CALIFORNIA TELEHEALTH RESOURCE CENTER
Part of OCHIN

病人常見問題 (FAQ) – 網上診症安全

1. 如何知道視像探訪是安全的？

閣下需要知道閣下的醫生有責任在視像會議期間，保護閣下的私隱。Health Insurance Portability and Accountability Act (HIPAA) 最重要事項之一，是要求保護和安全處理某些資訊，被稱為「受保護的健康資訊」 (Protected Health Information) 。例如，閣下的醫生必須設有適當的系統，以確保僅獲授權人士方能查看閣下的健康資料。該資料是以白紙黑字紀錄，還是紀錄於電腦系統中，均需設有適當的系統。 HIPAA 規例也適用於任何透過互聯網傳送的資訊，包括視像探訪。

閣下的醫生必須使用符合 HIPAA 嚴格標準的虛擬解決方案，以遵守 HIPAA 的規定。若閣下對遙距醫療期間分享資訊，有任何私隱和安全相關問題或疑慮，請與閣下的醫生聯絡。

2. 哪些是虛擬診症的保障措施？

HIPAA 要求各位醫生整合各種加密和其他保護措施，至他們與病人的互動中。所有醫療專業人員或醫療組織，為身處家中或社區中心的病人提供遙距服務，均需要遵守 HIPAA 指引。HIPAA 私隱和安全規例，為可識別身分的健康資訊，提供各種保護。 HIPAA 的「私隱規則」 (Privacy Rule) 為可識別身分的健康資訊，建立各種使用和披露限制，而 HIPAA 的「安全規則」 (Security Rule) 則為保護可識別身分的電子健康資訊，建立各種技術、實際和管理上的保障措施。例如，在「安全規則」下，靜態和傳送資料的加密是「可尋址的實施標準」。這表示除不「合理和適當」的加密外，各個 HIPAA 涵蓋實體均需要加密。此外，此規例也規定醫生必須採用各種身份管理協定和存取控制。

3. 遙距醫療探訪時，使用公共 Wi-Fi 會有哪些風險？

雖然咖啡廳、圖書館、機場、酒店和其他公共場所的 Wi-Fi 熱點是便利，但一般都是不安全的。儘管需要密碼方可登錄，但未必表示已加密閣下的線上活動。公共 Wi-Fi 可能會因各種理由，而造成閣下容易受到攻擊。當中理由之一是與某些無線網絡所用的加密協定相關，而另一個理由是可能連接假冒或惡意 Wi-Fi 熱點。因此，不建議使用公共 Wi-Fi 熱點作虛擬探訪。請考慮使用移動數據，而不是 Wi-Fi 作為替代方案。 （注意：閣下可能因流動數據計劃，而需要為此數據使用付費）。

4. 哪些是常見的安全威脅？

- **網絡釣魚攻擊**

  網絡釣魚者假冒可信賴的聯絡人時，發動網絡釣魚攻擊。網絡釣魚試圖誘騙用戶點擊惡意連結、下載惡意檔案或提供存取權限，以取得敏感資料、帳戶詳細資訊或身分驗證資訊。

- **惡意程式攻擊**

  惡意程式包括各種網絡威脅，如特洛伊木馬和病毒等。這些全部都與黑客建立惡意編碼有關，目的是獲得網絡存取權限、竊取資訊或破壞電腦資料。惡意程式通常來自惡意網站下載、垃圾郵件或與其他受感染裝置的連接。

- **勒索軟件**

  勒索軟件是一種特定類型的惡意程式，它會感染和限制讀取電腦資料，直至支付贖金為止。勒索軟件通常透過網絡釣魚電子郵件傳送，並利用軟件中尚未修補的漏洞。

- **「中間人」（MitM）攻擊**

  在這種情況下，攻擊者處於電子訊息的傳送者和接收者之間，建立一席位和截取當中的訊息，並可能會在訊息傳送過程中，改變當中的訊息。然而，傳送者和接收者皆認為彼此正在直接溝通。

---

5. 防病毒和抗惡意程式軟件如何保護電腦？

防病毒和抗惡意程式軟件的好處

- 即時檢查和防禦惡意程式、病毒和其他有害軟件
- 當中包括主動防勒索軟件、防漏洞檢測和回應組件
- 阻止黑客攻擊和揭發網絡釣魚企圖
- 以手動和預定掃描模式，提供靈活性
- 提供分層方法，以保護閣下的電腦

---

6. 遙距醫療探訪時，使用防火牆有哪些好處？

防火牆保護閣下的電腦或網絡，免受惡意或不必要網絡流量影響，以抵禦外部網絡攻擊者。防火牆還可以防止惡意程式，透過互聯網進入電腦或網絡，並可以設定允許相關和必要的數據通過，以阻止來自某些位置（例如：電腦網路位址）、應用程式或埠的數據。

7. 惡意程式是什麼？該如何避免？

「惡意程式」(Malware) 是「惡意程式軟件」的縮寫——黑客用來破壞裝置功能、竊取資料，甚至控制裝置本身的軟件。一般來說，當不知情用戶打開受感染檔案或瀏覽受感染網站時，無意中下載惡意程式。當它在閣下的電腦內，它會根據其設計發動特定類型的攻擊。例如，鍵盤記錄器記錄每次輸入，並報告該資訊予尋找用戶名稱、密碼和其他敏感身分驗證資訊的黑客。木馬偽裝成有用的或良性軟件——例如，假冒防病毒軟件或遊戲。這誘騙使用戶打開木馬，從而授予系統檔案的存取權限，或促使下載更多惡意程式。

