正本

檔　　號：
保存年限：

收文日期 112.10.18
編　　號 2822

新北市政府衛生局 函

地址：220205新北市板橋區英士路192之1號
承辦人：張雅玲
電話：(02)22577155 分機2139
傳真：(02)22557926
電子信箱：af3249@ntpc.gov.tw

22069
新北市板橋區三民路2段37號11樓

受文者：社團法人新北市牙醫師公會

發文日期：中華民國112年10月13日
發文字號：新北衛醫字第11219994901號
速別：普通件
密等及解密條件或保密期限：
附件：基層醫療院所資安防護參考指引1份

裝

主旨：為提升個資保護意識及加強防護措施，提供衛生福利部「基層醫療院所資安防護參考指引」，惠請協助轉知基層醫療院所，請查照。

說明：

一、依衛生福利部112年10月6日衛部口字第1122060943號函辦理。

訂

二、檢附基層醫療院所資安防護參考指引1份，並公告於本局網站供下載參閱，建請善用指引中之「資訊安全自我檢核表」，以強化診所內的資訊安全措施，防止非公務機關個資外洩。

正本：社團法人新北市醫師公會、社團法人新北市牙醫師公會、社團法人新北市中醫師公會
副本：

線

局長 陳潤秋

本案依分層負責規定授權業務主管決行

衛生福利部

基層醫療院所資安防護參考指引

衛生福利部資訊處

中華民國 109 年 8 月 17 日

目錄

壹、前言

醫療領域具高度醫療專業、精密儀器設備佈署及巨量病患隱私資料等特性；醫療系統之高度資訊化與醫用儀器聯網應用不斷提升的趨勢，網際網路安全與個資保護已然成為醫療產業所面臨的重要課題與挑戰。

對醫療機構而言，醫院間需要進行必要的病歷資料分享，以能更有效率的做到疾病治療並優化病患照護。醫療機構對病患有病歷資料保密義務；目前醫療機構的行政管理重心大多放在如何進化病歷資料分享這個環節。整體醫院資訊化的規劃範疇，往往只注意到如何提昇醫療專業技術及醫療服務品質，在資訊安全的投資相形見絀，以致資安觀念的提升與落實亦較為緩慢。

正如歷年來多數遭駭的醫療院所，在事件發生後檢討其資安防禦的設備或觀念的確相對落後，資安佈署不夠縝密周延，資料備份作業不確實，甚至依舊使用無法更新作業版本的老舊系統...等會是讓自身醫療/醫務系統暴露在高風險的資安威脅之下，都將可能造成超乎預期的損失，影響其醫療經營的專業形象。

一、 國內外醫療產業資安事件的省思

2017 年勒索病毒 WannaCry 就曾造成一百五十個國家、二十萬台以上電腦中毒，當時英國的醫療系統（NHS）也遭受了嚴峻考驗，據 CNN 報導，大約有許多家醫院遭到大範圍攻擊而無法正常運轉，這些被攻擊的醫院，內網被攻陷、電腦被鎖定、電話不通，駭客勒索要求每家醫院需支付一定數量的比特幣作為贖金，否則將刪除所有資料；當時造成受害醫院手術因此被迫取消，救護車轉院等醫療救護的困擾。

2019 年 8 月據媒體報導國內有多家醫療院所遭受駭客攻擊，病歷資料被駭客加密勒索，威脅需支付虛擬貨幣來保存資料。這次事件，衛福部證實於事件發生當日即接獲情資，於次日由電子病歷交換中心平臺發出 EEC GATEWAY 故障排除建議程序的公告，也證實該事件有多家醫院受害。所幸各院所工作電腦主機已及時復原，不致影響醫療業務運

作，也無傳出個資外洩的狀況。然而此次的攻擊事件又再次突顯出醫療資訊系統仍存在著未知的資安弱點，故平時的高度的資安維安概念、發生資安事件能即時查找原因並能緊急應變得宜才能將資安威脅造成的風險降到最低。

鑑於國內外多起資安威脅所造成的影響，醫療領域資安聯防的建立已刻不容緩。這也正是 2019 年正式施行的資安管理法將醫療業（關鍵基礎設施）納入管理的主要目的。衛福部於 2018 年已完成醫療資安資訊分享及分析中心(H-ISAC)之建置，與轄下 CI 醫院合作進行資安聯防，彼此分享即時醫療情資。於 2019 年度接續建置通報應變中心(H-CERT)及並規劃於 2020 年度完成二線監控中心(H-SOC)之建置。同步也著手進行資安防護基準(baseline)之訂定，以供基層醫療機構(含診所)能藉此加強資安概念以逐步落實醫療資安防護。

