行政院衛生署
96 年度「診所電子病歷實作推廣案」
期末專案執行報告

Ver2_970630

耀聖資訊科技股份有限公司

中華民國九十七年六月三十日

文件制/修訂記錄

版次	日期	變更說明	修訂者	審稿者	備註
V1	97/06/12	制定初稿	邱裕佐	何俊聰	
V2	97/06/30	正式版本完成	邱裕佐	何俊聰	

目　　錄

圖表目錄

壹、 專案概述

一、 專案名稱

本專案名稱為「診所電子病歷實作推廣案」(以下簡稱本專案)。

二、 專案目標

本專案主要目標為推廣診所電子病歷之實作，並至少輔導完成 80 家以上符合「醫療機構電子病歷製作及管理辦法」規範之實例個案診所。

三、 專案範圍

(一)、 依據「醫療機構電子病歷製作及管理辦法」內容，制定相關作業系統，以做為欲推動電子病歷之醫療院所參考，促進電子病歷業務之發展。

(二)、 推廣輔導 80 家以上符合規範之實例個案診所;且需涵蓋市場 80%以上之資訊廠商。(本次實際上線的廠商包含耀聖資訊、方鼎資訊、展望亞洲、常誠資訊、仜詮資訊等廠商之系統)

(三)、 專案時程

自簽訂合約後至 97 年 6 月 15 日止，並自驗收合格之次日起免費保固一年。

貳、 研究背景與現況分析

行政院於90年1月29日以台九十經字第006016號函核定實施「知識經濟發展方案具體執行計畫」，行政院衛生署所提「網路健康服務推動計畫」係計畫之一，奉准積極推動辦理。又行政院精心規劃國家長程建設藍圖，旋即在91年5月提出「挑戰2008：國家發展重點計畫」， 貴署「網路健康服務推動計畫」亦改列其中，而推廣病歷電子化則為「網路健康服務推動計畫」之子計畫之一。

為因應未來醫療ｅ化的需求，於93年4月28日修正「醫療法」第六十九條明定：「醫療機構以電子文件方式製作及貯存之病歷，得免另以書面方式製作。」，爰依上開規定訂定「醫療機構電子病歷製作及管理辦法」（以下簡稱本辦法），並於94年11月24日發布。屆時凡符合本辦法規定者，得免另以書面方式製作及儲存病歷。因傳統的紙張病歷有保存不易、需要龐大保存空間、無法多人共用等缺點，醫療機構實施電子病歷，除可節省儲存病歷的空間，亦能讓醫護人員利用電子ｅ化資訊之特性，整合病患分散於各醫療機構之病歷資料，減少醫療資源的浪費，提供病患連續性、高品質的醫療服務，故醫療機構在降低經營成本及提高作業效率下，勢必朝向無紙化、無片化目標發展。

本辦法發佈後，醫療機構製作電子病歷已有其法源。診所為因應健保申報之需求，均已逐步電腦化，相對而言，醫院之資訊系統較為複雜，實施電子病歷需要分階段進行，因此本案選定由診所作為實例個案。

行政院衛生署已於95年度輔導10家實例個案診所，為持續推廣診所電子病歷之應用，故辦理此案。

近年來醫療資訊化發展快速，基層診所電子病歷製作，並非從零開始，在診所內原有的管理機制及作業流程均不變動下，建置一套基層診所電子病歷之實作流程並非遙不可及。

目前基層西醫、中醫診所之醫療應用作業系統均委由外

包資訊廠商負責開發設計與維護為主，有關電子病歷相關開發技術條件均相當成熟，因此也間接形成基層診所電子病歷推廣有利之條件。茲就現行基層診所電腦資訊現況與電子病歷發展可能之問題依政策面、應用面兩方面評述如下：

一、　政策面

(一)　政府為建立安全及可信賴之網路環境，確保資訊在網路傳輸過程中不易遭到偽造、竄改或竊取，且能鑑別交易雙方之身分，並防止事後否認已完成交易之事實；於 90 年 11 月 14 日電子簽章法開始執行推動安全的電子交易系統，建立電子應用之環境。

(二)　為因應未來醫療 e 化的需求，於 93 年 4 月 28 日修正「醫療法」第六十九條明定：「醫療機構以電子文件方式製作及貯存之病歷，得免另以書面方式製作。」，爰依上開規定訂定「醫療機構電子病歷製作及管理辦法」，並於 94 年 11 月 24 日發布，而「醫事憑證收費標準」亦於 95 年 2 月 13 日發布。屆時凡符合本辦法規定者，得免另以書面方式製作及儲存病歷。

