

**衛福部**

**關鍵基礎設施資安聯防強化案計畫**

**111年5月份醫療資安情資分析月報告**

版本 1.00

數聯資安股份有限公司

中華民國111年6月25日

版本資訊

| 日期 | 版次 | 說明 | 撰寫人 | 覆核人 |
| --- | --- | --- | --- | --- |
| 111/6/25 | 1.00 | 新制訂 | 許建隆 許晉銘  王思詠 | 欒自雨 |

目錄

[1. 報告摘要 1](#_Toc106654687)

[2. 近期N-ISAC資安情資分享資訊分析報告 10](#_Toc106654688)

[2.1 聯防監控範圍 10](#_Toc106654689)

[2.2 整體威脅趨勢 11](#_Toc106654690)

[2.3 威脅來源分析 13](#_Toc106654691)

[2.4 中繼站黑名單分析 22](#_Toc106654692)

[2.5 威脅種類分析 24](#_Toc106654693)

[2.6 聯防監控回饋建議 38](#_Toc106654694)

[2.7 IP位址範圍情資分享 79](#_Toc106654695)

[2.8 N-ISAC資安警訊(EWA、INT)統計 80](#_Toc106654696)

[2.9 H-ISAC分享給N-ISAC 或其他領域ISAC 之情資摘要 82](#_Toc106654697)

[2.10 H-SOC研擬情資轉警訊 84](#_Toc106654698)

[2.11 H-CERT通報 85](#_Toc106654699)

[3. 近期H-ISAC資安情資於醫療領域相關分析 93](#_Toc106654700)

[3.1 國內外重要醫療資安情資 93](#_Toc106654701)

[3.2 國內外重要資訊安全漏洞 107](#_Toc106654702)

[3.3 國內外重要醫療資安暗網情資 108](#_Toc106654703)

[4. 醫療領域資安案例分析—保護遠距醫療病患監測生態系統 112](#_Toc106654704)

[4.1 網路安全架構 114](#_Toc106654705)

[4.1.1分層架構 115](#_Toc106654706)

[4.1.2安全能力 116](#_Toc106654713)

[4.1.3最終架構 118](#_Toc106654714)

[4.2 RPM測試實例 119](#_Toc106654715)

[5. 醫療領域資安趨勢分析-軟體材料清單最基本要項 123](#_Toc106654716)

[5.1 摘要…. 123](#_Toc106654717)

[5.2 最基本要項 125](#_Toc106654718)

[5.3 結論…. 133](#_Toc106654719)

[6. 參考文獻 134](#_Toc106654720)

**圖目錄**

[圖1：H-SOC參與機構概要 10](#_Toc106654761)

[圖2：H-SOC通報案件資訊摘要 11](#_Toc106654762)

[圖3：111年5月每日案件類別趨勢 12](#_Toc106654763)

[圖4：111年5月份案件來源國家IP分布(含台灣) 13](#_Toc106654764)

[圖5：111年5月通報案件國外來源IP之分布 14](#_Toc106654765)

[圖6：111年5月國外來源之案件清單 15](#_Toc106654766)

[圖7：本月通報重大國外來源案件清單(單一類超過10件(含)以上) 17](#_Toc106654767)

[圖8：111年5月前十大國內來源所在城巿/區域 18](#_Toc106654768)

[圖9：111年5月前十大國內來源案件 19](#_Toc106654769)

[圖10：本月通報重大國內來源案件清單(單一類超過10件(含)以上) 21](#_Toc106654770)

[圖11：通報案件類別概要 24](#_Toc106654771)

[圖12：通報案件依類別統計（與前月相較） 25](#_Toc106654772)

[圖13：111年5月每日案件類別趨勢 26](#_Toc106654773)

[圖14：5/3(二) 各機關觸發情形 27](#_Toc106654774)

[圖15：5/3(二) 個別案件觸發情形 28](#_Toc106654775)

[圖16：5/18(三) 各機關觸發情形 29](#_Toc106654776)

[圖17：5/18(三) 個別案件觸發情形 30](#_Toc106654777)

[圖18：5/23(一) 各機關觸發情形 31](#_Toc106654778)

[圖19：5/23(一) 個別案件觸發情形 32](#_Toc106654779)

[圖20：Medical Pharmacies 機構資料外洩資訊 109](#_Toc106654780)

[圖21：Salud Total 機構資料外洩資訊 110](#_Toc106654781)

[圖22：RPM分佈式架構 114](#_Toc106654782)

[圖23：企業、安全、基礎設施架構等層面示意圖 116](#_Toc106654783)

[圖24：最終架構圖 119](#_Toc106654784)

**表目錄**

[表1：中繼站IP連線統計 22](#_Toc106654785)

[表2：中繼站黑名單實際威脅之攻擊種類 22](#_Toc106654786)

[表3：本月資安案件類別、主要影響機關業務類別及案件彙整 33](#_Toc106654787)

[表4：本月可疑案件來源IP與相關案件機構清單 38](#_Toc106654788)

[表5：部立醫院之跨國別連線阻擋行為整理 69](#_Toc106654789)

[表6：本月Log4j漏洞相關攻擊紀錄 77](#_Toc106654790)

[表7：本月前 10 大之外部威脅連線來源 IP 78](#_Toc106654791)

[表8：本月N-ISAC資安警訊統計表 80](#_Toc106654792)

[表9：本月H-ISAC分享給N-ISAC之情資統計 82](#_Toc106654793)

[表10：H-SOC情資轉警訊列表 84](#_Toc106654794)

[表11：H-CERT醫院通報案件\_光田醫療社團法人光田綜合醫院 85](#_Toc106654795)

[表12：H-CERT醫院問題分析\_光田醫療社團法人光田綜合醫院 85](#_Toc106654796)

[表13：H-CERT醫院通報案件\_彰化基督教醫療財團法人彰化基督教醫院 87](#_Toc106654797)

[表14：H-CERT醫院問題分析\_彰化基督教醫療財團法人彰化基督教醫院 87](#_Toc106654798)

[表15：H-CERT醫院通報案件\_安泰醫療社團法人安泰醫院 89](#_Toc106654799)

[表16：H-CERT醫院問題分析\_安泰醫療社團法人安泰醫院 89](#_Toc106654800)

[表17：H-CERT醫院通報案件\_恆基醫療財團法人恆春基督教醫院 91](#_Toc106654801)

[表18：H-CERT醫院問題分析\_恆基醫療財團法人恆春基督教醫院 91](#_Toc106654802)

[表19：編號1-情資資訊統整 94](#_Toc106654803)

[表20：編號2-情資資訊統整 95](#_Toc106654804)

[表21：編號3-情資資訊統整 96](#_Toc106654805)

[表22：編號4-情資資訊統整 97](#_Toc106654806)

[表23：編號5-情資資訊統整 98](#_Toc106654807)

[表24：編號6-情資資訊統整 99](#_Toc106654808)

[表25：編號7-情資資訊統整 100](#_Toc106654809)

[表26：編號8-情資資訊統整 101](#_Toc106654810)

[表27：編號9-情資資訊統整 102](#_Toc106654811)

[表28：編號10-情資資訊統整 102](#_Toc106654812)

[表29：編號11-情資資訊統整 103](#_Toc106654813)

[表30：編號12-情資資訊統整 105](#_Toc106654814)

[表31：編號13-情資資訊統整 106](#_Toc106654815)

[表32：CVE編號資訊統整表 107](#_Toc106654816)

[表33：本月醫療資安暗網情資 109](#_Toc106654817)

[表34：RPM資產管理類別測試範例 119](#_Toc106654818)

[表35：最基本要項表 124](#_Toc106654819)

[表36：基準元件資訊 126](#_Toc106654820)

