縱覽近年來協助醫療院所導入 HCA 應用及討論電子病歷實務的經驗，發現許多醫療院所對 HCA 時戳服務不甚瞭解，因此將近年來相關經驗及看法提供予各醫療院所做為參考。

首先，讓我們先來談談何謂時戳服務以及何謂 HCA TSA 吧!!

時戳服務是提供為一份資料「押時戳」以建立該資料在某一時點就已存在的服務。而被簽署時戳的文件，更可擴充解釋即使是已失效的憑證之前所簽署，亦可被驗證。在作業截止時間是非常重要的情況下，時戳可用來表示交付時間；或在交易日誌裡，時戳用來表示每一項記錄的時間，且是可以提出證據且被查核的。這種可提出證據、可被驗證、可被查核的道理其實源自於 PKI 特性，因為時戳回覆封包內含被 TSA 專屬私密金鑰採用 PKI 機制簽署過之簽章，因此整包時戳回覆封包內的所有屬性內容(包含可信賴之公定時間)皆擁有 PKI 的鑑定性(Authenticity)、私密性(Confidentiality)、完整性(Integrity)、不可否認性(Non-repudiation)等資訊安全特性。由於時戳擁有 PKI 資訊安全特性，因此若是採用時戳方式來呈現時間時，此時間點所留下的證據將擁有高強度證據力，此證據並是可被驗證、可被查核的。

而何謂 TSA？TSA 全名為 Time Stamp Authority，也就是營運時戳服務的組織或單位，即 HCA 時戳服務由 HCA TSA 提供。TSA 角色就是要能提供某一資料在某一時點就已存在的公正證明服務，因此 TSA 在行政管理上應由公正第三方來運行，或者由具有公信力之政府單位角色來運作較為適當。而若是能在技術層面上控制得宜，也可以考慮採用較彈性之方式來實行，例如醫院可以自行建立 TSA 提供內部使用之時戳服務，但先決條件是需以「技術設計層面及管理層面上能控制得宜」為前提。

由於使用 HCA 時戳服務擁有可在截止時間前表示交付時間，或在交易日誌裡表示每一項記錄的時間等特性，加上 HCA 憑證實務作業基準定義 HCA 的適用範圍為醫療應用範疇，因此，HCA TSA 最適切的服務對象將以醫療電子病歷應用為主。而從另外一個角度思考，對電子病歷的發展及需求而言，電子病歷是否適用 HCA 的時戳服務呢？以下就歸納並列舉**「醫療機構電子病歷製作及管理辦法」(98 年 08 月 11 日修正)**適用 HCA 時戳服務的主要條文，並彙整進行說明。

適用 HCA 時戳服務的主要條文：

- 第三條　醫療機構電子病歷資訊系統(以下稱系統)，應有符合下列規定之管理措施：

  三、於本法第七十條所定病歷保存期間內，電子病歷之存取、增刪、查閱、複製等事項，及其執行人員、**時間**及內容**保有完整紀錄，可供查核**。

  五、訂有保障電子病歷資料安全之機制及有**保持資訊系統時間正確之機制**，並據以執行。
- 第四條　電子病歷依本法第六十八條所為之簽名或蓋章，應以電子簽章方式為之。前項**電子簽章，應於病歷製作後二十四小時內完成之**。

■ 第五條　電子病歷於本法第七十條所定保存期間內，其**內容應可完整呈現**，並得隨時列印或取出供查驗。

綜觀上述條文精神，彙整說明如下：

1. 在電子病歷有存取、增刪、查閱、複製作業發生時，時間這個欄位需要被完整紀錄，且還要能夠被查核。而我們就病歷製作及管理之存取、增刪、查閱、複製等行為的不同，一部分的紀錄應包含在病歷內容中，一部分將存在於系統的稽查存證資料內。而怎樣形式的時間紀錄是完整可以供查核的？恰巧時戳擁有 PKI 資訊安全特性，從技術的角度撇開模糊解釋空間，時戳完全符合了此條法規要項之要求。
2. 就法規整體面向而言，醫療機構電子病歷資訊系統保持資訊系統時間正確之機制，其實是必要條件。原因就是因為電子病歷需要”時間”這個資訊，所以才會要求電子病歷資訊系統時間的正確。法規內他項要求包含：時間必須保有完整紀錄、電子簽章應於病歷製作後二十四小時內完成之、電子病歷內容之時間紀錄應可完整呈現。然而，若系統無法保持其時間正確性，上述法規他項要求即無意義。因此，保持資訊系統時間正確之機制的意義，在於支援法規他項要求而存在，並不僅是單純的讓系統時間正確。而時戳的應用，恰巧可支援法規他項要求，遠比單純保持資訊系統時間正確這種作法有效。
3. 如何確保電子病歷的電子簽章，於病歷製作後二十四小時內完成，且病歷沒有被惡意修改？時戳剛好亦符合如是需求。原因為時戳擁有 PKI 資訊安全特性，當電子病歷內容的任一欄位(包含時間)被惡意修改後，時戳是驗證不過的。因此透過此技術應用，可確保電子病歷二十四小時內完成之證據力。
4. 時戳應用亦保障了電子病歷在其保存期間內，其內容應可完整呈現之機制。由於 PKI 特性的關係，病歷本文與時戳是完全相依的，若是病歷本文在取出供查驗時沒有完整呈現，則時戳的驗證將不會成功。

