行政院衛生署

「電子病歷索引中心」建置與推廣計畫書

計畫名稱: **電子病歷索引中心之建置與推廣**

Implementation and Operation for a Master Index Center of Electronic Health Records

計畫重點: 指定之醫療院所病歷內容文件化並建置電子病歷資料庫

建置電子病歷索引中心並與指定醫療院所連線運作

以醫事卡與病患健保IC卡連線上網查詢病歷

申請單位: **行政院國軍退除役官兵輔導委員會台中榮民總醫院**

主 持 人: 溫嘉憲 （資訊室主任） 簽名：

填報日期: 中華民國九十二年六月十二日（第三版）

註:本計畫書限用**中文**書寫

目　　錄

頁　碼

貳、計畫摘要：請摘述本計畫之目的與實施方法及關鍵詞

關鍵詞：電子病歷索引（Master Patient Index）、國民健康記錄（Electronic Health Record）、電子簽章（Electronic Signature），醫療憑證管理中心（HCA）

衛生署於九十一年六月公開徵求醫院參與「醫療院所病歷電子化試辦計畫」，本院以「一個快速且安全的電子病歷分享模式」計畫，獲選為八家試辦醫院之一。衛生署有鑑於本院之試辦計畫，包括建置「電子病歷索引中心」，作為跨院際病歷資料交換平台，而針對醫療資訊交換的安全問題，亦應用 HCA 所提供的醫療憑證服務，對電子病歷簽署電子簽章，確為一個技術可行且可充分信賴的交換機制。基於樽節原則，避免重複投資，要求本院依現有基礎架構，研提九十二年度「電子病歷索引中心」推廣計畫書。

推廣計畫目的：一、建置電子病歷索引中心，進行初始階段之試辦作業，評估及驗證其推廣性及效益性。二、分階段逐步擴展電子病歷索引中心使用率，減少重複檢驗檢查，使病患獲得連續性的醫療照顧。三、提供一個全國醫療資訊交換或流通平台，整合醫療體系系統，使全國民眾享有更優質的醫療服務。

參與推廣計畫之醫療院所擬請衛生署指定，需配合事項包括：建立電子病歷資料庫，將現行HIS病歷資料轉成XML格式並簽署電子簽章，將上述資料存放於電子病歷資料庫，將電子病歷索引及電子簽章上傳至病歷索引中心。

本計畫擬分兩階段進行，第一階段舉辦專家諮詢會議，制定相關規範，包括電子病歷應包括內容、XML電子病歷標準、病歷文件大小（granularity）的分割、電子病歷查詢權限、電子簽章使用憑證、電子簽章時機、上傳電子病歷索引及簽章時機等。第二階段才進行本計畫實際建置部分。

參、計畫內容

一、主旨：請分點具體列述本計畫所要達成之目標以及所要完成之工作項目，應避免空泛性之敘述。

本計畫是應衛生署委託，將本院九十一年度試辦計畫架構與經驗，推廣至其他醫療院所，協助衛生署建置全國性「電子病歷索引中心」。參與推廣醫療院所需將 HIS 病歷資料轉換成 XML 格式，並以醫事機構憑證（或醫事人員憑證）簽署電子簽章，一面存放於醫院的電子病歷資料庫內，一面將該份病歷之索引及電子簽章上傳至電子病歷索引中心。

臨床醫師不再受限只能看到病人在某一家院所的就醫記錄，而是病人在所有醫療院所的病歷記錄都能查看，因此醫師能對病人的病史有全盤掌握。參與推廣醫療院所，醫院內建立的電子病歷資料庫可取代現行紙本病歷，使醫院病歷無紙化（Paperless）成為可行。同時將電子簽章存放於電子病歷索引中心，則可防止病歷內容被任意竄改(Tampering)，及不可否認性(Non-repudiation)等安全問題。

本計畫所要達成目標：

（一） 提供一個全國醫療資訊交換或流通平台，整合醫療體系系統，使全國民眾享有更優質的醫療服務。

（二） 設計電子病歷交換的安全機制：儲存在電子病歷資料庫中的文件，經過電子簽章後，一面存放在醫院的電子病歷資料庫內，一面將病歷索引及電子簽章送到電子病歷索引中心儲存；電子病歷交換或分享時，經比對此兩份電子簽章是否相同，以確保病歷未遭篡改。

（三） 配合衛生署醫療憑證管理中心及健保 IC 卡應用：本計畫以病人健保 IC 卡及醫事人員卡，以防範冒名或偷窺隱私。使用者查看電子病歷時必須以醫事人員卡及健保 IC 卡登入系統。

1. 電子病歷分享系統預設的使用者是醫事人員，為防非醫事人員登入系統取得病歷，引用衛生署規劃的醫事人員憑證 IC 卡，

做為辨識登入者是否為合法使用者的機制。

2. 此外，為保障醫療隱私權，電子病歷分享系統也必需在確認醫事人員是經病人授權的情況下，方能開放醫事人員讀取電子病歷的權限。因此，本系統以患者的健保 IC 卡做為索引電子病歷的依據，以保障患者的醫療隱私權。

經由上述兩道關卡，將可確保系統的使用者是合法的讀取經患者授權的電子病歷。

（四） 使醫療院所具備實施病歷無紙化條件：醫療院所現行 HIS 系統上的電腦資料並不能直接取代紙本病歷，一面是現行的醫院資訊系統，資料均以記錄（record）及欄位觀念（data fields）儲存在資料庫中，一份檢查報告或出院摘要或手術記錄，在資料庫內可能是分散在數個資料表格中，由數十或甚至數百個欄位組合而成，而不是以一份病歷記錄為一個單元來儲存。本計畫是以病歷文件的觀念來管理病歷資料，可取代現有紙本病歷；使用 XML 資料格式加以存放，可符合醫療院所的資料差異；電子病歷資料庫獨立於 HIS 外，可因應各醫療院所資訊系統的變動。

（五） 利於衛生署對電子病歷有效管理及監督：醫療院所對於已轉入電子病歷資料庫的資料，即刻加以簽章並上傳索引資料及簽章資料，管理單位只需管理索引中心，而非所有病歷資料。醫療院所對資料修改或作廢時，索引中心對異動或作廢的資料仍儲存，以備查詢。

本院九十一年度試辦計畫的整體系統架構如圖 1，包括醫療院所 HIS 系統、電子病歷資料庫、醫療憑證管理中心、電子病歷索引中心、電子病歷查詢伺服器、使用者病歷查詢等部分；本推廣計畫仍以該圖架構為基礎，不同的主要是在設備擺放地點、設備等級方面。根據圖 1，本計畫所要完成的工作項目可以分成三個部分。

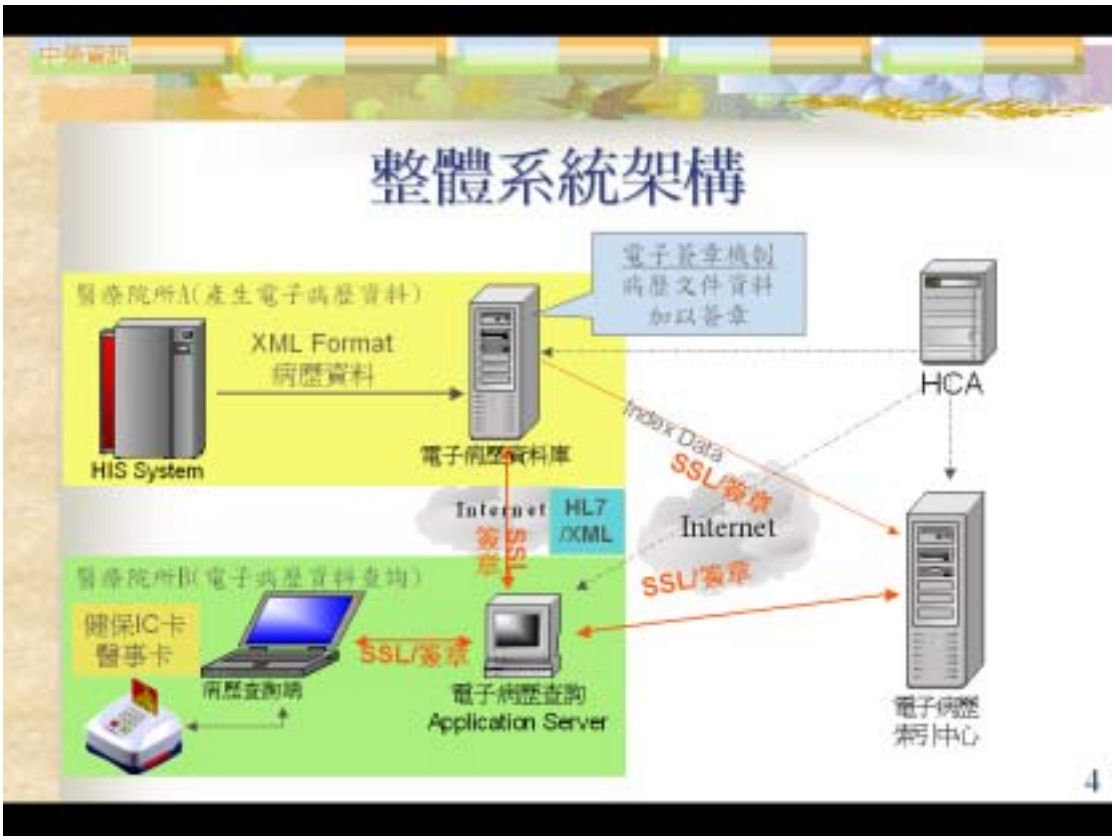


圖 1 台中榮總九十一年度試辦計畫整體系統架構

（一）於衛生署指定處所建置電子病歷索引中心：

1. 設計電子病歷索引資料庫，資料庫 Schema 如附表 1
2. 接收醫療院所上傳之病歷索引及電子簽章，寫入電子病歷索引資料庫
3. 驗證欲查詢病歷使用者是否為合法醫事人員
4. 安裝電子病歷索引的查詢程式，將符合使用者查詢條件之病歷索引傳回使用者端
5. 網際網路資料傳送採 SSL 安全機制

附表 1：電子病歷索引資料庫 Schema

Table Name: INDEX			
欄位名稱	資料型態	欄位說明	備註
HospitalId	Char(10)	醫療機構代碼	
PatientId	Char(10)	病患 ID,身分證號	

PatientName	Char(20)	病患姓名	
ClinicalDate	Char(08)	日期(醫療行為日)	
ClinicalType	Char(01)	病患分類	O:門 E:急 I:住
Department	Char(02)	看診科別	
DoctorId	Char(10)	負責醫師 ID	
DoctorName	Char(20)	負責醫師姓名	
DocumentType	Char(04)	文件類別	HL7 Table 0270
DocumentId	Char(20)	文件唯一鍵值	
DocumentName	Char(40)	文件唯一名稱	
ContentType	Char(10)	文件資料格式	HL7 Table 0191
CreateDate	DateTime	文件產生日	
AuthorId	Char(10)	簽章人 ID	
AuthorName	Char(60)	簽章人名稱	
AuthorDateTime	DateTime	簽章時間	
ExpireDate	DateTime	簽章有效日期	
Signature	BLOB	簽章資料(訊息指紋)	
Certificate	BLOB	憑證資料	
DC	Char(01)	是否已刪除	Default N:未刪除未異動 D:已刪除 U:資料已被異動異動
InsertDateTime	DateTime	存入 Index 日期時間	
ModifyDateTime	DateTime	異動日期時間	此兩欄位有值表示已被此文件代碼更新，DC='U'
ModifyDocumentId	Char(20)	更新之文件代碼	
ReplaceDocumentId	Char(20)	取代的文件代碼	表示此筆資料是取代掉哪一份文件
DeleteDateTime	DateTime	刪除日期時間	
SecureLevel	Char(01)	機密等級	

（二）參與推廣計畫之醫療院所：

1. 建立電子病歷資料庫，其 Schema 如附表 2
2. 將 HIS 上病歷資料轉成 XML 格式，寫入電子病歷資料庫中
3. 將電子病歷簽署電子簽章
4. 將病歷索引及電子簽章上傳至電子病歷索引中心

（以上 2~4 項可參考圖 2，電子病歷產生過程）

5. 安裝電子病歷查詢程式--（1）將使用者查詢條件及查詢端讀卡機所讀取的資料，轉給病歷索引中心；(2）將病歷索引中心傳回的病歷索引資料送給使用者端電腦顯示；(3）將使用者選定要後要查看之病歷索引及電子簽章轉送給原始病歷之醫院；(4）接受從其他醫院送來的查詢，經比對電子簽章後，將電子病歷以 HL7 格式傳回給請求端
6. 網際網路資料傳送採 SSL 安全機制

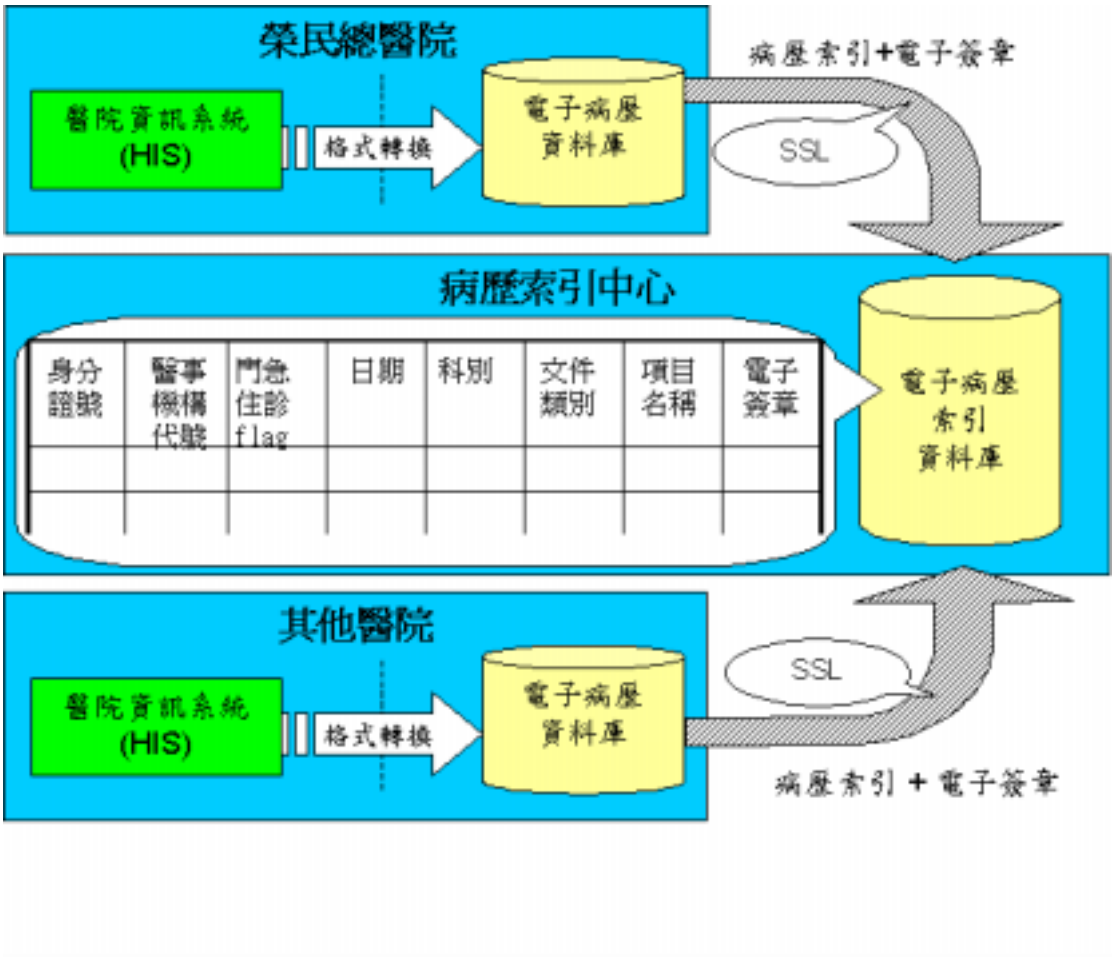


圖 2　醫療院所電子病歷產生過程

附表 2 電子病歷資料庫 Schema

Table Name: EMRDOC				
欄位名稱	資料型態	欄位說明	備註	
PatientId	Varchar2 (10)	病患 ID,身分證號		醫
PatientName	Varchar2 (20)	病患姓名		療