1. 報告摘要

本月報告之重要摘要說明如下：

* 本服務月報的資安通報案件總數量較4月份增加82.3%。其中，尚須調查類增加45.7%、掃描刺探類增加2.3%、阻斷服務類增加47.6%，其中入侵攻擊類增加107.4%、惡意程式類增加143.4%、政策規則類增加131.4%，以及網路攻防演練類增加718.1%。值得注意的是，這個月有四類案件類型新增案例超過100%，其中又以網路攻防演練類增加718.1%。針對持續發生入侵攻擊類、惡意程式類以及政策規則類之事件的醫療機構，本團隊建議可以進一步了解可能發生的根因，以利強化防護工作重點。本團隊能協助欲了解事件根因的醫療機構，透過取得進一步的事件分析數據或原始監控數據，可透過數位鑑識技術來進行事件根因分析，以確立真正的事件根因與類型。經數位鑑識分析後，可針對高風險事件完成去識別化的事件調查報告或案例分析報告，以供機關或資安監控單位參考，期能強化資安監控與防護能量。
* 本月資安通報案件中，政策規則類的通報比例最高，案件通報數佔32.2%，其他類的前三名案件分別為掃描刺探類(30.6%)、經同意之網路攻防演練類(17.7%)，以及尚須調查類(9.5%)。相較四月份的資安通報案件，政策規則類增加131.4%、掃描刺探類增加2.3%、經同意之網路攻防演練類增加718.1%，尚須調查類增加45.7%。本月份幾乎每天皆有發生的案件類型為(依數量多寡排序)掃描刺探類、政策規則類、尚須調查類，建議各單位朝三大類型之案件優先提升防護能力。經同意之網路攻防演練類增加的資安案件為本月最多的，但未有進一步深入調查報告，主要的觸發條件為疑似技服滲透測試事件。
* 本月份資安通報案件與機關之關聯整理如下表。根據下表所示，建議各類型機關可關注本月份資安通報案件類型，作為資安防護或資安認知教育訓練之參考。值得注意的是，其他醫療機構和上個月(111年4月)一樣有來源單一帳號持續登入失敗的案件，已經持續兩個月有相同案件發生，且為政策規則類的主要觸發事件，本月佔比高達90.9%。建議醫療機構可針對持續發生的事件進行根因分析，以利強化資安防護作為。若有需要，本計畫可以透過取得進一步監控數據，進一步分析特定案件的登入帳號是否需要修改、嘗試登入哪個資通訊系統，以及該案件風險分析等，以供醫療機關參考。本月份的資安事件較集中於主管機關與醫學中心之系統，除了建議該類機關提高防護作為外，可進一步研析是否具有特定目的之APT攻擊行為，以強化資安監控與防護重點。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 類型 | 攻擊手法 | 主管機關 | 醫學中心 | 部立醫院 | 區域醫院 | 其他醫療機構 |
| 掃描刺探類 | * 第二級[外部VPN存取登入行為]案件 * 第二級[跨國別連線阻擋行為]案件 * 單一目標主機短時間內觸發大量WAF事件 |  | V | V |  |  |
| 惡意程式類 | * 無法清除刪除病毒通報 | V |  |  |  |  |
| 尚需調查類 | * 可疑對外連線 * 國外IP登入SSLVPN |  | V |  |  |  |
| 政策規則類 | * 來源單一帳號持續登入失敗 |  |  |  |  | V |
| 阻斷服務類 | * 第二級[大量DNS查詢行為]案件 |  |  | V |  |  |
| 系統服務類 | * 第三級[網頁連線異常]案件 | V |  |  |  |  |
| 入侵攻擊類 | * 外部主機執行弱點掃描攻擊 * TeamViewer連線行為 * 已知中繼站網域連線 |  | V |  |  |  |
| 經同意之網路攻防演練類 | * 疑似技服滲透測試事件 | V |  |  |  |  |

* 本月份資安通報案件中，攻擊IP來源主要以台灣地區的IP為主（約佔56.4%），其他國家的IP來源前三名分別為美國、英國，以及中國，相較前一月份(111年4月)，美國、中國仍為國外攻擊來源IP數量前三名之國家。前一月份數量最高的國家是美國(4月為644筆，本月減少345筆)，第二高為英國(本月為81)，第三高為中國(4月為109筆，本月減少40筆)，其中值得注意的是，雖然本月份的國外來源案件數減少，但本月份的【單一目標主機短時間內觸發大量WAF事件】和上月一樣，同為前三名之案件。若是因為WAF規則設定太嚴謹，導致一直觸發警告造成WAF效能低落，可以嘗試調整規則。若規則設定無誤，可嘗試檢視紀錄檔(Log)分析細節，以利了解案件之根因。針對本月IP攻擊案件整理與資安防護建議如下：

|  |  |  |
| --- | --- | --- |
| IP來源 | 本月份重要攻擊手法 | 資安防護建議 |
| 國內IP  重要案件 | 第二級[外部VPN存取登入行為]案件 | * 定期將VPN軟體版本更新。 * 定期更新VPN登入存取之密碼。 * 使用無資安疑慮之VPN廠商。 * 若設備不會使用到VPN功能，則應將相關軟體移除、關閉相關埠。 |
| 攻防演練字串偵測 | 了解受影響的設備為何，持續進行攻防演練、弱點掃描，建立關鍵設施備援措施與SOP，並再次確認網通資安設備之設定是否正確，其偵測到的惡意輸入是否也出現在其他設備上。 |
| 跨國別連線阻擋行為 | 限制特定時間範圍接收數量、建立黑洞路由、使用進階安全性防火牆阻擋非法連線。 |
| 國外IP  重要案件 | 國外IP登入SSLVPN | * 定期更新安裝於路由器、網路非武裝區域(DMZ之VPN版本。 * 使用者需定期更新VPN登入存取之密碼。 * 使用無資安疑慮之VPN廠商。 * 若網通設備不會使用到VPN，則應將相關軟體移除、關閉相關埠。 |
| 單一目標主機短時間內觸發大量WAF事件 | * 若是因為WAF規則設定太嚴謹，導致一直觸發警告造成WAF效能低落，可以嘗試調整規則。 * 若規則設定無誤，可嘗試檢視紀錄檔(log)分析細節。 |

* 本月份5/3與5/18的案件數特別高，其中 5/3(二)案件總數高達483件為本月最高，而5/18(三)案件總數達414件為本月次高。值得注意的是，5/3的惡意程式類共計293件，明顯高於本月平均，依個別案件分析，發現無法清除刪除病毒的通報案件最高，建議了解病毒類型及影響的層面。相關單位應研析並追蹤該機構後續動作，並追蹤其他機構是否也有觸發相關案件。
* 本計畫發現近幾個月的Log4j漏洞之資安案件頻傳，本月份Log4j漏洞惡意攻擊通報案件共有6個機關受影響，分別為：國民健康署、國家衛生研究院、臺北市立萬芳醫院、臺北榮民總醫院、衛生福利部附屬醫療及社會福利機構管理會，以及衛生福利部食品藥物管理署，其中國民健康署已經連續4個月持續遭到Log4j漏洞惡意攻擊，顯然仍未改善其資安防護作為。建議可進一步了解該機關的Log4j漏洞惡意攻擊之影響範圍、資安防護作為與困難，並適時給予輔導、建議、教育訓練或要求，以強化Log4j漏洞惡意攻擊之防護。
* 本月份的H-CERT醫院通報案件共有4件，分別如下：
  + 光田醫療社團法人光田綜合醫院通報案件：有關於健保VPN IDC無法認證。此通報事件為非核心業務之運作受影響或停頓，根因為健保署系統當機，建議醫院可以藉由這次事件，重新審視事件應變機制是否適宜，有無可改善之空間。
  + 彰化基督教醫療財團法人彰化基督教醫院通報案件：有關於網路設備故障導致部分門診及病房網路斷線。此網路設備故障導致部分門診及病房網路斷線，根因為Switch死當，本案例發生的設備為新設備(提及設備為2021/5/10啟用)，發生設備死當的機率理應較低。即使重啟服務後可以順利運作，仍必須檢視該設備是否異常(即便在使用年限內)，以及相關系統、韌體是否定期更新。導致建議藉此次事件檢視該設備(Switch)提供的效能是否足夠供目前組織使用，若效能不足則需更換設備至符合效能所需。
  + 安泰醫療社團法人安泰醫院通報案件：有關於HIS DB主機故障，切換至備援主機等候設備修復。此通報事件為HIS DB主機故障，切換至備援主機等候設備修復，根因為主機板壞損，本案例為舊設備(提及設備於2015/08上線服務)，建議藉此次事件重新檢視所有設備使用年限、效能、是否有發生異常，以及相關系統、韌體是否定期更新。對於切換至備援主機應變機制部分，建議重新審視事件應變機制是否適宜，有無可改善之空間，避免出現預期外之錯誤或是暴露資安風險。
  + 恆基醫療財團法人恆春基督教醫院通報案件：有關於防火牆遭遇來自俄羅斯的IP進行DOS的攻擊。此通報事件為防火牆遭遇來自俄羅斯的IP進行DOS的攻擊，根因為，因為有IPS的阻擋下，並未造成損失，只有短暫時間的服務中斷而已，建議可以使用政府公告之惡意中繼站IP黑名單進行阻擋，如果有院內有遠距需求的Server，建議使用白名單，僅允許需要使用的設備IP即可。
* 本月份之重要醫療資安情資共計13則，其中包含網路攻擊相關的情資共有5則、資料外洩相關的情資共有5則、勒索軟體相關的情資共有3則、社交工程相關的情資有1則。本月份所蒐集之情資可供機關了解近期國際醫療資安重大案件或報告，以作為資安防護與教育訓練之參考。就情資內容分析，醫療院所的個資外洩仍是重要威脅，近期有新增不同的攻擊手法，需多關注不同的攻擊手法並針對其做防禦。值得注意的是，幾件資安案件供我國醫療體系資安防護之借鏡，例如：醫療安全文化的趨勢是正確的，但仍需要改進，在嚴苛的規範要求下獲得74分(滿分100分)，有一定的基礎但需更加精進，實施定期員工培訓、教育訓練以及技術和管理保障措施可以幫助醫療組織建立強大的安全文化。
* 本月份的資安情資中，網路攻擊的比例最高，除了基本的完善防護，更需要對員工進行資安教育訓練以提高其安全意識，例如：不下載來路不明的檔案，並教授如何識別常見的攻擊。
* 本月份國際最新公告的資訊安全漏洞CVE都是注入攻擊，強烈建議各醫療單位有使用LibreHealth EHR 2.0.0，請盡速更新進行修補(目前皆已經釋出修補方法)，以防止攻擊案件的發生。
* 本月醫療資安暗網情資以美國為大宗，值得注意的是，尚未發現有台灣醫療機構資料外洩於暗網中，此顯示台灣醫療資安已達成相當程度的基礎防護，須繼續保持相同防護水準。本計畫團隊仍會持續關注暗網情資，以監控我國醫療情資是否被揭露於暗網中，並即時回報給衛生福利部。
* 本月份考量醫療機關因應疫情時代之遠距醫療服務資安需求，以及國際醫療供應鏈安全趨勢，特別完成2個醫療資安專題報告，分別為「保護遠距醫療病患監測生態系統」以及「軟體材料清單的最基本要項」。
* 「保護遠距醫療病患監測生態系統」專題報告：此報告主要根據2022年2月美國國家標準暨技術研究院(National Institute of Standards and Technology，NIST)所發布的「保護遠距醫療病患監測生態系統指南」(Securing Telehealth Remote Patient Monitoring Ecosystem, NIST SPECIAL PUBLICATION 1800-30)，其建議醫療服務機構(Healthcare Delivery Organizations，HDO)在提供遠距醫療服務時，應該確保其網路安全和隱私保護，才能避免遠距醫療的資安風險。內容將會介紹保護遠距醫療病患監測生態系統的最終架構，並提出RPM實例。
* 「軟體材料清單的最基本要項」專題報告：軟體材料清單(Software Bill of Materials，SBOM)是構成軟體的成分表，用來描述軟體的組成架構、內容、生產與整合軌跡，以提供軟體組成的透明性，內容針對軟體材料清單的三個最基本要項，即資料範圍、自動化支持以及實踐與流程進行詳細的說明。