(三)　整體政策之宣導，包含主管之衛生機關及健保局之溝通協調與認可，同時未來針對實作診所電子病歷之查驗辦法，是未來電子病歷推動之助力。

二、　應用面

（一）　目前醫療管理及醫療資訊已有朝向國際化發展之趨勢，醫療資訊網路化傳遞交換之發展更具有其重要性;且近年來醫療資訊科技發展迅速，各院所基於作業方便，普遍設置電腦工作站有利病歷電子化之發展。

（二）　診所應用之推廣目前尚無明確之利基;是否可有效取代診所現行健保申報、抽審等行政作業流程，尚待健保局政策之宣視與推廣，方可有效推廣應用至基層診所端。

（三）　電子病歷到目前為止已有 95 年度輔導 10 家的實例並，如何增進擴展電子病歷的功能及用途，以改善現有的醫療環境及醫療行政效率，還需要有進一步的實作應用來驗證及推廣。

（四）　現階段病患至診所就醫無法有效累積個人病歷資料隨身攜帶，對於病患個人無法提升有效連續性之照護。

（五）　病患的醫療權益意識抬頭民眾既希望醫療健康隱私獲得充分保障，又期盼醫師診療時能有更完整的醫療資訊，以提供高品質的醫療服務。

參、 材料與方法

一、 標準作業流程規劃

建構診所電子病歷作業，首先必須先將診所電子病歷作業流程標準化，並依據標準之作業流程進行資料之轉換及傳遞與管理；本次專案之目的即是規劃診所電子病歷之標準流程制定。因此，我們將擬定診所實施電子病歷之標準作業流程以及各基層醫療資訊服務廠商共同遵循之標準規範，以確保基層診所所執行之電子病歷為同一標準。

「醫療機構電子病歷製作及管理辦法」發布後，醫療機構製作電子病歷已有其法源。診所為因應健保申報之需求，均已逐步電腦化，相對而言，醫院之資訊系統較為複雜，實施電子病歷需要分階段進行，礙於本案之時程，因此本案選定由診所作為實例個案。本案期能透過推廣 85 家以上的診所進行實際的應用，透過實例個案診所所產生之效益，進而帶動電子病歷於診所之應用，亦能藉由本案驗證本辦法於實施上並無窒礙。

二、 法源依據

本次專案係依據中央主管機關相關規範辦理，包括：

(一) 醫療法(民國 75 年 11 月 24 日公布，民國 94 年 02 月 05 日 修正)：第 68 條至第 70 條。

(二) 醫師法(民國 32 年 09 月 22 日公布，民國 96 年 12 月 12 日修正)：第 12 條。

(三) 電子簽章法(民國 90 年 11 月 14 日公布)： 第 9 條。

(四) 醫療機構電子病歷製作及管理辦法(民國 94 年 11 月 24 日公布)：第 2 條至第 4 條。

三、 診所電子病歷實作的推動

本次專案推廣目標為 85 家診所，本次的推廣上線的

診所包含了台北市電腦公會所轄的資訊服務廠商，包括耀聖資訊科技股份有限公司、展望亞洲科技、方鼎資訊、常誠資訊、上佺資訊。

四、 簽章與認證

在邁入知識爆炸，資訊技術迅疾發展的二十一世紀新紀元，網際網路的應用已然蔚為世界性風潮，全球各個角落及各行各業無不爭相競逐利用此等新興資訊科技，藉以提高市場競爭力，並拓展生存空間。隨著這股潮流趨勢的迅速蔓延開來，醫療資訊的應用應如何因應，以期達到醫療資源共享及避免造成資源浪費的目的之議題，已引發國內醫療界熱烈的討論與迴響。綜觀國內醫療資訊環境的發展腳步，時有聽聞國內大型醫療機構倡議推動病歷電子化的建言，而實際付諸建置行動的案例更與日俱增。

本次專案要求病歷需採用醫療憑證管理中心簽發之醫事憑證 IC 卡進行簽章及加註時戳後以符合專案之要求。本專案規劃之電子病歷製作流程依循 HCA 數位簽章之應用流程及說明如下：

