居家醫療的安全連接——第一部分：

診所之外的挑戰

本文介紹 ADI 如何提供安全連接解決方案，以解決居家醫療中使用的各種醫療裝置的獨特安全要求和患者安全擔憂。

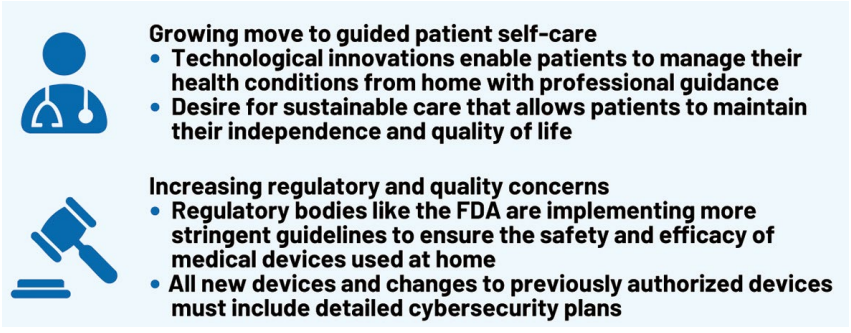
■作者：Jackson Coole /ADI 系統應用工程師
Michael Haight / ADI 產品線總監

引言

本文以「一次性醫療用品的安全認證」中描述的一次性醫療用品安全認證為基礎，探討醫療保健日益從醫院轉移到患者家中的趨勢 (圖 1)，並討論在醫療設施之外提供醫療保健服務的獨特安全挑戰，以及探討在網路傳輸過程中保護資料安全的相關要求。

居家醫療的趨勢

圖 1：居家醫療的趨勢



引導式患者自我護理逐漸普及

在技術創新的推動下，患者得以在舒適的家中管理自己的健康狀況，「引導式患者自我護理」模式也隨之展現出強勁的發展態勢。穿戴式裝置、手機健康應用和遠端醫療平台等先進工具透過提供即時健康資料和專業指導，使患者能夠監測自己的病情，並對自身的護理做出有理有據的決定。這種向自我護理的轉變不僅關乎便利性，也是為了推廣可持續的醫療健康應用。引導式自我護理不僅能夠讓患者保持獨立性、保證生活品質、支援長期健康管理，且拓寬了醫療健康護理的途徑，同時還能有效減輕醫療機構的負擔。