1. 近期H-ISAC資安情資於醫療領域相關分析
   1. 國內外重要醫療資安情資

本月份重要醫療資安情資統計，累計期間為111/5/1~111/5/31，情資資訊包含編號、類別、標題、日期、內容、攻擊手法、資料來源，共計13則。就情資內容分析，醫療院所的個資外洩仍是重要威脅，大部分的威脅手法為網路攻擊及勒索軟體為主，因此仍需持續關注這兩個攻擊手法並針對其做研究。值得注意的幾件資安事件供我國醫療體系資安防護之借鏡，例如：Salusive醫療中心在遭受網路攻擊後關閉服務、南佛羅里達州的醫院在網路攻擊中配置不當的IT服務、伊利諾伊胃腸病學組織遭受資料外洩影響22萬人、NH醫療器材公司面臨資訊安全事件以及SAC Health報告偷竊事件和多次勒索軟體攻擊等。本月情資可供機關了解近期國際醫療資安重大事件或報告，以作為資安防護與醫療資安教育訓練之參考，詳見表19~表31。

表19：編號1-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-001 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | Salusive醫療中心在遭受網路攻擊後關閉服務  Salusive Health Closes Business Following Cyberattack |
| 日期 | 中華民國111年05月03日 |
| 內容 | 幫助醫生實踐簡化疾病管理的myNurse 平台的開發商Salusive Health經歷了一次網路調查證實，未經授權的個人存取了患者的個人和受保護的健康資訊。  Salusive Health表示，它實施了額外的安全措施以防止進一步的侵害行為，已通知受影響的個人並提供免費的身分盜竊保護服務，並向聯邦調查局報告了網路攻擊。  位於俄亥俄州蒂普市的新創造諮詢中心(NCCC)最近開始通知24,029名患者，他們的一些受保護的健康資訊可能在最近的網路攻擊中受到損害。NCCC確認勒索軟體已被用於加密文件，第三方網路安全顧問一直在協助響應和恢復。NCCC表示，在整個過程中繼續為患者提供護理，並且已確認勒索軟體已從其係統中根除。 |
| 攻擊手法 | 網路攻擊 |
| 資料來源 | HIPPA JOURNAL  https://www.hipaajournal.com/salusive-health-closes-business-following-cyberattack/ |

表20：編號2-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-002 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 三家機構分別成為網路釣魚、電子郵件安全事件的受害者  3 Orgs Fall Victim to Separate Phishing, Email Security Incidents |
| 日期 | 中華民國111年05月04日 |
| 內容 | Valley View醫院、Fairfield County植牙和牙周病以及洛杉磯縣精神衛生部門都遭受了網路釣魚或電子郵件安全事件。  VALLEY VIEW醫院21K受影響。Valley View迅速保護了電子郵件帳戶，並聘請了一家法醫安全公司調查此事件，也確認了電腦系統的安全性。  CT植牙和牙周病供應商遭受PHI侵害。康涅狄格州提供商於2022年3月2日發現了一個被盜用的電子郵件帳戶，包含社會安全號碼、健康保險資訊、姓名、地址、出生日期、電話號碼、病史、電子郵件地址和治療資訊。FCIP於4月15日開始通知受影響的患者，並提供免費的身分盜竊保護服務。  洛杉磯精神衛生局成為社交工程的受害者，因遭受了「惡意網路攻擊」，導致客戶資訊洩露。4月21日，該部門表示已完成向受影響個人的郵寄通知，其網站上的通知用於未找到聯繫資訊的客戶。在此事件發生後，實施了審查和更新安全政策、程序和控制措施，還通知了Microsoft Office 365多因素身分驗證中的漏洞，該漏洞已被惡意行為者利用。 |
| 攻擊手法 | 社交工程、資料外洩 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/3-orgs-fall-victim-to-separate-phishing-email-security-incidents |

表21：編號3-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-003 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 南佛羅里達州的醫院在網路攻擊中配置不當的 IT 服務  South Florida hospitals misplaced IT service in cyber assault |
| 日期 | 中華民國111年05月06日 |
| 內容 | 海厄利亞的帕爾梅托綜合醫院是邁阿密戴德和布勞沃德的五家醫院之一，四月份遭到網路攻擊。根據衛生部的資料，對 Tenet 的網路攻擊是2022年對醫院的一波威脅中的最新一次。  由於公開報導的Tenet遭受網路攻擊，Steward邁阿密醫院的資訊技術系統服務中斷。據報導，St.Mary's和Good Samaritan至少24小時失去電話和電腦服務，迫使醫生和護士使用紙質記錄，並使用救護車將急診患者轉移到其他地區醫院。  Tenet尚未發布更新，但當時表示「關鍵應用程序已基本恢復」，其受影響的設施正在恢復正常運營。Tenet及其前南佛羅里達醫院都沒有在2022年向HHS報告駭客或IT事件。 |
| 攻擊手法 | 網路攻擊 |
| 資料來源 | Fitnessformulax  https://fitnessformulax.it/south-florida-hospitals-misplaced-it-service-in-cyber-assault/ |

表22：編號4-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-004 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 伊利諾伊胃腸病學組織遭受資料外洩影響22萬人  Illinois Gastroenterology Group Data Breach Impacts 228K |
| 日期 | 中華民國111年05月09日 |
| 內容 | EvergreenHealth、SAC Health和Optima Dermatology最近也面臨醫療資料外洩。伊利諾伊胃腸病學集團(IGG)遭遇了可能影響227,943人的資料安全事件。  IGG於2021年10月22日發現了異常的網路活動。11月18日IGG確定未經授權的行為者獲得了對其系統的存取權限，並且這些系統中包含的資訊可能已被查看或取得。IGG加快了增強型託管安全運營中心的實施，包括部署端點檢測和回應平台以回應這一事件，立即重置密碼，擁有敏感系統特權存取權限的員工被註冊到多因素身分驗證平台。  EVERGREENHEALTH面臨第三方EMR侵害，在西雅圖大都市區營運的華盛頓衛生系統表示，未經授權的一方在2021年12月4日左右存取了myCare Integrity資料，隨後刪除了資料庫和系統配置檔案。EvergreenHealth於2022年4月22日開始向可能受影響的患者郵寄通知信，任何非眼科診所的患者都不會捲入此事件。  SAC HEALTH記錄儲存設備遭受入侵，加利福尼亞州聖貝納迪諾的社會行動社區衛生系統(SAC Health)發布了關於在場外儲存設備發生闖入事件的通知。SAC Health迅速採取行動進行調查並做出回應，目前沒有證據表明資料被濫用。  OPTIMA皮膚科電子郵件安全事件影響 60K，印第安納州皮膚病學中心和高級皮膚病學和皮膚癌中心，向59,872人通知可能暴露受保護健康資訊的電子郵件安全事件。Optima Dermatology沒有證據表明任何資訊已經或將被濫用，但出於謹慎考慮還是通知了個人資訊包含在受影響員工電子郵件帳戶中的檔案中，也額外實施的安全措施，以防止未來發生類似事件。 |
| 攻擊手法 | 資料外洩 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/illinois-gastroenterology-group-data-breach-impacts-228k |

