2008 年 **12** 月 **8** 日

參考文件

立法會資訊科技及廣播事務委員會

資訊保安

目的

本文件旨在告知各委員關於政府資訊保安改善計劃的進展。

背景

2. 自 2008 年 4 月中，一些涉及政府決策局／部門(下稱“各局／部門各局／部門”)泄漏個人資料的事件，引起公眾對政府資訊保安的關注。在資訊科技及廣播事務委員會 2008 年 5 月 30 日的特別會議上，我們向各委員闡述政府從這些事件所汲取的經驗，以及將會推行的改善計劃。該計劃的目的，是加強各局／部門對個人或敏感資料的保護，以及確保因應《個人資料(私隱)條例》的規定，採取所有可行的步驟，以防泄漏未經授權的個人資料。

資訊保安改善計劃的進展

3. 資訊保安改善計劃的首要工作重點，是如何處理近期事件所突顯的風險。我們亦同時研究長遠的措施，以期改善資訊保安的管理和保證工作。

4. 改善計劃中較爲迫切的項目有四個主要範疇，包括員工的認知和教育、技術和程序措施、保安要求遵行的查核，以及對保安規例、政策和指引的檢討。我們認爲必須特別關注員工的認知和教育，使他們能夠遵從資訊保安的要求。我們亦協助各局／部門購置保安工具和技術解決方案，以減低外來威脅所造成的風險，和減少出現員工疏於保護敏感或個人資料的情況。改善計劃的進展，詳載於以下各段：

(i) 員工的認知和教育

5. 我們優先協助員工得知和了解資訊保安措施，以及運用合適的保安機制。我們已訂立一個員工溝通計劃，以加強政府各級員工對資訊保安的認知；增發指引，提供有關良好作業守則的資料和意見；以及舉行一系列研討會，介紹資訊保安的最新發展。

(a) *員工溝通計劃*

6. 員工遵從資訊保安的要求，是改善資料保護的關鍵。政府資訊科技總監辦公室已聘請有關顧問公司，設計連串爲期一年的活動，以協助政府員工建立和維持高度的認知水平、工作知識和良好習慣，致力保護敏感和個人資料。這個新的溝通計劃，將切合各階層肩負不同職責的持份者的需要，包括決策者、部門管理層和行政人員、資訊科技專業人員、終端用戶和部門資訊科技保安主任。這些活動亦會因應不同的服務對象，採用各種溝通工具和渠道[1]。

(b) *加強員工認知的提示和指引*

7. 使用未經授權的軟件，可引起意外泄漏敏感或個人資料及資料被濫用的風險。因此，政府禁止員工使用未經授權的軟件。政府資訊科技總監辦公室於 2008 年 7 月發出通告，給予各局／部門首長有關技術和程序措施的意見，以供指示轄下人員遵守這方面的規例。

---

[1] 這涵蓋出版刊物、培訓(包括電子培訓課程和教材)、問答比賽、宣傳錄影帶、智能提示、最佳作業守則論壇、管理層贊助的活動、展覽等。

8. 爲了向高層人員、主管和前線員工等不同持份者介紹資訊保安的最佳作業守則，政府資訊科技總監辦公室在《公務員通訊》刊登多篇關於資訊保安的文章，以淺易的方法，讓所有公務員獲取有關資訊。我們還透過資料單張和海報，傳達預防資料外泄的信息，供眾多員工閱覽。

(c) *<u>員工培訓</u>*

9. 互聯網的保安威脅確實是日新月異。員工必須掌握最新的資訊科技保安課題和發展，及市場上有關的技術解決方案，以減低風險。自 2008 年 5 月起，政府資訊科技總監辦公室已爲 80 個局／部門的 700 多名員工安排不同的研討會和產品示範，內容包括資料加密技術、保護便攜式電子裝置，以及在辦公室以外工作的保安措施。另外，我們亦爲 200 名剛入職的行政主任舉辦了 8 個培訓課程。由於行政主任在各局／部門工作，經常有需要處理敏感或個人資料。