依據以上法規精神及彙整說明內容，電子病歷確實非常適用 HCA 的時戳服務。然而 HCA 的時戳服務是否隱藏了其他使用上的門檻？就近期輔導醫療院所電子病歷應用之經驗，把醫療院所使用 HCA 時戳服務常碰到的問題及回應說明如下：

1. 不清楚為何要使用 HCA 時戳服務，現行法規僅要求醫療機構電子病歷資訊系統保持資訊系統時間正確之機制，用 NTP 方式對時不行嗎？

   為了讓系統時間正確，系統當然可採用 NTP 方式進行對時。但回顧上述法規彙整說明內容，保持資訊系統時間正確之機制其重點不在於單純的讓系統時間正確，目的是要能夠支援法規內他項條文要求。因此，若實作電子病歷之醫療院所僅有做到系統時間正確的要求，還

是需要自行花功夫舉證支援法規內他項條文要求的對應作法及證明方式，且由於缺乏技術上強度的支援，需找尋各種設計方式才能解釋模糊空間。同時，NTP 的對時在技術上的保障卻也是有疑慮的，原因為無法得知對時單位的 Domain Name 或 IP 是否已由 Hacker 取代，更嚴重的是時間真的正確嗎？在沒有加密驗證的 NTP 校時傳輸過程中，時間是很容易被替換而無察覺亦無法被驗證的。

2. 不知道 HCA 時戳服務怎麼用，是不是在系統上設定就好？

多數從未使用過 HCA 時戳服務的醫療院所，會預設立場認為時戳服務在應用上必須和程式整合勢必非常麻煩。其實時戳的應用當然不是在作業系統上進行設定後就可以使用，而是需要透過程式在電子病歷資訊系統上進行整合，原因為時戳應用就像電子簽章應用一樣，本就和電子病歷內容直接相關，當然勢必需要整合程式邏輯，這種設計在面對取出供查驗的電子病歷完整呈現要求上，也才能達到效果。而使用 HCA 時戳服務究竟有多複雜？其實一點也不麻煩，HCA 時戳服務提供的函式僅 3 個，其一為取得時戳；其二為驗證時戳；其三為解析時戳內容。除此之外，HCA 並提供了不同類別程式語言範例供醫療院所參考，亦有客服及技術人員給予支援，醫療院所應可善加利用此資源，而非預設時戳應用會非常麻煩的立場。

3. 時戳所需容量空間很大，存取速度很慢浪費時間？

多數醫療院所會預設立場認為 HCA 時戳佔太大容量，會影響電子病歷整體作業效率。其實不然，一個 HCA 時戳所佔空間最大不到 3K 位元組，以現在電腦硬體的運作效率而言，簡直微不足道。所以影響時戳應用作業效率的原因並不是因為時戳所需容量空間而引起。歸咎真正造成時戳應用作業效率不彰的原因大致如下：

(1) 程式邏輯開發設計問題

電子病歷製作過程中，取得 HCA 時戳後不需再馬上進行時戳驗證，驗證工作是在病歷交付、交換，或是取出供查驗時，才應有的必要工作。醫療院所應要能相信從 HCA TSA 取回的時戳內容是正確的，因此在有應用作業需求發生時，才有必要因應作業流程執行驗證。否則多了一項沒有必要的驗證工作，程式還要載入電子病歷本文、時戳主體等要項至記憶體，另外再執行驗證函式等等工作，當然會覺得時戳應用效率不彰，而其實這些程序相較多餘。另外，有些醫院在取得 HCA 時戳後，又去解析時戳內容，之後把時戳內的時間取出寫入電子病歷中。此作法就有點本末倒置，因為時戳內的時間屬性其具有意義之原因就在於它和時戳整個封包為一體，而整個時戳封包才有完