表23：編號5-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-005 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | NH醫療器材公司面臨資訊安全事件，8萬人受到影響  NH Medical Device Company Faces Data Security Incident, 81K Impacted |
| 日期 | 中華民國111年05月16日 |
| 內容 | 總部位於新罕布什爾州的醫療設備公司 NuLife Med在3月份遭遇了一起資料安全事件，影響了81,244人。在得知此事件後，迅速採取行動對事件進行調查和回應，評估系統的安全性，並識別任何受影響的資料。  俄克拉荷馬城印度診所更新網路攻擊資訊，其在3月份經歷了一次網路攻擊，導致某些藥房服務癱瘓。OKCIC的藥房自動補充熱線和郵購服務將「在不確定的時間內」關閉。診所指示患者在需要補充處方時致電藥房。  受影響的資料包括姓名、出生日期、處方資訊、醫療記錄、醫生資訊、部落身分證號碼、社會安全號碼、駕駛執照號碼和治療資訊。  在發現此事件後，重置了帳戶密碼並實施了額外的安全措施，還為可能受影響的個人提供信用監控和身分保護服務，作為額外的預防措施。 |
| 攻擊手法 | 資料外洩 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/nh-medical-device-company-faces-data-security-incident-81k-impacted |

表24：編號6-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-006 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | Schneck醫療中心、NuLife Med和FPS醫療中心通報發生網路攻擊  Cyberattacks Reported by Schneck Medical Center, NuLife Med, & FPS Medical Center |
| 日期 | 中華民國111年05月17日 |
| 內容 | 總部位於新罕布什爾州曼徹斯特的醫療設備公司NuLifeMed LLC在2022年3月11日前後受到網路攻擊，檢測到可疑網路活動，並立即採取措施防止進一步未經授權網路存取。資料外洩已向HHS的民權辦公室報告，影響了81,244人。  位於亞利桑那州哈瓦蘇湖市的FPS醫療中心受到勒索軟體攻擊，影響28,000名患者，它是加密其網路上文件的惡意軟體事件的受害者。該安全漏洞於2022年3月3日被發現，對受影響網路部分的所有檔案進行了審查，於2022年4月25日結束。  Schneck醫療中心宣佈網路攻擊和資料盜竊事件，於2022年3月17日確定檔案已在2021年9月29日左右從其系統中洩露。Schneck醫療中心表示，沒有發現任何證據表明任何實際或企圖濫用患者資料；但是作為預防措施，有向可能面臨風險的個人提供了免費的信用監控服務。已向 HHS的民權辦公室報告，影響了92,311人。 |
| 攻擊手法 | 網路攻擊 |
| 資料來源 | HIPPA Journal  https://www.hipaajournal.com/cyberattacks-reported-by-schneck-medical-center-nulife-med-fps-medical-center/ |

表25：編號7-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-007 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | AvosLocker 聲稱對Christus醫療中心的勒索軟體攻擊負責  AvosLocker Claims Responsibility For Christus Health Ransomware Attack |
| 日期 | 中華民國111年05月18日 |
| 內容 | 總部位於德克薩斯州達拉斯的Christus Health面臨勒索軟體攻擊，AvosLocker聲稱對其負責，但Christus Health表示該事件並未對患者護理產生不利影響。  AvosLocker聲稱直接處理贖金談判，以及在其附屬機構感染目標後發布和託管洩露的受害者資料。如果受害者拒絕談判或支付贖金，AvosLocker就會在其公共洩密網站上公開受害者資料。  聯合諮詢鼓勵組織實施恢復計畫並維護敏感資料的多個副本。醫療組織還應強制執行嚴格的密碼衛生，使用多因素身分驗證，並要求管理員憑據來安裝軟體。 |
| 攻擊手法 | 勒索軟體 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/avoslocker-claims-responsibility-for-christus-health-ransomware-attack |

表26：編號8-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-008 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 醫療安全文化的趨勢是正確的，但仍需要改進  Healthcare Security Culture Trending in the Right Direction, But Needs Improvement |
| 日期 | 中華民國111年05月19日 |
| 內容 | 2022年5月19日KnowBe4 Research透露，醫療行業在保持強大的安全文化方面獲得了74分（滿分100分），可能是由於醫療網路攻擊的頻率和嚴格的合規要求。最重要的發現是，沒有發現任何行業的安全文化得分差或平庸。醫療和製藥組織長期以來一直在保護知識產權和財務資訊方面保持警惕。醫療身分盜竊，通常包括患者的社會保障和信用卡號碼，對於網路犯罪分子來說是非常有利可圖的。醫療行業的安全文化比較強，但仍有工作要做。實施定期員工培訓、教育以及技術和管理保障措施可以幫助醫療組織建立強大的安全文化。 |
| 攻擊手法 | 無 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/healthcare-security-culture-trending-in-the-right-direction-but-needs-improvement |

表27：編號9-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-009 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 眼科供應商EMR違規影響數十萬人  Eye Care Leaders EMR Breach Impacts Hundreds of Thousands |
| 日期 | 中華民國111年05月23日 |
| 內容 | Eye Care Leaders的myCare Integrity EMR產品遭到未經授權的存取，影響了至少八家眼保健提供者和數十萬人。  myCare Integrity EMR產品是一個基於雲的系統，旨在改進工作流程，專為眼科業者構建。Eye Care Leaders經歷了一起資料安全事件，其中未經授權的一方存取了EMR系統並刪除了資料庫和系統配置檔案。為了防止未來發生此類侵害行為，供應商已經實施了技術、管理和物理保護措施，包括審查和更新存取控制、權限和資料儲存安全程序。 |
| 攻擊手法 | 資料外洩 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/eye-care-leaders-emr-breach-impacts-at-least-342k-individuals |

表28：編號10-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-010 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 醫療組織網路攻擊增加，內部威脅依然存在  Verizon DBIR: Healthcare Cyberattacks Increase, Insider Threats Remain |
| 日期 | 中華民國111年05月24日 |
| 內容 | Verizon 資料外洩調查報告(DBIR)顯示，隨著所有行業網路攻擊的增加，醫療領域的基本Web應用程式攻擊和系統入侵呈上升趨勢。基本的Web應用程式攻擊、雜項錯誤和系統入侵占所有醫療漏洞的76%。隨著基本Web應用程式攻擊模式在這個垂直領域的興起，內部參與者不再佔據主導地位。外部攻擊者在醫療及其他領域變得越來越強大和成功。醫療越來越成為普通駭客攻擊和更具影響力的勒索軟體活動的目標。隨著加速邁向日益數字化的世界，有效的技術解決方案、強大的安全框架以及對教育的日益關注都將在確保企業保持安全和客戶受到保護方面發揮作用。 |
| 攻擊手法 | 網路攻擊、勒索軟體 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/verizon-dbir-healthcare-cyberattacks-increase-insider-threats-remain |

表29：編號11-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-011 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | SAC Health報告偷竊事件和多次勒索軟體攻擊  SAC Health Theft Incident and Multiple Ransomware Attacks Reported |
| 日期 | 中華民國111年05月25日 |
| 內容 | 社會行動社區衛生系統(SAC Health) 通知149,940名患者，包含他們受保護的健康資訊的文件在儲存患者記錄的異地儲存位置的闖入中被盜。闖入事件於2022年3月4日被發現，隨後的調查於2022年4月22日確認。SAC Health表示，作為防止身分盜用和詐欺的預防措施，已向受影響的個人提供免費的信用監控服務、並正在對其有關紙質資料儲存的政策和程序進行審查。  Bryan County救護車管理局勒索軟體攻擊影響了14,000名患者，該攻擊是在 　　　　　　2021年11月24日檢測到的，俄克拉荷馬州布賴恩縣救護車管理局立即採取行動防止進一步未經授權的存取，並聘請第三方網路安全顧問協助取證調查，已向受影響的個人提供身分盜竊保護服務的免費會員資格。  Lifespan Services遭受勒索軟體攻擊，總部位於北卡羅來納州夏洛特的Lifespan Services是一家為殘障人士提供服務的非營利性提供商，證實是勒索軟體攻擊的受害者，Lifespan表示多層保護已經到位，實施了額外的安全措施，已向8,006名受影響的個人免費提供為期一年的身分盜竊保護服務會員資格。  Vice Society聲稱對Atlanta Perinatal Associate的勒索軟體攻擊負責，Atlanta Perinatal Associates是專門治療高危妊娠的母親，並與其他醫療提供者協調護理。醫療提供者尚未確認它是勒索軟體攻擊的受害者；但是，Vice Society已將資料上傳到其洩漏站點，據稱這些資料在攻擊中被盜。由於該事件尚未向監管機構報告，目前尚不清楚有多少患者受到影響。 |
| 攻擊手法 | 勒索軟體 |
| 資料來源 | HIPPA Journal  https://www.hipaajournal.com/sac-health-theft-incident-and-multiple-ransomware-attacks-reported/ |