10. 除了中央統籌資訊保安研討會／培訓外，政府資訊科技總監辦公室亦協助多個局／部門爲其員工設計專門課程，以切合部門和員工工作上的需要。

(ii) 技術及程序措施

(a) *員工在家中工作*

11. 有很多勤奮員工都希望利用科技，協助他們在家中工作，而不需要在辦公室作長時間逗留，達致工作與生活的平衡。爲確保敏感及個人資料得到保障，一個安全的家中工作環境是必要的。政府資訊科技總監辦公室已向各局／部門建議一些包含硬件、軟件及服務等方面的技術及程序措施，以加強員工在家中工作時的資訊保安。我們亦協助各局／部門尋求及實施解決方案，以增加對電腦系統、便攜式裝置、網絡及數據的保護。

(b) *預防及偵察違規情況*

12. 爲協助需較精密解決方案的決策局／部門達到更高或特定的數據保護要求，政府資訊科技總監辦公室透過與業界及供應商緊密聯繫和合作，獲得在數據保護方面最新科技發展及技術解決方案的資料。政府資訊科技總監辦公室亦正進行可行性評估，研究設立中央執行的設施，用作協助偵察違犯資訊保安政策的情況，或減低用戶透過電郵或檔案共享軟件而意外泄漏當事人的身分。

(iii) 加強管理安排以確保要求得以遵行，以及向各局／部門、公共機構和非政府機構提供建議及支援

(a) 規例遵守審計及跟進行動

13. 近期發生的資料泄漏事件，均涉及違反某些保安要求。爲了減低違反保安要求的風險，政府規定各局／部門對轄下資訊系統最少每兩年進行一次保安風險評估。爲確保這些評估得以進行，以及向各局／部門提供獨立意見和建議供進一步改善，政府在 2007 年 5 月開始實行由中央管理的保安審計。最新的審計結果顯示，所有局／部門已使用加密功能，保護儲存於便攜式電子裝置中的敏感資料，並且設立了正確程序，供匯報因使用便攜式電子裝置而遺失數據的事件。

(b) 公共機構

14. 在 2008 年 8 月 及 9 月舉行的奧運會與殘疾人奧運會馬術項目期間，政府資訊科技總監辦公室作出了特別安排，協助各局／部門及其轄下的公共機構交換資訊和執行適當保護措施，以減低資訊保安風險。我們定期建議各局／部門與其轄下的公共機構分享有關資訊保安的政策、指

引及技術資訊，以協助他們提升保安狀況。例如在 2008 年 11 月以《全城電腦清潔日 2008》爲主題所舉辦的公開研討會，共有超過 20 個公共機構及 90 個中小企業參加。

(iv) 檢討資訊保安規例、政策及指引

(a) *匯報資訊保安事故和通知受影響人士*

15. 政府已就處理涉及敏感和個人資料的保安事故，檢討及更新現時的相關規例和政策。如保安事故涉及個人資料，有關決策局／部門須向個人資料私隱專員公署及政府資訊保安事故應變辦事處報告。另外，有關決策局／部門還須在可行情況下，通知受事故影響的人士。例外的情況只限基於公眾利益考慮，例如可引致防止和偵察非法行爲受到影響。任何例外的情況，必須獲得局／部門首長的批准。經修訂的規例和程序，已於 2008 年 11 月公布。

資訊保安事故的調查結果及建議

16. 在 2008 年 5 月 30 日舉行的資訊科技及廣播事務委員會特別會議上，有關決策局／部門及公共機構已向各委員闡述資料泄漏事故和補救措施。相關的調查結果顯示，這些資料泄漏事故並沒有牽涉惡意或刑事的意圖，如資料盜竊

之類，而主要的原因，是有關員工沒有審慎保護所處理的敏感或個人資料。

17. 爲防止這類保安事故再發生,所有局／部門均須檢討保護敏感及個人資料的內部規則。爲此，各局／部門已安排培訓和推廣計劃，以加強員工對資訊保安的認知，亦同時鞏固電腦系統和技術配套。對於加緊保護資訊資產和給員工提供更安全的工作環境，政府在加強技術和程序措施方面，尚可再作改善。政府資訊科技總監辦公室已把必要的跟進的事項，納入上文各段所述的改善計劃內。