閣下可以透過安裝防病毒軟件和進行例行掃描，以保護電腦免受惡意程式的攻擊。若閣下的電腦運作緩慢或執行異常指令（例如「提醒」下載奇怪軟件），則可能感染了惡意程式。請進行防病毒掃描，以檢查、識別和刪除裝置中的惡意程式。

8. 強密碼為何很重要？如何建立強密碼？

這不僅閣下遙距診症的密碼，而所有線上登入和帳戶，均務必建立獨一無二的強度密碼。強度密碼對於保護閣下的線上帳戶和個人資訊，免受網絡犯罪分子入侵是非常重要的。啟用雙重身分驗證，可提供額外安全保障。

建立強度密碼：

第 1 步：利用與閣下獨一無二記憶相關的五個不同單詞。（例如：Learntorideabikeatfive）

密碼越長，越難猜中。請勿用個人資料，例如閣下的姓名、國民身分證 (NRIC)、出生日期或其他可以透過線上搜索，輕鬆獲得的資訊。

第 2 步：採用大小寫字母、數字或符號，使密碼難以破解。（例如：LearnttoRIDEabikeat5）

請謹記保持密碼是隨機的，以確保是無法預料的模式，這表示即使他人利用特殊工具也難以猜中。明顯模式的例子如下：

- 使用常用短語（例如：maytheforcebewithyou）
- 密碼的第一個字母為大寫（例如：Livelongandprosper）
- 在密碼末增加一個數字（例如：qwerty1）
- 利用數字或符號取代字母（例如：p@ssw0rd）

閣下現已成功建立強度密碼，請啟動 2FA。這代表雙重身分驗證，為閣下的帳戶增加額外安全保障。

9. 如何更新互聯網瀏覽器，以保護電腦？

閣下的互聯網瀏覽器更新，可針對詐騙、病毒、特洛伊木馬、網絡釣魚攻擊和其他威脅，提供有效的保護。它還可以解決當前瀏覽器中，存在的安全漏洞。許多瀏覽器更新發布，以解決這些實際問題。為了最安全使用互聯網，請使用作業系統支援的最新版本瀏覽器。

11. 哪些騙局需多加注意？

請勿打開可疑附件或點擊郵件中不尋常的連結，而它們可以出現在電子郵件、推文、帖子、線上廣告、訊息或附件中，並有時偽裝成已知和可信賴的訊息來源。

了解如何以及何時聯絡閣下進行遙距醫療探訪，或獲取任何後續資訊。若閣下收到遙距醫療探訪相關的可疑電話或電子郵件，請與閣下的醫生聯絡。安全總比後悔好。

12 網絡釣魚是什麼？該如何避免？

網絡釣魚是指以惡意為目的，而設計的任何數碼或電子類型通訊。它是一種使用假冒和欺騙手段的社交工程攻擊，通常說服無辜的受害者提供個人資料，例如登入身分驗證資訊、銀行賬戶資訊、社會安全號碼或其他敏感資料。

網絡犯罪分子的目標是利用這些資訊，以某種方式欺騙受害者——偷錢、接管一個或多個賬戶、建立新詐騙賬戶或增加信用卡簽賬。在某些情況下，攻擊者的最終目標是利用惡意程式，以控制受害者的裝置。犯罪分子還可能希望（透過受害者）存取其他有價值的資源，包括企業網絡、系統、資料或知識產權。

為個人提出的建議：

- 警惕所有非應邀的電子郵件和短訊。
- 鼠標停留在嵌入式連結上（毋需點擊），以顯示實際 URL，並比較所示的連結。
- 即使閣下認為嵌入式連結是可信的，也請勿點擊。然而，請利用瀏覽器，搜索正確的 URL。
- 請勿打開非應邀電子郵件中，任何類型的附件。然而，來自已知寄件人的電子郵件，則先另作驗證，方打開該電郵中的附件。
- 請聯絡閣下的醫生，了解電子郵件或短信內的嵌入式連結或附件，以驗證此資訊，並確保閣下的私隱得到保護。
- 在閣下的個人裝置，使用和更新防病毒和抗惡意程式軟體。
- 每個帳戶均使用多重身分驗證（如有），有助防止網絡犯罪分子存取閣下的帳戶。

13. 應該如何備份資料？

閣下可以使用外部媒體或雲端為本服務，定期備份於裝置上建立和儲存的有價值資訊。此過程可透過利用第三方備份應用程式，作簡化和自動化。請務必加密備份，以保護資料機密和完整。若資料遺失、損壞、感染或被盜，資料備份對盡量減低負面後果，非常重要。

14. 在遙距醫療診症前，應該移除哪些物品？

開始與閣下醫生交談前，請確保已移除非健康問題討論所需的物品。應移除各種非用於聯絡閣下醫生的資訊科技裝置，例如家庭安全攝影鏡頭或語音助手等，以免紀錄潛在敏感資訊。