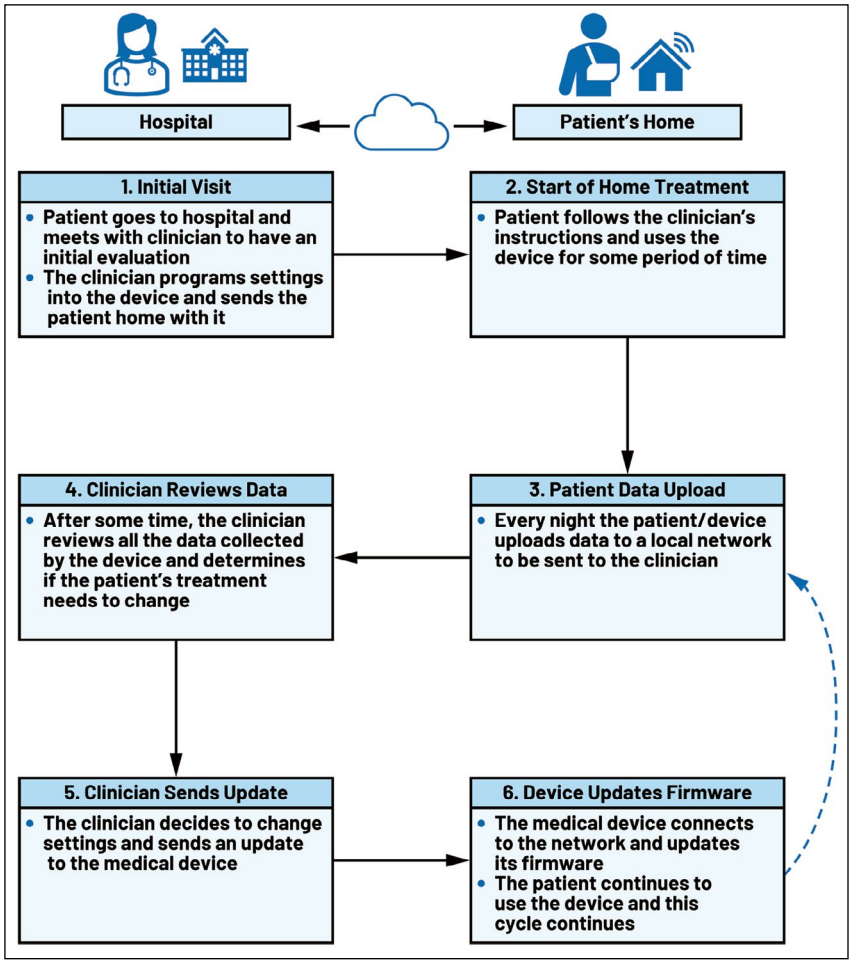
監管和品質要求不斷升高

隨著居家醫療服務的覆蓋面不斷擴大，FDA 等監管機構正著手建置更嚴格的指導方針 (FDA-2021-D-1158；《國會法案 HR 2617》第 524B 條；UL2900-2-1；IEC62443)，以確保家用醫療裝置的安全性和療效。這些規定對於保護患者和維持高標準護理非常重要。新裝置和現有裝置的改版，現在必須包含詳細的網路安全計畫，以解決潛在的漏洞並保護敏感的健康資料。加強對合法合規和品質保證的重視，對於建立人們對居家醫療方案的信任，以及確保患者獲得安全、可靠、有效的護理非常重要。

居家醫療的典型工作流程

1. 初步評估和裝置設定：居家醫療流程的起點通常是患者前往醫院或診所初診，由臨

圖 2：居家醫療的典型工作流程



床醫生進行全面評估 (圖 2)。就診期間，臨床醫生會評估患者的病情並確定適當的治療方案。然後，臨床醫生根據患者的具體需求，將相應的設定寫入醫療裝置。配置完成後，患者會收到詳細說明，介紹如何在家中有效使用裝置。

2. 開始居家治療：患者返家後，按照臨床醫生的指示和醫囑要求，開始使用醫療裝置進行治療。這段時間對於患者適應裝置並將其融入日常生活非常重要。提醒、警報和直覺易用的介面等特性，有助於患者遵循治療計畫，提升自主管理能力，並改善健康狀況。

3. 患者數據上傳：居家醫療的一個關鍵部分是持續監測和傳輸患者資料。這些資料可能包括生命體徵、藥物依從性和其他相關的健康指標。例如，在裝置連接到充電器且患者入睡時，裝置可自動將患者的日常活動記錄上傳到本地網路；裝置也可以僅在發生特定事件時發送資料 (例如檢測到使用者操作錯誤或不良事件)；或者由患者手動將資料登錄手機應用來實現資料傳輸。資訊的無縫傳輸確保臨床醫生能夠獲得最新的資料，進而在必要時及時干預和調整治療方案。

4. 臨床醫生評估資料：經過規定的時間後，臨床醫生會查看醫療裝置收集的資料。透過這種綜合分析，臨床醫生可以評估患者的康復進展，並判斷是否需要調整治療方案。裝置提供的詳細資料讓臨床醫生能夠進行更全面性的評估，進而比傳統定期檢查更能精準地掌握患者的健康狀況。這種積極主動的方法有助於及早發現潛在問題，並調整治療方案以更進一步滿足患者的需求。

5. 臨床醫生發送更新：如果臨床醫生決定需要調整治療方案，可以遠端更新醫療裝置的設定。治療方案的變化可以是調整關鍵感測參數 (如壓力感測器的增益)，或改變給藥 / 治療進行的頻率。為了實現這些調整，通常需要將新版本的韌體安全上傳到患者家中的醫療裝置。此更新需要安全地發送到裝置，確保患者接受最新、最有效的治療。遠端調整能力是現