智慧醫療時代的來臨，國內醫療體系將面臨更嚴峻的資安挑戰與威脅。各醫療單位除依靠來自政府各領域資安所建置的資安防護支援外，在資安建設方面，各醫療單位自身亦需投入更多的資源以做到資安防護的強化，內部人員資安概念的提升與落實也屬之必然且刻不容緩。綜合以上，才得以因應無可預知且攻擊手段不斷演化的資安威脅。

二、 基層醫療院所常見的資安事件類型與因應

目前醫療機構在資安投資與認知的普遍不足，而較無經費規劃佈署專業資安人員駐守的基層診所或是區域醫院或地區醫院更可能因疏於資安管理，成為駭客入侵潛伏的跳板對象；駭客入侵後經潛伏一段時間，極有可能透過虛擬私人網路（VPN，如健保 VPN）或其他受信賴的網路連結模式入侵醫療資源核心以發動大規模的感染或攻擊。

遭受攻擊的醫療機構若無完整的資安防護，除了將影響其醫療運營之外，更可能因此成為駭客利用的對象，透過網路並利用作業系統漏洞竄至核心醫療機構，再經平行感染後造成大規模的資安威脅，進而導致整體醫療營運停擺的連鎖反應，釀成難以想像的巨大損失。因基層醫療院所的網路存取應用較為單純，診所或小型醫院鮮少會佈署機房架構網路環境，故資安威脅型態大多會以遭受病毒感染的模式，可能是經由社

交工程郵件或釣魚站網下載夾帶惡意程式的軟體潛伏在系統為主。

常見的資安事件如 DDoS 攻擊造成網路癱瘓導致服務中斷及從 2016 年開始出現爾後猖獗於各重要領域造成資安威脅的加密勒索病毒(Ransomware)，還有利用社交工程郵件以釣魚的方式誘引後植入惡意程式所造成的資安威脅。另外，內部人為的不當行為造成的意外或非意外的資料遺失、疏於資安防護的操作科技(OT)應用的連網醫療設備等也都會造成醫療領域的資安問題；而無完善的資安機制管理，也將會影響到既有的醫療服務以及醫療個資的外洩，不得不謹慎以對。

倘若基層醫療院所於平時就有離線備份資料的良好習慣，並且隨時提醒院所成員提升必要的資安概念之外，在遇到資安威脅時，做到即時通報並妥善後續處理才能避免因資訊外洩而受害。而以下，針對勒索病毒與 DDoS 攻擊做重點說明，並提供處理方式如下供參：

1. 加密勒索病毒：

- 狀態：電腦資料被加密鎖定並遭勒索
- 說明：新型的勒索病毒 WannaCry 至今仍橫行歐洲、俄羅斯及台灣，包含金融體系、高科技產業及醫療體系中部分單位都遭受過其威脅攻擊。所謂的勒索病毒是會將電腦中的檔案加密，並要求限期三天內支付其要求的金額或是虛擬貨幣作為贖金。若不付款，贖金會再加倍，七天內沒有付款，就會刪除解密金鑰，檔案即無法回復。
- 基層醫療院所因應方式：

I. 預防：

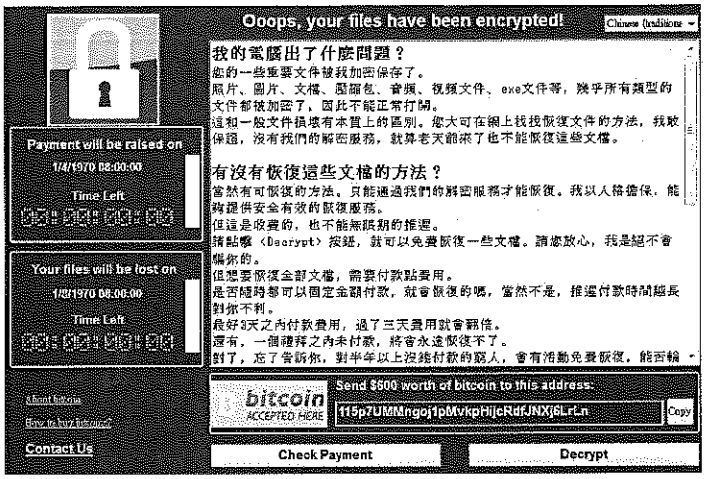
➢ 此常見於微軟漏洞遭駭客利用作為攻擊途徑之應用。故定期更新作業系統或儘速更新作業系統以避免遭遇此類型資安威脅，甚或成為駭客的中繼跳板，對上感染至上級主管機關，進而擴散至其他連結的醫療單位，導致業務營運中斷或經營損失。

