處應監察有關措施的實行。

[28] 根據醫管局的定義，綠色保安區查閱是指查閱接受治療病人的資料是在與病人正接受治療期間進行，或是在病人求診/入院的合理期間內查閱其資料。醫管局初始規定該期間爲求診前/後的 365 日。

25. 任何不尋常的查閱追蹤記錄應連接到監察系統，而該監察系統可以適時（例如每日）及有系統地進行追溯檢討，將檢查程序標準化。

V 監督、教育及培訓

關注範圍：

6.25 由於很多在醫管局及其他地方發生的遺失個人資料事件是人爲因素造成，因此員工的私隱意識有需要改善。這方面可通過更嚴格地監察每日的運作(例如保留使用手提電子儲存裝置的記錄、監督病人資料是否適當及安全地刪除、監察第三者如資訊科技承辦商及碎紙服務公司等，是否妥善地遵守資料私隱規定)而達到。一個良好的通報系統的設立，可確保當局能夠在有需要時迅速行動。

6.26 若刪除醫療記錄的工作是由指定的承辦商負責，應該規定他們承擔合約責任，以確保他們小心處理資料，防止資料受未經准許的或意外的查閱、處理及使用。醫管局亦應採取相應的保安措施，確保有關人士盡可能在指定地點閱覽醫療報告或化驗報告硬拷貝內的病人資料，以免他們隨意攜帶著這些報告，導致不慎放錯他處。

6.27 小組關注有關醫院目前沒有制定程序，確保員工當交還使用完畢的活動式電子儲存裝置時，按業界標準把所有資料刪除，並由有關醫院的資訊科技部門核實。

6.28 醫管局舉辦的研討會及講座出席率偏低，令人關注。雖然部分原因歸咎於醫院的輪班制，但他們亦應研究如何令培訓更爲集中及讓更多人參與。醫管局總辦事處應經常定期主動籌辦研討會及講座、評估這些研討會及講座的有效性，並設計可鼓勵更多人參與的有效培訓模式。

<u>下述建議的目的</u>：

嚴格監督員工遵從保安規定，並爲員工提供更多教育課程及培訓。

建議

26. 在發生最近的遺失病人資料事件之後，醫管局制定了 USB 記憶體使用者申請表，但該表只適用於 USB 記憶體。由於有關醫院亦可以提供其他手提電子儲存裝置予員工使用，例如活動式硬碟、手提電腦、數碼相機等，因此醫管局亦應考慮制定政策及特定的申請表，規管其他手提電子儲存裝置的使用。

27. 檢討目前醫療人員閱覽醫療記錄及化驗報告硬拷貝的做法，考慮把有關程序規限在指定地點進行，以減低攜帶這些載有病人資料的文件時而引致的資料遺失事件。

28. 爲了確保在公開或無出入限制的地點處理病人資料時有足夠保障，考慮加強這些地方的保安措施及進行定期監督。

29. 應制定程序，確保員工當交還使用完的活動式電子儲存裝置時，把內藏的所有資料按業界標準刪除，並由有關醫院的資訊科技部門核實。

30. 應增加定期及適時地向員工重新發出有關處理病人資料保安的通告。

31. 應檢討現時入職課程及在職研討會所使用的材料，確保在醫管局網絡內使用的材料包含最新資訊，並特別提醒員工注意保障病人資料的需要，尤其是當資料是以電子形式儲存。

32. 考慮有效傳遞研討會材料的模式，例如透過互動平台（如內聯網上的自學工具），讓更多員工參與。

33. 採取步驟設立培訓導師課程，以確保醫管局網絡內培訓導師的授課能力，及評估和評核他們的表現。

34. 檢討或續訂承辦商（例如資訊科技承辦商及碎紙服務承辦商）合約時，應以承辦商遵從資料保安原則的水準作爲指定的考慮因素，如情況適合，應以標準條款形式納入所有有關合約之中。

VI 私隱影響評估

關注範圍：

6.29 鑑於醫管局以電子形式持有及累積大量病人資料，並有計劃全面落實建議中的電子醫療平台，因此在處理病人資料時需要加倍小心謹慎。在實行任何儲存及使用病人資料系統之前，需要小心進行私隱風險評估。醫管局應該制定並實行足夠的保障私隱措施，以減輕在採用有關系統時可能引致對個人資料私隱的任何不利影響。

> 下述建議的目的：
>
> **強制規定進行私隱影響評估**
>
> **建議**
>
> 35. 在展開任何涉及以電子方式建立、收集、移轉或儲存大量病人資料或涉及特別敏感資料的新工作或項目之前，醫管局應進行私隱影響評估。醫管局應實行足夠的保安措施，以應付有關項目帶來的私隱風險，評估過程及步驟應清楚地記錄存檔。

VII 應變方法

關注範圍：

6.30 在發生違反資料保安事件後，資料使用者應採取切實可行的步驟，減低對資料當事人的損失或可能造成的損失。有些遺失資料事件，專員或資料當事人均不獲告知，而要從其他途徑得知。公共機構如醫管局應遵行具透明度及問責性的良好管治，如情況適合，應把違反資料保安事件通知受影響的個人及公眾。

6.31 專員欣悉醫管局在發生連串遺失資料事件後，已採取新措施，透過 AIRS 把遺失資料事件公開。其他醫療服務提供者也應遵行這個良好

的行事方式。

<u>下述建議的目的</u>：

在發生違反資料保安事件後，發出違規通知。

建議

36. 在發生違反資料保安事件後，採取適當步驟，進行快速私隱風險評估，考慮涉及個人資料的性質、受影響人士的數目及遺失資料的數量，以減低對受影響人士可能造成的損失。如遺失是由系統缺陷或漏洞造成，應即時採取步驟修補缺陷或漏洞，以免損失擴大。如情況適合，應向執法機構報告違反資料保安事件，以便進行調查。

37. 通知受影響人士違反資料保安事件，以便他們採取適當的補救行動。把事件通知專員，讓專員採取適當的規管行動，亦是良好的行事方式。

6.32 專員知道，尖端科技發展迅速。嚴格規定醫管局使用市場上的指定產品，或採用剛研發的資訊科技系統是徒勞無功的，因爲它們最後都會過時。因此，醫管局的長遠保安策略應該是定期進行檢討，留意科技的發展及所衍生的私隱問題。基於同一個原因，本報告所作的建議是科技中立的，是對醫管局的一般指引，以促進醫管局遵守條例的規定[29]。

[29] 條例在訂立時是科技中立的，條例下的保障資料原則作一般性的應用。

第七章

結語

本人撰寫本視察報告時，注意到會有人期望這報告會確認近期醫管局轄下多間醫院接連遺失病人資料事故需要負責的人士。就此而言，他們將會感到失望，因爲這次視察的法定目的，是在於對醫管局提出建議，改善它的個人資料系統。

調查個別遺失資料事故是本署目前跟進的另外工作，旨在詳細了解個別遺失資料事故、起因及有否違反條例的規定。這些問題將會在日後個別報告中交代。

發生遺失資料事故後，醫管局已採取一些補救措施，例如規管員工使用 USB 記憶體儲存病人資料，以及實施資料違規通報機制。本人歡迎醫管局所作的措施，然而，這些零碎的措施並不足以完全解決病人資料保安系統上不足之處。接連發生的遺失資料事故，顯示醫管局的病人資料系統存在重大漏洞。