代居家醫療系統的一大優勢，不僅減少了頻繁親自就診的需求，而且提升了醫療護理的彈性和回應速度。

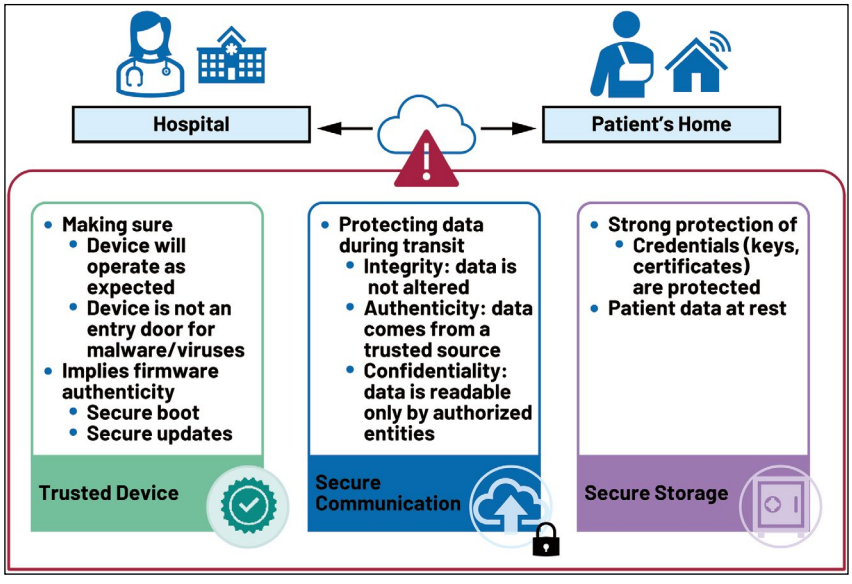
6. 裝置更新韌體：一旦臨床醫生發送更新，醫療設備通常會連接到網路，以接收和安裝韌體更新。此過程通常自動進行，以儘量減少患者干預，確保設備採用最新設置和安全協議運行。更新完成後，患者將繼續使用原設備進行後續治療。資料收集、查看和調整構成一個迴圈並持續進行，使得醫療環境能夠動態回應患者不斷變化的需求。

居家醫療的安全挑戰

為了確保患者資料和醫療設備的安全，還有一些重大的挑戰需要克服。由於對數位平台和聯網裝置的依賴，敏感的健康資訊面臨潛在的網路威脅，包括資料洩露和未經授權的存取。解決這些安全挑戰對於維護患者信任、確保遵守醫療法規和保護居家醫療服務的完整性非常重要。下一節將說明典型居家醫療工作流程的每個步驟所特有的安全挑戰 (圖 3)。

1. 初步評估和設備設定：在初次就診和開始居家治療期間，必須解決一些安全擔憂。其中一個關鍵方面是安全引導，目的是確保裝置在啓動時只運行受信任的軟體。如此惡意軟體就無法載入，裝置的功能和患者的安全也就不會受到影響。此外，安全資料儲存對於防止未經授權的存取和篡改非常重要。這涉及對裝置上儲存的資料進行加密，並進行嚴密的存取控制，以確保只有授權人員才能修改裝置設定。最後，必須保證韌體參數的完整性。例如，對於患者安全而言，必須確保 10 mL/hr 的劑量設定不會被錯誤地改成 100 mL/hr。這個要求可以透過驗證韌體真實性和完整性的加密演算法校驗碼和數位簽章來實現。
2. 患者資料上傳和傳輸：當患者資料從醫療裝置上傳至臨床醫生時，需要採取多種安全措施來保護傳輸過程中的資料。真實性是首要考量，必須確保臨床醫生收到的資料確實來自相應的患者。這可以透過唯一患者識別字和安全身份驗證協議來實現。完整性也非常重要，必須確保資料在傳輸過程中不被更改，此時可以利用雜湊和數位簽章等技術來驗證資料是否保持不變。臨床醫生依靠準確可靠的資料來評估患者的病情，並相應地調整治療方案。如果資料損壞，則可能導致評估不正確。例如，損壞的資料點可能錯誤地指示患者的血壓處於穩定狀態，但實際上血壓已升高到危險水準。最後，確保機密性對於保護傳輸過程中的敏感患者資訊至關重要。這涉及保護資料免遭未經授權的

