調查報告

根據香港法例第 486 章《個人資料(私隱)條例》
第 48(2) 條發表

康健醫療及牙科服務有限公司

病人醫療紀錄遭意外棄置

報告編號：R22 - 12326
發表日期：2022 年 6 月 13 日

調查報告：康健醫療及牙科服務有限公司
病人醫療紀錄遭意外棄置

香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第48(2)條訂明，「[個人資料私隱]*專員在完成一項調查後，如認為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、專員認為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、專員認為適合作出的任何其他評論；及

(b)　以他認為合適的方式發表該報告。」

現根據《私隱條例》第 48(2)條履行所賦予的權力，發表本調查報告。

鍾麗玲
個人資料私隱專員
2022 年 6 月 13 日

目錄

調查報告

根據香港法例第 486 章《個人資料（私隱）條例》第 48(2) 條發表

康健醫療及牙科服務有限公司
病人醫療紀錄遭意外棄置

摘要

背景

1. 2021 年 6 月 2 日，康健醫療及牙科服務有限公司（康健）向個人資料私隱專員公署（私隱公署）作出資料外洩事故通報（該資料外洩事故通報），表示旗下一間位於炮台山的醫務中心（該醫務中心）意外棄置了一個載有病人醫療紀錄的紙箱（該紙箱）。康健表示，一名受聘於康健的清潔員工於 2021 年 3 月 14 日錯誤地將該紙箱當作廢物處理並棄置（該事件）。

2. 該事件涉及該醫務中心 294 名病人，當中喪失的個人資料包括他們的姓名、電話號碼、香港身份證號碼、地址、出生日期、診斷紀錄、使用藥物紀錄及實驗室結果等。

3. 在接獲該資料外洩事故通報後，私隱公署隨即對康健展開循規審查，以取得更多有關該事件的資料。在收到康健所提供的進一步資料後，個人資料私隱專員（專員）相信康健在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2021 年 7 月根據《私隱條例》第 38(b)(ii)條就該事件對康健展開調查。

調查

4. 專員在進行調查的過程中，審視及考慮了康健提供與該事件有關的資料，包括對康健處理醫療紀錄的程序及所採取的保安措施進行了六次的查訊。專員亦派員前往該醫務中心進行實地視察，以了解該醫務中心處理及儲存有關醫療紀錄的處所的佈局及所採取的保安措施。此外，專員亦考慮了康健在該事件發生後的跟進及補救工作。

調查結果及違例事項

<u>資料外洩事故</u>

5. 在調查過程中，專員確定該事件屬資料外洩事故，當中康健旗下的該醫務中心意外棄置了一個載有病人醫療紀錄的紙箱，喪失 294 名病人的個人資料。

6. 由於康健控制受該事件影響的個人資料的收集、持有、處理或使用，康健屬《私隱條例》下的資料使用者，須遵從《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

<u>資料保安的嚴重不足</u>

7. 根據保障資料第 4(1)原則，資料使用者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受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

8. 根據調查所獲得的證據，專員發現康健在員工的資料保障意識、政策層面，以至員工培訓方面均存在嚴重不足，導致載有該醫務中心病人的醫療紀錄在可避免的情況下遭意外棄置，主要原因歸納如下：—

(1) **員工的資料保障意識欠奉**：該事件主要涉及人為疏忽。涉事的醫護助理為了其工作便利，對個人資料的保安掉以輕心，未有把正在處理的該紙箱妥善存放，亦未有在該紙箱貼上任何標示，說明箱內載有甚麼物品及其用途，甚至將該紙箱放置在垃圾箱附近，完全漠視該紙箱所載的個人資料的重要性，做法屬明顯的疏忽。同時，涉事的清潔員工單憑該紙箱放置在垃圾箱附近，便把該紙箱當作廢物棄置。

(2) **欠缺有效的政策及程序**：康健就保障醫療紀錄所制訂的政策及指引有欠全面及具體。即使康健有向該醫務中心的員工傳達當中的規定，都不足以有效預防該事件的發生。

(3) **欠缺員工培訓**：康健未曾向前線的員工提供資料保障方面的培訓亦是導致他們欠缺資料保障意識的重要因素。

<u>資料保留</u>

9. 該紙箱載有準備搬移至康健的中央倉庫儲存的醫療紀錄，這些紀錄屬於超過七年未曾前往該醫務中心求診的 292 名病人，以及兩名於 2019 年最後一次前往該醫務中心的病人。

10. 專員考慮到為應付病人可能再次求醫或要求索取其醫療紀錄的情況，醫療機構在一般情況下有實際需要把醫療紀錄存放一段較長的時間。整體而言，專員認為本個案沒有資料顯示康健涉及過長時間地保存該事件遺失的醫療紀錄，康健並沒有違反《私隱條例》附表一保障資料第 2(2)原則有關資料保留的規定。

<u>資料外洩事故通報</u>

11. 雖然《私隱條例》沒有規定資料使用者須向專員及資料當事人通報資料外洩事故，亦沒有規定資料使用者須在指定時間內作出通報，但考慮到該事件所涉及的個人資料性質敏感，專員認為康健可在更