有見及此，本人認爲有必要根據條例第 36 條視察醫管局的病人資料系統。本人進行視察後所作出的建議，應有助醫管局全面檢討病人資料系統的安全措施，長遠而言，會有助減少像過往數月接連發生的遺失資料事故。

本人選擇了律敦治醫院及鄧肇堅醫院（兩者的運作已合併）作爲這次視察的實例，探討醫管局如何管理轄下醫院的病人資料保安工作。我選擇有關醫院的其中一個原因，是它至今並無傳出任何遺失資料事故。

這次視察集中於審視醫管局現行有關保障病人資料的政策及措施、如何實施和執行有關政策及措施，及增進員工的私隱意識。據視察所得，醫管局是有認真地構思及設計病人資料保安系統，務求保障病人的敏感資料。然而，對於大機構如醫管局，僱用超過 53,000 名員工，執行有關政策及措施的困難是顯然易見的。在沒有整體性的統籌下，醫管局發出大量的政策、手冊及通告，只令工作繁重的醫護人員難以理解及遵從，亦妨礙了適當的施行。在缺乏一個有原則、有系統，並適用於所有醫院的私隱審核方法下，正正突顯了實施保障病人資料政策時的不足之處。雖然律敦治醫院及鄧肇堅醫院對重視

審核私隱循規方面令人印象深刻，但我注意到這主要歸因於個別高層人員所作的努力及主動實行的措施。其他的公立醫院是否做得一樣好，則仍是疑問。我發覺醫管局的員工對私隱保障的認知程度不足，但我對此並不驚訝，這從多宗遺失資料事故皆因人爲錯誤而引起，即可證明。爲改善有關情況，向醫管局的員工提供更多培訓及教育是刻不容緩的。

本人在本報告內提出多項建議，期望醫管局轄下各醫院進一步改善工作程序，以更安全的方式保護病人資料。本人認同醫院的首要職責是醫治病人及阻止疾病蔓延，亦應清楚保障資料第 4 原則規定資料使用者須採取*「所有切實可行的步驟」*，以確保由其持有的個人資料受保障。本人向醫管局提出的建議是切實可行的，不會無理干預醫院履行主要職責，但可以確保病人的個人資料得到妥善保護。建議當中不少是針對提升醫護人員的保障私隱意識，藉此大幅減少任何人爲錯誤。本人希望提出的建議，在滿足首要的醫療需要，與妥善保障病人敏感資料不受未獲准許或意外的查閱、處理及使用這兩者之間達至良好的平衡。

可能有人會質疑，在醫管局轄下眾多醫院之中，僅抽樣視察一間醫院能否準確代表醫管局病人資料系統的運作方式。本人詳細視察了一間 (二合爲一的) 醫院，研究有關醫院如何在醫管局的管理下，遵守及符合各個保障資料原則。爲求達致這個有限的目標，本人於視察過程中的多個不同時段調派公署過半人手參與行動[30]。本人當然希望能夠對醫管局轄下其他醫院進行更廣泛的研究，但礙於資源及經費所限，本人不得不考慮以最有效的方式，將資源用於處理與遺失病人資料事故相關的迫切問題。本人認爲，與其倉猝觀察多間醫院，不如詳細視察一間規模及架構均屬中等的醫院，則資源運用會更具效益。醫管局有必要確保系統的透明度，以挽回公眾信心。本人相信，此報告會令公眾對醫管局的病人資料系統有更深入的了解。

本人衷心期望本報告不僅對所有公立醫院有價值，亦對其他私立醫院具價值，並期望有關醫院的實例及本人的建議對這些醫院有所助益。

在結束本報告之前，本人在此向眾多曾經作出貢獻的人士致謝。沒有他們的協助，本人絕不可能迅速有效地完成視察。

[30] 小組成員詳情載於附件 II。

視察得以順利進行，有賴有關醫院的員工衷誠合作。我們非常明白，除了日常醫療及行政工作外，他們需要在接獲短時間通知後，忙於籌備大量與視察有關的工作。

在視察期間，本人有幸得到一眾員工竭誠盡力的支持，他們的表現，充份顯示他們對工作的承擔與熱誠，盡力發揮一己所長，完成一項嶄新的任務。

最後亦是最重要的，本人特別感謝各位顧問獻出他們的時間及專長，以專注及積極的態度處理這項視察工作。他們的寶貴意見已反映在本報告內，定必有助改善公立醫院體制中的病人資料保安情況。

吳斌
個人資料私隱專員
香港特別行政區

2008 年 7 月 22 日

辭彙

AIDS	*後天免疫力缺乏症候群* *Acquired Immune Deficiency Syndrome*
AIRS	*醫事匯報系統* *Advanced Incident Reporting System - 一個用以支援危機處理的通報系統，可作出事件匯報、分類、分析及管理。*
審核追蹤	*所有人經由醫管局資訊系統以電子形式查閱病人資料時均會被記錄。有關的審核追蹤可用作法律程序中的證據，並保留至病人資料不再存在。*
審核追蹤記錄	*進行審核追蹤的記錄*
黃色保安區	*醫管局訂定的保安層級。它表示查閱病人資料時介乎綠色保安區與紅色保安區間的中等保安層級。*
CDARS	*醫療資料分析及匯報系統* *Clinical Data Analysis and Reporting System – 一個醫管局用以抽取病人資料作醫學研究用途的電子系統。*
CDPC	*聯網資料私隱委員會* *Cluster Data Privacy Committee*
CEC	*聯網倫理委員會* *Cluster Ethics Committee*

CMS	*臨床管理系統* *Clinical Management System – 一個醫管局在提供醫療服務時用以處理資訊（包括病人資料）的電子系統。*
專員	*根據條例第 5(3)條委任的個人資料私隱專員*
公署	*根據條例第 5(1)條設立的個人資料私隱專員公署*
顧問	*專員爲協助其視察而委任的 4 位顧問，詳情請參閱附件 II*
資料管控員	*每所醫院爲確保依從條例要求而委任的人士／人等。*
保障資料原則	*條例附表 1 的保障資料原則*
保障資料第 4 原則	*條例附表 1 的保障資料第 4 原則*
綠色保安區	*醫管局訂定的保安層級。指基於與病人面診、或病人應診／入院後短時間內所進行的低保安層級的資料查閱。*
醫管局	*醫院管理局*
醫管局行政總裁	*醫院管理局的行政總裁*
醫管局總辦事處	*醫院管理局總辦事處*
港島東聯網	*港島東醫院聯網*
身份證	*香港身份證*
有關醫院	*律敦治醫院及鄧肇堅醫院*