圖 3: 居家醫療的安全挑戰



存取，並確保資料在傳輸過程中保持私密。機密性可以透過安全通訊協議 (如傳輸層安全 (TLS) 和虛擬私人網路 (VPN)) 實現，此類協定會對傳輸的資料進行加密。此外，進行嚴格的存取控制和身份驗證機制可確保只有授權人員才能存取患者資訊。

3. 韌體更新：當臨床醫生向醫療裝置發送更新時，必須確保更新過程的安全。未經授權的存取或更新可能賦予入侵者改變醫療裝置行為的許可權；在最壞情況下，甚至會讓入侵者完全掌控裝置。一種常見的攻擊方法是惡意軟體注入，也就是將惡意程式碼插入韌體更新中。如果攻擊者成功安裝欺詐性韌體，則可能導致嚴重後果。例如，被入侵的裝置可能會在未經授權的情況下開始傳輸機密和敏感性資料，如來自可攜式健康監護器的私人醫療資訊。更進一步來說，惡意韌體可能會將加密金鑰公諸於世，以致破壞整個系統的安全。此外，裝置可能被迫錯誤運行，對患者安全和資料完整性造成重大風險。因此，必須驗證新韌體的真實性，確認其來自可信來源。韌體來源的真實性可透過數位簽章和證書進行驗證。就像醫療裝置在診所首次設定時一樣，韌體更新的完整性非常重要，必須確保所有參數準確且未被篡改。韌體的完整性可以透過加密校驗碼和完整性檢查來驗證。最後，在韌體更新的傳輸過程中，必須保持機密性以保護敏感性資料。加密升級韌體則可確保其不會被未經授權方攔截和存取。