(一) 醫事人員透過醫療資訊系統(HIS)進行診療紀錄。

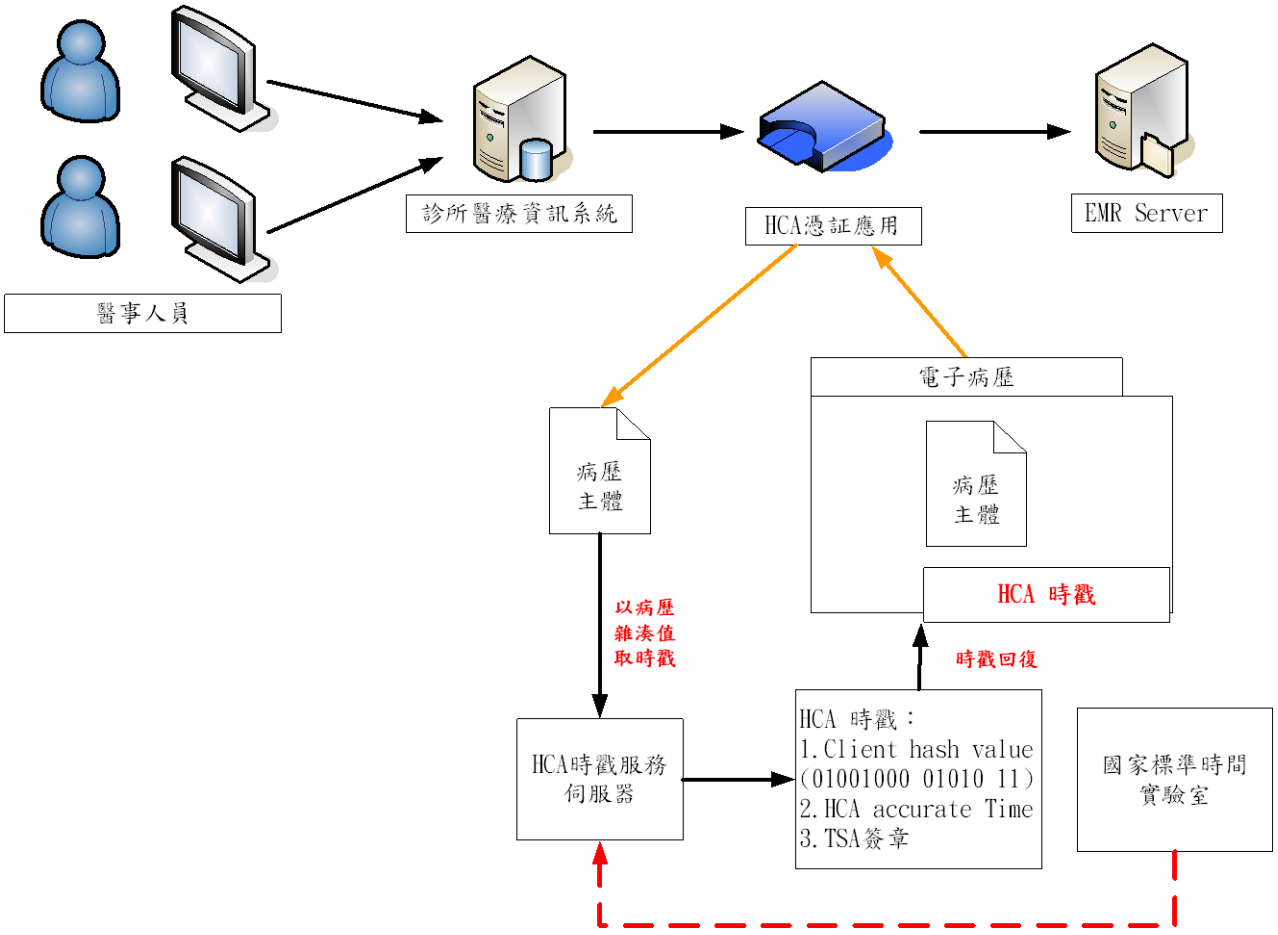
(二) 診療內容紀錄於醫療資訊系統資料庫時，並即時進行文件格式轉檔作業。

(三) 依文件格式紀錄之病歷透過『HCA 醫事憑證應用系統』，依下列原則完成簽章及時戳加註作業：

1. 針對病歷內容簽署醫事人員數位簽章，以確定醫事人員之身分，同時符合法規之規範。

2. 經由 HCA 時戳服務伺服器取得時戳，透過時戳之加註，達到病歷製作內容及時間不可否認性之目的。

3. 病歷內容簽署經由醫事人員數位簽章及時戳加註，以確保診所認定並對此份病歷負責，也可解決醫事人員離職而病歷該由誰負責之疑慮。時戳簽署示意圖如下:



圖表 1 時戳簽署示意圖

五、 資訊安全

隨著網際網路的誕生及蓬勃發展，網路的使用已具備迅速便捷，無遠弗屆的特性，民眾對保障自身所擁有資料的安全性及私密性的意識，也跟著提高許多，且醫療資訊多涉及個人隱私，攸關個人生命安全影響至鉅。因此，如何確保資料在儲存及製作過程中的安全性及不可否認性，避免日後病歷交換及應用上之首要任務。

(一) 身份確認與保密性

病歷電子化的快速發展，不僅僅帶給醫療資訊的改變，也改變了醫師與病患之間的溝通方式，因此傳統上訊息與資料的儲存及傳遞也同樣發生了巨大的變化；面對這樣巨大的變化，醫療保健產業亦無法置身於革命的

潮流之外，因此衛生署近年來除積極鼓勵引進國外最新技術，期能藉由科技帶來的便利提升醫療照護的品質，提供較精確、清晰且隨時可方便取得的資訊；一方面也建設安全的網路傳輸基礎建設及加強法規制度的配合措施，以期能同時確保醫療資訊的安全，保障個人隱私資料醫事憑證 IC 卡即為此原因而誕生，大家都知道電子很方便，但對於重要的東西，大家卻常常缺乏信心，最主要有以下兩個原因：

1. 無法確認製作電子文件的個人的身分。
2. 無法在安全的資訊環境中確認所傳遞資料的準確性。

而憑證的產生就是為了解決以上的問題。簡單的說，憑證就是個人的網路身分證，以辨別個人在網路上之身分；而醫事憑證呢?也就是更進一步的証明在網路上具備醫事人員資格及醫事機構資格的身分，政府可以依據這個醫事憑證來確認身分及資格，提供網路上方便的服務及確保資料傳輸的安全。

(二) 醫事憑證 IC 卡分類：

1. 醫事機構憑證 IC 卡
   - 代表醫事機構法人於醫療資訊電子化環境之法人行為—機構關防。
   - 用途：加密、簽章：如電子公文、網路出生通報系統等。
2. 醫事人員憑證 IC 卡
   - 代表醫事人員於醫療資訊電子化環境之個人行為—印鑑證明。
   - 用途：權限控管：健保第二階段存放內容讀取權限憑證(限醫師卡)、簽章：如電子病歷醫事機構憑證 IC 卡副卡。

- 為因應醫事機構有多重應用系統或單一系統多位承辦人，有同時使用醫事機構卡作業的需求，針對有該項需求之醫事機構發放副卡。

3. 醫師備用卡機制

- 因應健保 IC 卡加值行動方案實施時，醫師可能無法即時以醫師卡讀取健保 IC 卡。
- 醫事機構可申請醫事人員(醫師)備用卡。
- 備用卡發卡時即廢止該卡片憑證功能(即 HCA PKI 功能)。

4. 核發醫事憑證對象包括：

- 領有衛生署核發醫事證照之醫事人員。
- 領有衛生署核發開業執照之醫事機構。
- 經核准之醫療資訊相關之伺服器應用軟體。

六、 推廣與宣導

為了推廣診所電子病歷實作，並期望透過經驗交流及成果觀摩，以凝聚診所電子病歷未來發展方向之共識，本計畫依據衛生署指示，共舉辦「基層診所電子病歷實作推廣說明會」，會中將邀請對基層診所電子病歷有興趣之診所及資訊廠商，進行專案之推廣。