HR	*人力資源* *Human resources*
視察	*在本報告中所指，根據條例第 36 條就醫管局的個人資料系統所展開的視察*
資訊科技通告	*醫管局總辦事處於 2008 年 5 月 14 日發出的資訊科技通告第 1/2008 號《在加強個人資料保安方面的改進措施》*
資訊科技委員會	*該醫院的資訊科技發展委員會*
該手冊	*醫管局的《臨床資料政策手冊》*
條例	*香港法例第 486 章《個人資料（私隱）條例》*
非綠色保安區	*它表示查閱病人資料時屬綠色保安區以外的保安層級*
按職能需要知道原則	*醫管局制訂的原則，用以控制醫護人員查閱醫管局持有的病人資料。在「按職能需要知道」的原則下，醫護人員可爲「負責醫護」目的以外的其他各類有必須性的目的而查閱病人資料*
負責醫護原則	*醫管局制訂的原則，用以控制醫護人員查閱醫管局持有的病人資料。在「負責醫護」原則下，醫護人員有權查閱其所負責的病人的相關醫護資料*
個人資料	*條例第 2(1)條定義「個人資料」爲符合以下說明的任何資料：(a)直接或間接與一名在世的個人有關的；(b)從該等資料直接或間接地確定有關的個人的身分是切實可行的；及(c)該等資料的存在形式令予以查閱及處理均是切實可行的。*

個人資料系統	*條例第 2(1)條定義「個人資料系統」爲全部或部分由資料使用者用作收集、持有、處理或使用個人資料的任何系統（不論該系統是否自動化的），並包括組成該系統一部分的任何文件及設備。*
切實可行	*根據條例第 2(1)條，「切實可行」的定義爲「合理地切實可行」*
紅色保安區	*醫管局訂定的保安層級。它表示查閱屬高保安風險的病人資料的高保安層級。例如：查閱醫院僱員的醫療資料，或公眾有興趣知道的病人資料*
本報告	*根據條例第 48(1)條所發表的本報告*
小組	*由專員帶領、副個人資料私隱專員偕公署審查部、執行部、法律部人員提供協助的視察小組。小組還包括具醫學、私隱、資訊科技及法律背景的顧問（見附件 II）及秘書支援*
USB 記憶體	*通用序列匯流排(Universal Serial Bus)快閃記憶體*
Wi-Fi	*Wi-Fi 是一個無線網絡通信的工業標準的標誌，用以認證達到該標準的產品*

附件 I

醫院名稱縮寫

港島東聯網	
CCH	春磡角慈氏護養院
PYNEH	東區尤德夫人那打素醫院
RHTSK	律敦治醫院及鄧肇堅醫院
SJH	長洲醫院
TWEH	東華東院
WCH	黃竹坑醫院

港島西聯網	
DKCH	大口環根德公爵夫人兒童醫院
FYKH	東華三院馮堯敬醫院
GH	葛量洪醫院
MMRC	麥理浩復康院
QMH	瑪麗醫院
TWH	東華醫院
TYH	贊育醫院

九龍中聯網	
BH	香港佛教醫院
HKEH	香港眼科醫院
KH	九龍醫院
QEH	伊利沙伯醫院
BTS	香港紅十字會輸血服務中心
RC	復康專科及資源中心

九龍東聯網	
HHH	靈實醫院
TKOH	將軍澳醫院
UCH	基督教聯合醫院

九龍西聯網	
CMC	明愛醫院
KCH	葵涌醫院
KWH	廣華醫院
OLMH	聖母醫院
PMH	瑪嘉烈醫院
WTSH	東華三院黃大仙醫院
YCH	仁濟醫院

新界東聯網	
AHNH	雅麗氏何妙齡那打素醫院
BBH	白普理寧養中心
NDH	北區醫院
PWH	威爾斯親王醫院
SCH	沙田慈氏護養院
SH	沙田醫院
TPH	大埔醫院

新界西聯網	
CPH	青山醫院
POH	博愛醫院
SLH	小欖醫院
TMH	屯門醫院

附件 II

視察小組

組長

吳斌先生（個人資料私隱專員）

顧問

1. 白景崇教授
   （香港大學社會科學研究中心主任）
   （法律改革委員會私隱問題小組委員會前主席）

2. 陳爵先生
   （前高等法院司法常務官）

3. 何仲平醫生
   （香港醫學會資訊科技委員會主席）

4. 譚偉豪博士
   （香港工程師學會 2007/08 年度資訊科技委員會主席）

小組秘書

穆士賢先生
（前香港律師會秘書長）

公署人員

(i) 核心小組

副私隱專員
首席律師
署理首席私隱審查主任
首席個人資料主任
一名律師
一名高級個人資料主任
二名個人資料主任

(ii) 問卷小組

一名高級個人資料主任
四名個人資料主任
三名助理個人資料主任
一名資訊科技主任
一名行政主任

(iii) 機構傳訊小組

機構傳訊經理
機構傳訊主任（教育）
署理機構傳訊主任（推廣）

(iv) 行政支援

私隱專員私人助理
副私隱專員行政助理
法律部私人秘書
三名助理個人資料主任
法定語文主任

附件 III

聯網資料私隱委員會

工作範圍

1. 按照醫管局的醫療資料政策、其他有關政策及法例，制訂及監察港島東聯網的資料私隱及保安方面的政策和指引，範圍包括：
   i. 查閱控制的管理
   ii. 批准查閱資料的申請
   iii. 進行查閱審計
   iv. 調查可能違規的情況

2. 就港島東聯網在資料私隱和保安的事宜上，向聯網管理層提出持續的質素改善策略和行動

3. 向港島東聯網的所有員工教育及發佈有關醫療資料私隱方面的資訊

4. 就其他相關管理委員會向高級管理委員會作出匯報

附件 IV

聯網倫理委員會

工作範圍

醫療道德

1. 在道德倫理範疇上領導及統轄聯網的政策決定及醫療實務。

2. 推動發展聯網在醫療事務上的道德倫理指引。

3. 制訂適當的原則以指引聯網的政策發展、服務規劃及與資源有關的決定。

4. 爲道德倫理附屬委員會提供在醫療道德及倫理方面的意見及支持。

5. 透過教育提升在作出醫療決定時在道德倫理方面的意識和專業能力。

研究道德及倫理

6. 設定標準，以協調聯網醫院在醫療研究方面的道德及倫理事宜。

7. 爲道德倫理附屬委員會成員籌組訓練。

8. 爲涉及聯網醫院病人的醫療試驗保存中央記錄。

9. 爲聯網在醫療研究道德及倫理方面的表現進行審計。

10. 監察全球在醫療研究道德及倫理方面的發展。

醫療系統架構

醫護過程	醫院／診所辦公室	使用的電腦系統
病人登記	前往急症室、入院處與出院櫃位的病人	IPAS OPAS
病人診治	於醫院／診所（病房、手術室、急症室等）接受治療的病人	AEIS, CMS OTMS, ePR
X 光檢驗及病理測試	於 X 光部及病理部進行的測試	LIS, RIS
配藥	於配藥房分發藥物	PMS, PHS

- IPAS — 入院病人行政系統
  InPatient Administration System
- OPAS — 出院病人預約系統
  OutPatient Appointment System
- AEIS — 急症資訊系統
  Accident & Emergency Information System
- CMS — 醫療管理系統
  Clinical Management System
- OTMS — 手術室管理系統
  Operating Theatre Management System
- LIS — 實驗室資訊系統
  Laboratory Information System
- RIS — 放射科資訊系統
  Radiology Information System
- PMS — 藥房管理系統
  Pharmacy Management System
- PHS — 藥房補給系統
  Pharmacy Supplies System
- ePR — 電子病人記錄
  Electronic Patient Record