各局／部門作出的保安風險評估

(a) *高層管理支援*

18. 建立保護個人及敏感資料的工作文化，需要得到高層管理人員的關注與支持。爲了確保所有局／部門對維持高水平的資訊保安給予充分和高度的重視，政府資訊科技總監向各局／部門首長作出簡報，解述資訊保安的重要性和他們對作出保安保證的責任。政府資訊科技總監辦公室更安排了簡介會給四十個來自不同局／部門的高層管理人員，分享有關英國政府曾經遺失數百萬英國居民的個人資料的事件檢討中

所汲取的教訓。簡介會由該檢討小組的一位成員講解。

(b) *保安風險評估*

19. 政府資訊科技總監要求各局／部門首長對員工(包括在辦公室以外的地方）處理個人或敏感資料時所採取的保安措施，作出特別的保安風險評估。各局／部門首長亦須要定出改善計劃，以防止任何已確認的保安風險。

20. 各局／部門已作出適當的跟進，以減低已確認的風險，例如對付“相信違規行爲不被察覺和懲罰”、“試圖在未經批准下在家裏處理敏感資料”和“對數據保護的重要性和有關規例缺乏認知”。各局／部門已根據各自的評估作出跟進措施，列舉於附件一內。

資料泄漏事故的最新發展

21. 在資訊科技及廣播事務委員會於2008年5月30日舉行的特別會議中所匯報的進展情況後，有關決策局／部門已採取適當的修正和風險緩解措施，以防止資訊保安事故再次發生。香港警務處和醫院管理局就各自的進展情況，分別提供進展報告，詳情請參閱附件二及附件三。

22. 上次會議至今，政府資訊保安事故應變辦事處共收到五宗有關資料泄漏事故的新報告。這些事件和過去的事故相類似，都是涉及遺失便攜式儲存裝置，和員工使用家中安裝了檔案共享軟件的電腦處理資料時泄漏。有關決策局／部門已在可行的情況下，通知受影響的當事人和採取跟進的措施。有關的事故亦已知會個人資料私隱專員。事故的詳情載於附件四。

公衆的資訊保安

(a) *資訊保安參考資料*

23. 政府已採取措施，告知市民如何保護電腦資源和資訊資產。政府資訊科技總監辦公室透過一站式資訊保安入門網站(www.infosec.gov.hk)，發布政府所採用的資訊保安政策及指引，讓市民閱覽。公共和私營機構也可以參考這些政策及指引，以提升其保安設備。

(b) *青少年*

24. 自 2008 年年初，政府資訊科技總監辦公室與香港警隊學校聯絡員合作，連同一些專業資訊保安機構，走訪了 30 所學校，向超過 7 000 名師生舉辦講座和討論會，就使用資訊

科技和互聯網的正確態度和資訊保安的知識提供意見。透過這項活動，我們期望令年輕一代培育出對資訊保安更高的警覺性，和更具責任感的電腦用戶文化。

(c) *商界企業*

25. 政府資訊科技總監辦公室將繼續與香港生產力促進局營運的香港電腦保安事故協調中心、專業資訊保安機構和業界團體攜手，向商界企業，特別是中小企業，推廣資訊保安。政府資訊科技總監辦公室會在 2009 年資助香港電腦保安事故協調中心，強化爲市民提供的電腦保安應變支援服務。

總結和未來路向

26. 資訊保安管理是一個持續不斷的過程，需要每個人的承擔和關注。由於科技不斷的發展，嶄新風險的出現，用戶行爲的改變和社交網絡的逐漸流行，資訊保安將會繼續面對挑戰。政府會不遺餘力維護資訊保安的狀況、政策、規例及作業模式，及協助所有員工遵守有關處理敏感或個人資料的保安規定。爲了讓各委員知悉政府就有關資訊保安和數據保護等措施的進展，我們打算每年向資訊科技及廣播事務委員會，定期匯報有關現行及計劃中措施的進展。