➢ 定期資料離線備份(病歷資料與診所營運之業務資料)。

➢ 醫護人員及員工都必須具備高度資安意識。

II. 遭遇入侵之通報處理：

如電腦以遭駭客鎖定入侵(如下圖)，則須立即通報主管機關(如各縣市衛生局)，以儘速做必要的網路隔離及啟動相關防禦機制，並主動報警處理與備案



圖一 加密勒索病毒入侵電腦畫面示意

2. DDoS 攻擊(分散式阻斷服務攻擊)

- 狀態：對外聯網無效，網際網路無法發揮作用。

- 說明：此攻擊手法主要是透過大量合法或偽造的請求占用大量網路以及設備資源，以達到癱瘓網路及系統之目的。這樣的攻擊手法及對象會是選定具有對外服務之系統網路維運環境的醫療院所，如醫學中心或區域醫院等級的醫療院所就會是此手法的主要攻擊對象或目標。而這樣的資安威脅因網路應用條件不足，不會發生在基層小醫院及診所。

- 基層醫療院所因應方式：如上所提，此攻擊手法不會作用在小型醫療院所，而中大型的醫療院所如遭遇到網路被癱瘓導致無法對外順利聯網存取，這就可能是遭受到 DDoS 攻擊的型態，可請求與院所配合的資安廠商協助處理，並通報業務主管機關。

然若基層醫療院所僅以電腦作為醫務作業相關使用，以ADSL 對外作為對外的網路連線，無內建網路環境設置，就比較不會遇到這樣的攻擊威脅型態。這樣的攻擊型態經過及時且適當的處理，不致造成營運資料的遺失；但即便如此，平時提升醫護人員及員工的資安意識仍是不在話下，須落實執行且養成固定資料備份的習慣以避免無謂的資料損失影響病患的權益。

貳、診所篇

基層診所通常沒有專屬的資訊人員或資安人員，並大多利用電腦、筆電執行醫療約診、病歷資料記載並透過簡單的網路連結模式對外聯網，透過健保 VPN 完成與健保署的健保資料界接。

根據美國 Healthcare & Public Health Sector Coordinating Councils 的報告(Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients)指出，58%的惡意軟體攻擊受害者是小型企業，9 成的小型企業根本不使用任何資安措施來保護公司與客戶的資料，6 成的小型企業在遭受攻擊後的 6 個月內破產。而在醫療領域中的基層醫療院所也可能面臨類似的資安隱憂，故資安概念的提升與合宜的資安措施也是當務之急。

對於診所內的資訊安全措施，建議可以如下指引自我檢核與改善執行：

一、 電腦須安裝防毒軟體並隨時更新作業系統。

許多的惡意攻擊程式是透過作業系統的漏洞滲透執行。所以使用無法更新作業版本的老舊系統須儘速汰換，並應安裝合法的防毒軟體，或至少更新至 Windows 10 並開啟內建之 Windows defender 進行防護。

二、 強化內部基層及管理人員資安意識

1. 診所員工到職時，建議提供資訊安全相關之教育訓練至少 3 小時。
2. 診所員工每年至少接受 3 小時之資安教育訓練課程。
3. 於診所電腦的明顯處提醒 USB 限用機制，也可以友善提醒資安宣導標語。例如以下：
   - ✓ 資安守則最重要；權限控管要確實。
   - ✓ 密碼外洩風險高；定期更改才安全。
   - ✓ 機密資料慎處理；個人資料要保密。

- ✓ 不明軟體勿下載；駭客入侵機會少。
- ✓ 網路安全要規範；資安檢核要精實。

4. 建議可由診所委外廠商協助提供相關教育訓練，並提供專業訓練教材(如影片檔、資安基礎文件等)，若廠商增設線上學習系統設定學分制以規範從業人員取得學分，並委由合格廠商執行訓練並發給證明尤佳。

三、 加強委外廠商管理

1. 外包廠商須充分了解資訊安全對醫療院所之重要性，建議診所可提供資訊安全宣導文件給廠商並由廠商閱讀後簽署留存。

2. 外包廠商使用 USB 存取診所裝置時，須由最新版之防毒軟體進行掃描，並將掃描結果及時間目的進行登載。

3. 診所需與外包廠商簽具資安及個資保密相關合約及違約規定。

4. 外包廠商需符合資安認證資格或接受資安課程之訓練並取得證明。

四、 落實網路隔離

1. 獨立使用連結健保署 VPN 之電腦，與任何連結形式之網際網路區隔，如：有線網路連結、無線網路連結及透過手機上網連結。

2. 避免透過遠端連線之方式來維護診所連結中央醫療體系專用 VPN 之電腦。

3. 供民眾使用或內部員工使用之 Wifi 應與內部作業電腦網段進行隔離。

4. 遠端連線須增設管理機制，如：增設密碼或登錄允許等方式。

五、 強化 IoT 設備管理

要求維護廠商將相關 IoT 設備(如：監視器、門禁、事務機...等)之韌體更新至最新版本。

六、 落實設備預設帳號密碼並使用較強的密碼規則

1. 至少 8 個字元以上；混合字母大小寫、數字及特殊符號，任選三種。
2. 避免和使用者帳號相同；避免使用有意義之單字。
3. 避免使用相同密碼於不同網站。
4. 定期變更密碼。