ClinicalDate	Varchar2 (08)	日期(醫療行為日)		院所資料轉入時填入的欄位
ClinicalType	Char(01)	病患分類	O:門 E:急 I:住	
Department	Varchar2 (02)	看診科別	健保科別	
DoctorId	Varchar2 (10)	負責醫師 ID	醫師證號	
DoctorName	Varchar2 (20)	負責醫師姓名		
DocumentType	Varchar2 (04)	文件類別	HL7 Table 0270, 目前共分為 SOAP:門診 SOAP DS:出院病歷摘要 OBR:檢驗檢查報告	
DocumentId	Varchar2 (20)	文件唯一鍵值	文件的唯一編碼(Unique)	
DocumentName	Varchar2 (40)	文件名稱		
ContentType	Varchar2 (10)	文件資料格式	HL7 Table 0191	
XmlFile	Blob	文件資料	實際 XML 病歷資料	
CreateDate	DateTime	文件產生日	轉入資料庫的時間	
AuthorId	Varchar2 (10)	簽章人 ID	醫療機構代碼	簽章後填入
AuthorName	Varchar2 (60)	簽章人名稱	醫療機構名稱	
AuthorDateTime	DateTime	簽章時間		
ExpireDate	DateTime	簽章有效日期		
Signature	BLOB	簽章資料(訊息指紋)		
Certificate	BLOB	憑證資料		
SecureLevel	Char(01)	機密等級	預留欄位	
Method	Char(01)	文件異動狀態	N/U/D, 內定為 N	
UpdatedDocId	Varchar2 (20)	要修改的文件序號	若 Method=U, 這欄位才會有值	
Status	Char(01)	處理狀況	Y/N/E	
ErrMsg	Varchar(2)	錯誤訊息		

附表 3 全民健保就醫科別

Value	科別
01	家庭醫學科
02	內科
03	外科
04	小兒科
05	婦產科
06	骨科
07	神經外科
08	泌尿科
09	耳鼻喉科
10	眼科
11	皮膚科
12	神經科
13	精神科
14	復健科
15	整型外科
40	牙科

HL7 User-defined Table 0270 - Document type

Value	**Description**
AR	Autopsy report
CD	Cardiodiagnostics
CN	Consultation
DI	Diagnostic imaging
DS	Discharge summary
ED	Emergency department report
HP	History and physical examination
OP	Operative report
PC	Psychiatric consultation
PH	Psychiatric history and physical examination
PN	Procedure note
PR	Progress note
SP	Surgical pathology
TS	Transfer summary
SOAP	門診 SOAP

OBR 實驗室檢驗報告

This field identifies the type of document ， The organization is free to add more entries.

於試辦計畫時，發現本表格所定義的文件種類並不夠用，像門診 SOAP、實驗室檢驗報告等，因此增加了文件種類”SOAP”用來表示門診 SOAP，”OBR”用來表示實驗室檢驗報告。

HL7 Table 0191 - Main type of referenced data
（Document content presentation）

SI	Scanned image (HL7 V2.2 only)
SI	Scanned image
NS	Non-scanned image (HL7 V2.2 only)
NS	Non-scanned image
SD	Scanned document (HL7 V2.2 only)
SD	Scanned document
TX	Machine readable text document (HL7 V2.2 only)
TX	Machine readable text document
FT	Formatted text (HL7 V2.2 only)
FT	Formatted text
TEXT	Machine readable text document (HL7 V2.3.1 and later)
IM	Image data (new with HL7 v 2.3)
AU	Audio data (new with HL7 v 2.3)
AP	Other application data, typically uninterpreted binary data (new with HL7 v 2.3)
Image	Image data (HL7 V2.3 and later)
Audio	Audio data (HL7 V2.3 and later)
Application	Other application data, typically uninterpreted binary data (HL7 V2.3 and later)

對於醫學影像（PACS）資料，上述電子病歷索引資料庫及電子病歷資料庫 Schema 中，Document type 欄位的值使用”DI”，Content type 欄位的值使用 ”Image” 來表示。

（三）使用者(醫師)欲查詢電子病歷內容時，需具備以下的條件：

- PC 設備

- 瀏覽器(Microsoft Internet Explorer 4.0 以上)
- 可連結 Internet 的網路環境
- 健保 IC 卡讀卡機(可驗證之環境)
- 持有有效之醫事人員卡及健保 IC 卡

本推廣計畫擬分兩階段進行，第一階段藉由舉辦專家諮詢會議，制定出相關規範，作為第二階段建置的參考依據；這些規範包括：(1) 電子病歷應包括內容 - 除各種病歷記錄（住院摘要、病程記錄、手術記錄、出院摘要、轉科摘要、門診 SOAP、會診報告）及各種檢驗檢查報告外，還應包括那些資料, 如各種同意書 (住院同意書、手術同意書), 過敏 (Allergies) 記錄，已接受過疫苗注射(Immunizations)等。(2) XML 電子病歷標準 - 針對上述各種病歷，訂定全國通用的 XML DTD 或 Schema，以增加電子病歷後續應用。(3) 病歷文件大小的分割 -以一次門診為例，主要病歷可能包括門診 SOAP、門診處方及治療處置、各種檢驗檢查報告、診斷證明書等；電子病歷文件大小，是以該次門診所有病歷資料整合成一份文件，或按資料性質及產生時機各自成為一份文件。若是以一次門診為分割，則需等待該次門診所有資料都完成，才能產生電子病歷、簽章並上傳；如此將會產生病歷時效問題，例如該次門診是由別院轉診來的，原本可於當天看完診後先將門診 SOAP 及處方回覆對方醫院。(4) 電子簽章使用憑證 – 本推廣計畫應採用 HCA 發給的醫事機構憑證或醫事人員憑證，作為電子病歷簽章的憑證，希望藉由事先的諮詢及討論，取得共識。本院於試辦計畫時是採用醫事機構憑證對電子病歷簽章，基於執行速度考量，使用的是 AP 憑證而非醫事機構卡憑證。(5) 電子簽章及上傳時機 – 於電子病歷完成時立即簽章並上傳，或採用批次方式，於每天離峰時間簽章及上傳。本院於試辦計畫時，是採批次方式對電子病歷簽章，醫院每天將完成的病歷轉成 XML 格式，存放電子病歷資料庫內；再批次從電子病歷資料庫內，篩選仍未簽章的病歷，逐一完成簽章後，寫回電子病歷資料庫，並將索引及簽章上傳。(6) 電子病歷查詢權限 – 對於電子病歷資料的查詢，必須考

量病人的隱私權與醫師查看病歷的完整性；另外，是否需要針對科別或專長，規範醫師查看範圍。

二、背景分析：請敘述本計畫產生之背景及重要性，如：(1)政策或法令依據，(2)問題狀況或試辦需求，(3)國內外相關之文獻探討，(4)本計畫與醫療保健之相關性等。(5)醫療院所電腦資訊化之程度。

本推廣計畫案背景說明：

行政院衛生署於九十二年五月二日，以「衛署資訊字第０九二一０００一六七號」函，請本院研提九十二年度「電子病歷索引中心」推動計畫書，以協助衛生署推動「網路健康服務推動計畫」之「成立醫療資訊交換中心」子計畫。

相關的政策或法令依據：

1. 衛生署曾於八十四年底函文解釋醫療機構使用電腦製作實體病歷者，於輸入電腦時，應隨即將記錄內容列印，並由診治醫師簽名，以依法製作實體病歷資料，並依規定年限保存。對於電腦保存之病歷記錄，亦應妥善管理，善盡法令所規定之保密義務。
2. 醫師法修正草案第六十六條，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；其資格條件與製作方式、內容及其他應遵行事項之辦法，由中央主管機關定之。
3. 電腦處理個人資料保護法 ，中華民國八十四年八月十一日華總義字第五九六○號令公布
4. 電腦處理個人資料保護法施行細則，中華民國八十五年五月一日法務部法令字第一０二五九號令公布
5. 電子簽章法，中華民國 90.11.14 總統府公告，910401 生效。
6. 行政院衛生署，醫療機構實施電子病歷作業要點〈草案〉，91/08/28
7. 行政院衛生署，設置及營運「醫療憑證管理中心」實施計畫書，中華民國 91 年 2 月

美國 IOM（Institute of Medicine）於 1989 組織一委員會著手病歷改進的調查與研究，該委員會於 1991 發表其調查研究報告：「The Computer-based Patient record : An Essential Technology for Health care」 [9]。自此以後，「電子病歷」相關名詞、協會、文章、標準、研討會、研究計畫、書籍等如雨後春筍般湧現。

電子病歷的定義：CPRI（Computer-Based Patient Record Institute）將電子病歷描述為「以電子式儲存關於個人一生的健康狀況及醫療照護的資訊」，它取代紙本病歷當作主要的照護紀錄，滿足所有臨床上、合法性及管理上的需求。一個電子病歷系統要能提供提醒與警示，與知識庫連結以輔助臨床決策支援，提供治療結果研究所需要的資料，及改善醫療照顧遞送系統的管理等「IOM 1997、p.11」。一位病人，終其一生可能到過許多不同的醫療院所就醫，其就醫記錄也就分散在這些不同的醫療院所，每個醫療院所所擁有的，並不是這位病患全部的病歷，而只是這位患者完整病歷的一部分；每位醫師所能看到的病歷，也只是該位病患病歷的片斷。因此有急迫的需求，將這些分散在各處的病歷資料組合起來成為單一虛擬的完整病歷（Single virtual patient record）「IOM p181，13」。

要將同一位病人分散在各處的病歷組合起來，成為單一虛擬的完整病歷，本院於去年試辦計畫提出的構想，便是建立全國性電子病歷索引中心，儲存每一位國民每一份電子病歷的索引及其簽章，而完整的電子病歷內容則儲存於原始醫療院所。

國內多數醫療院所都已實施電腦化作業，本院更在民國八十年底，就已將醫療相關作業全面電腦化，醫師直接在電腦上輸入病歷記錄、開立醫囑、查看報告。但是由於電子病歷仍不具有合法性，醫院只好採取雙軌作業，將電腦化的病歷記錄、醫囑、及報告從電腦印出，由醫師蓋章後再由人工粘貼病歷，醫院無法完全享受電腦化的好處。

我國電子簽章法已於去年四月一日生效，賦予電子病歷的合法地位；

醫療院所也企盼衛生主管機關，能儘早訂出電子病歷的相關施行辦法，好讓醫院儘快使用電子病歷，而不再使用傳統的紙本病歷，以提升醫院整體的效率及品質。大多數醫院長久以來，均對紙本病歷存放空間及管理人力不足的問題所困擾，實施電子病歷，這些問題自然解決。其次，醫療院所間對於病歷的交換及共享亦是非常迫切，因此本院過去數年曾發展「Web-Based 轉診檢報告查詢系統」，提供特約轉診醫療院所，直接上網查詢轉來本院病人的病歷及檢驗檢查報告等，不需再以人工方式執行轉診回覆。民國八十九年參加行政院衛生署「二代全國醫療資訊網計畫」提出「電子轉診作業模式的建立」，主要的做法為開發一套以網際網路為基礎的電子轉診系統供轉診醫院及後送醫院相互傳送完整之轉診病歷資料。

已全面電腦化的醫療院所，在因應電子病歷潮流，仍有格式轉換問題。因為過去電腦化時，資料均以欄位觀念（data field）儲存在資料庫中，一份檢查報告或出院摘要或手術紀錄，在資料庫內可能是分散在數個資料表格中，由數十個欄位組合而成，而不是將整份病歷記錄視為一個單元來儲存。以下面（圖 3）血液常規檢查報告為例，本院使用 IBM 大型主機資料庫 IMS/DB 儲存，其資料庫結構如圖 4，總共欄位接近 80 個之多。但是電子簽章是以一份文件為單位，而非個別對一份文件的所有欄位逐一簽章。雖然醫院的資訊系統，可以從資料庫重新產生出原先的報告格式。

圖 3 血液常規檢查報告範例

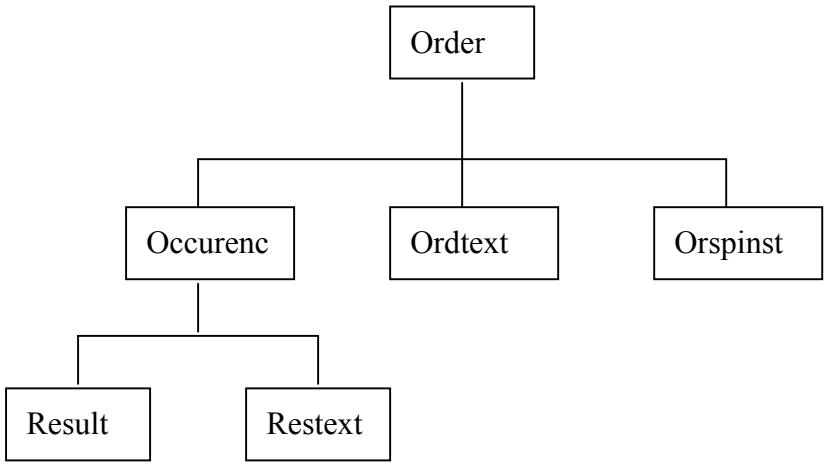


圖 4 本院 IMS/DB 醫囑資料庫結構

XML 能同時兼具傳統資料庫欄位的特性，又能滿足電子病歷文件（document）的特性，已廣泛的被應用在醫療資訊上；1997 年的 Kona Proposal 描述一種方法，電子病歷可以使用 SGML/XML 建立、交換及處理「11」 ；1998 年由 KEG 發表 HL7 文件病患記錄架構草案（HL7 Document Patient Record Architecture -PRA）「2」，同年 Gloria Shobowale 發表以 SGML/ XML 文件為中心之方式的電子病歷記錄「3」。HL7 PRA

於 2000 年改名為 HL7 CDA（Clinical Document Architecture），一份 CDA 文件主要的元素如圖 5，同時 CDA 文件是採用 XML 編碼；從以上說明可以看出 XML 已被普遍的使用在醫療資訊上，而且處理病歷資料的觀念也從傳統記錄（record）的觀念演變為文件（document）觀念。圖 6 是 HL7 CDA Release 2.0 草案中所提供關於會診記錄的文件範例（Good Health Clinic Consultation note），圖 7 則是該草案中對於文件識別、修改及補充的說明，而該文件範例完整 CDA 的 XML 內容，接近 1200 行，若單獨存成 Word 檔案，其檔案大小約 140KB，實在大得驚人。

```
<ClinicalDocument>
  ...
  <StructuredBody>
    <Section>
      <text>...</text>
      <Observation>...</Observation>
      <Observation>
        <reference>
          <ExternalObservation>...</ExternalObservation>
        </reference>
      </Observation>
    </Section>
  </StructuredBody>
</ClinicalDocument>
```

圖 5、一份 CDA 文件主要的元素 [6]

Good Health Clinic Consultation note

Consultant: Robert Dolin, MD

Date: April 7, 2000

Patient: Henry Levin, the 7th **MRN**: 12345 **Sex**: Male

Birthdate: September 24, 1932

History of Present Illness

Henry Levin, the 7th is a 67 year old male referred for further asthma management. Onset of asthma in his ~~twenties~~ teens. He was hospitalized twice last year, and already twice this year. He has not been able to be weaned off steroids for the past several months.