早的時間作出資料外洩事故通報。**專員對康健在該事件發生接近三個月後才作出該資料外洩事故通報，表示遺憾。**

康健違反保障資料第 4(1)原則

12. 專員認為醫療紀錄屬性質敏感的個人資料，康健作為管理過百間醫務中心的資料使用者，持有大量市民的醫療紀錄，理應就收集、持有、處理及使用這些醫療紀錄制訂完善的政策、進行適當的風險評估、以及向員工提供足夠的培訓以灌輸資料保障意識，並按照保障資料第 4(1)原則採取所有切實可行的保安措施，以確保其持有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、喪失或使用所影響。

13. 該事件揭示了康健：—

(1) **沒有檢視及評估人為疏忽的風險，以致未能採取適當措施應對因員工欠缺保障個人資料的意識而存在的風險；**

(2) **沒有制訂清晰及足夠的資料保安政策及指引，以保障性質敏感的個人資料；及**

(3) **沒有就妥善處理個人資料向所有相關人士提供足夠培訓。**

14. **在本個案中，專員發現康健在個人資料的保安方面存在嚴重不足，專員認為康健沒有採取所有切實可行的步驟以確保涉事的醫療紀錄受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了保障資料第 4(1)原則有關個人資料保安的規定。**

執法行動

15. 專員已向康健送達執行通知，指示康健採取以下步驟以糾正，以及防止有關違規情況再發生：

(1) 對適用於康健旗下的醫務中心有關資料保障方面的所有書面政策、標準操作程序／指引進行全面檢視及更新，以提供具體的政策及操作程序／指引；

(2) 制訂有效措施，以確保員工依循更新後的有關資料保障的書面政策、標準操作程序／指引；

(3) 制訂有效措施，監督員工及任何負責在醫務中心執行清潔工作的第三方遵守「*清潔守則*」的規定；

(4) 為員工提供資料保障方面的培訓，並妥善記錄培訓進度，以及就員工培訓的參與及有效程度作出評估；及

(5) 由執行通知的日期起計兩個月內向專員提供文件，證明已完成上述第 (1)至 (4)項指示。

建議

醫療紀錄屬敏感個人資料 應加倍重視

16. 個人資料無論是遭意外丟失、洩漏還是不當處置，對個人潛在的傷害實在不容忽視，尤其是涉及屬敏感資料的醫療紀錄。醫療紀錄是醫療行業的重要資產，它包含有關個人健康和病史的資料，因此醫療機構應加倍重視有關資料，必須確保這些資料在其整個生命週期內得到妥善的管理，這不僅是為遵守《私隱條例》的規定，更是為病人負上道德責任的表現。

17. **專員建議，機構應建立及維持一套遵從《私隱條例》規定的系統，循規地使用及保留個人資料。個人資料私隱管理系統有助機構管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，並確保遵從《私隱條例》。同時，機構應委任保障資料主任，負責監察《私隱條例》的遵從並向高級管理層匯報。**

18. 除了制訂有效的保障資料政策和程序外，資料使用者應採取措施持續地檢視其僱員是否遵從這些政策和程序的要求行事，並為僱員提供全面的培訓，以降低人為錯誤的可能性。**專員建議，機構應全面提升僱員的個人資料保障意識，並為機構建立保障個人資料文化。機構應向僱員提供全面的培訓，將個人資料保障的意識滲入其日常工作之中，以減低因意識不足而引致的人為錯誤。**

19. 雖然在數碼時代，資料外洩事故在網絡世界時有發生，但資料外洩事故在「離線」的世界亦不可忽視。除了康健應該從這次事件中汲取教訓，所有會以文件或其他實體形式處理個人資料的資料使用者也應予以借鏡，防範於未然。**專員建議，機構應同樣重視以電腦或是實體系統處理資料的保安措施，採用可靠的系統及保安設置以保障系統免受網絡世界攻擊的同時，亦應投放資源，加強處理實體資料的保安措施。**

通報資料外洩事故非懲罰 資料使用者不應逃避

20. 專員留意到，很多資料使用者在面對資料外洩事故發生時，往往不知所措。儘管現行《私隱條例》沒有規定資料使用者必須向專員及資料當事人通報資料外洩事故，亦沒有規定資料使用者須在指定時間內作出通報。然而，事實上，當私隱公署收到資料外洩事故通報，會向資料使用者提供適切的建議，協助他們迅速應對資料外洩的事故，適時採取恰當的措施及行動，以減低資料外洩事故對相關機構及受影響的資料當事人的損害。私隱公署亦會提供建議，協助資料使用者完善他們處理個人資料的系統及政策，以避免同類事件再次發生。相反，一旦延遲處理資料外洩事故或向專員作出通報，

資料外洩事故對相關機構及資料當事人的損害（包括情感及實際財務損害）可能倍增，甚至無可挽回。**專員建議，當資料使用者懷疑或發現資料外洩事故發生時，應盡快向私隱公署作出通報，讓私隱公署提供協助及建議，減低資料外洩事故的傷害，以及改善處理個人資料的系統。**