參、區域醫院或地區醫院篇

有資訊專屬人員但沒有專屬資安人力資源配置的區域醫院或地區醫院屬之。通常在沒有專屬資安人員配置及有限的資訊預算下，資安預算通常與資通訊需求合併運用，故資安相關需求大多直接委外由資訊廠商統合處理。

對於非「資通安全管理法」規範對象之區域醫院或地區醫院內的資訊安全措施，建議可以如下指引自我檢核與改善執行：

一、 醫療/醫務專屬使用設備

建議醫療/醫務使用之設備需與其他用途之設備區隔，並應定期盤點、造冊列管以維持最新狀態。

二、 電腦須安裝防毒軟體並隨時更新作業系統

許多的惡意攻擊程式是透過作業系統的漏洞滲透執行。所以過舊的電腦及作業系統須儘速汰換，並應安裝合法的防毒軟體，或至少更新至 Windows 10 並開啟內建之 Windows defender 進行防護。

三、 強化內部基層及管理人員資安意識

1. 資安教育訓練:

   ✓ 每年應安排資安教育訓練，建議時數如下:
   - ■主管及一般人員：3 小時
   - ■資訊人員：每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練。

   ✓ 每年定期辦理資安教育訓練，請一般同仁與主管務必參加，以提昇資訊安全認知及相關技能。

2. 建議於電腦的明顯處提醒 USB 限用機制，也可以友善提醒資安宣導標語。例如以下：

- ✓ 資安守則最重要；權限控管要確實。
- ✓ 密碼外洩風險高；定期更改才安全。
- ✓ 機密資料慎處理；個人資料要保密。
- ✓ 不明軟體勿下載；駭客入侵機會少。
- ✓ 網路安全要規範；資安檢核要精實。

四、 加強委外廠商管理

1. 委外廠商須充份了解資訊安全對醫療院所之重要性，建議於委外廠商簽訂合約時，合約內容應新增/包含資安條款要求。
2. 委外廠商使用 USB 存取診所裝置時，須由最新版之防毒軟體進行掃描，並將掃描結果及時間目的進行登載。

五、 落實網路隔離

1. 獨立使用連結健保署 VPN 之電腦，與任何連結形式之網際網路區隔，如：有線網路連結、無線網路連結及透過手機上網連結。
2. 避免透過遠端連線之方式來維護醫院連結中央醫療體系專用 VPN 的電腦。
3. 供民眾使用或內部員工使用之 Wifi 應與內部作業電腦網段進行隔離。

六、 強化 IoT 設備管理

要求維護廠商將相關 IoT 設備(如：監視器、門禁、事務機、醫療設備...等)之韌體更新至最新版本。

七、 落實設備預設帳號密碼並使用較強的密碼規則

1. 至少 8 個字元以上；
2. 混合字母大小寫、數字及特殊符號，任選三種。
3. 避免和使用者帳號相同；避免使用有意義之單字。
4. 避免使用相同密碼於不同網站。
5. 定期變更密碼。

八、 設備報廢/再利用之管制

設備及媒體報廢或改為其他用途時，應檢查其內容是否包含敏感資訊，確認其內容已被適當的處理後（格式化、刪除內容或實體銷毀），方可移交至相關人員作後續處理。

所有銷毀/報廢的電子設備應留存紀錄(設備名稱/型號、銷毀日期、處理人員、照片..等)，以備日後查詢。

九、 進階資安防護建置建議

為了強化醫院之資訊安全，可導入資安雲端訂閱型服務以介接健保署VPN 及民用網路並強化防護；對於經費預算及服務內容亦可保有較大的選擇彈性。

肆、附錄

一、 醫療資安範圍不再只是 IT，還包括 OT

醫療大樓光是伺服器就有上百臺，再加上各式設備更達上萬臺，光是管理這些設備，就耗費許多力氣；而在網路架構方面，則包括了院區網路、無線網路、聯外網路、終端網路和體系 VPN，要如何把關這些網路的資安，就是個挑戰。而最基本的處理，不外乎是防火防駭、Email 防護、網路流量監測和活動監控，以及特權帳號管理等。

不過，醫院該注重的資安範圍不只是 IT，還包括操作型技術（Operation Technology，OT）的安全，也就是醫療儀器。近年來各家醫院紛紛發展智慧醫療 4.0，利用大數據、AI、雲端和 IoT 技術來分析醫療資料、開發新服務，甚至發展遠距照護和個人化基因分析。

為了推動智慧醫療、加速醫療資料的傳輸與分析，醫院勢必採用可連線的醫療儀器，但這也成為資安隱憂。醫療資安防護不只要把個人電腦和伺服器管理好，還要注重醫療儀器的資安檢測，比如護理工作車、電腦斷層掃描設備、醫療檢測儀器等。