整呈現及可被驗證的特性，因此寫入電子病歷的應是整個時戳封包，非僅時間屬性。若僅是取出時戳內的時間，就技術角度而言，此時間完全沒有辦法被驗證，既無法發揮時戳之特性，又額外浪費了解析時戳內容及應用整合時間，亦是造成時戳應用效率不彰的原因。

（2）網路繞送或網路穩定度問題

造成時戳應用作業效率不彰最大的主因，其實是網路問題。雖然 HCA TSA 建置於衛生署 HIN 網路內，對外可連線至網際網路，同時與政府 GSN 和健保 VPN 皆有連接，不論醫療院所網路架設於健保 VPN、網際網路還是 HIN 網路中，理應能和 HCA TSA 溝通順暢，但事實卻不然。過去曾造訪南部某大醫院，發現存取 HCA 時戳服務時有時沒有，非常不穩定。而在同一時間從北部某大醫院對 HCA 時戳服務進行存取，卻非常順暢。事後並檢視 HCA TSA 紀錄發現並無南部某大醫院存取時戳的拒絕阻斷訊息。也就是說，南部某大醫院對 HCA TSA 取時戳失敗的原因與 HCA TSA 無關，因為 HCA TSA 沒有收到取時戳要求，當然就沒有辦法回應時戳訊息。追究原因是網路封包掉包或是網路繞送 timeout，存取時戳服務之訊息因此沒辦法送至 HCA TSA 而造成。此類問題發生時將大幅影響時戳應用效率，但由於此問題之釐清需要投入太多跨單位資源，甚至會有衍伸性鉅額成本投入問題，因此醫院自建時戳即是一個不錯的考量，當然醫療院所應先就本身網路環境及網路繞送設定進行確認，避免因為網路設定問題造成存取時戳門檻。

4. 遠端連線至 HCA TSA 存取時戳服務，若網路斷線或網路速度受限怎麼辦？

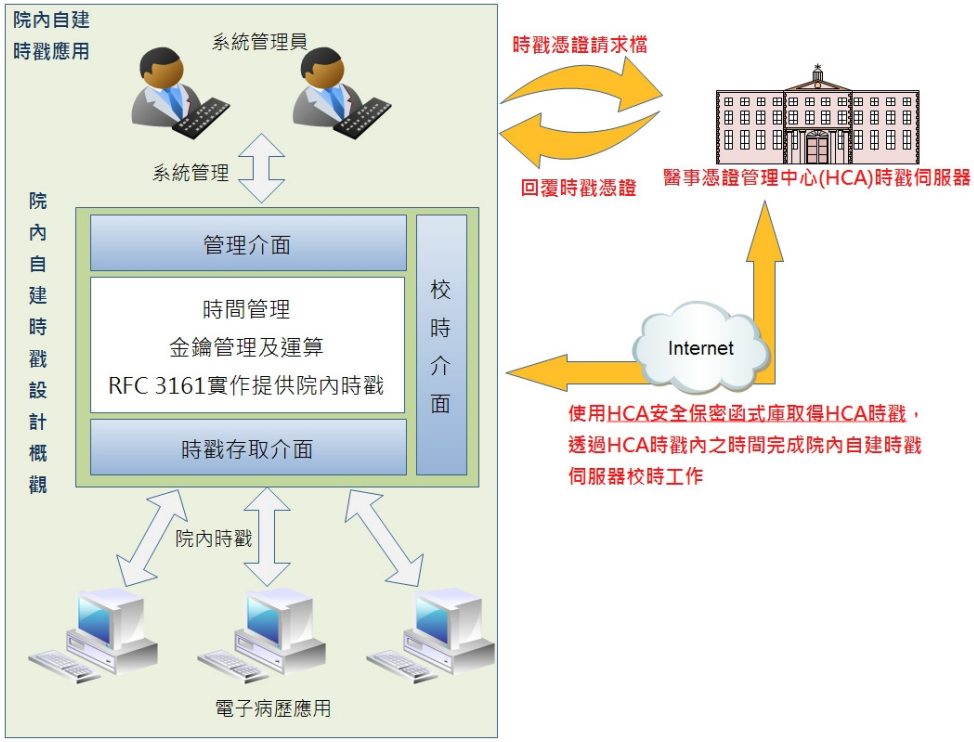
HCA TSA 透過網際網路媒介提供時戳存取服務，確實會因為網路斷線或網路速度受限而造成醫療院所存取時戳之困擾。在醫療院所都確認過其網路環境及網路設定無虞的狀況下，其他造成時戳應用受限的原因大致就是 HCA TSA 負載能量不夠，或是網路本身頻寬受限問題。而截至目前為止，HCA TSA 在尖峰時間負載量其實還未達其 1/10 的負載能力，因此負載能力是可以暫時不列入考量的。而網路速度受限的處理方式則是增加雙向網路頻寬，亦不難處理。然而網路斷線就是個問題，HCA 依附於衛生署的 HIN 網路強度勢必要足夠，醫療院所對外的網路亦要夠穩定才行，此議題亦是個大哉問，醫院自建時戳的理念當然就此開始衍伸。