I. 背景

1. 2021 年 6 月 2 日，康健醫療及牙科服務有限公司（康健）向個人資料私隱專員公署（私隱公署）作出資料外洩事故通報 （該資料外洩事故通報），表示旗下一間位於炮台山的醫務中心（該醫務中心）意外棄置了一個載有病人醫療紀錄的紙箱（該紙箱）。根據該資料外洩事故通報內容，一名受聘於康健的清潔員工（該清潔工）於 2021 年 3 月 14 日錯誤地將該紙箱當作廢物處理並棄置（該事件）。

2. 該事件涉及該醫務中心 294 名病人，當中喪失的個人資料包括他們的姓名、電話號碼、香港身份證號碼、地址、出生日期、診斷紀錄、使用藥物紀錄及實驗室結果等。

3. 在接獲該資料外洩事故通報後，私隱公署隨即對康健展開循規審查，以取得更多有關該事件的資料。在收到康健所提供的進一步資料後，個人資料私隱專員（專員）相信康健在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2021 年 7 月 30 日根據《私隱條例》第 38(b)(ii)條就該事件向康健展開調查。

II. 法定權力及相關法律規定

法定權力

4. 專員的權力是根據《私隱條例》所賦予的。根據《私隱條例》第8(1)條，專員須就遵守《私隱條例》條文作出監察及監管，以及促進對《私隱條例》的條文的認識及理解以及遵守。

5. 《私隱條例》第 38 條授權專員在下述情況下可進行調查：

(i) 當專員收到由受影響的資料當事人或其代表作出的投訴，除《私隱條例》第 39 條另有規定外，專員須根據第 38(a)(i)條對有關的資料使用者進行調查，以確定在有關的投訴中指明的作為或行為是否屬違反《私隱條例》下的規定；或

(ii) 當專員有合理理由相信有資料使用者已經或正在作出或從事關乎個人資料的作為或行為，而有關作為或行為可能違反《私隱條例》下的規定，專員可根據第 38(b)(ii)條對資料使用者進行調查，以確定有關行為或作為是否屬違反《私隱條例》下的規定。

6. 專員在展開調查後，可根據《私隱條例》第 43(1)(a)條，為調查的目的而自她認為合適的人處獲提供她認為合適的資訊、文件或物品，以及作出她認為合適的查訊。

7. 《私隱條例》第 48(2)(a)條訂明，專員在完成調查後，如認為如此行事是符合公眾利益的，可發表報告列明該項調查的結果及由該項調查引致的、專員認為適合作出的任何建議或其他評論。

8. 根據《私隱條例》第 50(1)條，如專員在完成一項調查後，認為有關的資料使用者正在或已經違反《私隱條例》的規定，專員可向該資

料使用者送達書面通知，指示該資料使用者糾正該項違反，以及（如適當的話）防止該項違反再發生。

9. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

<u>相關法律規定</u>

資料使用者

10. 《私隱條例》，包括附表一的保障資料原則，旨在規管資料使用者的行為及作為。根據《私隱條例》第 2(1)條，就個人資料而言，資料使用者指「*獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人*」。

個人資料

11. 《私隱條例》涵蓋的資料使用者在處理「個人資料」時須遵守保障資料原則，而根據《私隱條例》第 2(1)條，「個人資料」是「*指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) 該資料的存在形式令予以查閱及處理均是切實可行的。」

資料保留

12. 保障資料第 2(2)原則訂明資料保留的原則：—

「*須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的（包括任何直接有關的目的）所需的時間。*」

資料保安

13. 保障資料第 4(1)原則訂明資料保安的原則：—

「 *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、喪失或使用所影響，尤其須考慮—*

(a) *該資料的種類及如該等事情發生便能做成的損害；*

(b) *儲存該資料的地點；*

(c) *儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；*

(d) *為確保能查閱該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) *為確保在保安良好的情況下傳送該資料而採取的措施。*」

14. 根據《私隱條例》第 2(1)條，「*切實可行*」指「*合理地切實可行*」。

15. 保障資料第 4(1)(a)原則所述的「損害」測試，需考慮資料使用者就其持有的個人資料而採取的保安措施是否與資料的敏感程度及資料被未獲授權或意外查閱所導致的損害相稱。

資料外洩事故

16. 《私隱條例》沒有界定何謂資料外洩事故，但一般指資料使用者持有的個人資料懷疑或實際外洩，當中包括資料遭受遺失、未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險、未獲授權取覽或查閱及轉移、不當棄置或管理含有個人資料的文件等。

資料外洩事故通報

17. 雖然目前《私隱條例》並沒有強制規定資料使用者必須向專員或受影響的資料當事人通報資料外洩事故，但專員已出版經修訂的《資料外洩事故的處理及通報指引》[1]，建議資料使用者在發生資料外洩事故時須依從的步驟。

[1] https://www.pcpd.org.hk//chinese/resources_centre/publications/files/DataBreachHandling2015_c.pdf

III. 調查所取得的資料及證據

18. 專員在進行調查的過程中，審視及考慮了康健提供與該事件有關的資料，包括對康健處理醫療紀錄的程序及所採取的保安措施進行了六次的查訊。專員亦派員前往該醫務中心進行實地視察，以了解該醫務中心處理及儲存有關醫療紀錄的處所的佈局及所採取的保安措施。此外，專員亦考慮了康健在該事件發生後的跟進及補救工作。