MAXQ1065 如何解決上述安全問題

MAXQ1065 是一款安全輔

圖 4：MAXQ1065 解決了居家醫療環境中的諸多安全問題

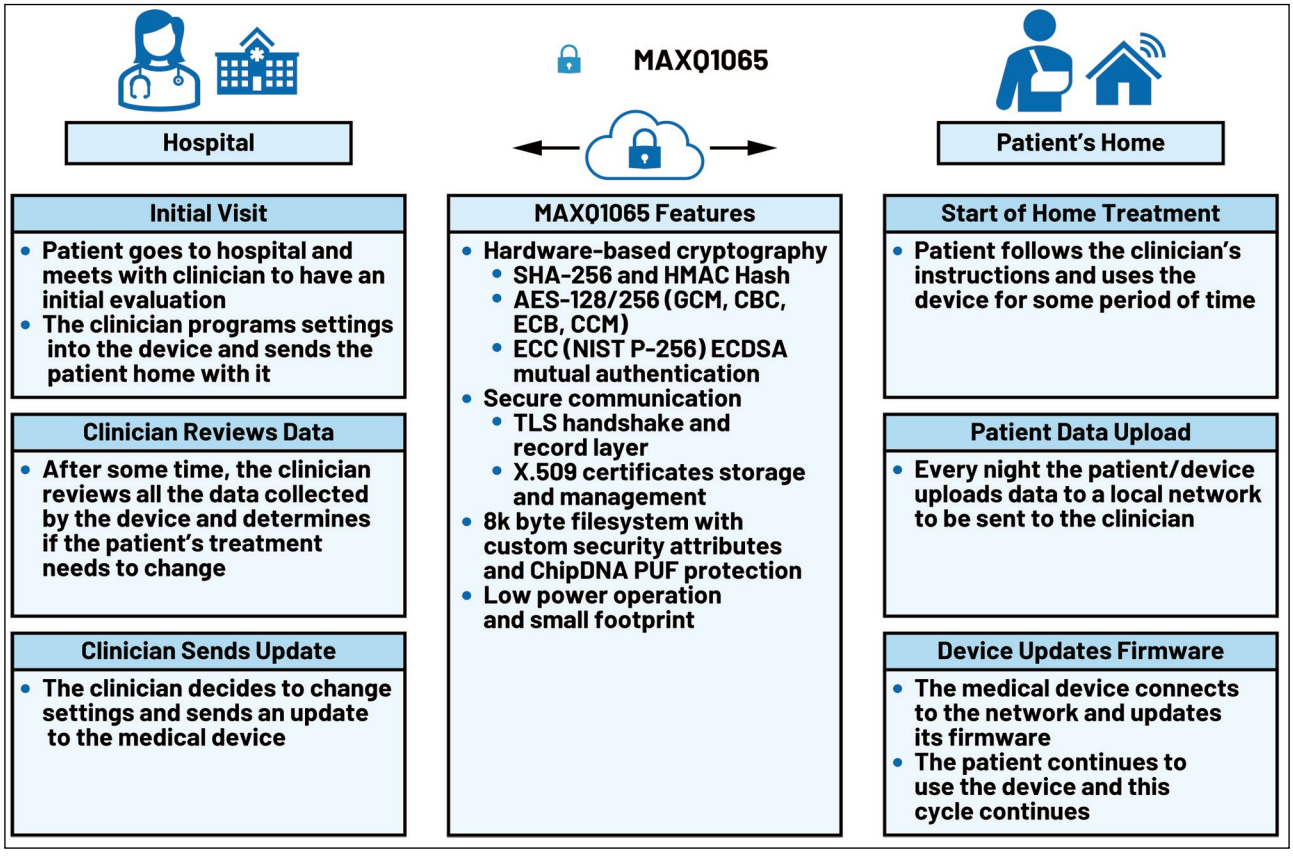


表 1：MAXQ1065 特性

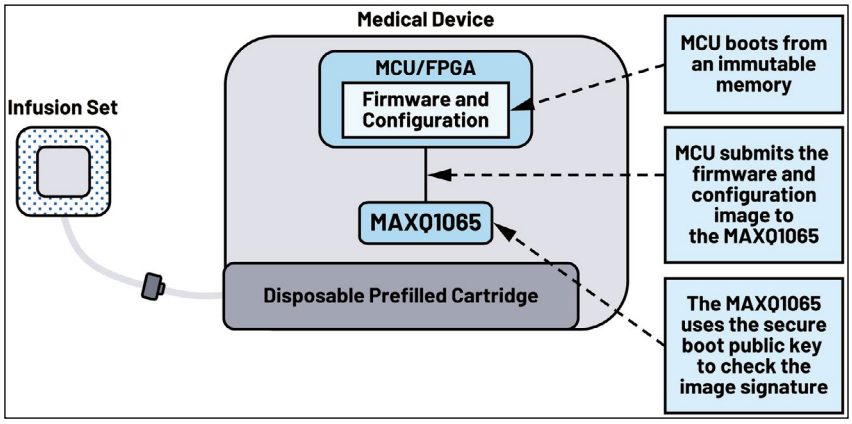
特性	說明
基於硬體的加密	SHA-256 和 HMAC 雜湊；AES-128/256（GCM、CBC、ECB、CCM）；ECC (NIST P-256) ECDSA 相互認證。
ChipDNA PUF 技術	提供對加密金鑰和敏感性資料的終極保護。 透過確保安全金鑰永遠不會靜態駐留在暫存器或記憶體中，也不會離開 IC 的電氣邊界，以此避免安全密碼的洩露。
安全通訊	支援透過 TLS/DTLS 1.2 協定安全傳輸資料。TLS 握手和記錄層。X.509 憑證存放區和管理。
安全儲存	8 kB 的安全儲存空間，用於儲存使用者資料、金鑰、證書和計數器。
篡改檢測	識別並回應物理篡改企圖。
通訊介面	SPI/I2C。
低功耗	居家醫療裝置通常依賴電池供電，因此能源效率是一個關鍵因素。MAXQ1065 的超低功耗確保裝置可以長時間運行，無需頻繁更換電池。這對於穿戴式健康監護儀和其他可攜式醫療裝置尤其有利。

助處理器，提供整套加密功能，用於信任根、相互認證、資料機密性和完整性、安全引導、安全韌體更新和安全通訊 (圖 4)。表 1 列出了其主要特性。

安全引導和安全韌體更新

在基於非對稱加密的安全韌體下載過程中，基本原理是韌體開發者使用私密金鑰進行簽名，並使用醫療裝置上儲存的對應公開金鑰進行驗證。透過這種方法，尤其是採用橢圓曲線數位簽章演算法 (ECDSA) 時，可確保攻擊者無法獲取用於簽署韌體和資料的私密金鑰，即使透過複雜的侵入式攻擊也不能得逞。攻擊者唯一能從醫療裝置中獲得的資訊是公開金鑰；而採用 ECDSA 時，從公開金鑰推導出私密金鑰在數學上是無法實現的。