本次共計於北、中、南、東舉辦七場推廣說明會如下，詳如推廣說明會紀錄如附錄，活動剪影如附呈之光碟。

肆、　專案交付項目

96 診所電子病歷驗收事項表				
項次	交付產品項目	要求及樣態	應交付時程	實際交付時程
1	專案管理計畫書	書面資料 8 份及電子檔	簽約後兩週	96.10.23
2	實例個案診所之甄選標準及作業流程	書面資料 8 份及電子檔	96.10.30 前	96.10.23
3	召集專家小組會議	活動紀錄及簽到	96.10.30 前	96.10.26
4	期中專案執行報告書(含系統初步展示)	書面資料 8 份及實機展示	96.12.15 前	96.12.14
5	專家小組期中實地查核報告	活動紀錄及簽到	96.12.15 前	96.12.20
6	推廣說明會計畫書	書面資料 8 份及電子檔	96.12.15 前	96.12.12
7	自由回饋項目網站查詢系統建置完成	系統建置	96.12.15 前	96.12.15
8	依據甄選標準作業確認實作診所名單	書面資料 8 份及電子檔	97.02.01 前	97.02.01
9	期末專案執行報告書(含期中交付之資料更新本)	書面資料 8 份及電子檔	97.06.15 前	97.06.15
10	系統運作說明書	書面資料 8 份及電子檔	97.06.15 前	97.06.15
11	北、中、南、東區至少各辦理一場推廣說明會成果報告(含照片、簽到表與現場意見及回應整理)	活動紀錄及簽到	97.06.15 前	96.12.15
12	專家小組期末實地查核報告	活動紀錄及簽到	97.06.15 前	97.06.15
13	保固維護計畫書	書面資料 8 份及電子檔	97.06.15 前	97.06.15
14	實作診所合作、建置及操作教育訓練完成證明書	診所簽署書面資料正本(診所大小章)	97.06.15 前	97.06.15
15	保固期間欲實施電子病歷之診所之建置工本費與維護費收費標準及成本分析	書面資料 8 份及電子檔	97.06.15 前	97.06.15

伍、 專案執行成果

一、 完成 88 家診所進行『診所電子病歷實作』

二、 建立診所電子病歷認證之可行模式

（一） 病患持健保 IC 卡就診，就診流程與未實施電子病歷前相同。

（二） 醫師於診間看診，其原 HIS 作業方式沒有改變。

（三） 醫師完診後列印處方簽交付病患取藥，可同時完成電子病歷之製作，並將製作之電子病歷存放於電子病歷檔案管理系統儲存。

三、 提交參加『診所電子病歷實作』診所查詢網站

四、 完成診所電子病歷管理系統

五、 提交『診所實作電子病歷標準作業程序書』

作為診所實施電子病歷之參考依據，協助診所進行電子病歷之規劃執行依據。

六、 診所實施電子病歷的差異

編號	主題內容	會	不會	其他	說明
1	參加本計畫對於診所現行HIS系統是否產生影響？		※		目前規劃參加電子病歷實作之診所，其電子病歷產生之作業係應用診所現行HIS系統進行Batch作業，對於醫務人員現行電腦作業不影響。
2	對於病患就診流程是否會有影響？		※		病患就診流程不變。
3	對於診所現行健保申報作業是否會有影響？		※		診所每月定期申報作業仍依中央健保局規定辦理，與現行作業相同。
4	對於現行診所行政管理(病歷管理)作業是否有影響？			※	1.進行實作之診所若有法令可完全無須整理紙上病歷備查，則可減少紙上病歷整理之工作。 2.若尚無法源依據或規範，則現行作業不變。
5	是否增加診所資訊服務管理費用？			※	1.參加專案試辦之診所無須增加費用負擔，全額由專案費用補助。 2.若將來要參加電子病歷實作之醫療院所，則需負擔軟硬體及保固費用約新台幣5~6萬。(含軟體、硬體及備份與保固一年)

圖表 2 診所實施電子病歷實作前後差異比較表

七、 建立 HCA 認證運用模式

依據 HCA 驗證憑證流程，確認診所電子簽章之流程

項次	安全檢查項目	是否合格	說明
1	系統應該由安全管道取得 HCA 的自簽憑證（Self-Signed Certificate)，並妥善地安全保存於系統中	■是 □否	原因:（由中華電信提供*） - Root CA本身的憑證是自簽（Self-Signed rtificate）。 - 自簽憑證的特性是其憑證簽發者名稱（Issuer Name）與憑證主體名稱（Subject Name）是完全相同的，而自簽憑證的簽章可以被該自簽憑證所記載的公開金鑰檢驗通過。 - 此自簽憑證中所記載的公開金鑰可以用來檢驗下層CA憑證的真偽，而下層CA憑證所記載的公開金鑰可以用來檢驗用戶憑證的真偽。所以說此自簽憑證是整個PKI的信賴起點（Trust Anchor）。 - 然而自簽憑證卻沒有另外一張憑證的公開金鑰可以檢驗其真偽。（也就是說沒有另一個CA來為Root CA的自簽憑證背書。） - 意圖不法者如果擁有足夠的技術與工具，就可以自己產製一對金鑰對，並簽出一張自簽憑證，且故意讓該自簽憑證之憑證簽發者及憑證主體名稱都與真正的Root CA名稱相同，由於此憑證是自簽的，所以該自簽憑證簽章一定可以被其所記載的公開金鑰檢驗通過，所以容易被誤以為是真正的Root CA自簽憑證。 - 所以Root CA的自簽憑證有可能被偽造。 本系統所採取對策: 由 HCA 網站手動下載，人工驗證過後放入安裝程式中，在安裝系統時