公司背景

19. 康健在香港營運超過 100 間醫務中心，包括普通科醫務中心、專科中心及牙科中心等。康健屬康健國際醫療集團的全資附屬公司。

20. 該醫務中心的地址為香港炮台山電氣道 160 號木蘭苑地下 D2 舖。

該醫務中心的正門

受影響的個人資料

21. 根據康健提供的資料，該紙箱載有該醫務中心 294 名病人的醫療紀錄，當中 292 名病人已超過七年未曾前往該醫務中心求診，其餘兩名病人則於 2019 年最後一次前往該醫務中心。該紙箱的醫療紀錄載有相關病人以下的個人資料：

(i) 姓名

(ii) 電話號碼

(iii) 香港身份證號碼

(iv) 地址

(v) 出生日期

(vi) 病人編號

(vii) 醫療卡號碼

(viii) 診斷紀錄

(ix) 使用藥物紀錄

(x) 實驗室結果

康健的資料保安政策

22. 在調查過程中，康健提交了以下與保障醫療紀錄相關的政策和指引：—

23. 康健向私隱公署提供了一份沒有正式名稱，聲稱是康健向前線員工發出有關處理個人資料的指引，當中包含五項有關康健對員工處理客戶個人資料的要求，以及三項有關處理資料外洩事故的規定，當中列明：「*離開工作崗位前，均需確保任何客戶資料已存放妥當（例如：病人資料需反轉或作遮蓋）以免讓第三者或以外的人仕容易看到，方可離開其工作崗位。*」

24. 康健向私隱公署提供另一份沒有正式名稱，聲稱是康健向員工提供有關醫療紀錄的處理、使用及儲存的指引，訂明員工在處理、使用和儲存醫療紀錄方面的應有行事方式。然而，這份醫療紀錄指引未有提及處理「不活躍醫療紀錄」的規定及程序。

「*清潔守則*」

25. 康健表示所有醫務中心的員工在處置廢物時均須遵守這份「*清潔守則*」，而康健在聘用清潔工時會向他們提供該份守則。專員特別注意到「*清潔守則*」的以下兩項規定：

(i) *清潔人員不可擅自取走或棄掉診所任何文件及『所有物品』，除垃圾桶內的垃圾必須清理。*

(ii) *未經負責人許可，不可擅自取走或棄掉診所櫃內、架上、檯上及醫生房內的『所有物品』。『所有物品』包括：所有藥物、醫療物品、醫療用具、醫療器皿、病人記錄、有個人資料之表格、病人醫療報告及 X-ray 片、電腦所有軟件、硬件等...*

26. 康健表示在該事件發生之前已把上述三份指引張貼在各醫務中心的牆壁或櫃上，康健的優質服務部及區域主管須共同確保各醫務中心的員工依循這三份指引的規定行事。

康健對該事件的解釋

27. 康健表示，根據一貫程序，旗下的醫務中心（包括該醫務中心）會將過去三年內曾前往醫務中心的病人醫療紀錄存放在有關醫務中心的檔案櫃，以便在這些病人求診時使用。同時，醫務中心會將超過三年未有前往有關醫務中心就診的病人的醫療紀錄歸類為「不活躍

醫療紀錄」，並會定期安排將這些醫療紀錄搬移至康健的中央倉庫儲存。

28. 就該醫務中心而言，病人的醫療紀錄存放在登記檯後的檔案架上，只有職員或獲授權人員才能存取。

29. 2021 年 3 月 14 日，該醫務中心的一名醫護助理（該醫護助理）對檔案架上的醫療紀錄進行檢視，以抽取「不活躍醫療紀錄」。過程中她把這些紀錄放入該紙箱中，以便稍後安排運往康健的中央倉庫儲存。由於該醫護助理未有即時完成檢視並打算於翌日繼續進行工作，她遂將該紙箱臨時放置在醫護助理的工作範圍的地上（即登記檯後面垃圾箱附近的位置）。負責該醫務中心清潔工作的該清潔工誤把該紙箱當成廢物，於當日中午將其運離該醫務中心棄置。

30. 2021 年 3 月 15 日早上，該醫護助理發現遺失了該紙箱，遂將事件通知主管。

31. 2021 年 6 月 2 日，康健向私隱公署作出資料外洩事故通報，表示一名受聘於康健的清潔員工於 2021 年 3 月 14 日錯誤地將一個載有病人醫療紀錄的紙箱當作廢物處理並棄置。

該事件的其他資料及證據

32. 康健表示，該清潔工解釋由於該紙箱沒有貼上標籤，並且放置在垃圾箱附近，他因而誤把該紙箱當作廢物棄置。

33. 康健向專員提交了事發時的閉路電視影像，片段顯示該清潔工把該紙箱移往該醫務中心的出入口方向。從影像中可見，該紙箱是一個普通的硬皮紙箱，體積約為 40 x 30 x 20 立方厘米，紙箱頂部是開啟的。