Past Medical History

- Asthma
- Hypertension (see HTN.cda for details)
- Osteoarthritis, right knee

Medications

- Theodur 200mg BID
- Albuterol inhaler 2puffs QID PRN
- Prednisone 20mg qd
- HCTZ 25mg qd

Allergies & Adverse Reactions

- Penicillin - Hives
- Aspirin - Wheezing
- Codeine – Itching and nausea

Family History

- Father had fatal MI in his early 50's.
- No cancer or diabetes.

Social History

- Smoking :: 1 PPD between the ages of 20 and 55, and then he quit.
- Alcohol :: Rare

Physical Exam

- **Vital Signs**

Date / Time	**April 7, 2000 14:30**	**April 7, 2000 15:30**
Height	177 cm (69.7 in)	
Weight	194.0 lbs (88.0 kg)	

BMI	28.1 kg/m^2	
BSA	2.05 m^2	
Temperature	36.9 C (98.5 F)	
Pulse	86 / minute	84 / minute
Rhythm	Regular	Regular
Respirations	16 / minute, unlabored	14 / minute
Systolic	132 mmHg	135 mmHg
Diastolic	86 mmHg	88 mmHg
Position / Cuff	Left Arm	Left Arm

- **Skin** :: Erythematous rash, palmar surface, left index finger.

- **Lungs** :: Clear with no wheeze. Good air flow.
- **Cardiac** :: RRR with no murmur, no S3, no S4.

Labs

- CXR 02/03/1999: Hyperinflated. Normal cardiac silhouette, clear lungs.
- Peak Flow today: 260 l/m.

In-office Procedure

- Suture removal, left forearm.

Assessment

- Asthma, with prior smoking history. Difficulty weaning off steroids. Will try gradual taper.
- Hypertension, well-controlled.
- Contact dermatitis on finger.

Plan

- Complete PFTs with lung volumes.
- Chem-7
- Teach peak flow rate measurement
- Decrease prednisone to 20qOD alternating with 18qOD.

- Hydrocortisone cream to finger BID.
- RTC 1 week.

Signed by: Robert Dolin, MD April 8, 2000

圖 6 HL7 CDA Sample [6]

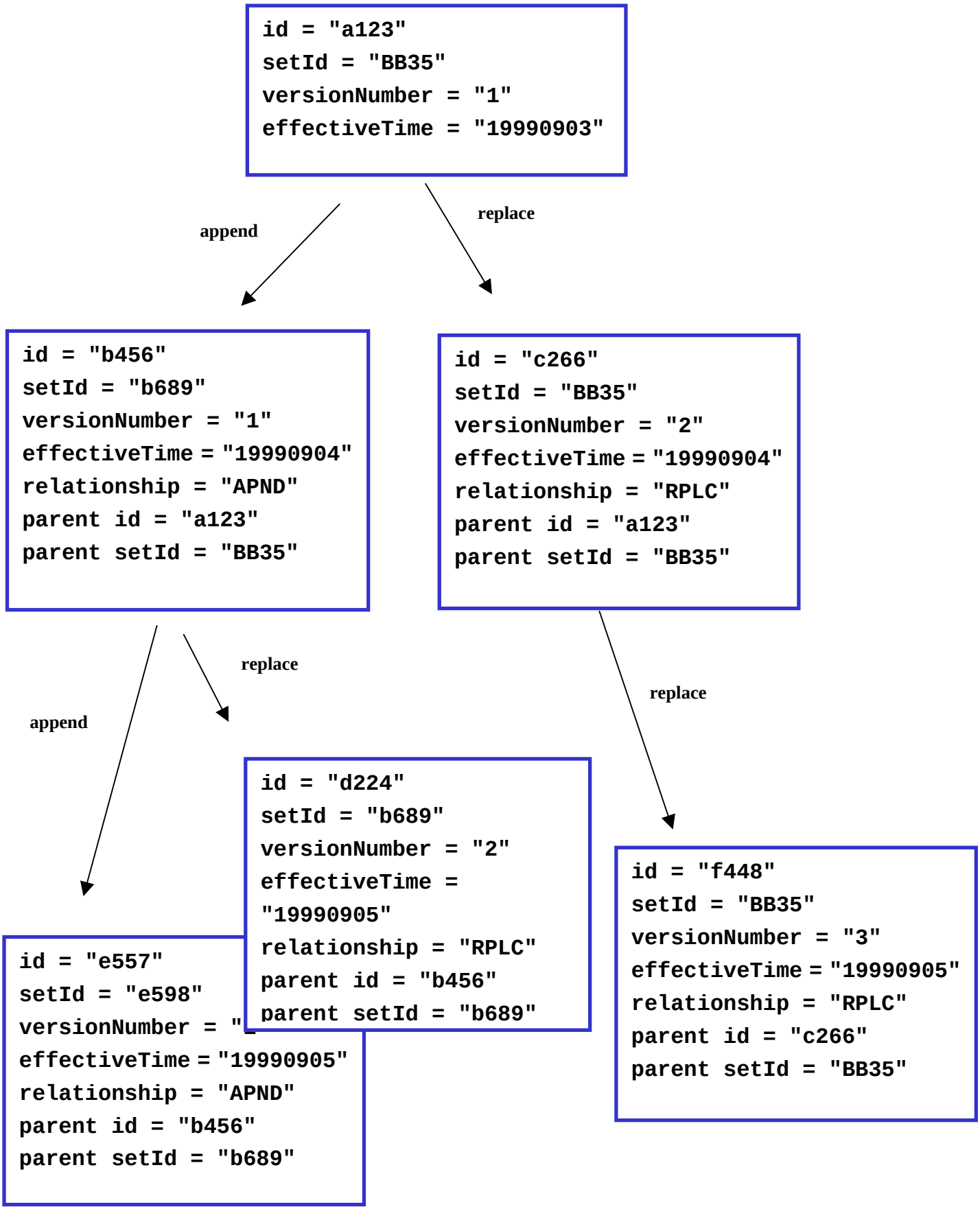


圖 7　HL7 CDA 草案關於文件識別、修改及補充說明 [6]

ASTM E31 於 1999 年 10 月提出 XML DTD 草案，包括處方、出院摘要、手術記錄、住院摘要、診斷影像報告等，以診斷影像報告 DTD 為例，建議應包括如圖 8；目前 ASTM E31 的「Standard Specification for Clinical XML DTD in Healthcare」為 Standard E2183-02 [1]，所包括的 XML DTD 有：

1. Admission Notes
2. Discharge Summaries
3. History and Physical Examinations
4. Operative Reports
5. Pathology Reports
6. Radiology Reports
7. Radiation Therapy Summaries

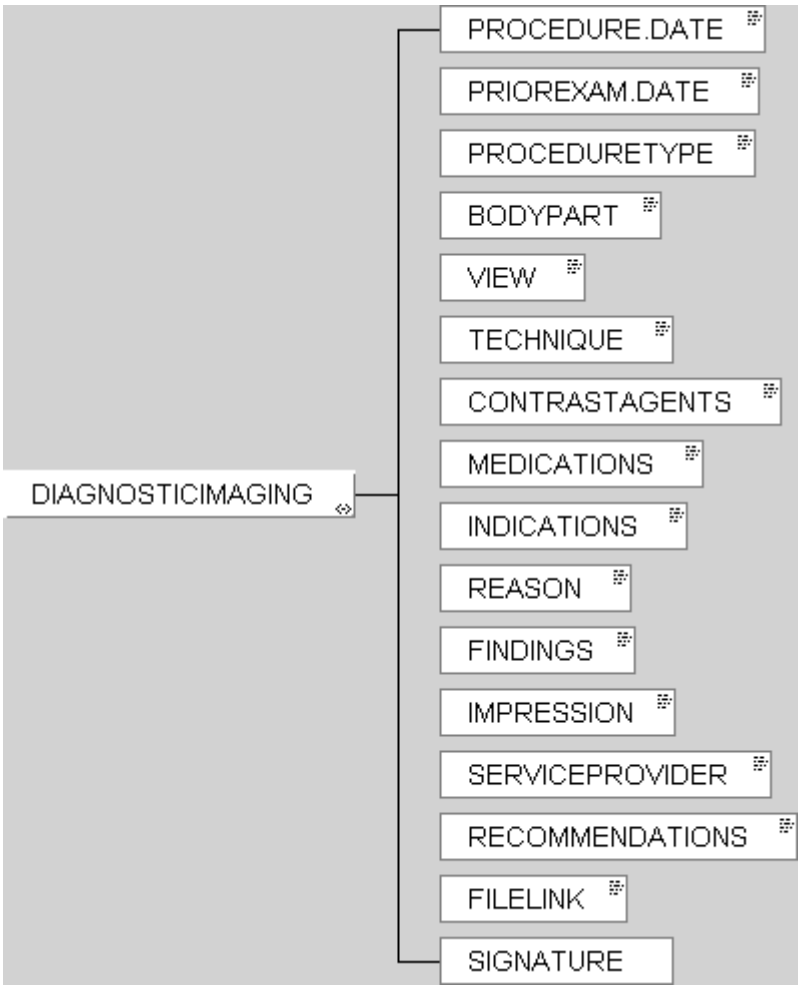


圖 8　ASTM E31 Diagnostic imaging DTD draft

我國「電子簽章法」已在去年四月一日生效，確立電子病歷的法律地位，然而電子病歷在網路交換過程的安全問題，如何解決？數位簽章是指使用數學演算法（或稱雜湊函數）將電子文件轉化為固定長度之數位資料（訊息摘要），並用簽署者之私鑰（代表簽署者本人之數位資料）對其加密形成一簽體，使任何人可藉未轉化前之原始資料訊息、簽體及與私鑰相關連之公鑰（公開之數位資料），驗證該簽體是否使用與簽章公鑰相對應之私鑰所製作，以及簽體製作後，原始資料訊息是否遭受竄改。

數位簽章是目前技術較為成熟且廣泛使用之加密方法，其運作必須有一公正之第三者成立憑證機構，由憑證機構製作簽章用的公、私鑰，並提供電子文件存證、公證及時戳的服務。私鑰就好比是私人的印鑑，公鑰則好比是印鑑證明，簽署者利用私鑰（印鑑）在電子文件（書面文件）上簽章，產生的電子文件稱為簽體（已簽章之書面文件），收到簽體的一方則可以向憑證機構申請簽署者之公鑰（印鑑證明），以驗證簽體之真偽。

雖然有了法源依據，但是醫療院所仍不知所從，沒有相關規範或指引可供參考。在九十一年度試辦計畫申請作業說明中，已載明試辦計畫目的：（一）期望試辦後能釐定相關規範或指引，再逐步推廣至全國。（二）藉由試辦之規範或指引提供其他醫療院所實施電子病歷時正確的做法，避免試誤、浪費人力及金錢。（三）鼓勵醫療院所發展電子病歷，以促進院際間醫療資訊的交換與流通。

電子簽章可用來鑑別送出訊息者或文件簽章者本人，確保訊息或文件的原始內容在傳送時沒有被改過。電子簽章製作的過程中(如圖 9)，為求速度及正確性，本模式將 XML 格式病歷內容全文經雜湊函數運算後得到一份訊息摘要（簽體），此摘要再經醫事人員或醫院的私鑰加密後，方得到電子簽章。

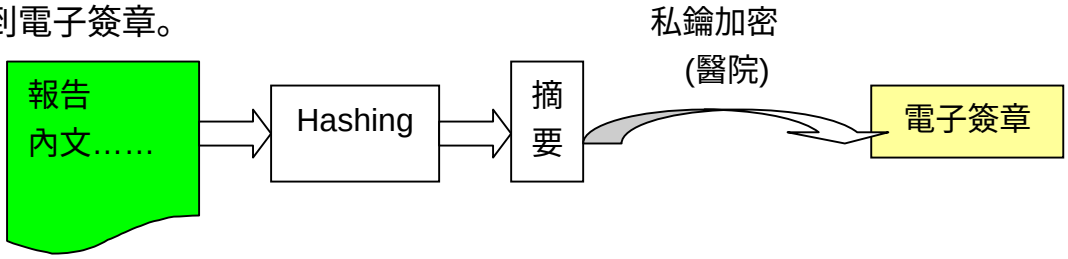


圖 9 電子簽章製作方式

當查詢方從電子病歷伺服器取得報告後，若對該報告的內容產生懷疑，則可利用認證的方式(如圖 10)來確定報告的正確性。首先將病歷的內容以雜湊函數取得摘要 A，接著把存證管理中心取得的電子簽章以被查詢醫院的公鑰解密，若解密後的摘要 B 與摘要 A 完全相同，則可確定病歷未被更動，反之亦同。

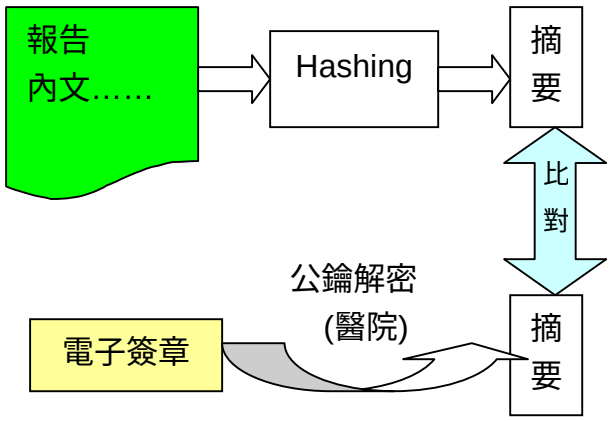


圖 10 電子簽章驗證方法

醫療憑證管理中心：

行政院衛生署亦於去年委託設置及營運「醫療憑證管理中心」(Health-care Certification Authority, HCA)，本文摘錄其目標與安全保證需求如下：

目標：

1. 設置及營運「醫療憑證管理中心」，提供醫療體系一安全及可信賴的電子交易環境。
2. 建立安全可靠的網路認證制度，促進醫療資訊電子化的普及應用。
3. 訂定適合醫療憑證管理中心之憑證政策(Certificate Policy,CP)，以達到對醫療憑證之有效管理。
4. 訂定醫療憑證管理中心之憑證實務作業基準(Certification Practice Statement , CPS)，以達到電子憑證之公正性及網路服務之安全性。