27. 科技方案對資訊保安風險的管理有莫大影響，由於影響深遠，因此需要認真地計劃其部署和使用。政府資訊科技總監辦公室會評估有關在中央或部門應用科技的情況，以協助各局／部門更有效地進行資訊保安管理，包括上文第 12 段所述的科技方案，和協助用户對包含敏感或個人資料的電子文件作出存取權限管理。

28. 政府資訊科技總監辦公室會繼續協助各局／部門持續改善資訊保安管理，例如採用評估資訊保安管理技巧的工具。

徵詢意見

29. 請各委員察悉本文報道的內容。

商務及經濟發展局

政府資訊科技總監辦公室

2008 年 12 月

附件一

立法會資訊科技及廣播事務委員會 2008 年 12 月 8 日會議

各局／部門已進行的風險評估和提出的改善措施

因應政府資訊科技總監辦公室的要求，所有局／部門已進行了風險評估工作，並制定了可減低已知風險的改善方案。在 2008 年 7 月 15 日，政府資訊科技總監已向各局／部門首長發出有關「在辦公室以外環境處理、儲存和查看個人／限閱資料的風險評估」便箋。

2. 各局／部門將因應已知的風險，落實進行個別的改善措施。各局／部門了解當中的風險，並積極準備／執行必要的措施，以提高保安狀況。在各局／部門的匯報中，有一些共同的改善措施，而這些措施亦配合政府整體的保安改善計劃，其摘要如下。

保安認知的宣傳和培訓

3. 各局／部門已進行多項員工認知的宣傳和培訓活動。各局／部門了解這方面的重要性。已經或正在採取的具體行動包括－

(a) 進行認知培訓、工作坊和內部簡報;

(b) 再行傳閱相關的規則和指引;

(c) 鼓勵員工參加保安簡報會和研討會;

(d) 爲新入職的員工提供信息材料和簡報會;

(e) 定期以電子信息提醒員工有關的保安要求;