衛福部推動醫療 OT 資安檢測，醫療器材依據功能、用途、使用方法及工作原理，分為 17 大類；依據風險程度，分為三等級，醫院必須根據這些類別，完成了醫院 OT 盤點與風險評鑑，包括麻醉機、呼吸機、心電圖儀器、數位 X 光攝影、核子醫學設備、透析機等。

雖然一些醫療儀器的廠商認為，具中央站架構的 OT 不需安裝防毒軟體，但具連線功能的 OT 中毒風險高，還是得安裝防毒軟體，並定期監測活動狀況，才能確保醫療資訊安全。

二、 落實醫療資安，醫院從組織改造開始

資通安全管理法自上路，對醫院而言，資安把關不再是整體資訊（IT）範圍，而是擴大為整體資通範圍。除了原有的資訊機房、骨幹網路和醫療資訊系統的管理外，還涵蓋了事務機、醫療儀器、工程電腦等 OT 設備；也就是說，資通法監管的是整體醫療機構的範疇。

因應資安新法，CI 醫院須成立資通安全管理委員會，於其設置資安長職位，掌管全院資安事宜。

資安長之下設置單位則包括負責訂定資安計畫的資通安全管理中心、負責執行資安計畫的執行單位，以及機動小組（如情資因應小組、緊急應變小組和稽核小組）。

執行單位除了把關IT安全，也掌管了醫院各種OT檢驗。將OT定義為所有連接到網路的設備；除了醫工 OT、工務 OT 之外，人資、總務和秘書也列入 OT 檢查單位(這三個單位管理了監視器、影印機和打卡鐘)。另外，由於執行單位負責檢核IT系統和OT設備，也因此需要把關這些設備的使用單位、保管單位，甚至是供應商，朝第三方資安認證發展，更嚴格地控管供應設備。

資通安全管理中心，負責了資安預防作業和管理作業。比如辦理資通系統防護分級、資通事件通報及應變管理，以及擬訂資安政策與目標、辦理內部稽核等。要是發生資安事件，該中心也將向衛生局和資訊局等主管單位報告。

另一方面，也訂立了資通安全維護計畫書，以全機關為中心，作為今年執行重點。該計畫書分為 3 個層面，包括了管理面、技術面、認知與訓練層面。

在管理層面，除了分級資通系統和設立防護基準，還有一個重要工作，也就是將資訊安全管理系統導入全數的核心資通系統，而且要在 3 年內完成第三方驗證。另一方面，也要聘請 4 名資通安全專職人員，來執行資安管理。

在技術層面，則包括了資通安全健診（如網路架構檢視、網路惡意活動檢視）、資安防護（如安裝及更新防毒軟體、網路防火牆、APT 攻擊防禦等），以及完成政府組態基準導入作業。

至於認知與訓練層面，聚焦於資安教育訓練、頒發資安專業證照和職能訓練證書。資安教育訓練對象為資安專員和一般使用者，分別要接受 12 小時的專業課程，以及 3 小時的一般資安教育訓練課程。而資安專業證照

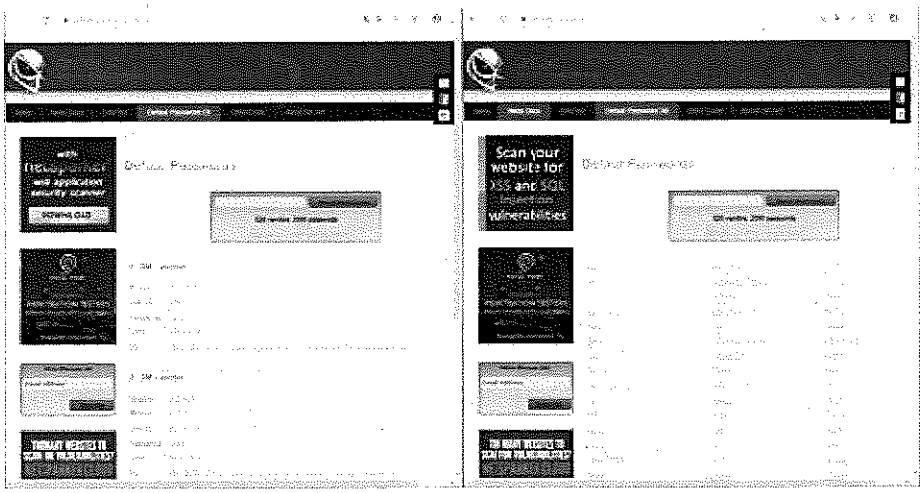
和職能訓練證書，則是資安專員必須持有的，以維持專業程度。透過這些做法，來全面強化醫療資安管理。