安全保證需求

1. 資料保密性(Confidentiality)：確保資料不遭第三者偷窺或竊取，以保障資料的隱私權益；可透過資料加密技術來完成。
2. 資料的完整性(Integrity)：確保資料未遭有心人士竄改，以保障資料之完整性及正確性；可藉由電子簽章及資料加密技術加以保護。
3. 來源辨識性(Authentication)：確認交易雙方的身分，防止身分被偽造及冒用；可經由電子簽章及公鑰基礎架構予以防範。
4. 不可否認性(Non-repudiation)：避免交易雙方事後否認有收發資料的行為事實；可透過電子簽章及公鑰基礎架構來達成。

醫療機構實施電子病歷作業要點〈草案〉：

第三條 - 醫療機構符合下列各款規定者，其以電子文件方式製作或保存之病歷〈以下簡稱電子病歷〉，得全部或部分免另以書面方式製作。

（一） 領有行政院衛生署〈以下簡稱本署〉認可之「醫療機構憑證」。

（二） 所屬醫事人員領有本署簽發之「醫事人員憑證」。

（三） 電子病歷於每次紀錄完成時，應即以電子簽章簽署，並記錄簽署之時間。

（四） 電子病歷於每次紀錄完成，經電子簽章簽署後，不得刪除。紀錄完成後，如須修改，應於增添新修正內容時，一併保留原有紀錄，再次以電子簽章簽署，並記錄簽署之時間。

（五） 列印電子病歷時，應能完整呈現其內容，以供日後查驗。醫療機構設置之電子病歷系統，應有防止竄改之功能。

（六） 醫療機構就電子病歷系統之當機設置回復設施，以確保醫療作業之進行。

（七） 醫療機構應設置電子病歷資料庫之異地備份或相當之設施，以確保病歷之完整保存。

（八） 醫療機構更新電子病歷系統時，應確保原有病歷之資料得繼續使用。

三、連續性計畫之執行成果概要（新申請之計畫可概述主持人過去曾執行之相關計畫成果）。

在本計畫之主持人及共同主持人曾發展之系統或參與過之研究計畫中，運用網際網路技術以提供醫療服務的相關計畫如下。這些計畫的推展不但在國內開風氣之先，也成功地引進適當的資訊科技到醫療資訊的實務應用上，成為國內各醫療院所的良好示範，目前開發完成的系統都仍在上線正常運作中。

（一）以下即為相關成果的扼要說明：

1. 行政院衛生署委託之「遠距醫療先導應用系統」：配合行政院 NII 之推行，於八十四年與台北榮總共同規劃與金門花崗石醫院之遠距醫療作業，協助提升離島之醫療服務品質，加惠離島地區之民眾。目前該系統仍然持續對金門地區軍民提供遠距會診服務。
2. 「醫療影像儲傳系統之遠端使用— NII 上醫療應用的先導計畫」（計畫編號：VGHTH-85-024-3）：於八十五年與清華大學資訊科學所共同設計一套遠程影像連線系統，可提供本院醫師在家或院外醫療診所，透過網路直接查詢院內醫療影像儲傳系統（Picture Archiving and Communication System, PACS）上之病患醫療影像資料。本系統成果曾在 RSNA 1997 (北美放射醫學年會)中實機展示，並獲大會主動邀稿將成果論文收錄於 RadioGraphics 雜誌中[16]。
3. 「Web-Based 轉診檢報告查詢系統」：於八十七年九月啟用，為國內第一套經由網際網路可線上查詢轉診檢報告之系統，使特約轉診醫院可使用網路瀏覽器來上網查詢之功能。該查詢系統有簡單易用、連線成本低廉、病歷資訊得以整合運用、可縮短轉介單位等待報告時間、提高轉診服務品質及降低成本等貢獻。[20]
4. 「醫療會診及諮詢環境之研製」：於八十八年起開始進行，為三年期之

國科會整合型計劃“國家寬頻網路上整體醫療服務系統之研製”之一子計劃。除自行研究並實作 DICOM 傳輸功能與 XML 格式轉換機制，以取得遠端醫療資料及影像外，並實作開發醫學影像處理相關軟體，整合視訊影像及語音之會診畫面同步機制，以提昇醫療會診互動效果。

5. 「電子轉診作業模式的建立」：民國八十九年本院參加行政院衛生署「二代全國醫療資訊網計畫」提出該項計畫，除發展一套實用的網基電子轉診系統外，同時也將此系統與本院現有之醫院資訊系統(HIS)及醫學影像儲傳系統(PACS)連線，以HL7及DICOM傳輸標準提供院內電子病歷交換機制。[21]

6. 「一個快速且安全的電子病歷分享模式」，本院於九十一年度參加行政院衛生署「醫療院所病歷電子化試辦計畫」所提出；整體系統架構如圖1，參與試辦的醫療院所除台中榮民總醫院外，還包括台中國軍總醫院及嘉義榮民醫院。[17]

（二）九十一年度試辦計畫簡介

1. 電子病歷資料庫建置並上傳至電子病歷索引中心

醫療院所自目前院內已建置的醫療資訊系統(HIS)中，將已完成的病歷，批次將資料轉成 XML 格式的文件資料，並依其索引資料填入電子病歷資料庫中的待處理表格中。系統程式不斷偵測待處理資料表格中是否有未處理的資料，將未處理的資料讀出後，以醫療機構的 Private Key，對於 XML 資料文件加以簽章，產生簽章資料(Signature)，完成簽章作業後，將病歷索引資料、病歷文件、簽章資料(Signature)及憑證資料(Certificate)存入正式的電子病歷資料表格中。

完成簽章作業後，將該筆病歷資料的索引資訊及簽章憑證資訊，以 XML 格式組成後，上傳至電子病歷索引中心，管理中心接收訊息後，依資料的類別，區分新增、異動及作廢的型態，分別寫入索引資料表

格中，並將寫入成功與否的訊息回傳至上傳醫療院所端。醫療院所資料上傳後，依電子病歷索引中心所回傳的處理回覆，將狀態回寫入資料表，如有錯誤則將錯誤訊息填入，可供管理人員查看錯誤並加以處理。

2. 病歷索引資料查詢

病歷資料查詢時，查詢端需具備可上 Internet 的環境，透過網際網路瀏覽器(Web Browser)，連結至電子病歷查詢網頁；同時，查詢端必須連接健保 IC 卡讀卡機，完成卡機驗證作業後，將病患的健保 IC 卡及醫事人員卡放入卡機當中，透過讀卡作業，將病患的身分證字號等基本資料及醫師基本資料讀出，並以此做為查詢的基本條件。

點選查詢資料的篩選條件，包含就診日期的起迄及就診的醫療機構，將查詢條件組成 XML 資料，為確認資料查詢端的身份驗證，所以在將查詢條件送出之前，先將資料送入醫事人員卡中簽章，完成後在送至電子病歷索引中心。

管理中心接收此查詢條件之後，先取得查詢醫師的公開金鑰(Public Key)，驗證資料成功後，再依此查詢條件自資料庫中查詢出符合條件的資料，組成 XML 資料後回傳。

查詢端取得回傳資料後，依目前病歷的狀態(一般、更新、刪除)加以顯示，供使用者依文件名稱選擇詳細查看的病歷。

3. 詳細病歷資料查詢及驗證

自醫療資訊存證中心查詢出的病歷索引資料中，可點選要查看詳細病歷的資料，點選後，查詢端依此筆病歷的索引值及自存證中心所取得的簽章(Signature)，組成 HL7 Message QRY^T12(Document Query)，並轉換成 XML 格式，傳送至病歷擁有端。

病歷擁有端收到此 HL7 Message 後，解譯訊息後，確認查詢端所傳送

的簽章(Signature)與本身電子病歷資料庫中找出相對應的資料的簽章是否一致，如果相同，亦組成 HL7 Message DOC^T12(Document Query Response)，轉換成 XML 格式後回傳，反之則傳送錯誤訊息。

查詢端接收到回覆訊息後，為確認病歷提供者未擅自修改病歷，必須將所傳回的 XML 病歷資料，運算後與自存證中心所取得的簽章加以比對，如果相同，則以新視窗顯示該筆病歷資料，並依醫療院所轉出病歷資料時所使用的 XSL，依其格式顯示，否則，則於畫面中顯示該筆資料未能通過電子簽章驗證。

4. 管理作業說明

對於病歷的查閱，提供使用者依查詢日期的起迄、病患身份證字號及查詢者的身份證字號等條件加以查詢，用以查看病歷調閱記錄。

提供錯誤記錄查詢，針對資料於簽章、上傳等作業中，如系統執行過程發生錯誤，將記錄錯誤訊息，系統管理人員可藉由查詢作業查詢是否有錯誤發生，並加以處理。

5. 憑證說明

公開金鑰基礎架構提供了公共的身分認證系統，目的在維護每個使用者的憑證的正確性，也就是使用者公開金鑰的正確性，能夠證明此公開金鑰是屬於某一位特定使用者所擁有。

公開金鑰基礎架構由下列幾個主要角色所組成：

- 終點實體(End Entity)：使用憑證的的主要對象，終點實體可視為一般使用者、團體、公司行號等。
- 憑證中心(CA, Certification Authority)：可信任的公正第三者，負責憑證、憑證廢止清冊之發行與管理等工作。
- 註冊中心(RA, Registration Authority)：位於憑證中心之前端，終端實體可透過註冊中心申請憑證。

- 憑證/憑證廢止清冊資料庫(Certificate/CRL Repository)：公開金鑰基礎架構中的資料儲存體，負責儲放憑證、憑證廢止清冊之資料。

憑證中心是一種組織，在公開金鑰基礎架構中扮演的是可信任的公正第三者，目的在對個人及機關團體提供認證及憑證簽發管理等服務，以建立具有機密性(Confidentiality) 、鑑別(Authentication) 、完整性(Integrity) 、不可否認性(Non-repudiation) 、存取控制(Access control)及可用性(Availability)的資訊通訊安全環境與機制。主要工作是負責憑證與憑證廢止清冊之發行、憑證與公開金鑰的管理以及處理與其他認證中心相互之間的信任關係。

然而，在實際的運作上，憑證中心不可能完全地處理每一個使用者申請憑證的作業，因為憑證中心不可能驗證所有申請憑證之使用者的身分，所以必須透過前端的註冊中心來當協助處理身分驗證的機制，再交由憑證中心發行憑證；如果註冊中心本身是一個可自行發行憑證的組織單位，亦可以由註冊中心代為發行憑證。註冊中心的角色並不一定為一特定的人或單位來執行，只要能夠確認使用者身分資料的單位，都可以是註冊中心。

憑證的發行機制可分成兩種，基本驗證機制(basic authenticated scheme)與集中管理機制(centralized scheme)。

- 基本驗證機制(basic authenticated scheme)：由申請憑證之使用者產生金鑰對(key pair)及憑證要求(certificate request)，將憑證要求以憑證中心之 IAK(Initial Authentication Key)加密傳回憑證中心進行驗證，再依憑證要求產生使用者之憑證並發行。
- 集中管理機制(centralized scheme)：使用者將 PSE(Personal Security Environment)資料送至憑證中心，由憑證中心產生金鑰對及憑證，並將憑證發行。

目前本計劃中，憑證中心為衛生署所成立的 HCA(Health Certification Authority)，而目前 HCA 提供兩種憑證發行機制，包含基本驗證機制的一般伺服器與 SSL 等憑證，以及集中管理機制的醫療機構與醫事人員憑證。

6. 簽章說明

就資訊安全的觀點而言，這樣環境必須能提供下列功能：

- 真確性（Integrity）：確保網路中所傳輸之資訊與原來的資訊一致，不會遭到竄改或偽造。
- 鑑別性（Authentication）： 確保網路中之個體（Entity）的身分確實如他所表明的， 或由網路所接收的資料確實為該傳送者（Sender）所傳送。
- 不可否認性（Non-repudiation）： 發送端不可否認其所同意傳送出的資料或他所完成的交易行為。
- 機密性（Confidentiality）： 防止非法使用者得知已保護之敏感資料的內容。

欲達到上述功能，必須仰賴密碼技術（Cryptography Technology）中的加密技術（Encryption Technology）與數位簽章（Digital Signature）等。 除了機密性功能以外，其他功能皆能透過數位簽章的使用來達成。

傳統的印章或親筆簽名與數位簽章最大的差異，除了所欲簽署的文件之形式不同外， 印章或親筆簽名與該文件內容是各自獨立且無關的。換言之，針對不同的文件，簽署者使用印章或親筆簽名以產生的簽章不會隨著文件內容不同而有所不同。 然而，從數位簽章的產生過程來看， 數位簽章是透過電子文件與簽署者所擁有的秘密資訊， 例如：密鑰（Secret Key）經簽章產生機制（類似數學函數）計算所得

的結果。 因此，數位簽章與電子文件的內容息息相關， 亦即，同一位簽署者所產生的數位簽章，會隨著電子文件內容不同而有所不同。目前實作上，數位簽章是以密碼學上的公開金鑰密碼系統（Public Key Cryptosystem），又稱「非對稱密碼系統（Asymmetric Cryptosystem）」為基礎來實作，亦即在該系統中，每一位使用者必須自行產生自己所擁有的金鑰對（Key Pair）：一把密鑰(Private Key)與一把公鑰（Public Key）。其中使用者必須秘密地保存自己的密鑰，並且將其公鑰公佈於網路中。之後，使用者可以利用自己的密鑰對文件進行簽署； 而數位簽章的接收者可以利用該簽署者的公鑰來驗證數位簽章的有效性。

一個安全且有效的數位簽章， 除了簽署者必須要以正確且有效的方法來對電子文件進行簽署外，其所產生的數位簽章之有效性亦需要一個合適的驗證方法來驗證。數位簽章機制（Digital Signature Mechanism）便是以密碼學（Cryptography）為基礎來定義安全的簽章產生與簽章驗證方法，此機制包括：簽章產生機制（Signature Generation Mechanism）與簽章驗證機制（Signature Verification Mechanism）。「簽章產生機制」是指簽署者產生數位簽章的方法或程序，而此機制可視為一個數學演算法。若簽署者要進行簽署時，他可以將欲簽署的電子文件與自己所擁有的密鑰當作該演算的輸入值，經過該演算法的計算後便能得到電子文件的數位簽章。另一方面，「簽章驗證機制」是指驗證者用來驗證數位簽章之有效性的方法或程序。若是驗證者收到簽署者的電子文件與數位簽章時， 他必須使用電子文件、數位簽章以及簽署者的公鑰，並且透過此機制來驗證此數位簽章的有效性。

與數位簽章息息相關的密碼技術為「單向雜湊函數」（One-Way Hash Function），此單向雜湊函數是一種可以將任意長度的輸入值壓縮成固定長度之輸出值的數學函數或演算法，並且無法從其輸出值去推算其

輸入值【MD5, FIP93】。在安全性（亦即防止非法者偽造一個合法的數位簽章，以及防止攻擊者從簽章訊息破解出簽署的密鑰）與效率性的考量下，安全的數位簽章機制必須引入單向雜湊函數於該機制中。換言之，在簽章產生機制中，簽署者必須先透過單向雜湊函數將電子文件轉換成固定長度的位元資料，稱之為資料摘要 (Data Digest)， 隨後再使用密鑰簽署該資料摘要以產生數位簽章；同樣地，驗證者亦需先使用此單向雜湊函數，將電子文件轉換成固定長度的資料摘要再進行驗證動作。