附件 VI

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

問卷

個人資料私隱專員現根據《個人資料（私隱）條例》第 36 條，視察醫院管理局（下稱「醫管局」）的個人資料系統，是次視察針對律敦治醫院及鄧肇堅醫院的病人資料保安情況。本問卷爲有關視察的一部分。

就本問卷而言，(a)「**病人資料**」指在醫護過程中所收集的統計、行政及醫療資料，不論是否以電子形式（例如儲存於臨床資料處理系統）或實體形式（例如紙張）儲存；(b)「**醫療資料**」指一名個人在身體或精神健康方面的資料，及／或該個人所接受的醫護服務的資料；(c)「**查閱**」指接觸病人資料（包括收集及產生），不論以電子形式或實體形式。

你並不需要在填寫本問卷時披露你的身份，本署亦不會向你的醫院及醫管局披露任何問卷中可用以核實你身份的資料。請詳閱各問題，然後以✓號選擇你的答案。**你可能會在部分問題中選擇多於一個答案**。謝謝你的協助。

甲部 － 一般問題

1. 你現時的職位是：

A. ☐ 行政／會計人員
B. ☐ 醫療人員
C. ☐ 護理人員
D. ☐ 資訊科技人員
E. ☐ 實驗室人員
F. ☐ 研究員
G. ☐ 關聯的醫護人士（例如藥劑師、物理治療師、語言治療師及職業治療師）
H. ☐ 其他，請說明：_____

2. 你受聘於醫管局的期間爲：

A. ☐ 少於 1 年
B. ☐ 1 年至少於 3 年
C. ☐ 3 年至少於 5 年
D. ☐ 5 年或以上
E. ☐ 不適用

3. 你於本醫院工作的期間爲：

A. ☐ 少於 1 年
B. ☐ 1 年至少於 3 年
C. ☐ 3 年至少於 5 年
D. ☐ 5 年或以上

4. 你履行職責時，是否需要查閱病人資料？

A. ☐ 是
B. ☐ 否（無需回答乙部，轉到丙部第 31 題）

如是，你是否需要查閱醫療資料？

i. ☐ 是
ii. ☐ 否

乙部 – 病人資料的處理

5. 你所處理的病人資料的存在形式爲：

A. ☐ 實體形式（例如紙張）
B. ☐ 電子形式（例如臨床資料處理系統）
C. ☐ 其他，請說明：_____

6. 除了正常職責，你曾否收到指示查閱病人資料（例如進行研究）前要獲得事先核准？

A. ☐ 是
B. ☐ 否
C. ☐ 不知道

7. 你是否獲告知「機密」資料和「未經分類」資料的分別？

A. ☐ 是
B. ☐ 否

如是，得知的途徑是

i. ☐ 正式培訓
ii. ☐ 由上司告知（口頭或書面）
iii. ☐ 自己找尋答案（例如透過內聯網）

8. 你曾否獲告知查閱病人資料只限於「負責醫護」及「按職能需要知道」此兩種目的？

A. ☐ 是
B. ☐ 否

如是，從何途徑得知？

i. ☐ 正式培訓
ii. ☐ 由上司告知（口頭或書面）

iii. ☐ 自己找尋答案（例如透過內聯網）

9. 假如你在開放地方工作，在有關地方以實體形式（例如紙張）存在的病人資料在不使用時有否受到妥善保管？

A. ☐ 有
B. ☐ 否
C. ☐ 不適用

10. 透過電腦查閱病人資料是否受到密碼保護？

A. ☐ 是
B. ☐ 否
C. ☐ 不適用

<u>如是</u>，你離開電腦時有否登出電腦？

i. ☐ 有
ii. ☐ 否
iii. ☐ 我依靠電腦的自動登出系統

11. 你曾否與其他使用者共用你的密碼？

A. ☐ 曾
B. ☐ 否

<u>如是</u>，醫院是否准許你與其他使用者共用你的密碼？

i. ☐ 是
ii. ☐ 否
iii. ☐ 不知道

12. 在過去 12 個月內，你有沒有因工作需要匯入病人資料？

A. ☐ 有
B. ☐ 沒有

<u>如有</u>，你如何取得資料？

i. ☐ 透過實體資料（如紙張）
ii. ☐ 透過內聯網
iii. ☐ 透過互聯網（例如電子郵件）
iv. ☐ 透過電子裝置
v. ☐ 其他，請說明：_____

及

你從何處取得資料？

a. ☐ 醫院的同事
b. ☐ 醫管局轄下其他醫院／診所／機構
c. ☐ 其他，請說明來源：_____

13. 在過去 12 個月內，你有沒有透過電郵附件匯入病人資料？

A. ☐ 有

B. ☐ 沒有

如有，這些匯入資料是甚麼形式

i. ☐ 受密碼保護的工作表

ii. ☐ 加密檔案

iii. ☐ 其他，請說明：_____

14. 在過去 12 個月內，你有沒有因工作需要下載或匯出病人資料？

A. ☐ 有

B. ☐ 沒有

如有，有關資料是否受密碼或加密保護

i. ☐ 是

ii. ☐ 否

如有，使用的頻密程度是

a. ☐ 經常

b. ☐ 很少

c. ☐ 只有在被指示時

15. 如以上問題的答案爲「有」，有關下載或匯出是否已獲授權？

A. ☐ 是

B. ☐ 否

如是，有關的授權者爲：

i. ☐ 直屬上司

ii. ☐ 私隱委員會

iii. ☐ 倫理委員會

iv. ☐ 其他，請說明：_____

16. 在過去 12 個月內，你有沒有透過電郵附件匯出病人資料？

A. ☐ 有

B. ☐ 沒有

如有，有關資料是否受密碼或加密保護

i. ☐ 是

ii. ☐ 否

iii. ☐ 其他，請說明：_____

17. 從系統中匯出有關病人資料的目的爲：

A. ☐ 持續醫護用途
B. ☐ 研究用途
C. ☐ 系統維護
D. ☐ 行政用途（包括調查投訴）
E. ☐ 其他，請說明：_____
F. ☐ 不適用

18. 你從系統中匯出病人資料之前，有沒有刪除可識辨身份的資料？

A. ☐ 有
B. ☐ 沒有
C. ☐ 只有在被指示時
D. ☐ 不適用

19. 有關的病人資料的匯出途徑爲：

A. ☐ 內聯網
B. ☐ 實體形式（如列印副本）
C. ☐ 電子郵件
D. ☐ 電子裝置
E. ☐ 其他，請說明：_____
F. ☐ 不適用

20. 假如你在過去 12 個月內曾使用電子裝置匯入或匯出電子資料，你曾否使用下列裝置？

A. ☐ 軟磁碟
B. ☐ CD/DVD
C. ☐ USB 儲存裝置
D. ☐ 手提電腦
E. ☐ 其他手提裝置，請說明：_____
F. ☐ 不適用

21. 有關手提電子裝置有沒有加密功能？

A. ☐ 有
B. ☐ 沒有
C. ☐ 不適用

<u>如有</u>，**在過去 12 個月內，你使用有關裝置時有否使用其加密功能？**

i. ☐ 經常
ii. ☐ 很少
iii. ☐ 從不

22. 有關手提電子裝置是否由醫院提供，用以下載病人資料？

A. ☐ 是
B. ☐ 否
C. ☐ 不適用

你有否申請下載資料？

i. ☐ 有
ii. ☐ 否