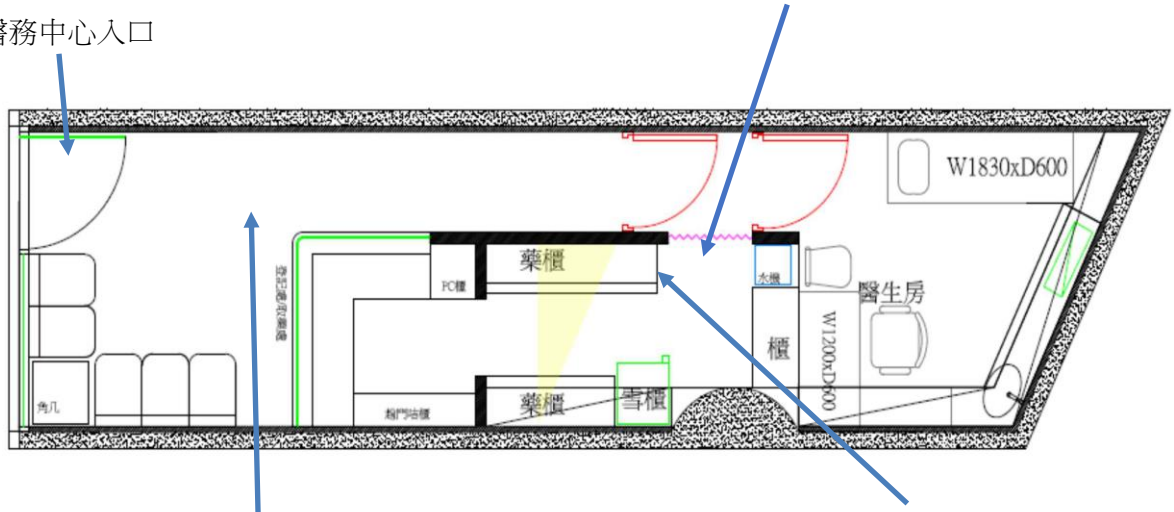
34. 康健相信該紙箱已與其他一般廢物一併被棄置於北角油街的垃圾收集站內（距離該醫務中心約 200 米）。

35. 根據康健提供的資料，以及私隱公署人員在該醫務中心的實地觀察所見，該醫務中心的範圍可分為三個主要部分：(i) 病人等候區； (ii) 醫護助理的工作範圍（主要是登記檯後面的空間）；及 (iii) 醫生會診室。在該清潔工移走該紙箱之時，該紙箱的存放位置是醫護助理的工作範圍內靠近垃圾箱的地板上。

36. 以下展示了由康健提供的該醫務中心平面圖，以及該醫務中心內部的照片，並標示了事發時該醫護助理存放該紙箱及垃圾箱的位置：

醫護助理工作範圍[2]

醫務中心入口



該醫護助理存放該紙箱及垃圾箱的位置

該清潔工把該紙箱移往該醫務中心的出入口方向

載有 294 名病人醫療紀錄，
被誤以為廢物棄置的紙箱

[2] 圖中所示的垃圾箱位置並非事發當時的位置

37. 康健承認當日該醫務助理放置該紙箱的位置並不合適。另外，康健表示該醫務中心於 2021 年 3 月 12 至 13 日期間曾進行裝修工程，包括小型天花板工程、照明工程和醫生會診室的翻新工程。康健的代表在私隱公署人員進行實地視察時表示，該清潔工有可能誤以為該紙箱是上述裝修工程所產生的廢物而將該紙箱棄置。

38. 康健承認在該事件發生之前未曾向前線員工提供任何有關保障個人資料的培訓。

39. 該紙箱除存放了 292 份「不活躍醫療紀錄」外，亦存放了兩份近年的醫療紀錄。康健推測該醫護助理將該兩份醫療紀錄從檔案架上取下後，暫時放進該紙箱以待檢視，而又因未完成檢視而暫存在內。

跟進工作及補救措施

40. 康健表示在得悉該事件後，立即派員前往前述的垃圾收集站及該醫務中心附近的回收公司尋找該紙箱的下落，但未能尋回該紙箱。

41. 康健表示他們已致電通知兩名於 2019 年最後一次前往該醫務中心而受事件影響的病人，亦已向其他受影響的病人發信。

42. 康健辭退了該清潔工，改為聘請外判清潔公司負責旗下醫務中心的清潔工作。

43. 康健於 2021 年 5 月對「*清潔守則*」進行了修訂[3]，加入以下規定：

(i) *所有垃圾和需棄置之物品必須放入垃圾桶內*；

(ii) *如未能放入垃圾桶內之垃圾，請放入垃圾袋或紙箱內並須於外面張貼註明是「垃圾」標示，放置特定位置，並必須預先通知負責清潔人員清理*；及

[3] 修訂後的守則名為「*處理垃圾及清潔守則*」。

(iii) *清潔人員不能棄掉醫務中心任何印有個人資料的物品。*

44. 康健向外判清潔公司提供了經修訂的「*清潔守則*」，並指示他們需確保其員工在康健的醫務中心執行清潔職務時遵守守則的規定。 此外，康健要求各醫務中心指派一名醫護助理對清潔公司的表現進行季度評估，包括清潔公司是否有依照「*清潔守則*」的規定行事。

45. 康健亦更新了醫療紀錄指引，加入妥善處理「不活躍醫療紀錄」的標準操作程序，當中明確要求任何載有「不活躍醫療紀錄」的儲物箱必須貼上標籤及註明內容、載有醫療紀錄的儲物箱不能在無人看管的情況下放置在地上，及儲物箱應在員工下班離開醫務中心前放置在指定位置。