			放入資料庫中，受資料庫保護。
2	系統應該設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求，並對於不符保證等級的憑證應該加以拒絕（例如正式上線系統應該對測試等級的憑證加以拒絕）	□是 □否 ■不適用	在 GPKI 架構中，明訂 5 個 CA 憑證等級，而且對於 ROOT CA 的憑證不需檢查。而針對 GPKI，由系統啟動載入 CA 憑時，將檢查 Certificate Policies 是否為第三級以上。而在 HCA 中，僅有一個 CA，因此不適用此檢查項目。
3	系統應該檢查 CA 本身的憑證確實為 HCA 所簽發的憑證（至少需檢查憑證的 Issuer Name (DN)是否 HCA 自簽憑證的 Subject Name(DN)相符，並以 HCA 自簽憑證所記載的 Public Key 檢驗 CA 本身憑證的簽章）	■是 □否	原因: 與第一點相同。 本系統所採取對策: 在系統載入設定時自動檢查，並使用其公鑰驗證憑證簽章確定憑證的正確性。此外，本系統同時檢查憑證的姆指紋(sha1 值)，比對是否與載入的憑證相符，檢查憑證完整性，以避免相關欄位被修改。

4	系統應該檢查 CA 本身的憑證確實為合法的 CA 憑證（BasicConstraints 欄位標示為 CA 憑證)且憑證之金鑰用途（KeyUsage）欄位允許 keyCerSign 及 cRLSign 的用途	■是 □否	原因:（由中華電信提供*） －唯有合法的CA才能簽發憑證，一般用戶是不能簽發憑證的。 －CA Certificate與一般用戶的End-Entity Certificate之格式是有區別的。 –所以應用系統應該檢查CA本身之憑證是否為合法CA Certificate。 本系統所採取對策: 在系統啟動時，自動檢查 CA 憑證 BasicConstraints 及 KeyUsage 欄位，是否符合 CA 憑證的要件。
5	系統應該檢查 CA 本身的憑證是否仍在有效期限之內	■是 □否	原因:（由中華電信提供*） －Root CA自簽憑證必須尚未過期，則該自簽憑證所記載之Public Key才能被用來檢驗憑證。 本系統所採取對策: 在系統啟動時自動比對系統時間與 CA 憑證有效期是否仍在有效期，並且在每次驗證時，檢查 CA 憑證鏈及 CA 憑證有效期限。
6	系統應該檢查 CA 本身的憑證是否已被廢止（例如定期下載 HCA 簽發的 CARL 來檢查憑證廢止狀態）	□是 □否 ■不適用	目前 HCA 並無 CARL，將來 HCA2.0 建置後將在系統啟動時，定期下載 CARL 檢查 CA 本身的憑證是否已廢止。
7	系統應該檢查 CARL 是否確實是 HCA 所簽發	□是 □否 ■ 不適用	目前 HCA 並無 CARL。
8	系統應該檢查 CARL 是否為最新公佈的 CARL（當天公佈的 CARL）	□是 □否 ■不適用	目前 HCA 並無 CARL。
9	系統應該檢查用戶的憑證確實為合法 CA 所簽發的憑證（至少需檢查用戶憑證的 Issuer Name (DN)是否 CA 憑證的 Subject Name(DN)相符，並以 CA 憑證所記載的 Public Key 檢驗用戶憑證的簽章）	■是 □否	原因:（由中華電信提供*） －除非用戶憑證是經過合法CA所簽發的，否則應用系統不應該信賴該用戶憑證。 本系統所採取對策: 在驗證用戶憑證時，檢查 Issuer Name 是否與 CA 憑證的 Subject Name 相符，並使用 HCA 的公開金鑰驗證憑證的簽章，確定該使用者憑證的正確性。此外，本系統並檢查用戶憑證的授權金鑰是否與 CA 憑證的主