如是，你有否在有關申請中述明該些資料的用途

a. ☐ 是
b. ☐ 否
c. ☐ 其他，請說明：_____
d. ☐ 不適用

23. 你有否於使用完畢後退還有關的手提電子裝置？

A. ☐ 有
B. ☐ 否
C. ☐ 不適用

24. 退還手提電子裝置前，你有否先刪除病人資料？

A. ☐ 經常
B. ☐ 從不
C. ☐ 很少
D. ☐ 不適用

如有，你如何刪除有關資料？

i. ☐ 以任何自選的軟件，或裝置的內建功能
ii. ☐ 依從醫院所建議的刪除程序
iii. ☐ 其他，請說明：_____

25. 如你持有實體形式的病人資料，在達到使用目的後，你如何確保安全棄置資料？

A. ☐ 碎掉
B. ☐ 交由第三者銷毀
C. ☐ 作爲循環再用紙張
D. ☐ 其他，請說明：_____

26. 你曾否將從系統匯出的病人資料移轉至工作以外的地方，例如你的家中、醫管局轄下其他機構或其他第三者（例如非醫管局僱員的人士）？

A. ☐ 是
B. ☐ 否

27. 你是否獲准將病人資料帶離工作場所？

A. ☐ 是

B. ☐ 否

不論你有否獲授權，假如你曾經將病人資料帶離工作場所，你曾將有關資料帶往：

i. ☐ 醫院管理局轄下的其他醫院／機構

ii. ☐ 你的居所

iii. ☐ 老人院

iv. ☐ 大學

v. ☐ 其他，請說明：_____

vi. ☐ 不適用

原因是：

a. ☐ 於醫院以外執行醫院所委派的職務

b. ☐ 下班後在家趕工

c. ☐ 於家中或其他地方進行研究工作

d. ☐ 其他，請說明：_____

e. ☐ 不適用

28. 你是否經常在先獲得特定人士的授權下，才將病人資料帶離工作場所？

A. ☐ 是

B. ☐ 否

<u>如是</u>，請提供授權者的職位名稱：_____

29. 你曾否使用屬你個人所有的電子裝置儲存病人資料？

A. ☐ 曾

B. ☐ 否

<u>如是</u>，你有沒有將有關裝置送交醫院的資訊科技部門以通過與公家電腦相同的處理？

i. ☐ 有

ii. ☐ 沒有

<u>如沒有</u>，你有否確保你的裝置沒有電腦病毒或可造成資料外洩的社交軟件（例如 **Foxy**，**MSN Messenger**，**Facebook**，**FTP** 伺服器及網頁伺服器）？

a. ☐ 有

b. ☐ 沒有

30. 將病人資料移轉至醫管局系統前，你在工作站處理病人資料時，通常以甚麼資料作爲其身份索引？

A. ☐ 姓名
B. ☐ 香港身份證號碼
C. ☐ 醫院編配的病人編號
D. ☐ 其他，請說明：_____

丙部 – 規管處理病人資料的政策、指引或措施

31. 你是否知道醫院有就規管處理病人資料方面訂立任何政策、指引或措施？

A. ☐ 是
B. ☐ 否

如是，你是否明白有關內容？

i. ☐ 是
ii. ☐ 否

如是，你明白的程度是

a. ☐ 1（我不明白）
b. ☐ 2（我明白少許）
c. ☐ 3（我大致明白）
d. ☐ 4（我非常明白）

32. 你是否知道醫院有就規管使用電子裝置匯入及匯出病人資料方面訂立任何政策、指引或措施？

A. ☐ 是
B. ☐ 否

如是，你是否明白有關內容？

i. ☐ 是
ii. ☐ 否

如是，你明白的程度是

a. ☐ 1（我不明白）
b. ☐ 2（我明白少許）
c. ☐ 3（我大致明白）
d. ☐ 4（我非常明白）

33. 你曾否遺失任何載有病人資料的列印本或載有病人資料的電子裝置？

A. ☐ 曾
B. ☐ 否
C. ☐ 不適用

如有，你有沒有將有關遺失告知你的上司或醫院？

i. ☐ 有
ii. ☐ 沒有

34. 你是否知道醫院有就遺失病人資料或載有病人資料的裝置的呈報方面，訂立任何政策、指引、規則或規例？

A. ☐ 是
B. ☐ 否

如是，你是否明白有關內容？

i. ☐ 是
ii. ☐ 否

如是，你明白的程度是

a. ☐ 1（我不明白）
b. ☐ 2（我明白少許）
c. ☐ 3（我大致明白）
d. ☐ 4（我非常明白）

35. 在 **2008** 年 **5** 月之前，你曾否接受下列任何培訓？

A. ☐ 病人資料保密
B. ☐ 保護個人資料私隱
C. ☐ 電子儲存裝置的使用
D. ☐ 電子通訊政策

36. 你認爲醫院提供的培訓是否足夠應付病人個人資料的保安問題？

A. ☐ 足夠
B. ☐ 不足夠
C. ☐ 不知道
D. ☐ 不關心

丁部 – 評估職員對個人資料私隱的意識

37. 員工依從私隱政策、指引及措施的程度是否包含於年度考績的評估項目？

A. ☐ 是
B. ☐ 否
C. ☐ 不知道

38. 你是否知道醫院設有資料保障主任一職？

A. ☐ 是
B. ☐ 否

如是，你是否知道其職責：

i. ☐ 是
ii. ☐ 否
iii. ☐ 不關心

如是，其職責是：

a. ☐ 處理病人的查閱資料要求
b. ☐ 籌劃及/或進行有關保障個人資料私隱的培訓
c. ☐ 向員工派發有關處理病人資料的通告及／或政策、指引或措施
d. ☐ 其他，請說明：_____

39. 你如何評價你的同事對保障病人資料私隱的意識？請填寫數字 1 至 10，1 爲最低，10 爲最高。

☐

40. 你如何評價醫院採取保障病人資料的措施，以免受未經准許或意外的查閱、處理及使用？請填寫數字 1 至 10，1 爲最不足，10 爲最足夠。

☐

41. 你如何評價你的同事在遵守醫院保障病人資料安全規定的程度？請填寫數字 1 至 10，1 爲最不滿意，10 爲最滿意。

☐

42. 你是否知道你的醫院存在下述問題？

i. ☐ 與他人共用密碼
ii. ☐ 使用電腦後沒有登出
iii. ☐ 大量使用手提電子裝置
iv. ☐ 隨意放置載有病人資料的手提電子裝置
v. ☐ 其他，請說明：_____

43. 如你有病人資料私隱方面的問題，你可以怎樣尋求答案？

A. ☐ 向同事查詢
B. ☐ 向上司查詢
C. ☐ 向資料保障主任查詢
D. ☐ 從內聯網尋找
E. ☐ 不知道
F. ☐ 其他，請說明：_____

44. 你認爲如何可以改善醫院現時的個人資料系統，以確保病人資料得到更佳保障？

_____

_____

_____

_____

—— 全卷完 ——
謝謝合作

附件 VI

問卷結果分析

甲部 – 一般問題

1. 你現時的職位是：（作答：107 份，空白：0 份）		
行政／會計人員	14	13%
醫療人員	15	14%
護理人員	41	38%
資訊科技人員	0	0%
實驗室人員	4	4%
研究員	0	0%
關聯的醫護人士	15	14%
其他	19	18%