表30：編號12-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-012 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 影子程式碼、第三方腳本會為醫療網路帶來安全風險  Shadow Code, Third-Party Scripts Pose Healthcare Cybersecurity Risks |
| 日期 | 中華民國111年05月26日 |
| 內容 | 第三方腳本可以啟用增強功能，可以通過允許開發團隊向Web應用程序引入增強功能而無需創建或維護它們來促進數字化轉型。但一份新報告表明，這些腳本還可能引入影子程式碼和醫療網路安全風險。Source Defense解釋說，第三方腳本是「加載到網頁中以提供網站核心功能之外的功能的JavaScript資源」。  醫療是金融服務行業背後最暴露的垂直行業之一，這兩個行業都是高度監管的行業，可以存取敏感資料。如果腳本被威脅者入侵或破壞，影子程式碼就會隨之而來。受影子程式碼感染的第三方腳本可能使威脅行為者能夠更改網頁上的內容、記錄擊鍵、監控按鍵以及截取和外洩憑證。 Verizon的2022年資料外洩調查報告 (DBIR)將基本的Web應用程序攻擊確定為2021年醫療資料外洩的最常見原因。 Source Defense報告建議安全團隊問問自己是否可以減少第三方腳本的數量，或者是否可以從處理敏感訊息的頁面中刪除一些腳本。 |
| 攻擊手法 | 資料外洩 |
| 資料來源 | HealthITSecurity  https://healthitsecurity.com/news/shadow-code-third-party-scripts-pose-healthcare-cybersecurity-risks |

表31：編號13-情資資訊統整

|  |  |
| --- | --- |
| 情資資訊 | |
| 編號 | HISAC-ANA-2022-05-013 |
| 類別 | 102-攻擊活動資訊 |
| 標題 | 前IT顧問被控告故意損壞醫療組織的伺服器  Former IT Consultant Charged with Intentionally Causing Damage to Healthcare Company’s Server |
| 日期 | 中華民國111年05月27日 |
| 內容 | 一名曾在芝加哥郊區醫療公司擔任承包商的資訊技術顧問被指控非法存取該公司的網路並故意損壞受保護的電腦。被入侵的電腦損害了醫療檢查、治療和多人的護理。這個案例凸顯了內部人士帶來的風險。最近發布的2022年Verizon資料外洩調查報告強調了外部威脅參與者攻擊的風險，其數量是內部攻擊的4比1，但還需要實施保護措施來防範內部威脅。當個人自願離職或被解僱時，需要立即撤銷對系統的存取權限，並對系統進行掃描以識別可能已安裝的任何惡意軟體或後門。 |
| 攻擊手法 | 網路攻擊 |
| 資料來源 | HIPPA JOURNAL  https://www.hipaajournal.com/former-it-consultant-charged-with-intentionally-causing-damage-to-healthcare-companys-server/ |

* 1. 國內外重要資訊安全漏洞

本計畫團隊整理5月份國內外重要資訊安全漏洞，詳細資訊請參考表32。本月份國際最新公告的資訊安全漏洞CVE-2022-31492至CVE-2022-31498為LibreHealth EHR Base 2.0.0的漏洞，會導致多個跨網站指令碼(XSS)之漏洞，另外，CVE-2022-30277為BD Synapsys™版本4.20、4.20 SR1和4.30的漏洞，如果被利用，威脅參與者可能能夠存取、修改或刪除敏感資訊，包括受保護的電子健康資訊(ePHI)、受保護的健康資訊(PHI)和個人身分資訊(PII)。

表32：CVE編號資訊統整表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 項次 | CVE編號 | 日期 | 內容 | 影響範圍 | 修補建議 |
| 1 | CVE-2022-30277 | 2022/05/04 | 會話到期不足漏洞，如果被利用，威脅參與者可能能夠存取、修改或刪除敏感資訊，包括受保護的電子健康資訊(ePHI)、受保護的健康資訊(PHI)和個人身分資訊(PII)。 | BD Synapsys™ 版本4.20、4.20 SR1和4.30 | 可參考以下網址進行及時修補。  https://cybersecurity.bd.com/bulletins-and-patches/bd-synapsys-insufficient-session-expiration |
| 2 | CVE-2022-31498、CVE-2022-31497、  CVE-2022-31496、CVE-2022-31495、  CVE-2022-31494、CVE-2022-31493 | 2022/05/23 | 允許interface/orders/patient\_match\_dialog.php key XSS、interface/main/finder/finder\_navigation.php patient XSS、incorrect interface/super/manage\_site\_files.php access、gacl/admin/acl\_admin.php return\_page XSS、gacl/admin/acl\_admin.php action XSS、gacl/admin/acl\_admin.php acl\_id XSS | LibreHealth EHR Base 2.0.0 | 可參考以下網址進行及時修補。  <https://github.com/LibreHealthIO/lh-ehr/tags>、https://nitroteam.kz/index.php?action=researches&slug=librehealth2\_r |
| 3 | CVE-2022-31492 | 2022/05/23 | 儲存跨站腳本 (XSS) 漏洞過 interface/usergroup/usergroup\_admin\_add.php 用戶名 | LibreHealth EHR Base 2.0.0 | 可參考以下網址進行及時修補。  <https://github.com/LibreHealthIO/lh-ehr/tags>、https://nitroteam.kz/index.php?action=researches&slug=librehealth2\_r |

* 1. 國內外重要醫療資安暗網情資

因應勒索軟體攻擊數量逐年上升趨勢，本計畫團隊持續監控勒索軟體暗網情資，累計期間為111/5/1~111/5/31，情資資訊包含項次、勒索軟體種類、案件機構國家、案件機構，共計6則。本月醫療資安暗網情資以美國為大宗，值得注意的是，尚未發現有台灣醫療機構資料外洩於暗網中，顯示台灣醫療資安已達成相當程度的基礎防護，須繼續保持相同防護水準，詳細資訊請參考表33、圖20~圖21。

表33：本月醫療資安暗網情資

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 勒索軟體種類 | 案件機構國家 | 案件機構 |
| 1 | LockBit2.0 | Singapore | Bioskin |
| 2 | LockBit2.0 | Hong Kong | Purapharm |
| 3 | Vice Society | United States | Atlanta Perinatal Associates |
| 4 | Vice Society | United States | Salud Total |
| 5 | Vice Society | Argentina | OSSEG Obra Social de Seguros |
| 6 | Snatch | Canada | Medical Pharmacies |

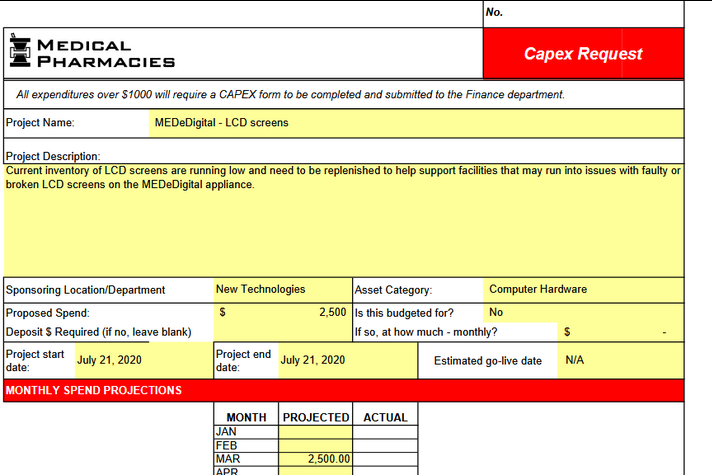


圖20：Medical Pharmacies 機構資料外洩資訊

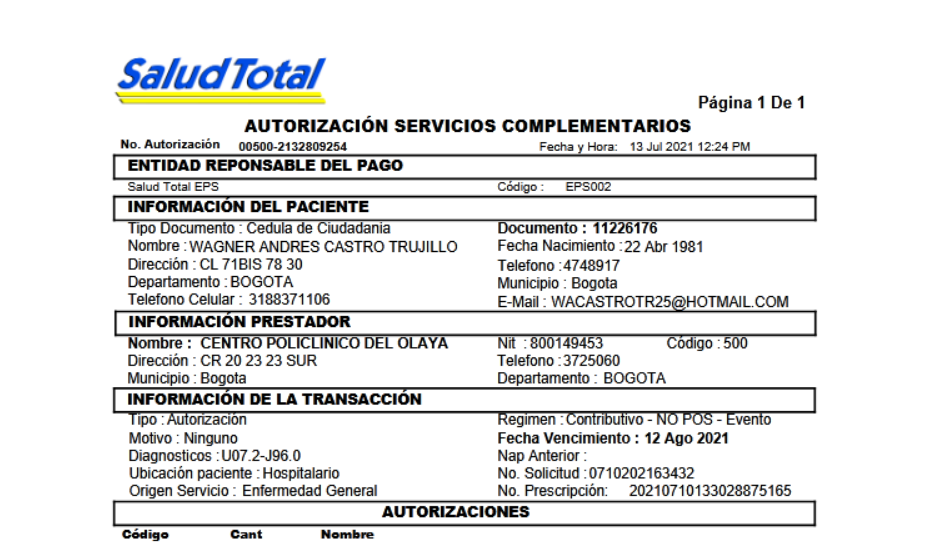


圖21：Salud Total 機構資料外洩資訊

1. 醫療領域資安案例分析—保護遠距醫療病患監測生態系統

根據2022年2月國家標準暨技術研究院(National Institute of Standards and Technology，NIST) 發布保護遠距醫療病患監測生態系統指南，顯示醫療服務機構(Healthcare Delivery Organizations，HDO) (以下簡稱HDO)如何實施網路安全和隱私控制，以增強遠距醫療服務的安全性。遠距病人監測服務(Remote Patient Monitoring，RPM)(以下簡稱RPM)可以帶來方便、經濟高效且因應疫情關素其需求不斷增長，然而它的便利性亦可能帶來資安與隱私風險。一般醫療設施環境常建置監測系統來監測病人生理特徵，然而RPM的監測系統所佈署的環境較為不同，其主要佈署於病患家中，因此可能無法提供與醫療機構環境相同的網路安全或實體安全控制資安防護水準，以防止醫療服務遭到濫用或機敏資料遭到揭露。值得注意的是，沒有隱私保護的RPM系統，或RPM生態系統中未提供完善的網路安全防護與通訊安全，此將影響病患資料的機密性，進而影響醫病關係。