三、 物聯網設備資安檢測修補強化建議

1. 使用者存取控制與授權檢測：使用物聯網設備時，應確實檢視設備所提供的功能，並設定使用者所能存取之權限。

   ✓ 關閉設備非必要之功能
   ✓ 透過安全性設定進行權限控管
   ✓ 透過其他防護設備限制使用者可存取之服務。

2. 初始密碼變更檢測之建議：可參考網站整理的各廠牌預設密碼資料庫 (https://cirt.net/passwords)。



圖二 初始密碼變更資料庫網頁示意圖

3. 「密碼複雜度與強度檢測」之建議：落實資安教育訓練，更改設備預設帳號密碼，並使用較強的密碼規則。

   ✓ 至少 8 個字元以上
   ✓ 混合字母大小寫、數字及特殊符號，任選三種
   ✓ 避免和使用者帳號相同
   ✓ 避免使用有意義之單字
   ✓ 避免使用相同密碼於不同網站
   ✓ 定期變更密碼

4. 資料儲存權限管控檢測之建議：使用物聯網設備時，應確實檢視設備所提供的功能，並設定使用者所能存取之權限。

✓關閉設備非必要之功能
✓透過安全性設定進行權限控管
✓透過其他防護設備限制使用者可存取之服務

5. 關閉不必要之網路連線及服務檢測之建議：

✓關閉設備非必要之功能
✓透過安全性設定進行權限控管
✓透過其他防護設備限制使用者可存取之服務

6. 網路連線安全防護檢測之建議：

✓關閉設備非必要之功能
✓透過安全性設定進行權限控管
✓透過其他防護設備限制使用者可存取之服務

四、 醫療器材的網路安全管理

早在 2013 年 6 月，美國 FDA 發布一份關於網路安全的指引草案(Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff)，即規劃要求產品含有軟體的醫療器材業者，在提出產品的上市申請時，應參考該指引提交產品在網路安全管控方面的技術文件，引述其中一段摘要敘述如下：

網路安全管理的一般原則：在這份指引草案所提及的"網路安全"，是指避免未經授權的變更 (modification)、誤用(misuse)或拒絕使用(denial of use)，抑或是防止未經授權 而透過器材存取或轉移資料到外部連結的過程。製造商應該建立一套安全控管的 方式來確定產品的機密性(confidentiality)、完整性(integrity)、可使用性 (availability)。

1. 機密性：只有授權的人員或單位可以使用或操作器材的資料、資訊或系統結構。

2. 完整性：器材的資料或資訊正確、完整，並且沒有被變更。
3. 可使用性：在正確操作下，能夠適時地使用器材的資料或資訊，及其資訊系統。
4. 器材的網路安全能力(Security Capabilities)。

網路安全的管控措施因不同的器材、不同的使用環境、不同的風險而異，一般具有傳輸或上網功能的器材比沒有外部聯結功能的器材，更容易有網路安全風險的疑慮。FDA 建議業者應該在上市申請時，提交關於器材網路安全管控方式的評估文件，例如:

1. 僅限由信任的使用者操作使用。
2. 確保資訊內容可信。
3. 採用自動防故障及回復裝置(fail safe and recovery feature)。

另，涉及網路安全的產品，上市申請應額外檢附的文件如下：

1. 網路安全風險清單，所列的風險項目已於產品設計階段時完成評估;
2. 器材的網路安全管制方式及其評估清單;
3. 器材的網路安全風險及其對應的管制措施追溯聯結;
4. 系統的規劃書，提供系統或器材軟體操作的更新或修補程式(patches)，以確保器材持續安全及有效的使用;
5. 證明製造商提供給使用者的軟體不是惡意軟體(malware)的說明文件;
6. 器材的使用說明與產品規格應提供建議的防毒軟體或防火牆資訊。

以下為相關資料參考與延伸閱讀：

1. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration. Staff (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm).
2. Medtronic Insulin Pumps Vulnerable, Says Hacker (https://www.youtube.com/watch?v=THpcAd2nWJ8)
3. Medical Devices: How Secure Are They? (http://www.mdtmag.com/articles/2013/09/medical-devices-how-

secure-are-they#.UnsEsvlHLng)
4. Could medical devices be the next target for cyberattacks? (http://www.ctvnews.ca/health/health-headlines/could-medical-devices-be-the-next-target-for-cyberattacks-1.1344331)
5. Hack Attacks: Are Your Medical Devices At Risk? (http://www.cardiosource.org/en/News-Media/Publications/CardioSource-World-News/2012/April/Hack-Attacks.aspx)