2. 你受聘於醫管局的期間爲：（作答：107 份，空白：0 份）		
少於 1 年	2	2%
1 年至少於 3 年	6	6%
3 年至少於 5 年	6	6%
5 年或以上	93	87%
不適用	0	-

3. 你於本醫院工作的期間爲：（作答：107 份，空白：0 份）		
少於 1 年	6	6%
1 年至少於 3 年	8	7%
3 年至少於 5 年	11	10%
5 年或以上	82	77%

4. 你履行職責時，是否需要查閱病人資料？（作答：107 份，空白：0 份）		
是	102	95%
否	5	5%
a) 如是，你是否需要查閱醫療資料？（作答：97 份，空白：10 份）		
是	82	85%
否	15	15%

乙部 – 病人資料的處理

5. 你所處理的病人資料的存在形式爲：（作答：103 份，空白：4 份）		
實體形式（例如紙張）	92	50%
電子形式（例如臨床資料處理系統）	90	49%
其他	1	1%

6. 除了正常職責，你曾否收到指示查閱病人資料（例如進行研究）前要獲得事先核准？（作答：101 份，空白：6 份）		
是	66	65%
否	34	34%
不知道	1	1%

7. 你是否獲告知「機密」資料和「未經分類」資料的分別？（作答：103 份，空白：4 份）		
是	63	61%
否	40	39%
a) 如是，得知的途徑是（作答：63 份，空白：44 份）		
正式培訓	44	38%
由上司告知（口頭或書面）	53	46%
自己找尋答案（例如透過內聯網）	19	16%

8. 你曾否獲告知查閱病人資料只限於「負責醫護」及「按職能需要知道」此兩種目的？（作答：102 份，空白：5 份）		
是	93	91%
否	9	9%
a) 如是，從何途徑得知？（作答：92 份，空白：15 份）		
正式培訓	68	40%
由上司告知（口頭或書面）	75	44%
自己找尋答案（例如透過內聯網）	28	16%

9. 假如你在開放地方工作，在有關地方以實體形式（例如紙張）存在的病人資料在不使用時有否受到妥善保管？（作答：103 份，空白：4 份）		
有	96	99%
否	1	1%
不適用	6	-

10. 透過電腦查閱病人資料是否受到密碼保護？（作答：103 份，空白：4 份）		
是	94	100%
否	0	0%
不適用	9	-
a) 如是，你離開電腦時有否登出電腦？（作答：94 份，空白：13 份）		
有	92	90%
否	0	0%
我依靠電腦的自動登出系統	10	10%

11. 你曾否與其他使用者共用你的密碼？（作答：97 份，空白：10 份）		
曾	3	3%
否	94	97%
a) 如是，醫院是否准許你與其他使用者共用你的密碼？（作答：3 份，空白：104 份）		
是	0	0%
否	3	100%
不知道	0	0%

12. 在過去 12 個月內，你有沒有因工作需要匯入病人資料？（作答：102 份，空白：5 份）		
有	44	43%
沒有	58	57%
a) 如有，你如何取得資料？（作答：44 份，空白：63 份）		
透過實體資料（如紙張）	36	57%
透過內聯網	18	29%
透過互聯網（例如電子郵件）	1	2%
透過電子裝置	3	5%
其他	5	8%
b) 及你從何處取得資料？（作答：43 份，空白：64 份）		
醫院的同事	30	44%
醫管局轄下其他醫院／診所／機構	25	37%
其他	13	19%

13. 在過去 12 個月內，你有沒有透過電郵附件匯入病人資料？（作答：101 份，空白：6 份）		
有	9	9%
沒有	92	91%
a) 如有，這些匯入資料是甚麼形式（作答：7 份，空白：100 份）		
受密碼保護的工作表	4	50%
加密檔案	3	38%
其他	1	13%

14. 在過去 12 個月內，你有沒有因工作需要下載或匯出病人資料？（作答：102 份，空白：5 份）		
有	27	26%
沒有	75	74%
a) 如有，有關資料是否受密碼或加密保護（作答：24 份，空白：83 份）		
是	20	83%
否	4	17%
b) 如有，使用的頻密程度是（作答：22 份，空白：85 份）		
經常	18	82%
很少	4	18%
只有在被指示時	0	0%

15. 如以上問題的答案爲「有」，有關下載或匯出是否已獲授權？（作答：32 份，空白：75 份）		
是	26	81%
否	6	19%
a) 如是，有關的授權者爲：（作答：26 份，空白：81 份）		
直屬上司	20	59%
私隱委員會	4	12%
倫理委員會	3	9%
其他	7	21%

16. 在過去 12 個月內，你有沒有透過電郵附件匯出病人資料？（作答：101 份，空白：6 份）		
有	10	10%
沒有	91	90%
a) 如有，有關資料是否受密碼或加密保護（作答：10 份，空白：97 份）		
是	8	80%
否	2	20%
其他	0	0%

17. 從系統中匯出有關病人資料的目的爲：（作答：98 份，空白：9 份）		
持續醫護用途	21	49%
研究用途	5	12%
系統維護	3	7%
行政用途（包括調查投訴）	13	30%
其他	1	2%
不適用	68	-

18. 你從系統中匯出病人資料之前，有沒有刪除可識辨身份的資料？（作答：96 份，空白：11 份）		
有	11	41%
沒有	11	41%
只有在被指示時	5	19%
不適用	69	-

19. 有關的病人資料的匯出途徑爲：（作答：98 份，空白：9 份）		
內聯網	13	29%
實體形式（如列印副本）	23	51%
電子郵件	4	9%
電子裝置	2	4%
其他	3	7%
不適用	65	-

手提電子裝置

20. 假如你在過去 12 個月內曾使用電子裝置匯入或匯出電子資料，你曾否使用下列裝置？（作答：99 份，空白：8 份）		
軟磁碟	3	19%
CD/DVD	3	19%
USB 儲存裝置	6	38%
手提電腦	2	13%
其他手提裝置	2	13%
不適用	89	-

21. 有關手提電子裝置有沒有加密功能？（作答：99 份，空白：8 份）		
有	7	64%
沒有	4	36%
不適用	88	-
a) 如有，在過去 12 個月內，你使用有關裝置時有否使用其加密功能？（作答：7 份，空白：100 份）		
經常	7	100%
很少	0	0%
從不	0	0%

22. 有關手提電子裝置是否由醫院提供，用以下載病人資料？（作答：99 份，空白：8 份）		
是	7	50%
否	7	50%
不適用	86	-
a) 你有否申請下載資料？（作答：10 份，空白：97 份）		
有	3	30%
否	7	70%
b) 如是，你有否在有關申請中述明該些資料的用途（作答：4 份，空白：103 份）		
是	3	100%
否	0	0%
其他	0	0%
不適用	1	-