康健對延遲作出資料外洩通報的回應

46. 在調查的過程中，專員曾詢問康健在得悉該事件後接近三個月（即 2021 年 6 月）才向私隱公署作出該資料外洩事故通報的原因。康健表示該事件的內部調查於事發後隨即展開，並於 2021 年 4 月仍繼續進行中。然而，由於康健沒有保存所有與該事件相關的紀錄，加上事發時負責調查及處理該事件的相關職員（包括一名總經理）經已離職，故康健未能確定延遲作出資料外洩事故通報的原因。

IV. 調查結果及違例事項

47. 根據保障資料第 4(1)原則，資料使用者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受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。在本個案中，專員考慮的因素包括：(i) 該事件是否屬資料外洩事故；(ii) 誰是需為該資料外洩事故負責的資料使用者；及(iii) 涉事的資料使用者是否已按保障資料第 4(1)原則的規定採取切實可行的步驟保障其持有的個人資料。

48. 此外，根據保障資料第 2(2)原則，資料使用者須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的所需的時間。在本個案中，專員亦已考慮涉案的個人資料的性質及其保存時間是否恰當。以下是專員的調查結果。

該事件的性質

49. 資料外洩事故一般指資料使用者持有的個人資料懷疑或已遭外洩，令此等資料被遺失或被未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，從而違反保障資料第 4(1)原則的規定。

50. 基於康健在該資料外洩事故通報中提供的資料，以及在調查過程中提供的進一步回覆，專員確定該事件屬資料外洩事故，當中該醫務中心意外棄置了一個載有醫療紀錄的紙箱，喪失 294 名病人的姓名、電話號碼、香港身份證號碼、地址、出生日期、診斷紀錄、使用藥物紀錄及實驗室結果等。

康健屬該事件的資料使用者

51. 該紙箱內的醫療紀錄是由該醫務中心收集，而該醫務中心是康健營運的。因此，康健屬《私隱條例》第 2(1)條釋義下的資料使用者，

須遵從《私隱條例》的規定行事，包括《私隱條例》附表一所列明的六項保障資料原則。

資料保安的嚴重不足

52. 保障資料第 4(1)原則訂明，資料使用者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受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮－

(a) 該資料的種類及如該等事情發生便能做成的損害；
(b) 儲存該資料的地點；
(c) 儲存該資料的設備所採取（不論是藉自動化方法或其他方法）的保安措施；
(d) 為確保能查閱該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) 為確保在保安良好的情況下傳送該資料而採取的措施。

53. 經考慮與該事件有關的事實及在調查過程中所獲得的證據，專員認為康健在員工的資料保障意識、政策層面，以至培訓方面都存在嚴重不足，是導致該紙箱遭意外棄置的主要原因。

(1) 員工的資料保障意識欠奉

54. 專員認為以下兩項單一事件導致該事件的發生：—

(i) 該醫護助理將該紙箱存放在工作範圍垃圾箱附近的位置；及
(ii) 該清潔工把該紙箱當作廢物處置。

55. 人為因素往往是資料外洩事故的主要起因，專員認為該事件亦不例外。 在該事件中，該醫護助理及該清潔工明顯地缺乏資料保障的意識，輕率地處理屬敏感性質的醫療紀錄。

56. 該醫護助理日常處理該醫務中心的大量醫療紀錄，因而掉以輕心，為了其工作便利，在暫停進行檢視「不活躍醫療紀錄」程序時未有把載有 294 名病人醫療紀錄的該紙箱妥善放置（例如將該紙箱蓋上並放在一個較隱蔽的位置，甚或將其放入上鎖的櫃內），亦未有貼上任何標示說明箱內載有甚麼物品及其用途。反而，該醫護助理將該紙箱放置在垃圾箱附近，完全漠視該紙箱所載的個人資料的重要性，做法屬明顯的疏忽，是直接導致該事件發生的主要原因。在調查的過程中，康健亦承認該位置（即垃圾箱附近）並非放置該紙箱的合適位置。以上反映了該醫護助理在資料保障方面的態度輕率。

57. 再者，該醫務中心在該事件發生前一天剛完成裝修工程，該醫護助理理應對該紙箱的保安情況格外留神，然而該醫護助理卻忽視了這方面的風險，隨意放置該紙箱，這或令該清潔工誤以為它是可被棄置的廢物。

58. 該清潔工單憑該紙箱放置在垃圾箱附近，便把該紙箱當作廢物棄置。從閉路電視影像可見，該紙箱是打開的，若該清潔工注意到該紙箱內盛載著文件，應在棄置前先主動向該醫務中心的職員查詢。

(2) *<u>欠缺有效的政策及程序</u>*

59. 所有收集及保留個人資料的資料使用者應制訂風險管理政策、進行盡職審查及資料私隱影響評估，以確保能識別出可能引致未經授權或意外遺失或使用資料的潛在風險和情況，並採取合理地切實可行的步驟和實施適當的保安政策及措施，以降低這些風險。