7. SSL 說明

為保護資料於網際網路傳送時具安全性及可信賴性，Netscape Communications 公司首先設計 SSL (Secure Socket Layer) Protocol，其介於應用層(Application Layer)及傳輸層(Transport Layer)之間，並將 SSL Protocol v3.0 之網路草案文件(Internet-draft)公佈於網站，在 1999 年被 IETF(Internet Engineering Task Force)接受後，更名為 TLS (Transport Layer Security) 1.0 版，是為 RFC 2246，並被廣泛應用在電子商務的安全機制。SSL Protocol v3.0 主要具備以下特性：

- 連線具隱密性，於交握協定時產生秘密金鑰(secret key)，以此秘密金鑰來對傳送之訊息進行加解密。
- 點對點(peer to peer)之間的身分驗證採非對稱式加密法 (Asymmetric cryptographic)。
- 連線具可信賴性，訊息傳送時包含訊息完整性之檢查，使用具金鑰之訊息鑑別碼(keyed Message Authentication Code, MAC)。SSL 協定是層次式的協定(layered protocol)，由兩層子協定所組成，分別為紀錄協定(SSL Record Protocol) 與交握協定(SSL Handshake Protocol)。
- 紀錄協定(SSL Record Protocol)：

紀錄協定主要負責的工作，是將欲傳輸之不固定長度的資料訊息，經過一連串的分割/組合(Fragmentation/Assembling)、壓縮/解壓縮(Compression/ Decompression)、加/解密(Encryption/Decryption)等處理，再傳送至上層(或下層)。當使用者欲傳送資料時，資料經由應用層傳送至紀錄協定層，經過分割(fragmented)、壓縮(compressed)、加入訊息鑑別碼(MAC)、加密(encrypted)之後，加上 SSL 紀錄標頭(SSL record header)，再傳送至傳輸層。反之，當使用者接收資料時，資料經由傳輸層送至紀錄協定層，經過解密(decrypted)、驗證訊息鑑別碼(verified)、解壓縮(decompressed)、組合(reassembled)後，再將資料送至應用層。

紀錄協定針對 SSL 連結提供兩大服務：

保密性(Confidentiality)：在 SSL 交握協定中，由連結的兩端協議出共享的秘密金鑰；以此金鑰來對傳送資料做加密，以達到保密性。

訊息完整性(Message Integrity)：在 SSL 交握協定中，由連結的兩端協議出共享的秘密金鑰；以此金鑰來對傳送資料加入訊息鑑別碼(MAC)，以達到訊息完整性。

- 交握協定(SSL Handshake Protocol)：

交握協定在整個 SSL 中是最複雜的一部份，主要目的在讓用戶端與伺服器端之間能相互認證(authentication)，並協議彼此加密及產生訊息鑑別碼的演算法以產生用來保護欲傳送之資料安全的金鑰。在進行任何 SSL 的連結之前，一定要先經過交握協定協議這些安全參數後，才能開始傳輸資料。建立一個新的安全通道連線的交握協定的流程分為下列四個主要步驟：

(1). 建立安全環境 (Establish Security Capabilities)

此一步驟主要為用戶端與伺服器端進行初始化的邏輯連結，協議彼此使用的安全環境參數。首先由用戶端送出 Client_hello 的訊息給伺服

器端，伺服器端收到後送回 Server_hello 的訊息，進行初始參數值的協議。

(2). 伺服器端認證及金鑰交換 (Server Authentication and Key Exchange)：

在此步驟中，首先由伺服器端傳送 certificate 訊息，並將伺服器端之憑證送出，此憑證為符合 X.509 規格的單一憑證或憑證鏈(如果伺服器端是使用匿名的 Diffie-Hellman 方式，則不需要傳送此訊息)。接著送出 server_key_exchange 的訊息，但如果在以下兩種情況下，就可以不需送出這個訊息：(1)伺服器端已經利用固定 Diffie-Hellman 的各項參數來傳送憑證，(2)即將進行 RSA 金鑰交換。

接著，如果伺服器端是一個非匿名的伺服器(不是使用匿名 Diffie_Hellman 的伺服器)可能需要從用戶端獲得一個憑證，便會送出 certificate_request 訊息，此訊息包含兩個參數：憑證類型、憑證中心，憑證類型參數指定了所使用的公開金鑰演算法與憑證的用途，憑證中心參數則是一個列表，用來記錄可接受的不同憑證中心。最後，伺服器端收到 certificate 訊息，再送出 server_hello_done 的訊息，表示伺服器端的這個階段已完成。

(3). 用戶端認證及金鑰交換 (Client Authentication and Key Exchange)

在此步驟中，若用戶端接收到伺服器端傳送之 certificate_request 訊息，則傳送 certificate 訊息，並將用戶端的憑證送出，同樣的，此憑證為符合 X.509 規格的單一憑證或憑證鏈。接著送出 client_key_exchange 的訊息，這個訊息是在此步驟用戶端必定要傳送的訊息，訊息內容則依金鑰交換的形式而定。

最後，用戶端會送出一個 certificate_verfity 訊息，讓伺服器端藉此來驗證用戶端的憑證。這個訊息必須在用戶端已經送出任何一個具有簽

章的憑證的情況下才會送出。這個訊息會根據之前所送出的訊息來簽署一個雜湊值。

(4). 完成(finished)

此步驟在建立一個安全連結。用戶端送出change_cipher_spec的訊息後，以前面步驟協議完成的加密演算法、金鑰及秘密資訊來對finished訊息做訊息封裝的動作，傳送至伺服器端，由伺服器端驗證此訊息，如果驗證成功，表示前述的金鑰交換及認證過程正確無誤。驗證無誤後，由伺服器端同樣送出finished訊息給用戶端做驗證。

（三）九十一年度試辦計畫成果：

1. 試辦計畫實體環境（參考圖11）
2. 簽署電子簽章並上傳病歷索引及電子簽章（參考圖12及說明）
3. 病歷索引查詢（參考圖13及說明）
4. 詳細病歷資料查詢及驗證 （參考圖14及說明）
5. 更動病歷文件比較 （參考圖15）查閱記錄 （參考圖16）

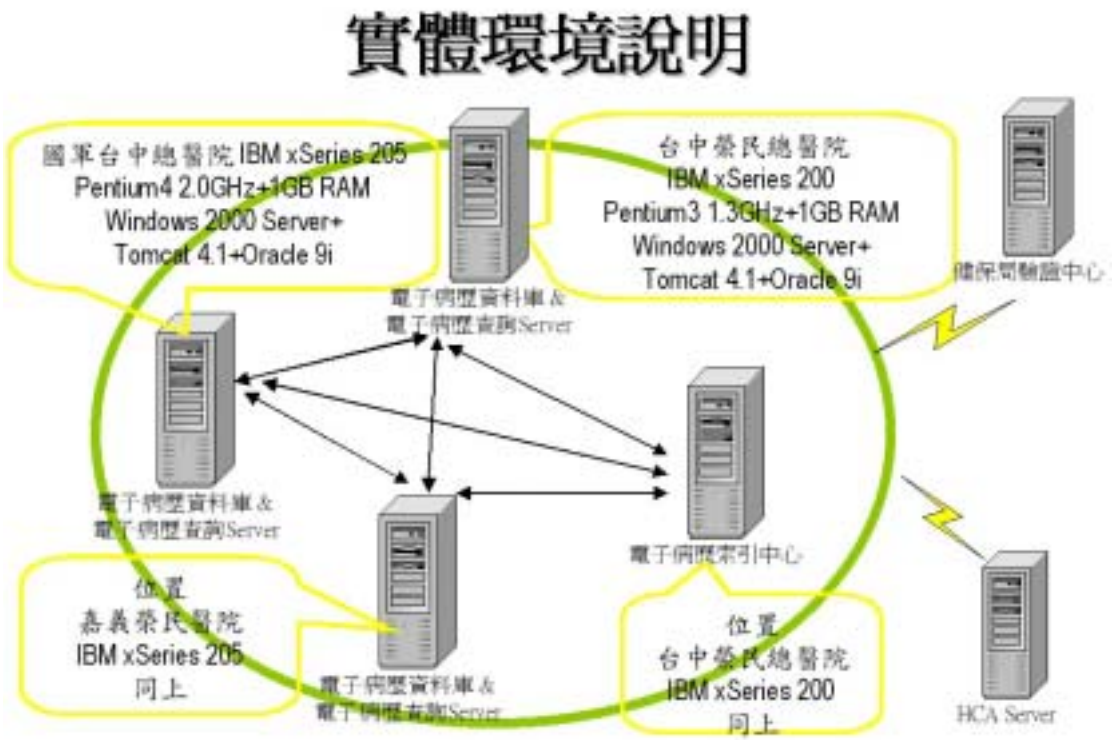


圖11 九十一年度試辦計畫實體環境

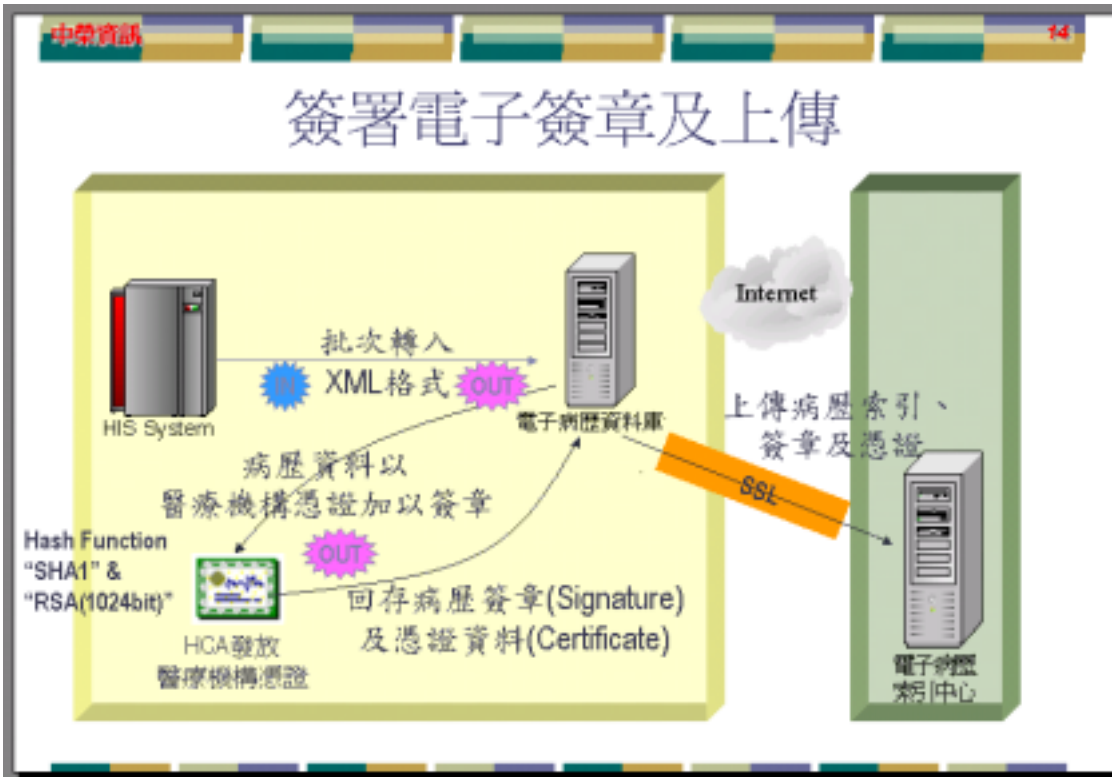


圖 12 簽署電子簽章及上傳

- 各醫療院所的醫療資訊系統，於病歷資料完成後，由醫療院所自行線上或批次處理，將病歷資料轉成XML資料格式，存放於電子病歷資料庫的待處理表格。
- 系統將未處理的病歷資料讀出後，以醫療機構憑證對每一筆病歷資料簽章，簽章所使用的Hash Function為”SHA1” & “RSA(1024 bit)”，並將簽章資料(Signature)及憑證資料(Certificate)回存至電子病歷資料庫。
- 將已完成簽章的病歷資料，其索引資料及簽章憑證資料上傳到電子病歷索引中心，索引中心收到資料後，依其資料的屬性(新增、異動、刪除)，存入電子病歷索引中心資料庫中。

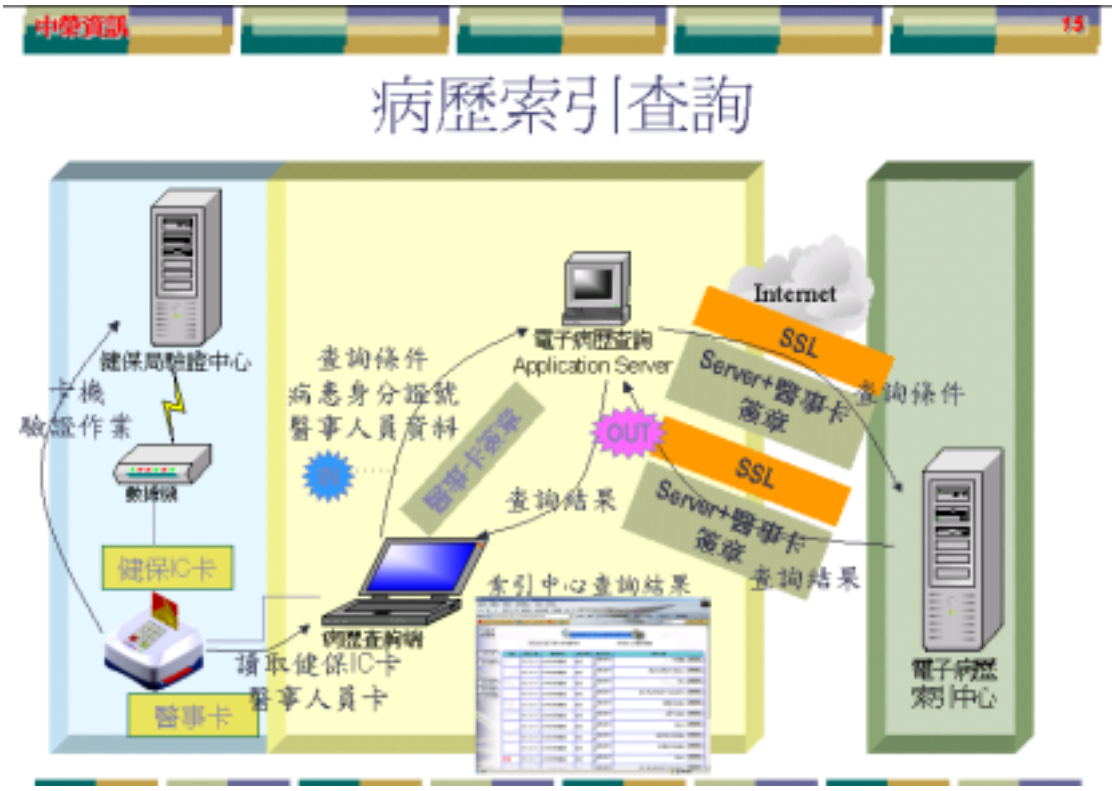


圖 13　病歷索引查詢

- 病歷查詢端，必須具備健保IC卡讀卡機的設備，卡機與健保局驗證中心認證後才可讀取卡片資料。
- 使用者將病患健保IC卡及醫事人員卡放入卡機中，自健保IC卡讀取病患基本資料，自醫事人員卡讀取醫事人員資料。
- 使用者點選查詢作業，自查詢端將查詢條件送出，並將查詢資料加以簽章。
- 由病歷查詢Application Server將查詢資料送至電子病歷索引中心，索引中心驗證所收到的資料是否來自認可的Server，以及查詢資料的簽章是否可通過驗證，以確認查詢者為合法使用者，通過驗證後將資料查出並回覆，以顯示於查詢者網頁；反之則回覆不可查詢的訊息。