23. 你有否於使用完畢後退還有關的手提電子裝置？（作答：99 份，空白：8 份）		
有	5	63%
否	3	38%
不適用	91	-

24. 退還手提電子裝置前，你有否先刪除病人資料？（作答：99 份，空白：8 份）		
經常	6	100%
從不	0	0%
很少	0	0%
不適用	93	-
a) 如有，你如何刪除有關資料？（作答：5 份，空白：102 份）		
以任何自選的軟件，或裝置的內建功能	3	43%
依從醫院所建議的刪除程序	1	14%
其他	3	43%

25. 如你持有實體形式的病人資料，在達到使用目的後，你如何確保安全棄置資料？（作答：**99** 份，空白：**8** 份）		
碎掉	45	35%
交由第三者銷毀	68	53%
作爲循環再用紙張	1	1%
其他	14	11%

26. 你曾否將從系統匯出的病人資料移轉至工作以外的地方，例如你的家中、醫管局轄下其他機構或其他第三者（例如非醫管局僱員的人士）？（作答：**99** 份，空白：**8** 份）		
是	9	9%
否	90	91%

27. 你是否獲准將病人資料帶離工作場所？（作答：**101** 份，空白：**6** 份）		
是	10	10%
否	91	90%
a) 不論你有否獲授權，假如你曾經將病人資料帶離工作場所，你曾將有關資料帶往：（作答：**69** 份，空白：**38** 份）		
醫院管理局轄下的其他醫院／機構	4	44%
你的居所	1	11%
老人院	2	22%
大學	0	0%
其他	2	22%
不適用	61	-
b) 原因是：（作答：**59** 份，空白：**48** 份）		
於醫院以外執行醫院所委派的職務	4	44%
下班後在家趕工	1	11%
於家中或其他地方進行研究工作	0	0%
其他	4	44%
不適用	50	-

28. 你是否經常在先獲得特定人士的授權下，才將病人資料帶離工作場所？（作答：**44** 份，空白：**63** 份）		
是	19	43%
否	25	57%

29. 你曾否使用屬你個人所有的電子裝置儲存病人資料？（作答：**100** 份，空白：**7** 份）		
曾	5	5%
否	95	95%
a) 如是，你有沒有將有關裝置送交醫院的資訊科技部門以通過與公家電腦相同的處理？（作答：**7** 份，空白：**100** 份）		
有	1	14%
沒有	6	86%
b) 如沒有，你有否確保你的裝置沒有電腦病毒或可造成資料外洩的社交軟件（例如 **Foxy**，**MSN Messenger**，**Facebook**，**FTP** 伺服器及網頁伺服器）？（作答：**7** 份，空白：**100** 份）		
有	7	100%
沒有	0	0%

30. 將病人資料移轉至醫管局系統前，你在工作站處理病人資料時，通常以甚麼資料作爲其身份索引？（作答：**90** 份，空白：**17** 份）		
姓名	46	29%
香港身份證號碼	68	43%
醫院編配的病人編號	38	24%
其他	5	3%

丙部 – 規管處理病人資料的政策、指引或措施

31. 你是否知道醫院有就規管處理病人資料方面訂立任何政策、指引或措施？（作答：**106** 份，空白：**1** 份）		
是	104	98%
否	2	2%
a) 如是，你是否明白有關內容？（作答：**102** 份，空白：**5** 份）		
是	100	98%
否	2	2%
a) 如是，你明白的程度是（作答：**101** 份，空白：**6** 份）		
1（我不明白）	0	0%
2（我明白少許）	2	2%
3（我大致明白）	64	63%
4（我非常明白）	35	35%

32. 你是否知道醫院有就規管使用電子裝置匯入及匯出病人資料方面訂立任何政策、指引或措施？（作答：**106** 份，空白：**1** 份）		
是	93	88%
否	13	12%
a) 如是，你是否明白有關內容？（作答：**88** 份，空白：**19** 份）		
是	85	97%
否	3	3%
b) 如是，你明白的程度是（作答：**87** 份，空白：**20** 份）		
1（我不明白）	2	2%
2（我明白少許）	8	9%
3（我大致明白）	42	48%
4（我非常明白）	35	40%

33. 你曾否遺失任何載有病人資料的列印本或載有病人資料的電子裝置？（作答：**106** 份，空白：**1** 份）		
曾	1	1%
否	101	99%
不適用	4	-
a) 如有，你有沒有將有關遺失告知你的上司或醫院？（作答：**3** 份，空白：**104** 份）		
有	1	33%
沒有	2	67%

34. 你是否知道醫院有就遺失病人資料或載有病人資料的裝置的呈報方面，訂立任何政策、指引、規則或規例？（作答：**106** 份，空白：**1** 份）		
是	98	92%
否	8	8%
a) 如是，你是否明白有關內容？（作答：**95** 份，空白：**12** 份）		
是	92	97%
否	3	3%
b) 如是，你明白的程度是（作答：**94** 份，空白：**13** 份）		
1（我不明白）	1	1%
2（我明白少許）	8	9%
3（我大致明白）	37	39%
4（我非常明白）	48	51%

35. 在 2008 年 5 月之前，你曾否接受下列任何培訓？（作答：93 份，空白：14 份）		
病人資料保密	87	38%
保護個人資料私隱	78	34%
電子儲存裝置的使用	30	13%
電子通訊政策	36	16%

36. 你認爲醫院提供的培訓是否足夠應付病人個人資料的保安問題？（作答：105 份，空白：2 份）		
足夠	77	73%
不足夠	13	12%
不知道	12	11%
不關心	3	3%

丁部 – 評估職員對個人資料私隱的意識

37. 員工依從私隱政策、指引及措施的程度是否包含於年度考績的評估項目？（作答：106 份，空白：1 份）		
是	36	34%
否	31	29%
不知道	39	37%

38. 你是否知道醫院設有資料保障主任一職？（作答：106 份，空白：1 份）		
是	85	80%
否	21	20%
a) 如是，你是否知道其職責：（作答：84 份，空白：23 份）		
是	68	81%
否	13	15%
不關心	3	4%
b) 如是，其職責是：（作答：68 份，空白：39 份）		
處理病人的查閱資料要求	41	23%
籌劃及/或進行有關保障個人資料私隱的培訓	63	36%
向員工派發有關處理病人資料的通告及／或政策、指引或措施	62	35%
其他	9	5%

39. 你如何評價你的同事對保障病人資料私隱的意識？請填寫數字 **1** 至 **10**，**1** 爲最低，**10** 爲最高。（作答：**106** 份，空白：**1** 份）		
1	1	1%
2	0	0%
3	0	0%
4	0	0%
5	3	3%
6	5	5%
7	13	12%
8	40	38%
9	22	21%
10	21	20%

40. 你如何評價醫院採取保障病人資料的措施，以免受未經准許或意外的查閱、處理及使用？請填寫數字 **1** 至 **10**，**1** 爲最不足，**10** 爲最足夠。（作答：**105** 份，空白：**2** 份）		
1	1	1%
2	0	0%
3	0	0%
4	0	0%
5	3	3%
6	6	6%
7	16	15%
8	29	28%
9	29	28%
10	21	20%