60. 康健是一間具規模的醫療服務機構，在本地經營超過 100 間醫務中心，恆常地持有並處理大量屬敏感性質的病人醫療紀錄。因此，康健應制訂全面的政策及程序以保障病人的醫療紀錄，合乎病人及持份者的期望。然而，專員在調查期間發現康健在這方面的表現嚴重不足。

61. 在調查過程中，雖然康健向專員提供的三份指引內的某些部分提及保障病人醫療紀錄的規定，但指引內容明顯不全面亦不具體，不足以防止該事件的發生，理由如下：—

62. 康健向前線員工提供有關處理客戶個人資料的指引，以及有關醫療紀錄的處理、使用及儲存的指引。專員注意到這兩份指引並無提及醫護人員在進行檢視「不活躍醫療紀錄」程序時的行事方式及應採取的保安措施，而只載列一般性的要求：

> 康健向前線員工提供有關處理客戶個人資料的指引訂明：「*離開工作崗位前，均需確保任何客戶資料已存放妥當（例如: 病人資料需反轉或作遮蓋）以免讓第三者或以外的人仕容易看到，方可離開其工作崗位*」。

63. 專員認為上述指引內容並不清晰、有欠具體，例如在此個案中，該紙箱放置於垃圾箱附近的位置是否代表已將該紙箱妥當存放？在調查過程中，康健向專員表示該醫護助理在該事件中並沒有違反指引。因此，專員認為即使康健有向該醫務中心的前線員工傳達上述指引的規定，亦無助預防該事件的發生。

64. 另一方面，專員認為康健的「*清潔守則*」屬康健的標準作業指引，但內容亦有欠清晰，故即使該清潔工依據「*清潔守則*」的規定行事，亦不一定能避免資料外洩事故。

65. 專員認為若然「*清潔守則*」清楚列出禁止棄置的物品種類外、清晰界定物品被視為可被棄置廢物的準則，例如存放的位置或任何可供識辨的標籤，錯誤棄置該紙箱的情況或可避免。

(3) *<u>欠缺員工培訓</u>*

66. 在調查的過程中，康健承認未曾向前線的員工提供個人資料保障方面的培訓。

67. 專員認為，所有資料使用者均有責任培訓負責處理個人資料的僱員，以作為保障個人資料的其中一項措施，這尤其對於需要處理敏感性質的醫療資料的康健來說屬不可或缺。因此，專員認為康健未有向處理該醫務中心內的前線員工提供保障個人資料方面的培訓，也是導致這次資料外洩事故的重要因素。

資料保留

68. 資料使用者在收集個人資料後，須慎重考慮應保存的時間，因為不必要地或過長地保留個人資料，將無可避免地造成或增加資料外洩的風險。

69. 根據康健提供的資料，該紙箱載有準備搬移至康健的中央倉庫儲存的醫療紀錄，這些紀錄屬於超過七年未曾前往該醫務中心求診的292名病人，以及兩名於2019年最後一次前往該醫務中心的病人。

70. 專員考慮到為應付病人可能再次求醫或要求索取其醫療紀錄的情況，醫療機構在一般情況下有實際需要把醫療紀錄存放一段較長的時間。整體而言，專員認為本個案沒有資料顯示康健涉及過長時間地保存於該事件遺失的醫療紀錄，康健並**沒有違反**《私隱條例》附表一保障資料第2(2)原則有關資料保留的規定。

資料外洩事故通報

71. 儘管《私隱條例》沒有規定資料使用者須向專員及資料當事人通報資料外洩事故，亦沒有規定資料使用者須在指定時間內作出通報，

專員留意到，康健於 2021 年 6 月 2 日向專員通報該事件，並採取步驟通知資料當事人（即受影響病人）。

72. 然而，考慮到該事件所涉及的個人資料的敏感性質（即醫療紀錄），專員認為康健可在更早的時間作出資料外洩事故通報。**專員對康健在該事件發生接近三個月後才作出該資料外洩事故通報，表示遺憾。**

結論 — 違反保障資料第 4(1)原則

73. 專員認為醫療紀錄屬性質敏感的個人資料，康健作為管理過百間醫務中心的資料使用者，持有大量市民的醫療紀錄，理應就收集、持有、處理及使用這些醫療紀錄制訂完善的政策、進行適當的風險評估、向員工提供足夠的培訓以灌輸個人資料保障意識，並按照保障資料第 4(1)原則採取所有切實可行的保安措施，以確保由資料使用者持有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、喪失或使用所影響。

74. 康健在個人資料保障方面的嚴重不足，導致載有該醫務中心病人的醫療紀錄的該紙箱在可以避免的情況下遭意外棄置。該紙箱自該醫務中心被運往垃圾收集站約 200 米的路程中，及在垃圾收集站內的時候，一直處於可被人隨意查閱或拿取的狀態。任何人士均有機會取得該些醫療紀錄。

75. 在考慮本個案所有有關的證據及是次資料外洩事故中的所有相關情況，專員認為康健：—

(1) 沒有檢視及評估人為疏忽的風險，以致未能採取適當措施應對因員工欠缺保障個人資料的意識而存在的風險；

(2) 沒有制訂清晰及足夠的資料保安政策及指引，以保障性質敏感的個人資料；及

(3) 沒有就妥善處理個人資料向所有相關人士提供足夠培訓。

76. 在本個案中，專員發現康健在個人資料的保安方面存在嚴重不足，專員認為康健沒有採取所有切實可行的步驟以確保涉事的醫療紀錄受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了保障資料第 **4(1)**原則有關個人資料保安的規定。