(f) 使用含有保安主題的預警信息和屏幕保護程式提醒用戶。

收緊控制在家工作及使用便攜式儲存裝置

4. 各局／部門意識到在家工作及使用便攜式儲存裝置的風險。爲了提供一個安全的工作環境和減低已知的風險，各局／部門已經或將會設立各種控制和／或程序，包括－

(a) 須事先得到批准並作記錄，方可儲存公務資料於便攜式儲存裝置和／或帶離辦公室；

(b) 統一控制提供和使用 USB 儲存裝置；

(c) 維持一份載有所有便攜式儲存裝置的清單；

(d) 只可用政府提供的設備儲存或處理可辨別個人身分的資料；

(e) 所有便攜式裝置儲存的資料均須加密及在使用後移除；

(f) 突擊檢查網絡和便攜式儲存裝置；

(g) 定期盤點便攜式儲存裝置。

<u>加強資訊科技設施或資源</u>

5. 各局／部門正在實施或計劃實施一些技術解決方案，以強化對數據的保護，包括－

(a) 加密工具或附設加密功能的 USB 儲存裝置；

(b) 採購更多筆記簿型電腦 ／ 安裝虛擬私人網絡解決方案，方便員工於辦公室以外的地方工作；

(c) 規劃加強資訊科技基礎設施，例如利用“虛擬工作站”的概念；

(d) 實施中央檔案伺服器或中央管理的部門檔案加密解決方案；

(e) 進行一些可以偵察／禁止使用有潛在風險的外部網絡電郵或其他開放設施的技術研究；

(f) 測試軟件，以減低通過手提電話泄漏資料的風險；

(g) 實施端點安全解決方案或主機保護軟件；

(h) 安裝數據泄漏防護系統或軟件，以禁止下載、列印、發放和傳送機密資料；

(i) 實施資訊權限管理系統；

(j) 調配人手，以監督資訊保安和數據保護。

檢討政策和指引

6. 許多局／部門正在或將會對現有政策和指引作出檢討，以便向員工提供有關工作程序的更明確指示，包括－

(a) 更新使用便攜式儲存裝置的政策；

(b) 檢討敏感資料的存取控制；

(c) 檢討在辦公室以外處理、儲存和查看個人／限閱資料的方法；

(d) 擴大未來資訊科技保安風險評估和審計的範圍，包括檢討對處理、儲存和保護個人或限閱資料的措施；

(e) 提供更明確的指引；

(f) 檢討使用互聯網的政策。

附件二

立法會資訊科技及廣播事務委員會 2008 年 12 月 8 日會議

有關香港警務處所採取的跟進措施

即時方案

1. 爲提升警隊各成員對資訊保安的警覺性，在警隊告示欄上定期地張貼一些信息，內容關於使用點對點（P2P）軟件的風險、在警隊電腦上使用未經授權的可移除儲存裝置（USB）的處分、電腦病毒感染事故的成因，以及其他有關資訊保安的提示。自 2008 年 5 月起，共貼有十五則相關告示。

2. 在 2008 年 5 月，一個屬警隊層面的工作小組成立，以督導找出數據泄漏的成因及相關的補救方法。

3. 爲加強對可移除儲存裝置的監管，在 2008 年 9 月，警隊開始購入有加密裝置的可移除儲存裝置（USB 手指），供各單位的初級警務人員共同使用，這類 USB 手指屬各單位自行擁有。該批裝置符合政府保安規例的標準，可以儲存至“限閱”級別的資料。爲確保人員能正確使用，一套使用守則亦同時公布。

4. 於推出 USB 手指的同時，在 2008 年 9 月，全部警隊電腦的 USB 連接埠都加入可認證名單程序，以確保該些已登記的 USB 裝置可以在警隊電腦上使用。對 USB 連接埠的監管，減低了未經授權數據的傳送及電腦病毒的風險。2008 年 10 月的數據顯示，在區域電腦發現病毒的情況大幅下跌。

5. 警隊現正購置 2 800 個具數碼證書加密功能的 USB 儲存器，用作儲存機密資料，以符合政府保安規例。該批 USB 儲存裝置將會以個人裝備的形式派發給督察級及以上的人員使用，以提升機密資料的安全儲存、處理及傳送。

6. 政府保安主任已經授權容許警隊成員在有數碼證書認證的情況下使用警隊電郵系統，發放級別至“機密”的附件。

7. 在 2008 年 6 月至 7 月期間，警隊就所有共用電腦進行清洗行動，以刪除在電腦上儲存的個人、敏感及／或限閱數據。一項保安覆核亦隨之執行。第二次保安覆核將在 2008 年 12 月底進行。

8. 爲加強在資訊科技保安上的工作，警隊曾參考海外的經驗及研究，例如 National Policing Improvement Agency (NPIA)有關限閱數據的處理程序，HM Revenue and Customs (HMRC)有關防止資料外泄的 Poynter Review 和有關政府數據處理程序的 Hannigan Report for UK Cabinet Office。

9. 在 2008 年 10 月，各單位及主要單位內亦分別成立工作改善小組及工作委員會，以評估行動需要，收集各人員的意見，並對有關措施提出改善建議。

使用虛擬工作站的長期方案(計劃正考慮中)

10. 爲更佳地保障數據，成立一個以數據爲本的結構，取替現時系統爲本的方式。

11. 爲用戶提供桌面虛擬設備及中央數據儲存／處理裝置，並可透過遙控方式操作，同時亦加強限制數據下載。

培訓

12. 全警隊的資訊保安培訓，將會繼續提供給所有人員，以提升他們對確保資訊安全及數據保護上的警覺性。

13. 爲了令前線單位有所得益，警察總部資訊系統課將繼續進行外展活動，用以提升各人員對資訊保安上應做及不應做事項的認知，亦回應他們對這方面的關注事項。自 2008 年 3 月起，已經進行了十三次類似的探訪。

14. 對受訓中的學員，在結業前提供關於資訊保安及數據私隱的訓示。

15. 爲所有須確保遵行各資訊保安守則的系統保安經理提供培訓。在 2008 年 10 月至 11 月期間，超過二百名屬總督察及警司級的人員已經接受培訓。這課程會繼續舉辦。