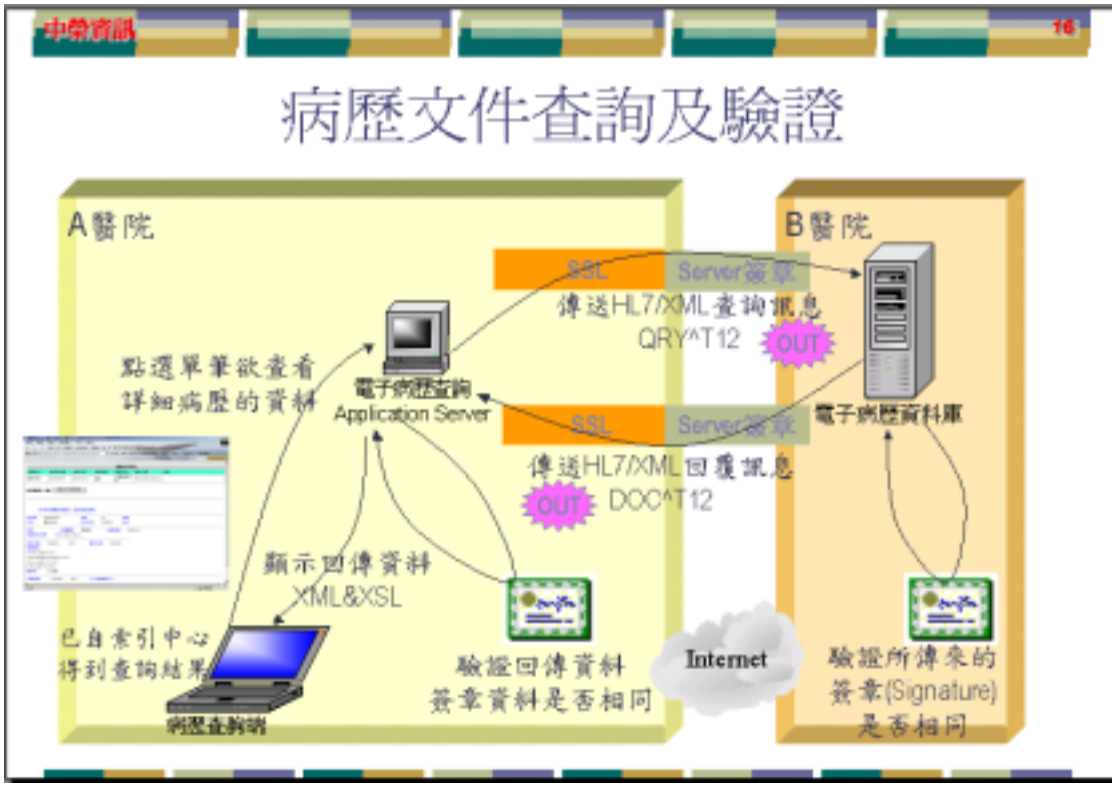


圖 14 病歷文件查詢及驗證

- 使用者點選要查看詳細病歷的資料，系統將此訊息送至電子病歷查詢Application Server。
- 電子病歷查詢Application Server將查詢資料組成HL7/XML QRY^T12 Message(包含自索引中心得到的索引資料及簽章資料)，依照其所查詢的病歷資料屬於哪個醫療院所，將訊息傳到該醫療院所的接收端。
- 接收端收到訊息後，將資料解譯後，查出該筆資料，並筆對其簽章資料是否相同，此作業目的為確保查詢者擁有來自索引中心的資料，確認相同後將資料組成HL7/XML DOC^T12回覆訊息，將資料傳回查詢端。
- 查詢端接收到HL7回覆訊息後，將資料加以解譯。
- 系統將收到的病歷資料，以相同Hash Function及索引中心所得到的憑證資料，加以驗證後，確認所得到的資料與該醫療院所上傳時的資料相同。

- 驗證通過則將資料套用XSL後顯示於畫面上，反之則顯示資料無法通過電子簽章驗證的訊息

圖 15　更動病歷文件比較

病患資訊		查詢單位資訊				病歷資訊	
身份證號	病患姓名	查詢時間	醫院名稱	醫師代號	醫師姓名	歸屬單位	文件代碼
Q88844403A	林榮泰	2003-03-20 16:00:24.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679501194702
Q88844403A	林榮泰	2003-03-20 16:30:23.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679501194702
Q88844403A	林榮泰	2003-03-20 16:59:03.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679601194702
Q88844403A	林榮泰	2003-03-20 16:59:31.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679601194702
Q88844403A	林榮泰	2003-03-20 17:00:09.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679501194702
Q88844403A	林榮泰	2003-03-20 17:00:15.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679601194702
Q88844403A	林榮泰	2003-03-20 17:02:13.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679601194702
Q88844403A	林榮泰	2003-03-20 17:02:52.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679601194702
Q88844403A	林榮泰	2003-03-20 17:28:29.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679801194702
Q88844403A	林榮泰	2003-03-20 17:29:02.0	台中榮民總醫院	test123	劉28	台中榮民總醫院	2523679801194702
Q88844403A	林榮泰	2003-03-20 19:23:56.0	台中榮民總醫院	test123	劉28	國軍台中總醫院	20030313000000010000
Q88844403A	林榮泰	2003-03-20 19:36:49.0	台中榮民總醫院	test123	劉28	嘉義榮民醫院	20030313000000010000
Q88844403A	林榮泰	2003-03-20 19:38:27.0	台中榮民總醫院	test123	劉28	嘉義榮民醫院	20030313000000010000

圖16 查閱記錄

四、實施方法及進行步驟：請詳細說明實施本年度計畫所採用之方法及步驟，試辦計畫應詳細說明試辦設計、資料收集及分析方法。

本計畫將配合衛生署階段推廣的策略，由衛生署選定參與推廣醫療院所，這些院所需建立各自的電子病歷資料庫；而電子病歷索引中心，在本推廣階段將採集中式方式，下一階段再視推廣情形考慮分散式架構及實施中小型院所病歷託管機制。

（一）計畫之實施方法

1. 參與推廣院所建立電子病歷資料庫：

電子病歷資料庫的主要功能是儲存醫療院所下載之電子病歷，其存放內容包括所有至醫院就診病患之基本資料、診斷、用藥記錄以及各類檢查報告。有關本伺服器的儲存內容及格式，除考慮現行醫療資訊系統看診作業的需求之外，最主要將參考 HL7 標準所傳送的內容來訂定。

除了電子病歷資料庫的儲存格式以外，關於電子病歷資料庫內容更新的部份，因電子病歷伺服器係提供給遠端的醫療院所查詢之用，是以只需於每日離峰時間將病歷由 HIS 批次下載進來即可，接著將該日有異動的病歷資料索引(index)經 SSL 加密協定上傳至電子病歷索引中心的電子病歷索引伺服器，供欲調閱病歷者索引之用。

此外，為防止病歷遭到竄改，本計畫將對每一份報告文件(如：住院摘要、檢驗報告、門診病歷…)分別做一份電子簽章，並將報告文件的索引與其所對應的電子簽章經 SSL 加密協定傳送至電子病歷索引中心存證，儲存於電子病歷索引中心的電子病歷索引資料庫中，以方便日後若對電子病歷存有疑議時，可比對資料之用。

本計畫之電子病歷伺服器系統，可沿用上一期計畫之成果，直接推廣至各參與本計畫之醫院使用。由於本期計畫參與的醫院數增加許多，

對系統的反應速度及操作效率部份，需視上線情形配合衛生署及各院的網路及軟硬體設備設定，做進一步的效能調校，以期整體運作能夠順暢。

考量病患的就醫習慣，及相同體系之轉診轉檢作業較為頻繁，所以建議以相同體系之考量逐步推廣，同體系醫院的推廣，透過電子病歷資料的分享，可加強醫院的垂直分工合作，另外以體系的推廣，不侷限於地理區域，其示範效果較大，參與推廣的醫院可作為後續階段的示範醫院，屆時可就近協助後續參與的醫院，以降低整體推廣成本。

實際推廣對象將請衛生署指定，並協調各院配合辦理。

2. 建立電子病歷索引中心

電子病歷索引中心的功能有二：(1)每天將來自各醫療院所上傳的電子病歷索引資料更新至電子病歷索引資料庫，以備各醫療院所醫事人員查詢患者電子病歷的索引。(2)若醫事人員對所取得電子病歷內容的正確性存疑，可透過電子病歷索引中心保存的電子簽章來確認電子病歷是否無誤。

基於電子病歷索引中心需能確認電子病歷是否正確無誤，因此，索引中心需由具公信力的機構擔任，本計畫僅建立電子病歷索引伺服器，並實作出上述兩項功能。

在電子病歷索引資料的儲存上，電子病歷索引伺服器僅提供新增(insert)功能，若已上傳的電子病歷索引資料須變更，為了防止電子病歷被不當竄改，本計畫採新增異動的機制，保留每筆被修改資料，並加註修改時間、日期及修改人…等資料，做為日後求證之參考，索引中心的資料欄位請參考附表一。

架構安全的網路環境 [26]：

一個基本安全的網路環境，包括使用者政策、防火牆、入侵偵測系統（Intrusion Detection System - IDS）、路由器安全、主機系統安全、稽核、及緊急應變計劃。

雖然防毒軟體與防火牆在許多企業已經十分普遍，但駭客可以獲得的情報與資源也增加，這也讓他們可繞過防護機制並存取有價值的企業資產。因此，今日複雜的威脅需要額外層級的安全，例如：入侵偵測系統。入侵偵測系統(IDS)是防火牆技術的輔助解決方案。

防火牆可以控制進出電腦的流量。然而，假使不想要的通訊流量穿過防火牆並試著利用合法應用程式內的安全漏洞，並逃過防毒軟體的掃描；則威脅仍然存在。有了入侵偵測就可以藉由檢查網際網路通訊流量中是否有惡意程式碼與攻擊來使企業獲得多一層的保護。入侵偵測元件會根據它們的特徵以辨識入侵行為，然後自動的做出適當的回應，可終止網際網路連線並防範進一步的存取。

例如，攻擊者可能撰寫出可以深入網路任何部分的新威脅，而且甚至可以進已經安裝並執行個人防火牆與防毒軟體的電腦。如 Code Red、Nimda 般的混合式威脅，仍然可以透過允許的網際網路應用程式來繞過防火牆，例如網路瀏覽器或 IIS (Internet Information Server)，而且因為許多混合式威脅不會在電腦的硬碟上執行，所以它們不會被防毒程式所發現。

建置入侵偵測可以讓潛在的入侵者無所遁形。不過，它無法取代防火牆或防毒程式，因為入侵偵測必須與這兩種技術協力合作。當這三種安全技術整合在一起時，它們可以說是安全的鐵三角，是電腦與網路協同運作的屏障。

網路型(NETWORK-BASED)

網路型入侵偵測系統(NIDS) 使用不區分模式的網路卡，以擷取並分析每一個經過的網路封包。每個偵測器只會檢查連接之網段所傳送的封包，因此可保護多個連到該網段的主機。企業必須在重要網段或在交換器等可以檢查所有子網路封包的周邊裝置部署偵測器，以進行監測。典型的

網路型 IDS 是由一個或多個可執行本機分析與回報攻擊資訊到集中式主控台的偵測器所組成。

主機型(HOST-BASED)

這種系統的軟體必須直接載入主機並加以監控。當部署在主機時，此軟體會監測系統檔案、程序與日誌檔中是否有可疑的活動。另外，某些主機型的 IDS 會監測使用者權限是否有改變。內部網路攻擊者常使用的手法為：取得最高權限或設定新使用者帳號。偵測這種在重要伺服器上的濫用是很重要的，且必須直接在主機上監測。因此專家建議大型網路應將主機型與網路型偵測結合使用。瞭解網路上的高風險區是成功部署網路型與主機型入侵偵測的重要關鍵。

混合型入侵偵測系統（Hybrid IDS）：

結合主機型與網路型技術，混合型的 IDS 以系統為基礎，並可識別流向或來自該單一主機網路封包上的攻擊。混合型的系統不像網路型 IDS，它不會檢查每一個經過的封包，所以它減緩了某些因為流量分析而造成的效能降低問題。混合式的 IDS 藉由監控系統的事件、資料、目錄及登錄檔中的攻擊行為，以提供更多的防護。平台的限制與部署問題仍是一個爭議，且它們傳統上在會耗費相當的系統資源，但是較之於網路型的 IDS，它們較不易發生誤報的情形。

HONEY POTS

honey pot 安裝在重要的網路上，是專為引誘潛在駭客而設計，以使他們遠離其他網路上重要的系統；當此區域有未經授權的活動時，系統管理員會被警示。 Honey pot 應被部署在整個企業與財務單位中，並與網路型與主機型 IDS 協同運作。Honey pot 可偵測到慢速掃描(當其他 IDS 無法做到時)使它可以作為一種輔助性的解決方案。

企業不應只依賴統計值來了解他們內部的威脅，內部網路也可以發生惡意的攻擊。內部人員是最危險的，因為他或她知道安全政策與企業的弱點在哪裡。如果企業依賴統計值來了解這種威脅的嚴重性，則他們必須承擔的風險會很高。相反的，將 honey pot 部署在整個企業中，可產生證據，