本指南探討醫療服務提供者部署RPM設備於病患家中的情形，RPM設備會定期選取生物辨識資料，將其資料傳送到臨床醫療團隊，並允許病患與臨床醫生進行交流，而無需病患親自至HDO。RPM 可以根據病患的需求進行醫療，而不受其他地理限制。RPM定期收集生物辨識資料，能夠讓臨床醫生了解病患的健康狀況。藉由更多的資料集，臨床醫生可以監測病患的狀況，並做出診斷和具有更可靠資訊的治療決策。RPM解決方案允許語音和視訊交流。值得注意的是，RPM除了利用生物辨識資料外，它們甚至協助建立病患與臨床醫生的關係。

實施RPM生態系統將涉及多方複雜的環境。在保護遠距醫療病患監測生態系統指南的參考架構中，美國國家網路安全卓越中心(National Cybersecurity Center of Excellence，NCCoE)(以下簡稱NCCoE)考慮在部署於含有RPM 生態系統的三個不同領域：病患家庭環境、遠距醫療平台供應商，以及HDO。NIST團隊參與提供雲端服務的遠距醫療平台、促進病患之間的語音和視訊會議的平台供應商和與HDO。遠距醫療平台供應商提供與管理的生物辨識設備，部署於病患住家中，並於病患住家與HDO之間採用通訊與傳送資料方式。NCCoE建立一個實驗室環境來模擬遠距醫療生態系統，執行一項風險評估，並進行一個實例演示HDO如何使用根據網路安全技術標準，並與遠距醫療平台供應商確保病患住家中其隱私和保護生物辨識設備。本次專題報告將先以遠距醫療的系統架構及框架來介紹，後續再針對詳細安全規格與規範進行介紹。

* 1. 網路安全架構

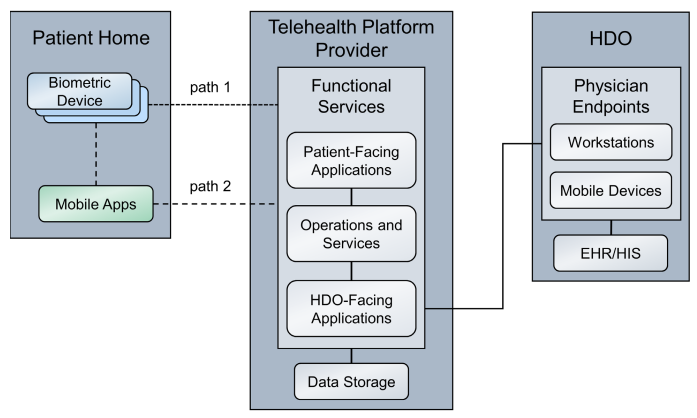
圖22顯示高階的RPM分佈式架構，其架構包含兩個網路通訊通過的主要路徑。路徑1顯示生物辨識設備與遠距醫療平台供應商通訊，而路徑2顯示行動應用程式的使用，行動應用程式在端口設備（即配置的平板電腦）上運行。對於路徑2，病患使用平板電腦從生物辨識設備收集資料。路徑2不涉及生物辨識設備與遠距醫療平台供應商之間資料傳輸。反之，路徑1顯示病患可透過平板電腦收集生物辨識資料與遠距醫療平台供應商進行資料交換。

圖22：RPM分佈式架構

(資料來源: NIST SPECIAL PUBLICATION 1800-30)

4.1.1分層架構

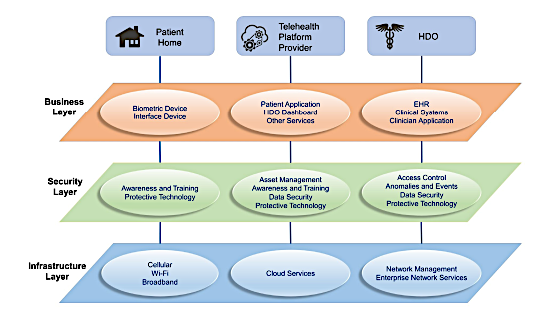
美國NCCoE 醫療實驗室將分佈式架構分為三個層面：企業、安全以及基礎設施。企業層面專注於功能部分，包括生物辨識讀卡器與病患互動；安全層面從概念上描述NCCoE實驗室如何實施安全部分。病患主要透過企業層面，使用生物辨識設備和端口設備與臨床醫療團隊進行溝通。遠距醫療包含一個安全層面的元件，用於隔離 RPM 之間的網路流量。遠距醫療平台供應商也實現三個層面，其中企業層面包括有助於處理病患資料、網路、語音會議功能的服務。安全層面用於保護環境的元件組成，例如身分驗證機制、憑證管理系統、安全日誌記錄功能等。基礎設施層面包含可以作為雲端服務的網路和伺服器元件。圖23顯示每個領域相交的三個層面示意圖以及組織如何在實驗室環境中實現它們。

圖23：企業、安全、基礎設施架構等層面示意圖

(資料來源: NIST SPECIAL PUBLICATION 1800-30)



4.1.2安全能力

NIST團隊建置一個實驗室環境，該環境代表企業、安全、基礎設施架構等層面。在構建 HDO環境時，團隊建立在分區網路之上NIST SP 1800-8 中描述的架構，詳細資訊請參考https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-wip-nist-sp1800-8.pdf，該團隊使用網路分區的方法作為 RPM 生態系統的標準基礎設施。根據標準，團隊選擇相關的安全功能以實現適當的領域。選定的安全功能包括：

1.遠距醫療平台供應商

2.風險評估控制

3.身分管理、身分驗證和存取控制

4.資料安全

5.異常和事件以及安全持續監控。

RPM 環境分佈在三個需要病患、遠距醫療平台供應商和 HDO 的參與並確保降低風險。本節架構描述部署三個領域中的元件，具有可能明顯影響每個領域的威脅和風險。作為組織實施 RPM 解決方案，他們必須包含參與、管理識別和防範與可能發生的隱私和網路安全事件。在HDO 可能的影響範圍中，將能力部署到其他領域。HDO 應建立調查問卷或他們可能在評估第三方（如遠距醫療平台供應商）時使用的審計方法。HDO 和遠距醫療平台供應商必須遵守監管相關要求，以確保病患的隱私和網路安全。遠距醫療平台供應商為第三方，可以實施不具備安全功能且為必須使用HDO 標準的工具。遠距醫療平台供應商應採用類似的措施解決風險問題，例如 NIST 網路安全框架(https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)和風險管理框架(https://csrc.nist.gov/projects/risk-management/about-rmf)，描述風險和控制方法。在評估遠距醫療時平台供應商、HDO 應審查隱私和安全控制政策以及其他檔案，以確保遠距醫療平台供應商採取的緩解措施工具符合 HDO的要求。HDO和遠距醫療平台供應商在實施安全功能時可能會遇到病患部分相關困難。病患可能會發現複雜或繁瑣操作。因此，他們不太可能參與RPM計畫。遠距醫療平台供應商可以實行端點設備的安全功能，例如生物辨識傳感器或行動設備等。HDO與遠距醫療平台供應商合作，可以提供教導和與病患討論如何使用RPM部署。

4.1.3最終架構

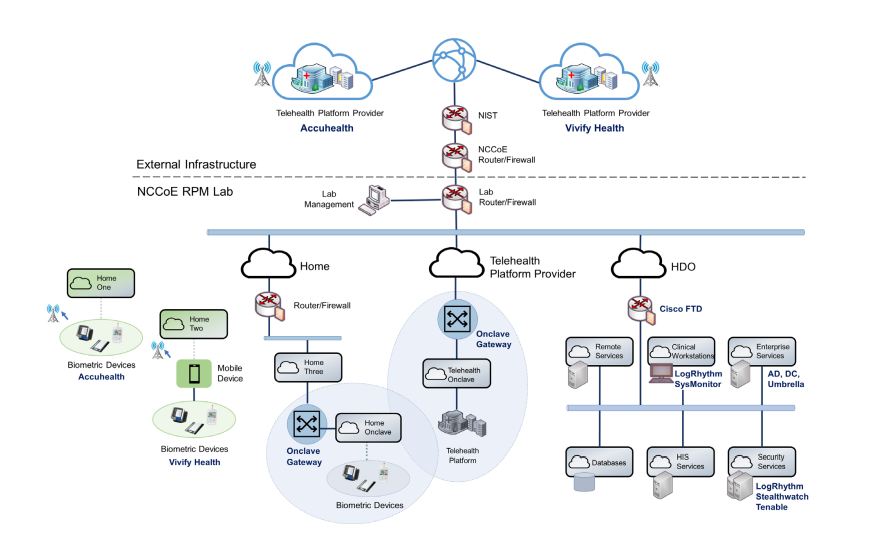
NIST團隊構建一個參考架構，包括兩個用於生物辨識的通訊路徑設備。在第一種情況下，病患住家中的生物辨識設備與遠距醫療進行通訊蜂巢式資料通訊平台供應商。兩家遠距醫療平台供應商：Accuhealth 和 Vivify ，其提供雲端代管解決方案，生物辨識設備分別部署於家庭環境，該架構還包括一個具有六個網路區域的 HDO 環境：遠距服務、臨床工作站、企業服務、資料庫、HIS 服務和安全服務，詳細資訊請參考圖24。