16. 爲了讓各人員認識資訊科技的發展及資訊保安的良好作業守則，邀請海外及本地的講者分享經驗。例如在 2008 年 11 月 26 日，三名來自 PricewaterhouseCoopers 的嘉賓在“管理及保障敏感資訊”的座談會上演講，超過 200 名人員出席。

17. 爲提升警隊成員在保障個人資料上的警覺性，已經制定了一個透過教育及培訓的行動計劃。該行動計劃集合了 11 項活動，包括海報設計比賽、座談會及巡迴展覽，而第一個活動已經於 2008 年 11 月初推出。

18. 在 2008 年 11 月 14 日，個人資料私隱專員主持了一個“保障個人資料”的座談會，集中討論法律框架、資料保障原則及資料保障監管。

19. 於 2008 年 11 月 25 日，超過 300 名紀律及文職的中層管理人員，出席了一個由總個人資料主任及高級個人資料主任主持的座談會，內容關於如何遵守《個人資料(私隱)條例》。

20. 一個針對加強初級警務人員對資料保護文化的培訓日項目已經製作完成。該項目將於 2009 年 2 月在整個警隊推出。

21. 於 2008 年 11 月 15 日警隊資訊科技學會在警察體育及遊樂會，舉辦了兩個關於個人電腦保安的工作坊。一位來自私人機構的專業資訊科技保安主任應邀主持講座，目的是增強警隊人員及其家屬在個人電腦的資訊及網絡保安的意識。在 2008 年 11 月 20 日至 26 日期間，警隊資訊科技學會亦在警察體育及遊樂會舉行展覽，內容關於個人電腦的資訊保安，讓警隊成員及其家屬從而獲益。

香港警務處

2008 年 12 月

附件三

立法會資訊科技及廣播事務委員會 2008 年 12 月 8 日會議

有關醫院管理局所採取的措施

目的

本文件旨在向各委員闡述自上次 2008 年 5 月 30 日會議後，醫院管理局（醫管局）就一連串遺失載有可識別病人身分資料的便攜式電子儲存裝置事件所採取的行動。

背景

2. 2008 年 5 月初，醫管局接獲 10 宗遺失載有病人資料的便攜式電子裝置的報告。基於對保障病人資料的關注，醫管局行政總裁（行政總裁）宣布成立醫管局病人資料安全及私隱專責小組（專責小組），檢討現時保障病人資料的政策和保安系統，並提出改善措施。完成檢討後，專責小組於 2008 年 8 月 5 日向行政總裁提交報告。

3. 2008 年 5 月，個人資料私隱專員（私隱專員）於接獲醫管局遺失資料的報告後，着手進行了連串調查。私隱專員於律敦治及鄧肇堅醫院檢查了醫管局的個人資料系統。私隱專

員於 2008 年 7 月 22 日公布調查報告。

4. 專責小組及私隱專員分別就八個範疇提出了 26 及 37 項建議，有關範疇包括醫管局的政策、架構及人事、員工在私隱保安意識方面的培訓、程序及指引、私隱影響評估、監察及審計、合約，以及科技。專責小組及私隱專員的主要檢討結果及建議，詳列於下文第 5 至 8 段。

<u>私隱專員的主要檢討結果及建議</u>

5. 私隱專員認同醫管局已有作出重大和顯著的努力，編製既可配合醫療需要，又能保障病人資料安全的病人資料系統。醫管局已制訂了良好和詳盡的政策，但在推行和協調方面則強差人意。實際執行的監察和進行有系統的保安審核方面，尚須倍加努力。此外，一般對私隱的警覺水平，亦有提升的必要。

6. 私隱專員作出 37 項建議，主要包括發展容易使用的保安政策及指引、研究在下載報告及數據時，減少使用香港身份證號碼的可能性、推行更有效和系統化的私隱審核、以及進一步提升員工對資料安全和私隱的意識。