伍、資訊安全自我檢核表

一、 基層診所適用

資訊安全自我檢核表 – 基層診所

機密等級：　　日期：

項次	檢核項目	檢核結果	簡述原因
A. 設備/醫務作業系統平台使用管理			
1	醫務/醫療作業所需使用之硬體設備(電腦、伺服器、筆電)或操作平台須區隔並為專屬使用。	□符合 □不符合 □不適用	
2	落實醫療/醫務作業系統平台所使用之硬體設備之控管(電腦/筆電)，且於該列管之設備僅得以執行醫療作業相關之事務(包含電子郵件)。	□符合 □不符合 □不適用	
B. 軟體安裝與更新			
3	醫務/醫療作業使用之電腦、筆電或伺服器皆已完成安裝防毒軟體。請檢視防毒軟體之病毒碼是否已更新至最新版本。 建議避免使用網路上提供之免費使用防毒軟體以降低風險。	□符合 □不符合 □不適用	防毒軟體： 最近更新日期：
4	確認最近一次作業系統安全性更新並將更新日期紀錄存查。每月更新一次為宜。 如設備使用之作業系統版本較老舊且品牌原廠不再提供版本更新服務(EOS, End of Service)，則須改採符合軟體更新時效之應用軟體，或進行存取權限控管、增加資安防護設備(如防火牆)以及密碼應符合高複雜度以確保整體資訊安全機制之運行。	□符合 □不符合 □不適用	版本更新日期：
C. 設備使用之安全性			
5	啟動螢幕保護並執行限制操作時間螢幕鎖定設定。建議螢幕鎖定之時間設定以不超過 15 分鐘為原則。	□符合 □不符合 □不適用	
6	電腦密碼安全性設定 - 密碼長度、複雜性需求及有效期限建議如下： 「最小密碼長度」是否為 8〔含〕或以上； 「密碼必須符合複雜性需求」是否為開啟； 「密碼最長有效期」是否為 90 天〔含〕或以下，但如有密碼外洩之風險則應立即修改。	□符合 □不符合 □不適用	

項次	檢核項目	檢核結果	簡述原因
7	密碼應妥善保管避免外洩，不得將密碼張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。	□符合 □不符合 □不適用	
8	執行醫療/醫務作業使用之電腦/筆電請啟動本機防火牆設定，可啟動設置阻擋可疑連線或白名單建立之功能設定。	□符合 □不符合 □不適用	
9	如業務需要安裝並開啟遠端連線軟體(如telnet)之設定使用，須檢視是否有限制連線時間/IP/Log 紀錄保存等管理機制。	□符合 □不符合 □不適用	
10	如業務需要使用可攜式媒體儲存(USB、行動硬碟)傳遞含有機敏性個資或機密資料，須另採加密機制保護本機資料。	□符合 □不符合 □不適用	
11	避免安裝或連結未經授權及來路不明之軟硬體。	□符合 □不符合 □不適用	
12	啟用作業系統安全性設定之稽核原則設定。	□符合 □不符合 □不適用	
13	定期執行重要資料之備份作業並加密處理。建議備份資料採異地(指非本機儲存空間)存放。	□符合 □不符合 □不適用	
14	內部員工私接 MODEM、ADSL 及無線網路卡等網路通訊設備易造成病患個資外洩風險，對外連線須有適切的管制措施。	□符合 □不符合 □不適用	
D. 設備資產保存或報廢處理			
15	醫療/醫務作業用電腦資產需造冊列管並設定專人保管並於安全場所存放，非授權作業人員不得操作使用。 可對設備使用/保存場所進行適當的監視錄影，監視錄影之影片建議存檔 3 個月以上。	□符合 □不符合 □不適用	
16	任何儲存資訊之電子設備於報廢/丟棄之前，應將儲存資訊刪除，並徹底消磁或銷毀至無法解讀之程度。	□符合 □不符合 □不適用	