圖24：最終架構圖

(資料來源: NIST SPECIAL PUBLICATION 1800-30)

* 1. RPM測試實例

本節使用 NIST 網路安全框架，詳細資訊請參考https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf模擬RPM相關應用實例，使我們能夠系統性的考慮參考設計對於預期安全特性的程度，詳細資訊請參考表34。

表34：RPM資產管理類別測試範例

|  |  |
| --- | --- |
| 網路安全框架類別 | 資產管理 |
| 測試要求 | (CR-1)設備管理 |
| 描述 | 證明能夠驗證配置的設備是  與已參加 RPM 的預期病患互相關聯程序 |
| 條件 | 已提供醫生等級的 Accuhealth 帳戶。Accuhealth RPM 設備已配置並交付，包括以下內容（混淆序列號）：   1. 血壓計 (1234567) 2. 血糖監測系統(22334455) 3. 電子磅秤(987654)   Accuhealth 已收集樣本病患並將其關聯使用上面列出的 RPM 設備，包括：   1. Regina Houston (1234567) 2. Regina Houston (987654) 3. Janelle Kouma (22334455) |
| 步驟 | 驗證 Accuhealth 系統中的病患/設備關聯:  1.以醫生等級使用者帳戶登入Accuhealth平台  2.點擊病患詳細訊息  3.在選擇病患條件下，再選擇Regina Houston  4.在選擇示意圖條件下，再選擇簡介  5.查看 Regina Houston 的病患資訊  6.轉至設備資訊  7.檢查設備ID欄位是否選取設備序列號、1234567 和 987654與Regina Houston 互相關聯  8.在選擇病患條件下，選擇Janelle Kouma  9.查看 Janelle Kouma 的病患資訊  10.轉至設備資訊  11.檢查Device ID欄位是否選取設備序列號、22334455與 Janelle Kouma 相關驗證來自 RPM 設備的資料是否正在傳送至Accuhealth並與正確的病患互相關聯  12.對於以下設備，打開每個設備並按照提供進行測量的相關說明：   1. 血壓計 (1234567) 2. 血糖監測系統(22334455) 3. 電子磅秤(987654) 4. 記錄時間和測量數字作為備註 5. 以醫生等級使用者帳戶登入Accuhealth平台 6. 單擊病患詳細資訊 7. 在選擇病患條件下，選擇Regina Houston 8. 在選擇示意圖條件下，選擇Vitals 9. 檢查血壓和體重測量值是否正確 10. 在選擇病患條件下，選擇Janelle Kouma 11. 在選擇示意圖條件下，選擇Vitals 12. 檢查血糖監測是否存在 |
| 預期成果 | * Accuhealth可以配置RPM設備並將它們連結到參與RPM的病患 * Accuhealth可以選取生物辨識測量於使用指定RPM 設備的患者 |
| 實際成果 | Accuhealth 提供了其遠距醫療平台的一個實例與醫生等級的使用者帳戶和與這些相關的樣本病患帳戶。我們還收到了來自 Accuhealth的三款RPM 設備：血壓計、血糖監測系統、電子磅秤。Accuhealth 將這些 RPM 設備與樣本病患互相關聯，我們通過檢查每個設備的設備 ID 資訊來驗證病患。收到設備後，我們對其進行配置並記錄每個樣本的測量值。 隨著進行測量後，我們使用以下命令登入 Accuhealth 平台之醫生等級的使用者帳戶並查看每個人的生命徵象資訊。正如預期的一樣，血壓、體重測量值與 Regina Houston有關且血糖測量與 Janelle Kouma 病患記錄有關。 |

1. 醫療領域資安趨勢分析-軟體材料清單最基本要項

現今大多數的軟體或韌體開發均依賴第三方套件(包括函式庫、可執行二進制文件或開源原始碼)，且相較於硬體供應鏈的管理，設備製造商對於軟體供應鏈的掌握與了解卻相對的缺乏，使得軟體或韌體中包含了許多未被記錄的第三方套件，並引入了不必要的已知弱點(CVE)，讓使用者與設備製造商曝露在包含個資外洩、商譽受損等各種風險造成的影響與損失。 軟體材料清單(Software Bill of Materials，SBOM)是構成軟體的成分表，用來描述軟體的組成架構、內容、生產與整合軌跡，以提供軟體組成透明性。美國 國家電信暨資訊管理局（National Telecommunications and Information Administration, NTIA），從2019年開始起草並核定了一系列的文件，提供SBOM的相關資訊與指引。

* 1. 摘要

SBOM為生產、購買和操作軟體的人員提供資訊，以增強他們對供應鏈的理解，從而帶來多種好處，尤其是跟蹤已知和新出現的漏洞和風險的潛力。SBOM不會解決所有軟體安全問題，但會形成一個基礎資料層，在此基礎上可以構建進一步的安全工具、實踐和保證。本文件中定義的最小元素是支持基本SBOM功能的基本部分，並將作為不斷發展的軟體透明度方法的基礎，詳細資訊請參考表35。這些最低限度的要項包括三個廣泛的、相互關聯的領域，詳細資訊請參考5.2。

表35：最基本要項表

|  |  |  |
| --- | --- | --- |
| 項次 | 要項 | 說明 |
| 1 | 資料範圍 | 記錄應跟蹤的每個元件的基準資訊：供應商、元件名稱、元件版本、  其他唯一識別碼、依賴關係、SBOM資料的作者以及時間戳。 |
| 2 | 自動化支持 | 能夠以機器和人類可讀格式，自動生成SBOM，以允許在整個軟體生態系統中進行擴展，用於生成和使用SBOM的資料格式  包括SPDX、CycloneDX和SWID。 |
| 3 | 實踐和流程 | 定義SBOM請求、生成和使用的操作  包括：頻率、深度、已知未知數、分發和遞送、存取控制和容錯。 |

本文件確定了支持基本應用的最基本要項，例如漏洞管理、軟體庫存和許可證。期望未來可開始就推薦的SBOM功能進行應用，並拓展可被進一步重視的最基本要項，例如關鍵的安全功能，SBOM完整性，以及跟蹤更詳細的供應鏈資料，詳細可以參考此篇原文。隨著其他SBOM元素變得可行、經過測試並設置到工具中，它們將支持更廣泛的應用。

* 1. 最基本要項

整個SBOM的最小組成部分(要項)是三個相互關聯且廣泛領域。這些要項將使軟體透明化的方法不斷發展。未來肯定會包含更多細節或技術進步，組織和機構可能會要求更多，軟體供應鏈的透明度能力可能會隨著時間的推移而提高和發展。 一個軟體可以表示為一個階層樹，由元件組成，這些元件又可以具有子元件，依此類推。元件通常是來自其他來源的「第三方」，但也可能是「第一方」，也就是說，雖然來自同一供應商，但能夠被標示為獨立的、可跟蹤的軟體單元。每個元件都應該有自己的SBOM，列出它們的元件，構建階層樹。資料範圍適用於每個元件，而這些元件又使用工具和格式進行編碼進行自動化支持，以便按照定義的實踐和流程。

1. **資料範圍**

SBOM的核心是一個一致的、統一的結構，它獲得並呈現用於理解組成軟體的元件的資訊。資料範圍包含有關應該跟蹤和維護的每個元件的基準資訊，這些範圍的目標是能夠充分識別這些元件，以便在整個軟體供應鏈中跟蹤它們，並將它們映射到其他有益的資料來源，例如漏洞資料庫或許可證資料庫。詳細資訊請參考表36。

表36：最基本要項資訊範圍

|  |  |  |
| --- | --- | --- |
| 項次 | 資料範圍 | 說明 |
| 1 | 供應商名稱 | 創建、定義和標識元件實體的名稱 |
| 2 | 元件名稱 | 分配給由原始供應商定義的軟體單元的名稱 |
| 3 | 元件版本 | 供應商用來說明軟體從先前已標識的版本發生變化的識別碼 |
| 4 | 其他唯一識別碼 | 用於識別元件或用作相關資料庫的查找鍵的其他標識別碼 |
| 5 | 依賴關係 | 表示軟體元件如何組合在壹起，上游元件X包含在軟體Y中的關係 |
| 6 | SBOM資料的作者 | 為此元件創建SBOM資料的名字 |
| 7 | 時間戳 | 記錄SBOM資料組裝的日期和時間 |