由於 HCA 時戳服務的最大門檻在於網路問題，此問題在短期內又無法找到最有效因應之道，加上為了符合醫療院所電子病歷自主性精神，是否可提出彈性解決方法？如同本文一開始就提出，若是能在技術設計層面及管理層面上控制得宜，也可以考慮採用較彈性之方式來實行時戳應用，例如醫院可以自行建立 TSA 提供內部使用之時戳服務。以下僅從 HCA 角度看醫療院所因應電子病歷需求，其自建時戳之設計和建議。

應從技術設計層面及管理層面上控制得宜為前提，來談醫院自行建立 TSA 之可行性為何。僅將輔導醫療院所經驗整理如下：

1. 需有確保醫院自建 TSA 其時間正確之機制。
2. 產製醫院自建 TSA 之金鑰對過程需安全，私密金鑰並應妥善保存。
3. HCA 提供簽署醫院自建 TSA 之時戳憑證服務可善加利用。
4. 醫院自建 TSA 提供院內之時戳封包應符合 RFC-3161 標準。
5. 自建 TSA 系統應有完善管理介面，並且留存電子病歷稽查所需之必要紀錄。

綜合上述，醫療院所自建 TSA 可採取之設計如圖所示，並說明如下：



1. 為確保醫院自建 TSA 時間之正確性，自建 TSA 校時可透過存取 HCA 時戳服務進行校時。本文內容曾提及 NTP 對時之風險，但是由於 HCA 時戳擁有 PKI 特性，因此透過取得 HCA 時戳進行校時可確保遠端提供標準時間之單位為 HCA TSA，校時過程亦不會有風險產生。且取得 HCA 時戳進行校時還有兩項優點，包含可證明確實在某個時間點自建 TSA 有進行校時動作；以及 HCA TSA 本就提供正確時間，自建 TSA 可透過取得 HCA 時戳

來確保其時間之正確性。但系統還是要有安全的時間管理機制，確保被校時過的時間無法任意透過作業系統進行修改。

2. HCA 提供簽署時戳憑證之服務，只要自建 TSA 提出的時戳憑證請求檔符合 HCA 標準及提供正確之醫療院所憑證主體名稱 Subject Name(DN)，即可向 HCA 申請時戳憑證，亦即自建 TSA 簽署時戳的金鑰對已經由 HCA 認可。但由於時戳金鑰對由自建 TSA 自行產生，因此 HCA 並不保證時戳金鑰對之安全，自建 TSA 系統還是要有安全的金鑰管理及運算環境，金鑰必須要能在安全環境下簽署院內時戳回應封包。
3. 自建 TSA 系統實作時戳封包時，需符合 RFC-3161 標準，在時戳驗證上才能夠符合國際標準規範，因應電子病歷交付、交換，或是取出供查驗時才可被驗證。
4. 自建 TSA 需有妥善管理之介面及留存電子病歷稽查所需之必要紀錄，紀錄至少需包含：對時紀錄、簽署院內時戳紀錄、系統存取紀錄、系統狀態或錯誤紀錄等。

本文從時戳存在的必要性、電子病歷應用時戳的可行性、HCA 時戳服務的門檻分析，談到從 HCA 角度看醫療院所因應電子病歷需求。醫療院所自建時戳不失為一個富有彈性且能夠符合法規、實務作業要求的解決方案，期待醫療院所以技術設計層面及管理層面上控制得宜為前提，建置其院內專屬 TSA 以提供內部使用之時戳服務。

(本文作者為現任 HCA 醫事憑證管理中心專案經理)