以協助管理人員瞭解內部人員未經授權的使用狀況。透過這個系統偵測濫用的證據，協助累積額外的安全。

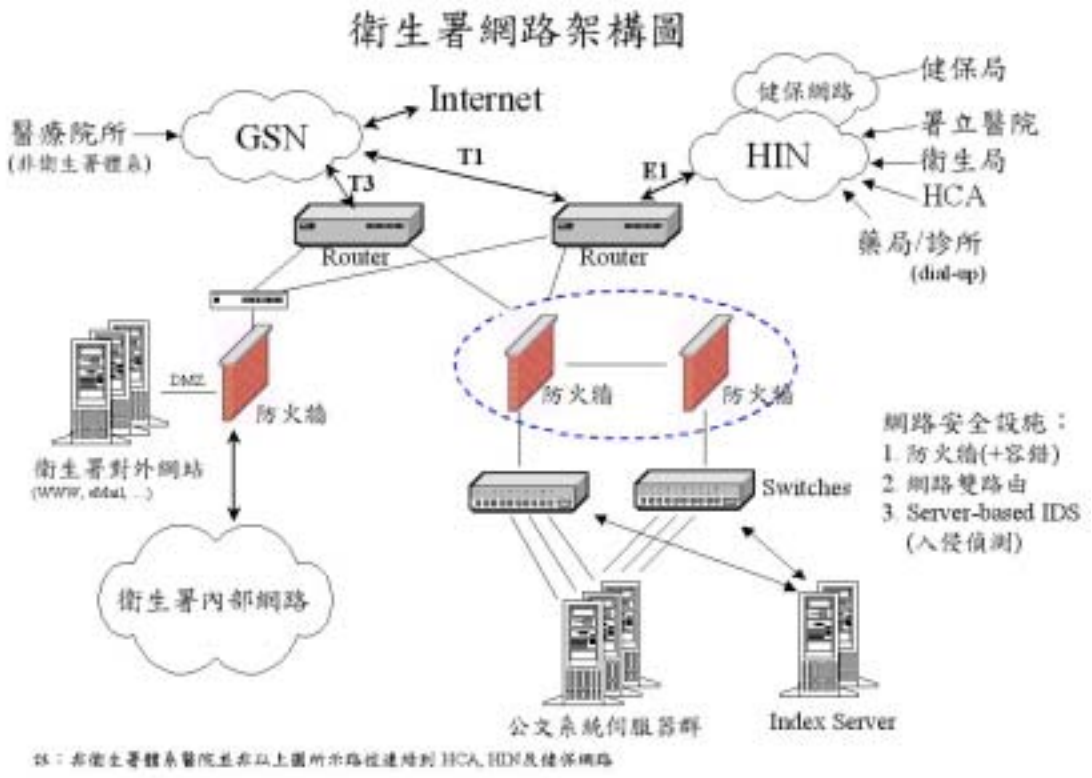


圖 17　衛生署電子病歷索引中心網路環境

資料庫的保護措施：

對於資料的保護，如同任何其他電腦機房資料庫運作，索引中心資料庫的保護應包括下列各項，但此處僅針對最後兩項稍作說明：

(1). 備份與復原（Backup and Recovery）

(2). 快照（Snapshots）抄寫

(3). 使用磁碟陣列（RAID）

(4). 遠端資料複寫（Remote Data Mirroring）

(5). 資料庫複製（DataBase Replication）等

點對點遠端資料複寫（Peer-to-Peer Remote Copy - PPRC）是用來提供在不同的兩地儲存子系統間同步的資料鏡映（synchronous data mirroring），它是一個即時的硬體功能，資料在兩地間總是保持正確的同步，並且與任何作業系統無關，儲存子系統間必須以 ESCON 或 FICON 光纖連接。

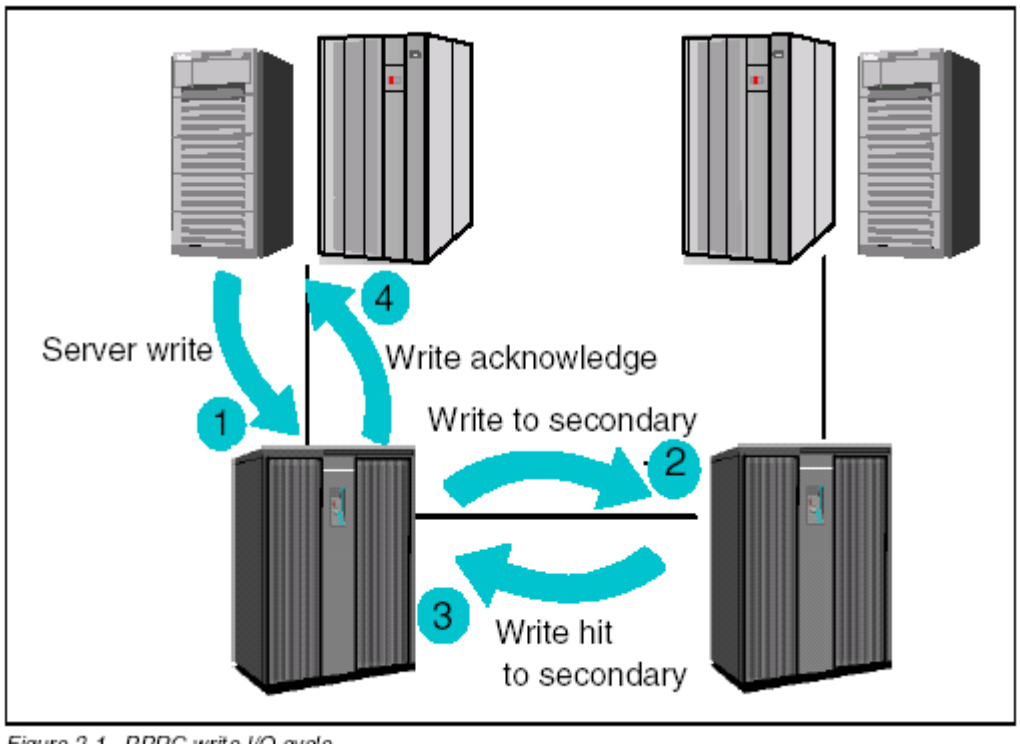


圖 18　Peer-to-Peer Remote Copy [8]

上圖說明：

1. The host server requests a write I/O to the primary ESS. The write is staged through cache and non-volatile storage (NVS).
2. PPRC dispatches the write over an ESCON channel to the secondary ESS. The write hits the secondary ESS's cache and NVS, and instigates a remote write hit.
3. The primary then expects acknowledgment of the remote write. If the secondary write fails, the acknowledgement does not return to the host server and is eventually "aged" from NVS, causing an I/O time-out to the host server, which in turn causes a retry from the host server.
4. The write returns to the host server's application.

- 資料庫複製（database replication）是一種程序，將資料庫物件（如資料庫表）複寫及維護到多個資料庫系統，這些資料庫們構成一個分散試資料庫系統；資料應用在一處的改變先於本地端被捕獲並儲存，之後再推進並應用到每一個遠端系統。複製使用分散式資料庫的技術以達到在許多個地點間分享資料，但是複製資料庫與分散式資料庫是不一樣；一個分散式資料庫，資料在許多的位置是可用的，但是一個特定的資料表僅僅存在於一個位置；例如在一個包括 DB1、DB2 及 DB3 分散式資料庫系統，EMP 資料表只能存在於 DB1 資料庫。複製意指相同的資料在多個地點可使用的，例如 EMP 資料表可能在 DB1、DB2 及 DB3 均是可用的。複製能提供應用程式效益是純粹分散式資料庫的環境無法辦到的，最普遍地應用在提升應用程式效能及保護應用程式的可用性是非常有用的，因為存在著替代的資料存取選項；例如一個應用程式正常情形是使用本地端資料庫而不使用遠端伺服器以減低網路交通流量並達到最大效能 ，而當本地端伺服器經歷失敗時，其他有複製資料的伺服器仍是可存取的。複製通常會遇到衝突情形，因此需要有衝突解決（Conflict Resolution）的策略。

3. 資料量預估及設備建議

各醫療院所醫療服務量及預估筆數, 如下表。其中, 每人次之門診、急診、住院之平均文件筆數，係參考臺中榮民總醫院近三個月的統計結果，平均住院病患每人次 28 筆、門診 3 筆、急診 13 筆，而平均每筆索引資料 0.5KB(儲存於電子病歷索引中心)，平均每筆文件資料 3.0KB(儲存於各院電子病歷伺服器)。底下以署立醫院、榮民醫院、慈濟醫院體系醫院資料量為例估計(實際推廣對象將請衛生署指定)：

	門診(人次)	急診(人次)	住院(人次)	資料筆數
署立醫院(30 家)	22,697	1,465	800	109,536

榮民醫院(15 家)	20,001		630	77,643
慈濟醫院(4 家)	4,400		150	17,400
合計	47,098	1,465	1,580	204,579

電子病歷索引中心之索引資料庫資料量預估

	資料容量			資料筆數
	每日(MB)	每年(GB)	七年(GB)	每日
署立醫院(30 家)	55	20	140	109,536
榮民醫院(15 家)	39	14.2	100	77,643
慈濟醫院(4 家)	9	3.2	22	17,400
合計	103	37.4	262	204,579

電子病歷索引中心之索引資料庫，預估能儲存 1.5 年本階段試辦醫院之索引量，所需的設備建議為：

作業平台	資料庫	CPU	時鐘速度	記憶體	系統硬碟容量	資料庫硬碟容量及規格
UNIX	ORACLE	RISC, 至少 64-bit, 至少支援 4 顆 SMP	至少 1000MHz	至少 2GB	至少 36GB	至少 40GB/年 *1.5 年+40GB DiskArray (Raid 5)=100GB

各院的電子病歷伺服器規格的將視其資料料而異。其預估方式，以下以台中榮民總醫院之資料量預估方式供參考：

門診：5000 人次/日 * 3 筆/人次 = 15000 筆/日

住院： 145 人次/日 * 28 筆/人次 = 4060 筆/日

急診： 120 人次/日 * 13 筆/人次 = 1560 筆/日

合計: (每日) 約 21,000 筆/日

(每年) 約 7,665,000 筆/年

電子病歷資料庫需要容量

每日 21000 筆 * 3 KB/筆 = 63 MB

每年 7665000 筆 * 3 KB/筆 = 23 GB

電子病歷資料庫預估所需的設備建議為：

圖 19　推廣計畫設備規格建議

另以某署立醫院之資料量預估方式供參考：

門診： 737 人次/日 * 3 筆/人次 = 2211 筆/日

住院： 20 人次/日 * 28 筆/人次 = 560 筆/日

急診： 44 人次/日 * 13 筆/人次 = 572 筆/日

合計: (每日) 約 3,343 筆/日

(每年) 約 1,220,195 筆/年

電子病歷資料庫

每日 3343 筆 * 3 KB/筆 = 10 MB

每年 1220195 筆 * 3 KB/筆 = 3.5 GB

4. 病歷查詢環境建置

使用者(醫師)欲使用本系統查詢各院的電子病歷資料，需具備以下的條件：

- PC 設備
- 瀏覽器(Microsoft Internet Explorer 4.0 以上)
- 可連結 Internet 的網路環境
- 健保 IC 卡讀卡機(可驗證之環境)
- 持有有效之醫事人員卡及健保 IC 卡

本系統查詢功能採 Web-Based 作業方式，故只需知道網路伺服器網址即可使用程式，不需事前申請或系統安裝工作。其主要目的即在考量能便於全國推廣。

5. 病歷資料庫委託代管機制

由於推廣至全國的應用，目前各試辦醫院皆須備有電子病歷資料庫，將形成中小醫院未來參與本計畫上阻礙。故計畫將九十一年度的執行架構加以擴充，增加病歷資料庫委託代管機制。至於中小醫院的實際病歷資料可託管的對象，可包括下列幾種可能做法：

- 委託由同體系之大型醫院代管
- 委託由政府單位代管：衛生機關、健保局、…
- 數家聯盟院所聯合建置，委由其中一家醫院(或廠商)代管

針對小型醫療院所及基層診所，可將電子病歷資料委託其他單位代管，可降低整體投資成本。當電子病歷資料庫為醫院自有的情形下，因為考量醫院資訊系統(HIS)與電子病歷資料庫皆位於院內安全信任下的網路環境，所以在 HIS 送出資料時未考量 SSL 的設計，且文件簽證動作在電子病歷資料庫進行，以簡化與系統整體的複雜度及成本。

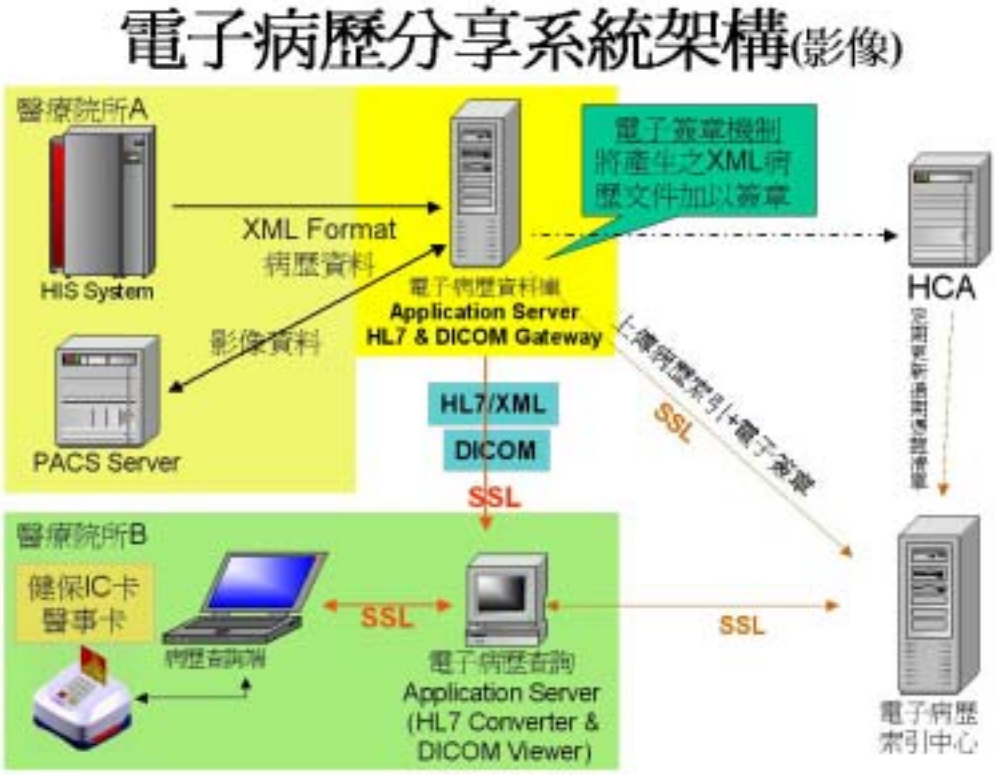
相對地，若電子病歷資料庫屬委託代管性質，則 HIS 送出資料時需考量 SSL 的設計，且文件簽證動作必須在送達電子病歷資料庫前即完成。為了簡化 HIS 的資料匯出動作，我們在 HIS 端，預計多設計一個 Gateway 模組，提供 SSL 連線及文件簽章/傳送等功能。

6、加入醫學影像資料交換

由於醫學影像檔案實在太大，本院於試辦計畫時並未將其資料納入，主要考量影像在網路上傳輸時需要較久的時間，查詢者是否能接受；但是本院所提電子病歷索引中心的架構是非常有彈性，欲在索引中心加入影像資料，於附表 1，2 資料庫 Schema 中，Document type 欄位的值使用”DI”，Content type 欄位的值使用 ”Image” 來表示。

由於儲存影像所需的容量會非常龐大，所以本計畫建議在電子病歷資料庫上並不會複製一份影像，而只記錄原影像的來源及影像 ID。影像只保留在原 PACS 伺服器中。當外面的電子病歷查詢伺服器提出查詢要求，經過電子病歷索引中心的驗證及加簽後，會送到電子病歷資料庫提取影像。此時，電子病歷資料庫將轉向原 PACS 伺服器讀取影像。電子病歷資料庫對外送出電子病歷資料時，將遵循 HL7/XML/CDA(文件型資料)及 DICOM(影像資料)等標準通訊協定。當電子病歷查詢伺服器收到 DICOM 影像資料時, 將以 Browser-Based 的 DICOM Viewer 供查詢者瀏覽影像；也就是說，查詢者端不需自備或先行安裝影像處理軟體。