這些範圍中的大多數有助於識別元件以明確啟用映射到其他資料來源。供應商是指軟體元組件的發起者或製造商，元件名稱由供應商確定，如果可能，應支持記錄供應商和元件名稱的多個名稱或別名的功能。 缺乏單一、易於理解和廣泛使用的軟體名稱，可能會帶來一定的挑戰。最佳實務作法是盡可能使用現有識別碼。如果沒有識別碼，則使用現有的元件標示系統，即使用可理解的供應商名稱與元件名稱。

軟體版本的複雜性是軟體生態系統的多樣性的另一個例子。因此如何在元件識別方法中建立一些靈活性，不同類型的軟體或軟體供應商以不同的方式跟蹤和分配版本。解決這個問題已超出了最初的SBOM討論的範圍。對於這些最低限度的要項，版本是由供應商提供的，因為該方對跟蹤與維護有問題的軟體負有最終責任，類似於元件名稱，版本字串的預期功能是識別特定的程式碼交付。雖然有版本控制最佳做法（例如語義版本控制），但它們在現今絕不是普遍存在。 其他唯一識別碼支持資料映射的自動化工作，並且可以在不確定的情況下加強確定性，常用唯一識別碼的示例有通用平台枚舉(Common Platform Enumeration，CPE)、軟體標識標籤(Software Identification，SWID)、統一資源定位符(Package Uniform Resource Locators，PURL)，這些其他識別碼可能不適用於每個軟體，但如果它們存在，則應該被使用。資料映射是大型資料遷移和資料集成過程的必要組成部分。它是一種將資料來源（系統A）中的欄位與資料倉庫或其他儲存庫（系統B）中的目標欄位進行匹配的機制。 依賴關係反映了軟體包含的方向性，它能夠表示從一個軟體到其元件和潛在子組件的傳遞性，最後，特定於SBOM的元資料有助於跟蹤SBOM本身。

作者反映了元資料的來源，可能來自SBOM中描述的軟體的創建者、上游元件供應商或某些第三方分析工具。請注意，這不是軟體本身的作者，只是描述性資料的來源。組裝資料時的時間戳記錄-SBOM創建點，這些進一步支持資料的來源，並幫助識別SBOM的更新版本。這些資料範圍為SBOM資料來源提供上下文，並且可以潛在地用於進行信任確定。

1. **自動化支持**

自動化支持，包括自動生成和機器可讀性，允許跨軟體系統擴展，特別是跨組織邊界。利用SBOM資料需要工具，這需要可預測的實施和資料格式，例如，一些機構可能希望將此功能集成到其現有的漏洞管理實踐中，其他人可能希望對安全策略的合規性進行即時稽核，自動化將是兩者的關鍵，而這又需要通用的、機器可讀的資料格式。

單一標準可以提供簡單性和效率，而生態系統中存在多種資料格式，並被用於生成和使用SBOM，這些規範是通過開放流程製定的，有國際參與，除了機器可讀之外，這些資料格式也是人類可讀的，更好地支持故障排除和創新，更重要的是，這些標準已被認為可用於核心資料範圍並使用通用資料語法表示。用於生成和使用SBOM的資料格式有：

1. Software Package Data eXchange，SPDX (https://spdx.dev/)
2. CycloneDX (https://cyclonedx.org/)
3. Software Identification (SWID) tags (http://dx.doi.org/10.6028/NIST.IR.8060)

SBOM必須以這些可互操作的格式之一跨組織邊界傳送，如果出現與其他資料格式兼容的新規範，則應在SBOM的最小元素上下文中包含自動化支持，類似地，如果確定資料格式不再交叉兼容，或者沒有得到積極維護和支持SBOM用例，則應從自動化要求中刪除該資料格式，作為SBOM最基本要項的一部分，不應包括使用專有資料格式的標準，這實現了在現有工具的基礎上構建易於採用、支持未來發展和可擴展性的目標。

1. **實踐與流程**

SBOM不僅僅是一組結構化的資料，要將其集成到安全開發生命週期的營運中，組織應遵循某些專注於SBOM使用機制的實踐和流程，在要求或提供SBOM的任何政策、合約或安排中，都應明確說明許多要項，其中一些（例如頻率）有直接的要求，在其他情況下（例如，存取），存在多種實踐並且正在開發更多實踐，因此最基本要項是指定特定的要求。

1. **頻率**：如果使用新版本或版本更新軟體元件，則必須創建新的 SBOM以反映軟體的新版本，這包括用於集成更新的元件或依賴項的元件構建。同樣，如果供應商了解有關基礎元件的新細節或希望更正現有SBOM資料中的錯誤，則供應商應發布新的、修訂的 SBOM。
2. **深度**：SBOM應包含所有主要（頂級）元件，並列出其所有傳遞依賴項，至少，所有頂級依賴項必須以足夠的詳細資訊列出，以便遞歸地查找傳遞依賴項。 進一步了解圖表將提供更多資訊，隨著組織開始SBOM，由於對子元件供應商的現有要求，可能不容易獲得超出主要元件的深度，最終採用SBOM流程將能夠通過子元件級別的更深層次的透明度獲得更多深度，應該注意的是，某些用例需要完整或大部分完整的圖表，例如能夠「證明否定」給定元件不在組織的網路上。 SBOM消費者可以通過傳遞步驟數指定深度，或者，他們可以在操作方面指定深度。這可能包括軟體屬性，例如「所有非開源軟體」，或具有特定功能或複雜性的所有元件，組織還可以通過對報告和修復SBOM中列舉的元件中的漏洞和未列舉的元件中的漏洞提供不同的要求來激勵更大的報告深度和完整性，此類規範超出了這些最基本要項的範圍。
3. **已知的未知數**：對於未在SBOM中枚舉完整依賴圖的實例，SBOM 作者必須明確標識「已知未知數」，也就是說，依賴關係資料在沒有進一步依賴關係的元件，和依賴關係的存在未知且不完整的元件之間做出了明確的區分，這必須集成到自動化資料中，為避免錯誤假設，對資料的默認解釋應為資料不完整，資料的作者應該肯定地說明元件的直接依賴關係何時已被完全枚舉，或者元件何時沒有進一步的依賴關係，現今，這是在依賴關係資料範圍中實現的。
4. **分發和遞送**：SBOM應及時提供給需要它們的人，並且必須具有適當的存取權限和角色，SBOM資料可以伴隨軟體的每個實例，或者僅可存取並直接映射到相關軟體的特定版本（例如，通過特定於版本的URL），在軟體供應鏈中共享SBOM資料可以被認為包括兩個部分：如何讓SBOM的存在和可用性被知曉（廣告或發現），以及如何將SBOM檢索或傳輸給擁有適當權限的人權限（存取），與軟體保障的其他領域類似，不會有一種萬能的方法，任何提供SBOM的人都必須有一些方法來使它們可用並支持消化，但這可以依賴於現有的機制，SBOM遞送也可以反映軟體的性質：存在於端點上的可執行文件可以將SBOM資料與編譯後的程式碼一起儲存在磁碟上，而嵌入式系統或線上服務可以具有指向在線儲存的 SBOM資料的指針。
5. **存取控制**：許多供應商，包括開源維護者和擁有廣泛可用軟體的供應商，可能認為公開SBOM資料最符合他們的利益，其他組織，尤其是起初，可能希望對這些資料保密，並限制對特定客戶或用戶的存取。如果需要存取控制，則必須指定條款，包括將SBOM資料集成到用戶安全工具中的特定許可和便利，此類規範可以通過許可、合約或其他現有機制來確定，這些機制用於限制軟體本身的使用和權利。
6. **容錯**：最後的實踐領域，即錯誤的適應，應該建立在SBOM的初始實施階段，允許遺漏和錯誤，正如許多評論員所觀察到的，雖然供應鏈資料的內部管理可能是最佳實踐，但它仍在不斷發展，美國政府已將SBOM確定為推動軟體保障和供應鏈風險管理的優先事項，從今天開始總比等待完美好。鑑於缺乏完美，SBOM的消費者應該明確容忍偶爾的偶然錯誤，這將促進工具的不斷改進，供應商應在遇到過去SBOM的問題時提供更新的資料。消費者應鼓勵這些更新，歡迎善意提供的補充和更正而不受懲罰。由上所述得知，針對頻率部分，當已知新資料時，應發布更新的SBOM。值得注意的是，這種容忍不應適用於故意混淆或無知。
   1. 結論

此報告是美國政府、私營部門和學術界的利益相關者仔細考慮投入，SBOM的最基本要項是一個起點。基於今天可以想像的內容，確定什麼構成SBOM的最小元素的過程不應到此結。由於上述拓展最低限度要項和SBOM的未來中確定的附加要項也變得可行、經過測試並內置到工具中。因此，應將這些要項添加到最低限度要項中。

1. 參考文獻
2. NIST SPECIAL PUBLICATION 1800-30，Securing Telehealth Remote Patient Monitoring Ecosystem, 2021, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-30.pdf>
3. https://www.informationsecurity.com.tw/article/article\_detail.aspx?aid=9316
4. https://kknews.cc/news/zb29jxl.html
5. https://fossa.com/blog/minimum-required-elements-software-bill-of-materials/