專責小組的主要檢討結果及建議

7. 專責小組的報告肯定了醫管局採用新科技對服務質素所帶來的重大改善，但同時對病人資料亦有機會構成安全及私隱風險。過去幾年，醫管局一直積極鑑辨和處理這些風險。不過，專責小組在評估今次資料遺失事件，及醫管局保障病人資料的個人資料系統後所汲取的經驗，認爲要保持及加強這些措施的成效，仍有需要下更多功夫。

8. 專責小組提出了 26 項具體行動的建議，範疇包括政策、架構及人事、程序及指引，以及科技，協助醫管局繼續改善其資訊保安及私隱措施。

建議的行動計劃及進度

9. 醫管局大會於 2008 年 9 月 10 日的內務會議上，獲悉專責小組和私隱專員報告的結果和建議，並批准醫管局就這些建議擬採取的行動計劃，以進一步加強保障病人資料安全及私隱。該行動計劃涉及 19 個綜合目標，並涵蓋上文第 4 段提及的八個範疇。醫管局計劃用 12 至 18 個月完成這些行動。

10. 以下是已採取及將於未來 3 至 6 個月內採取的主要行動撮要－

(a) 醫管局已提升病人資料系統，透過加密程序保障下載的可識別病人身分的資料（包括姓名及身份證號碼）；

(b) 強制使用設有加密及密碼鎖功能的 USB 記憶體，以保障病人資料；

(c) 提升系統，於發給病人載有個人資料的電腦打印文件印上“機密”標籤；

(d) 委任機構資訊保安及私隱主任，出掌新成立的醫管局資訊保安及私隱辦事處、設立醫管局總辦事處資訊保安及私隱委員會，以及制訂一份全醫管局使用的新資訊保安及私隱政策；

(e) 加強合約條款上資訊保安及私隱責任；

(f) 檢討及減少主要資訊科技系統內可以下載病人資料的戶口數目；

(g) 檢討及減少資料下載及電腦打印文件時使用香港身份證／姓名；

(h) 安裝供全醫管局使用的中央電郵伺服器，以推行安全電子郵件，有效代替使用便攜式儲存裝置輸送資料；

(i) 檢討及加強個人電腦安全及行政管控。

11. 預料餘下的行動計劃目標，可逐步於 2009/10 年度達致。

醫院管理局

2008 年 12 月

附件四

立法會資訊科技及廣播事務委員會 2008 年 12 月 8 日會議

政府資料泄漏事件的摘要(2008年6月後)

項目	事件日期 (2008 年)	部門	事件摘要
1	6 月 13 日	香港海關	本地傳媒報道，在互聯網上使用點對點分享軟件 FOXY 可以搜尋到一份屬於香港海關的案件口供紀錄。香港海關證實是一份內部文件。口供紀錄載有員工的姓名和職員號碼，以及案件的詳情，包括疑犯的姓名和身份證號碼。
2	6 月 24 日	政府統計處	統計處一名外勤統計主任發現遺失一枚 USB 手指。裝置存有一些從統計調查所得的商業機構內部資料。相關的兩間商業機構隨後已獲通知，並已接受部門的道歉。
3	7 月 6 日	入境事務處	本地傳媒報導，通過 FOXY 可在互聯網上找到屬於入境事務處的敏感資料。該資料涉及 11 份與入境處相關的文件。因沒有足夠的聯絡資料而不能通知事件中受影響的三名遊客。個人資料私隱專員已獲悉該事件。
4	8 月 8 日	香港警務處	本地媒體報道香港警務處的內部資料在 FOXY 網絡上泄漏。事件中泄漏的文件共有五份，包括相信是與警隊打擊賭博及搶劫行動有關的內部指令。
5	9 月 25 日	社會福利署	社會福利署遺失了兩枚已有密碼保護的便攜式儲存裝置。這兩枚裝置都是員工私人擁有的。其中一枚載有宣傳資料，而另外一枚則有 63 名服務使用者的個人資料。一共有 109 名可辨別身分者受影響。當中個人資料包括姓名、地址及個案檔號。已知會個人資料私隱專員。