V. 執法行動

77. 專員認為康健違反了《私隱條例》附表一的保障資料第 4(1) 原則，因此已根據《私隱條例》第 50(1)條所賦予的權力向康健送達執行通知，指示康健採取以下步驟以糾正，以及防止有關違規情況再發生：

(1) 對適用於康健旗下的醫務中心有關資料保障方面的所有書面政策、標準操作程序／指引進行全面檢視及更新，以提供具體的政策及操作程序／指引；

(2) 制訂有效措施，以確保員工依循更新後的有關資料保障的書面政策、標準操作程序／指引；

(3) 制訂有效措施，監督員工及任何負責在醫務中心執行清潔工作的第三方遵守「*清潔守則*」的規定；

(4) 為員工提供資料保障方面的培訓，並妥善記錄培訓進度，以及就員工培訓的參與及有效程度作出評估；及

(5) 由執行通知的日期起計兩個月內向專員提供文件，證明已完成上述第 (1)至 (4)項指示。

78. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

VI. 建議

醫療紀錄屬敏感個人資料 應加倍重視

79. 個人資料無論是遭意外丟失、洩漏還是不當處置，對個人潛在的傷害實在不容忽視，尤其是涉及屬敏感資料的醫療紀錄。醫療紀錄是醫療行業的重要資產，它包含有關個人健康和病史的資料，因此醫療機構應加倍重視有關資料，必須確保這些資料在其整個生命週期內得到妥善的管理，這不僅是為遵守《私隱條例》的規定，更是為病人負上道德責任的表現。

80. 正如我們在本個案中所見，雖然該事件從表面看來涉及一所醫療機構意外棄置了二百多份病人的醫療紀錄，屬單一事件，然而，專員的調查揭示了康健在個人資料的保安方面存在嚴重不足。若然康健只將該事件視為個別事件，而不採取治本的改善措施以加強保障個人資料私隱，相類似甚或更嚴重的資料外洩事故隨時都可以在康健旗下的任何一間醫務中心發生。幸而，康健重視專員對該事件的調查，並致力改善保障個人資料方面的政策及程序以避免類似事件再次發生。專員亦欣悉康健已委任資料保障主任負責監督康健內部有關保障個人資料私隱的事宜。

81. **專員建議，機構應建立及維持一套遵從《私隱條例》規定的系統，循規地使用及保留個人資料。個人資料私隱管理系統有助機構管理由收集至銷毀個人資料的整個生命週期，令機構可迅速應對任何資料外洩事故，並確保遵從《私隱條例》。同時，機構應委任保障資料主任，負責監察《私隱條例》的遵從並向高級管理層匯報。**

82. 除了制訂有效的保障資料政策和程序外，資料使用者應採取措施持續地檢視其僱員是否遵從這些政策和程序的要求行事，並為僱員提供全面的培訓，以降低人為錯誤的可能性。**專員建議，機構應全面提升僱員的個人資料保障意識，並為機構建立保障個人資料文化。**

機構應向僱員提供全面的培訓，將個人資料保障的意識滲入其日常工作之中，以減低因意識不足而引致的人為錯誤。

83. 雖然在數碼時代，資料外洩事故在網絡世界時有發生，但資料外洩事故在「離線」的世界亦不可忽視。除了康健應該從這次事件中汲取教訓，所有會以文件或其他實體形式處理個人資料的資料使用者也應予以借鏡，防範於未然。**專員建議，機構應同樣重視以電腦或實體系統處理資料的保安措施，採用可靠的系統及保安設置以保障系統免受網絡世界攻擊的同時，亦應投放資源，加強處理實體資料的保安措施。**

通報資料外洩事故非懲罰 資料使用者不應逃避

84. 專員留意到，很多資料使用者在面對資料外洩事故發生時，往往不知所措。儘管現行《私隱條例》沒有規定資料使用者必須向專員及資料當事人通報資料外洩事故，亦沒有規定資料使用者須在指定時間內作出通報。然而，事實上，當私隱公署收到資料外洩事故通報，會向資料使用者提供適切的建議，協助他們迅速應對資料外洩的事故，適時採取恰當的措施及行動，以減低資料外洩事故對相關機構及受影響的資料當事人的損害。私隱公署亦會提供建議，協助資料使用者完善他們處理個人資料的系統及政策，以避免同類事件再次發生。相反，一旦延遲處理資料外洩事故或向專員作出通報，資料外洩事故對相關機構及資料當事人的損害（包括情感及實際財務損害）可能倍增，甚至無可挽回。**專員建議，當資料使用者懷疑或發現資料外洩事故發生時，應盡快向私隱公署作出通報，讓私隱公署提供協助及建議，減低資料外洩事故的損害，以及改善處理個人資料的系統。**

85. 私隱公署正與政府研究修訂《私隱條例》的具體建議，當中包括設立強制性資料外洩通報機制。私隱公署將繼續積極進行相關工作，以更好地保障市民的個人資料私隱。

－完－