本次資訊安全自我檢核結果，須改善項目紀錄/備註如下(可委由委外廠商協助檢核)：

檢核日期：

檢核人員：

受查代表：

二、 區域醫院或地區醫院適用

資訊安全自我檢核表 –區域醫院或地區醫院

機密等級： 日期：

項次	檢核項目	檢核結果	簡述原因
A. 設備/醫務作業系統平台使用管理			
1	醫務/醫療作業所需使用之硬體設備(電腦、伺服器、筆電)或操作平台須區隔並為專屬使用。	□符合 □不符合 □不適用	
2	落實醫療/醫務作業系統平台所使用之硬體設備之控管(電腦/筆電)，且於該列管之設備僅得以執行醫療作業相關之事務(包含電子郵件)。	□符合 □不符合 □不適用	
3	醫務/醫療作業所需使用之硬體設備(電腦、伺服器、筆電)造冊列管並維持最新狀態。	□符合 □不符合 □不適用	
B. 軟體安裝與更新			
4	醫務/醫療作業使用之電腦、筆電或伺服器皆已完成安裝防毒軟體。請檢視防毒軟體之病毒碼是否已更新至最新版本。 (建議避免使用網路上提供之免費使用防毒軟體以降低風險。)	□符合 □不符合 □不適用	防毒軟體： 最近更新日期：
5	確認最近一次作業系統安全性更新並將更新日期紀錄存查，每月更新一次為宜。(如設備使用之作業系統版本較老舊且品牌原廠不再提供版本更新服務(EOS, End of Service)，則須改採符合軟體更新時效之應用軟體，或進行存取權限控管、增加資安防護設備(如防火牆)以及密碼應符合高複雜度以確保安全性。	□符合 □不符合 □不適用	版本更新日期：
6	確認最近一次應用系統與資料庫系統安全性更新並維持最新狀態，落實系統更新日期紀錄存查。 (如設備使用之應用系統與資料庫系統版本較老舊且品牌原廠不再提供版本更新服務(EOS, End of Service)，則須改採符合軟體更新時效之應用軟體，或進行存取權限控管、增加資安防護設備(如防火牆)以及密碼應符合高複雜度以確保安全性。	□符合 □不符合 □不適用	版本更新日期：
C. 設備使用之安全性			
7	啟動螢幕保護並執行限制操作時間螢幕鎖定	□符合	

項次	檢核項目	檢核結果	簡述原因
	設定。建議螢幕鎖定之時間設定以不超過15分鐘為原則。	□不符合 □不適用	
8	密碼安全性原則 - 密碼長度、複雜性需求及有效期限建議如下： ●「最小密碼長度」是否為8〔含〕或以上； ●「密碼必須符合複雜性需求」是否為開啟； ●「密碼最長有效期」是否為90天〔含〕或以下，但如有密碼外洩之風險則應立即修改。 ●密碼輸入錯誤超過五次則帳號鎖定15分鐘。	□符合 □不符合 □不適用	
9	密碼應妥善保管避免外洩，不得將密碼張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。	□符合 □不符合 □不適用	
10	執行執行醫療 / 醫務作業使用之電腦 / 筆電請啟動本機防火牆設定，可啟動設置阻擋可疑連線或白名單建立之功能設定。	□符合 □不符合 □不適用	
11	如業務需要安裝並開啟遠端連線軟體(如telnet)之設定使用，須檢視是否有限制連線時間/IP/Log紀錄保存等管理機制。	□符合 □不符合 □不適用	
12	如業務需要使用可攜式媒體儲存(USB、行動硬碟)傳遞含有機敏性個資或機密資料，須採加密機制保護相關資料。	□符合 □不符合 □不適用	
13	避免安裝或連結未經授權及來路不明之軟硬體。	□符合 □不符合 □不適用	
14	啟用作業系統、應用系統與資料庫系統安全性設定之稽核原則設定。	□符合 □不符合 □不適用	
15	定期執行重要資料之備份作業並加密處理。建議備份資料採異地(指非本機儲存空間)存放。	□符合 □不符合 □不適用	
D. 網路安全管理			
16	內部員工私接MODEM、ADSL及無線網路卡等網路通訊設備易造成病患個資外洩風險，對外連線須有適切的管制措施。	□符合 □不符合 □不適用	

項次	檢核項目	檢核結果	簡述原因
17	建立共用資料夾(如:網路芳鄰)存取限制。	□符合 □不符合 □不適用	
18	是否依網路服務需要區隔獨立的邏輯網域，並建立適當之防護措施，以管制過濾網域間之資料存取？	□符合 □不符合 □不適用	
19	是否有遠端作業政策及審查程序以便授權及控制電腦通訊遠距工作的活動？且建立使用限制、組態需求、連線需求及管控措施？	□符合 □不符合 □不適用	
20	如有遠端存取維護情形，針對透過遠端執行特定之功能及存取相關資訊是否採加密機制，以保護遠端存取連線之機密性？	□符合 □不符合 □不適用	
21	是否針對外部連接之資訊交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性(如採行識別碼通行碼管制、電子資料加密或電子簽章認證等)？是否針對重要資料的交換過程，保存適當之監控紀錄？	□符合 □不符合 □不適用	
E. 設備資產保存或報廢處理			
22	醫療醫療 / 醫務作業用電腦資產需造冊列管並設定專人保管並於安全場所存放，非經授權作業人員不得操作使用。 可對設備使用/保存場所進行適當的監視錄影，監視錄影之影片建議存檔 3 個月以上。	□符合 □不符合 □不適用	
23	任何儲存資訊之電子設備於報廢/丟棄之前，應將儲存資訊刪除，並徹底消磁或銷毀至無法解讀之程度。 所有銷毀/報廢的電子設備應留存紀錄(設備名稱/型號、銷毀日期、處理人員、照片..等)，以備日後查詢。	□符合 □不符合 □不適用	

本次資訊安全自我檢核結果，須改善項目紀錄/備註如下：

檢核日期：

檢核人員：

受查代表：