41. 你如何評價你的同事在遵守醫院保障病人資料安全規定的程度？請填寫數字 **1** 至 **10**，**1** 爲最不滿意，**10** 爲最滿意。（作答：**106** 份，空白：**1** 份）		
1	1	1%
2	0	0%
3	0	0%
4	0	0%
5	2	2%
6	3	3%
7	15	14%
8	32	30%
9	27	26%
10	25	24%

42. 你是否知道你的醫院存在下述問題？（作答：56 份，空白：51 份）		
與他人共用密碼	4	4%
使用電腦後沒有登出	33	31%
大量使用手提電子裝置	9	8%
隨意放置載有病人資料的手提電子裝置	3	3%
其他	18	17%

43. 如你有病人資料私隱方面的問題，你可以怎樣尋求答案？（作答：106 份，空白：1 份）		
向同事查詢	21	20%
向上司查詢	95	89%
向資料保障主任查詢	43	40%
從內聯網尋找	36	34%
不知道	1	1%
其他	7	7%

44. 你認爲如何可以改善醫院現時的個人資料系統，以確保病人資料得到更佳保障？

a) <u>政策與指引</u>

政策及指引應更準確，並以非專業用語寫成，以便員工參考
設立論壇以定期提醒他們有關政策、指引及定期檢討
更實在的指引；醫院提供電子裝置予職員

b) <u>切實執行</u>

下載／複製病人資料前必須先獲得批准
醫院要各職切實執行有關的指引
即日匯報遺失病人資料個案
載有病人個人資料文件要妥善保管
職員須注意規則及規例，以嚴厲遵從；減少工作量
上司應實質地加強遵從醫管局指示方面的督導工作
不可隨意將病人資料儲存於 USB 手指

c) 資源

提供足夠資源（例如用以儲存病人資料的袋）
提供私人空間以處理病人資料
更有效率的電腦系統以便在符合私隱條例下工作
改善病人的配置（即其佔用的空間）
提供有加密功能的 USB；定期培訓
增加空間以便更佳地分隔職員和病人，以及更妥善地放置文件

d) 保安措施

所有工作站均備安裝密碼保護的螢幕保護裝置
改良電子裝置的保安
當使用電腦處理病人個人資料後立即登出； 當使用完病人個人資料文件後立即銷毀
多用紙張去 Cover 病人資料； 減少在工作上製造不必要載有病人資料的名單； 減少隨處放置載有病人資料文件； 同事應多用有密碼保護的電腦文件
(1)OPAS 自動登出 (2)防火牆（包括偵測病毒功能）

e) 審計

進行更多審計
爲資料保護進行定期審計
提升系統，以便找出洩漏個人資料的人（例如時間記錄）
改進認證程序

f) 培訓

更多培訓
培訓應爲定期形式，並強制參加
持續教育；在入職階段有更詳盡的正式培訓；爲不同職級及職位提供統一籌辦的訓練
爲前線員工提供培訓 加強政策的監管
提升員工有關保障個人資料的意識，加強培訓及提醒員工
就私隱條例提供更多培訓
就個人資料保護提供更多講座
複修培訓
籌組更多培訓；複修課程
提供定期培訓
就病人資料私隱進行更多培訓
應就保護病人資料作出更多培訓；採用加密系統
更多培訓及工作坊
更多有力的職員教育
在該方面提供正式培訓／教育課程
提供更多培訓
定期公告或提醒
以便箋及通告更頻密地警戒員工
更多教育，提供／告知新的器材／技術
爲所有員工提供培訓；提醒員工；就查閱資料的授權提供清晰指示
提升員工在收集個人資料上的警覺性
提醒及警戒員工

g) 管理考量

提高醫院內所有員工於資料管理上的意識
病人不須處理自己的底片
在一般醫療工作中，採用單一而匿名化的病人身份
停止使用 USB 裝置儲存病人資料
同一聯網內的所有個人電腦應予連線

h) <u>滿意</u>

現時的系統已很足夠
不用改善
我認爲病人的資料在醫院內受到不錯的保護
醫院現有的個人資料系統不錯

附件 VI

問卷結果分析的註解

1. 合共收回 107 份問卷。除很少數的自願者外，絕大部分的回應者均在與個人資料私隱專員公署人員的面談過程中提交問卷。

2. 面談人員尊重回應者的自由選擇。以下是部分本署分析有關回應時觀察所得的事項：－

   - 在第 22 題中，其中一位回應者同時選擇了「是」和「否」。
   - 不少回應者選擇「是」後，沒有回答「如是」的問題。
   - 不少回應者選擇「否」後，繼續回答「如是」的問題。
   - 個別人士在選擇「是」或「否」時，同時選擇了「不適用」。

3. 「不適用」沒有包括在百份比的計算內。

4. 由於部分回應者在一條問題上選擇了多於一個答案，因此有關問題的作答次數會多於作答份數。後頁附表爲有關問題的統計撮要。

回應者在一條問題上選擇了多於一個答案的統計撮要

題號	作答份數（見結果分析）	作答次數（見結果分析）		選擇 1 個答案的問卷份數	選擇 2 個答案的問卷份數	選擇 3 個答案的問卷份數	選擇 4 個答案的問卷份數	選擇 5 個答案的問卷份數	作答份數	作答次數
1	**107**	14+15+41+0+4+0+15 +19	**=108**	106	1	0	0	0	**107**	**108**
5	**103**	92+90+1	**=183**	24	78	1	0	0	**103**	**183**
7 a)	**63**	44+53+19	**=116**	24	25	14	0	0	**63**	**116**
8 a)	**92**	68+75+28	**=171**	35	35	22	0	0	**92**	**171**
10 a)	**94**	92+0+10	**=102**	86	8	0	0	0	**94**	**102**
12 a)	**44**	36+18+1+3+5	**=63**	26	17	1	0	0	**44**	**63**
12 b)	**43**	30+25+13	**=68**	20	21	2	0	0	**43**	**68**
13 a)	**7**	4+3+1	**=8**	6	1	0	0	0	**7**	**8**
15 a)	**26**	20+4+3+7	**=34**	18	8	0	0	0	**26**	**34**
17	**98**	21+5+3+13+1+68	**=111**	90	5	1	2	0	**98**	**111**
19	**98**	13+23+4+2+3+65	**=110**	88	8	2	0	0	**98**	**110**
20	**99**	3+3+6+2+2+89	**=105**	94	4	1	0	0	**99**	**105**
22	**99**	7+7+86	**=100**	98	1	0	0	0	**99**	**100**
24 a)	**5**	3+1+3	**=7**	4	0	1	0	0	**5**	**7**
25	**99**	45+68+1+14	**=128**	71	27	1	0	0	**99**	**128**
27 a)	**69**	4+1+2+0+2+61	**=70**	68	1	0	0	0	**69**	**70**
30	**90**	46+68+38+5	**=157**	42	29	19	0	0	**90**	**157**
35	**93**	87+78+30+36	**=231**	18	33	21	21	0	**93**	**231**
38 b)	**68**	41+63+62+9	**=175**	6	21	37	4	0	**68**	**175**
42 a)	**56**	4+33+9+3+18	**=67**	47	7	2	0	0	**56**	**67**
43	**106**	21+95+43+36+1+7	**=203**	49	29	18	8	2	**106**	**203**