			體金鑰相符，以避免 CA 本身的金鑰被置換掉。
10	系統應該檢查用戶憑證金鑰用途（KeyUsage）欄位所記載的金鑰用途符合使用目的(簽章/驗簽或加密/解密)	■是 □否	原因:(由中華電信提供*) -X.509標準對公鑰憑證定義了許多種的金鑰用途（Key Usage），憑證的使用必須符合該憑證所記載之金鑰用途，否則便是不合法的使用。 本系統所採取對策: 在驗證用戶憑證時輸入 KU 用途，檢查該用途是否與憑證中的 KeyUsage 欄位相符。例如：若是使用只能用於加解密的憑證來簽章，該簽章視為無效。
11	系統應該檢查用戶的憑證是否仍在有效期限之內	■是 □否	原因:(由中華電信提供*) -用戶憑證必須尚未過期，則該用戶憑證所記載之Public Key 才能被用於該憑證所允許的金鑰用途上。 本系統所採取對策: 在驗證用戶憑證時檢查憑證有效期間與系統時間比對，確認憑證有效性。
12	系統應該檢查用戶的憑證是否已被廢止（例如定期下載CA 簽發的CRL 來檢查憑證廢止狀態或透過OCSP 來檢查憑證廢止狀態）	■是 □否	原因:(由中華電信提供*) -即使用戶憑證仍在有效期限之內，用戶憑證仍然可能被廢止或暫停使用，所以應用系統仍必須檢查用戶憑證是否被廢止或暫停使用了。 本系統所採取對策: 系統可設定在驗證用戶憑證時，檢查憑證是否在 CRL 中，確認憑證是否已被廢止。或者直接連接到 OCSP 檢查憑證狀態。
13	系統應該檢查 CRL 是否為最新公佈的 CRL（當天公佈的 CRL)(如果使用 OCSP 查詢，則本項不適用）	■是 □否 □不適用	原因:(由中華電信提供*) -應用系統必須確認 CRL 的來源正確，才能信賴該 CRL 中所記載之廢止或停用資訊，否則可能會受到假造 CRL 之欺騙，而誤信錯誤的廢止或停用資訊。 本系統所採取對策: 可在本系統設定更新時間及頻率(例:每天的凌晨 1:00)到 CRL 下載網址下載最新的 CRL，或讀取 CRL

			的有效日期，系統自動在 CRL 過期時下載更新 CRL。當更新時因 CRL 下載網站繁忙或臨時斷線而無法下載時，本系統有重新下載機制，而且超過一天無法下載成功時，系統將發通知給管理者。
14	系統應該要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分	■ 是 □否	原因:（由中華電信提供*） －在電子化／網路化的環境中，應用系統必須取得用戶的電子簽章，驗證簽章無誤後，才能向信用戶就是憑證身份資料所指之人。 本系統所採取對策: 本系統提供身份認證 API，當使用者要登入系統時，可導入憑證登入功能，由使用者針對系統所發的 Token 簽章，送到 server 後，server 判定簽章及 token 皆正確時，才予以放行。
15	系統應該要具備防止或偵測用戶加簽之訊息遭到非法重送（Replay）的機制（例如在加簽訊息中加入 Challenge-Response 或 Nonce 機制）	■ 是 □否	原因:（由中華電信提供*） －電子簽章的訊息如果沒有包含防止或偵測訊息重送（Replay）的機制，則意圖不法者可能可以經由竊聽而將該訊息記錄下來，日後再重送給應用系統，應用系統會誤以為該訊息是真正的用戶所傳送來的。 本系統所採取對策: 提供 Challenge-Response 機制，防止重送攻擊，包含: 序號、Nonce 及時戳。
16	系統傳送用戶隱私資料時應該要以強度 128 bits 以上的安全通道加以保護（例如使用 SSL 安全通道或是對傳送的訊息以數位信封加密)(若系統並不涉及傳送用戶隱私資料時，則本項不適用）	■是 □否 □不適用	原因:（由中華電信提供*） －簽章機制並不能增加訊息的保密程度，如果訊息只加上簽章，則訊息仍然還是維持原有明文，所以如果要防止隱私資料外洩，還需要另外使用加密技術，而且加密強度要達到 128 bits 以上，其安全度才足夠。 本系統所採取對策: 系統可架設在 SSL 安全通道上，保護用戶隱私資料。或者使用醫事機構憑證加密傳輸的資料。

以上文中註明*部分由中華電信提供, 文件出處, MOEACA 網站

圖表 3 HCA 審查意見表