由於計畫時程限制，本階段推廣將暫不包括影像病歷功能。



（二） 計畫進行步驟

1. 請衛生署儘速選定參與本計畫推廣醫療院所：
2. 舉辦專家諮詢會議，制定下列規範：
   (1). 明確訂定電子病歷應包含範圍 – 如各種同意書（住院同意書、手術同意書），各種病歷記錄（住院摘要、病程記錄、手術記錄、出院摘要、轉科摘要、門診 SOAP），各種檢驗檢查報告，會診報告、過敏記錄（如圖 21）、預防注射施打記錄、過去手術記錄等。

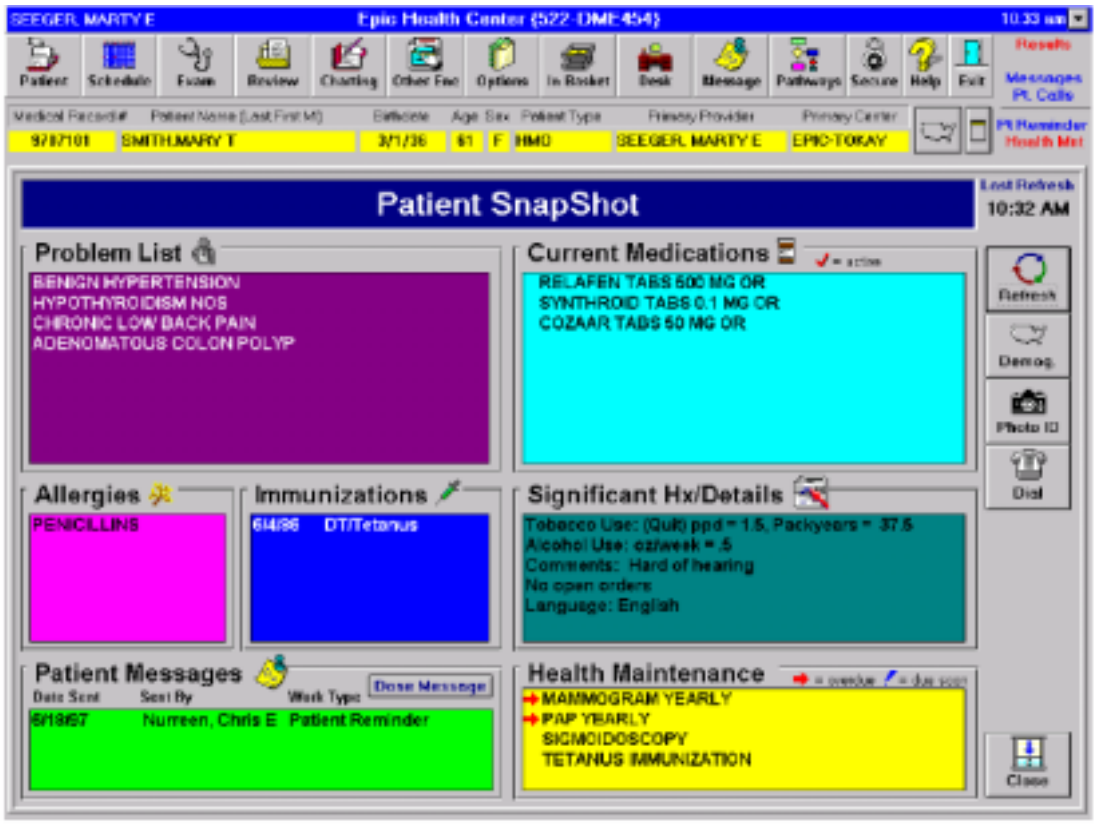


圖 21　病人資料的整體鳥瞰［Paul C. Tang 1991］

(2). XML 電子病歷標準 – 針對前項的各種病歷，訂定通用 XML 之 DTD 或 Schema 標準

(3). 病歷文件大小的分割 – 以一次門診為例，主要病歷可能包括門診 SOAP、門診處方及治療處理、各種檢驗檢查報告、診斷證明書等；電子病歷文件大小，是以一次門診所有病歷資料整合成一份文件，或由各醫院按作業方便性而定

(4). 電子簽章使用憑證– 目前 HCA 發給的憑證有兩種，醫事機構憑證及醫事人員憑證，本院於試辦計畫時是採用醫事機構憑證。採用醫事機構憑證有二種模式，一種是以醫事機構卡在電子病歷資料庫伺服器旁裝置卡機設備作簽章動作，另外一種是採用 HCA 發放之 AP 憑證簽章，基於運作速度考量，於試辦計畫時是使用醫事機構 AP 憑證。

(5). 電子簽章及上傳時機 - 本院於試辦計畫時，是採批次方式對

電子病歷簽章，醫院每天將完成的病歷轉成 XML 格式，存放電子病歷資料庫內；再批次從電子病歷資料庫內，篩選仍未簽章的病歷，逐一完成簽章後，寫回電子病歷資料庫，並將索引及簽章上傳。

(6). 電子病歷查詢權限 - 對於電子病歷資料的查詢權限，是否於電子病歷索引資料庫設定限制性資料，可針對醫師的科別或等級加以區分可查看的病歷，考量隱私權與醫療資訊完整性等相關議題，應請專家建議管理規範。

附表 1：擬藉由舉辦專家諮詢會議討論之議題的優先順序

優先順序	討論之議題	時程與場次
第一優先	電子病歷應包括那些內容 電子病歷文件大小分割 電子病歷查詢條件及展現方式	92/08 ~ 92/10 三場次
	電子病歷簽章使用憑證及簽章時機	92/10 二場次
	各種病歷內容通用 XML DTD /Schema 參考 HL7 CDA 標準	92/09 ~ 92/11 四~五場次
第二優先	以健保 IC 卡作為病歷查詢用途	參考備註 1
	查詢權限	
	病患隱私與公共利益平衡	
	敏感性資料應包括那些	
第三優先	新舊病歷應採 Append / Replace 時機	九十三年度
	是否提供研究用途查詢	
	病歷委託代管辦法	

備註 1：與病患隱私有關之議題部分，建議轉由 貴署委託資策會之「確立及推廣醫療資訊安全與隱私保護之政策」計畫研議

3. 建置電子病歷索引中心

電子病歷索引中心之系統可採用前期計畫的開發成果，安裝於衛生署所提供的主機系統上運行。除正式系統之外，建議亦應同時架設一套測試系統，供各醫院連結測試使用。同時，伺服器應配合衛生署所指定之機房的網管及備份作業中。

此外，本年度應持續做系統調校及程式維護更新工作，重點包括：

- 執行效能調校：包括各院索引及簽章的上傳效能，以及索引檢索的效能調校工作。
- 加強系統管理者功能及操作界面的開發，包括：錯誤主動警示、錯誤記錄/使用記錄檢視及追蹤、各類統計報表。
- 加強錯誤記錄的監控，以及程式系統除錯。

4. 協助醫療院所電子病歷資料庫建置

針對衛生署指定推廣對象，本計畫將提供電子病歷資料庫系統給試辦醫院安裝，並協助其建置作業。

(1) 舉辦系統推廣說明會：預計 1~3 場

(2) 建置電子病歷資料庫伺服器

為各醫療院所應具備一電子病歷資料庫主機，其設備需求將因院所每日業務量及單筆 XML 病歷資料量而有不同，應個案評估。並且需具備網路連線環境，固定 IP 方式。各院亦需配合處理網路防火牆之設定工作。

另外，在前期計畫中電子病歷資料庫係採 Java 標準平臺及 Oracle 資料庫。為能配合各醫療院所之資訊管理需求，我們計畫將本系統在不同的作業系統環境及資料庫系統上整合測試，預計將支援 Unix 及 Microsoft OS 環境，及 Oracle、SQL、db2 等資料庫系統。

(3) 病歷資料轉置 XML 格式

各醫療院所需將現有醫療資訊系統中已產生的病歷資料，以批次作業方式，將每日已完成的病歷，轉成 XML 格式的資料，連同索引資料存入電子病歷資料庫之待處理資料表中。XML 的格式並無一定的規範，只需符合 XML 的標準格式，醫療院所可依各自的資料需求，製作 XML 資料，並且針對每一種 XML 資料格式，製作顯示的 XSL。此部份預計將由醫院協調，請該院原醫院資訊系統(HIS)廠商配合處理。

(4) 加強系統效能調校及管理者功能之開發

5. 舉辦成果發表會/使用說明會

當下述的準備工作完成時，本計畫將在全國舉辦 2~4 場的成果發表會/使用說明會，讓全國各醫療院所之醫師能瞭解本系統功能並使用本系統。

- 衛生署之電子病歷索引中心上線運作

- 參與試辦醫院之電子病歷資料庫上線運作
- (查詢端) 病歷查詢時需使用醫事人員卡及病患健保 IC 卡，所以需於推廣時已完成 IC 卡的相關發放程序。
- (查詢端) 全國各醫療院所需具備讀卡機的設備。

限於本年度計畫時程太緊，建議使用者意見的調查工作於下年度再行追蹤執行。

6. 需衛生署配合辦理事宜

(1) 請衛生署指定本階段實際推廣對象(醫療院所)，並協調各院所配合辦理本案。

(2) 主辦專家討論會及系統推廣說明會/成果發表會。

(3) 提供索引中心伺服器及資料庫主機設備

- 設備包括正式系統及測試系統，含作業系統、應用伺服器、資料庫系統使用權。
- 請指定索引中心架設地點(衛生署或健保局…)。
- 請指定配合人員協助系統架設：機房環境準備、網路設定、…、等工作。

(4) 各醫院電子病歷伺服器(及資料庫)主機部份，請提供經費、撥發設備提供、或協調由醫院自備。

(5) 提供 HCA 醫事卡及健保 IC 卡之程式庫，以及其開發(development-time)和執行(run-time)所需之使用權。

(6) 協辦使用者教育訓練。

五、重要參考文獻：依一般科學論文之參考文獻撰寫體例，列出所引用之參考文獻，並於計畫內容引用處標註之。

頁數限制：2 頁

1. ASTM E 2182-02，Standard Specification for Clinical XML DTDs in Healthcare
2. Dolin R, Alschuler L, Behlen F, Biron P, Boyer S, Essin D, Harding L, Lincoln T, Mattison J, Rishel W, Sokolowski R, Spinosa J, Williams J, ”HL7 Document Patient Record Architecture: an XML document architecture based on a shared information model”. Fall AMIA, November 1999.
3. Gloria Shobowale , “SGML , XML and the Document-Centered Approach to Electronic Medical Records “, Bulletin of the American Society for Informatics Science , October/November 1998
4. Grace I. Patersona, Michael Shepherdb, Xiaoli Wangb, Carolyn Wattersb, David Zitnera，”Using the XML-based Clinical Document Architecture for Exchange of Structured Discharge Summaries”，Proceedings of the 35th Hawaii International Conference on System Sciences – 2002
5. HL7 Version 2.3.1
6. HL7 Clinical Document Architecture Framework Release 2.0，Cleveland draft; April 23, 2003
7. *IBM DB2 Universal Database Replication Guide and Reference, Version 7, SC26-9920*.
8. IBM Redbook sg245757 ， ” IBM TotalStorage Enterprise Storage Server, Implementing Copy Services in an Open Environment”
9. Institute of Medicine Committee on Improving the Patient Record.” *The Computer-Based Patient-Record: An Essential Technology for Health Care “ (2nd Edition).* Washington DC: National Academy Press, 1997.
10. ISIS European XML/EDI Healthcare Pilot Project (XMLEPR)，July 07, 2000
11. Kona Editorial Group chartered by HL7 SGML/XML SIG，HL7 Document Patient Record Architecture DRAFT - September 4, 1998
12. Liora Alschuler 等，The Kona Proposal - electronic healthcare records，Jul 1997；
13. Michael R. McGuire，”Automation of the Patient Medical Record: Steps Toward

a Universal Patient Record" , Edition 2p, December 12, 2001

14. Oracle9*i* Database Concepts Release 2 (9.2)，Part Number A96524-01
15. Paul C. Tang and Clement J. McDonald ,"Computer-Based Patient-Record Systems"，Chapter 9 of "Medical Informatics：Computer Applications in Health Care and Biomedicine"，Springer
16. Wu, T-C., Lee, S-K., Peng, C-H., Wen, C-H., and Huang, S-K.: An Economic PC-Based Picture Archiving and Communication System. RadioGraphics 19:523-530,1999.
17. 台中榮總，「一個快速且安全的電子病歷分享模式」，行政院衛生署九十一年度醫療院所病歷電子化試辦計畫書，2002
18. 行政院衛生署，醫療機構實施電子病歷作業要點〈草案〉，91/08/28
19. 行政院衛生署，設置及營運「醫療憑證管理中心」實施計畫書，中華民國 91 年 2 月
20. 黃章銘，溫嘉憲，黃興進，Extranet 在轉診之應用—以臺中榮總為例，醫療資訊雜誌第九期:19-38，民國 88/6。
21. 溫嘉憲、彭振興、姜文忠，電子轉診作業模式的建立，行政院衛生署「二代全國醫療資訊網計畫」，民國 90/03
22. 簡文山、李友專、唐大鈿、胡俊弘，建立臺灣醫療資訊交換中心之藍圖，醫療資訊雜誌第六期:54-66，民國 86/12。
23. 電腦處理個人資料保護法 ，中華民國八十四年八月十一日華總義字第五九六○號令公布
24. 電腦處理個人資料保護法施行細則，中華民國八十五年五月一日法務部法令字第一０二五九號令公布
25. 電子簽章法，中華民國 90.11.14 總統府公告，中華民國 910401 生效
26. 台灣賽門鐵客，"如何架構安全的網路"，2003 文章，參考網址：http://www.symantec.com/region/tw/enterprise/article/secure_network_structuring.html

本計畫預定進度：以 Gantt Chart 表示本年度之執行進度。

九十二年度預定進度：以 Gantt Chart 表示本年度之執行進度

月　份 工作項目	九十二年度					
	7 月	8 月	9 月	10 月	11 月	12 月
舉辦專家諮詢會議制定相關規範						
系統分析、設計及實做						
衛生署電子病歷索引中心測試環境安裝就緒						
衛生署電子病歷索引中心正式環境安裝就緒						
電子病歷索引中心推廣試行作業上線						
由衛生署溝通協調參與推廣之醫療院所						
參與推廣醫院測試環境設備安裝						
參與推廣醫療院所進行 HIS 資料轉換程式撰寫、電子簽章及上傳						
參與推廣醫院正式系統設備安裝						
參與推廣醫院整合測試						

九十三年度預定進度：以 Gantt Chart 表示本年度之執行進度。

月　份 工作項目	九十三年											
	01 月	02 月	03 月	04 月	05 月	06 月	07 月	08 月	09 月	10 月	11 月	12 月
舉辦專家諮詢會議制定相關規範												
電子病歷索引中心儲存醫學影像之索引規劃												
以瀏覽器瀏覽醫學影像軟體設計												
醫學影像電子簽章及索引上傳												
醫學影像交換分享測試												
衛生署指定本年度參與推廣之醫療院所												
舉辦參與推廣醫療院所說明會												
參與推廣醫院測試環境設備安裝就緒												
參與推廣醫療院所進行 HIS 資料轉換程式撰寫、電子簽章及上傳												
整合測試 /使用者教育訓練												
系統效能調校、程式維護												