圖 5：安全引導過程



當醫療裝置的微控制器需要執行韌體時，主機 MCU 引導管理器首先獲取韌體，並將其傳送到 MAXQ1065 進行 SHA-256 雜湊計算 (圖 5)。SHA-256 雜湊計算完成後，處理器提供韌體或資料的 ECDSA 簽名；該簽名是在開發階段計算的，並附加到文件中。主處理器隨後發送韌體或資料檔案及其期望的數位簽章。安全輔助處理器驗證簽名並返回結果，指示驗證是否成功或出錯。如果簽名驗證成功，則可以執行韌體。

有關此過程的更深入解釋，請參閱文章「安全引導和安全下載的基礎知識：如何保護嵌入式裝置中的韌體和資料」(https://www.analog.com/

en/resources/technical-articles/the-fundamentals-of-secure-boot-and-secure-download.html)。

安全儲存和攻擊檢測：MAXQ1065 具有攻擊檢測功能，可以識別物理攻擊意圖並作出回應。此功能增加了一層額外的安全保障，確保裝置即使在面對潛在入侵時也依然可信。ADI 的 ChipDNA 嵌入式安全物理不可克隆功能 (PUF) 技術，在抵禦駭客的侵入式攻擊和逆向工程攻擊方面，安全防護水準取得了指數級提升。如果駭客試圖探測或觀測 ChipDNA 的運行情況，系統會觸發修改基礎電路的特性，防止駭客找到晶片加密函數使用的唯一值。而駭客們費盡心力的反向工程攻擊也同樣會宣告失敗，因為要使 ChipDNA PUF 電路正常運行，必須保持出廠條件。只有在加密操作需要時，ChipDNA PUF 電路才會生成每個元件唯一的金鑰，然後立即刪除。

傳輸層安全性 (TLS) 保護：MAXQ1065 支援 TLS/DTLS 1.2 協定，能夠實現安全資料傳輸，確保資料的機密性和完整性。對於需要將患者資料傳送給醫療機構或雲端系統的居家醫療裝置而言，這一點十分重要。

在此種情況下，患者家中的醫療裝置使用 TLS 與雲端伺服器進行安全通訊。TLS 有兩個階段：握手和安全通訊。MAXQ1065 等安全 IC 透過將憑證授權 (CA) 根憑證存放區在非揮發性記憶體中來增強 TLS，確保只有經過身份驗證的管理員才能替換根證書。握手階段涉及協商安全設定和建立共用金鑰，而安全通訊階段會使用這些金鑰進行加密和身份驗證。在嵌入式裝置上進置 TLS 可能很複雜，存在跳過證書驗證或使用弱密碼套件等風險。MAXQ1065 提供基於硬體的保護，能夠防止未經授權的存取並確保 TLS 進程的完整性。其可以防禦中間人攻擊和工作階段金鑰洩露等威脅，在不影響裝置性能的情況下，維護醫療資料的機密性和完整性。

此外，此款加密控制器允許裝置製造商為相連裝置建立自己的 CA，進而安全地儲存根公開金鑰並防止未經授權的修改。ChipDNA 技術利用晶片製造過程中自然形成的物理差異生成私密金鑰，使私密金鑰安全性進一步提升，有效防止駭客攻擊和逆向工程。

有關使用安全配套 IC 來保護 TLS 實現方案的深入介紹，請參閱文章「使用安全配套 IC 來保護 TLS 實現方案」(https://www.analog.com/en/resources/app-notes/using-secure-companion-ics-to-protect-a-tls-implementation.html)。

結語

隨著居家醫療需求的不斷成長，確保醫療裝置的安全性和可靠性變得日益重要。ADI 的 MAXQ1065 加密控制器憑藉先進的安全功能、低功耗和易於整合的特性滿足了這些需求。透過將這款輔助處理器整合到家用醫療健康裝置中，製造商將可以確保患者資料安全無虞，並且裝置亦能夠長期可靠地運行。CTA

下期預告
智慧安全