以角色為基礎之醫療憑證安全機制

林廷憲[ac]　　劉立[ab]

臺北醫學大學醫學資訊研究所[a]
臺北醫學大學附設醫院副院長[b]
財團法人國泰綜合醫院[c]
E-mail：lin@cgh.org.tw

摘要

電子病歷系統中之各種資料，在產生、撰寫報告以及傳送的過程中，若產生有意或無意的篡改，以致於造成醫療糾紛，將違背電子病歷的美意。目前大家都重視電子病歷（文件）的安全性，於是衛生署為了加強醫療資訊安全的防範措施，建立以公開金鑰為基礎的醫療電子認證機制與「醫療憑證管理中心」，並開始並推廣使用『醫事機構』及『醫事人員』憑證IC卡，但對於電子病歷（文件）的制作或產生過程中，由誰來制作或是誰有權制作？這個角色卻少有人討論。因此本文將醫療憑證角色配合PKI融入放射線科作業流程中來探討其安全控管與重要性。

關鍵字：電子病歷、PKI、HCA、PACS、RIS、DICOM

前言

近年來，拜電腦軟、硬體與通信技術日趨成熟之便，資訊技術普遍應用於醫療上，並對醫療過程產生莫大的影響。醫療資訊系統(Healthcare Information Systems)不斷進步，各種臨床資訊之數位化程度與日俱增，對於病患就醫品質之提昇功不可沒。

醫療資訊系統除了傳統資訊系統的任務之外，另一個重要的任務即是電子病歷。所謂病歷乃是醫療人員執行醫療業務的過程中所為的各項診察、診斷及治療等所製作有關於醫療處置之記錄。而以電子文件方式製作、保存之病歷即稱電子病歷。電子病歷優於傳統手寫病歷（紙本病歷）是它可促進醫療資訊通暢，避免重覆性的檢驗，減少醫療資源浪費；提供完整的資料庫資源，增進醫學研究的發展；為使醫師提高診療之效率，彙整相關資訊如檢查值及報告結果，減少不必要之病歷書寫時間提升醫師對病患之醫療記錄品質的效率與正確性，透過網路及電子化病歷的搜尋及排序，醫療人員依據詳實資料，更精準的診斷，提高醫療品質；藉電腦之自動檢視與監控病患之相關資料，減少病歷存放空間，減少人工作業之錯誤並降低各項醫療成本，提升管理績效。

然而，電子病歷系統中之各種資料，在產生、撰寫報告以及傳送的過程中，若產生有意或無意的篡改，以致於造成醫療糾紛，將違背電子病歷的美意；就法律的層面而言，醫療機構實施電子病歷作業要點明訂以電子文件方式製作、保存之病歷（簡稱電子病歷），應經由行政院衛生署醫療憑證管理中心簽發憑證之醫事人員卡或醫事機構卡製作，並符合相關規定，得全部或部分免以書面方式製作，因此憑證應用之導入乃是電子病歷實施之關鍵。

文獻探討

在「建立台灣醫療資訊交換中心之藍圖」一文中[1]，將電子病歷資料的建構分為三階段：第一階段為文數字性的檢驗報告，第二階段為影像性的檢驗報告，第三階段為醫師的診斷及用藥，並建議使用HL7及DICOM為資料交換的標準。在「醫療資訊化與醫療管理品質」[2]一文中，對慈濟綜合醫院所發展出的新醫療資訊系統加以介紹，其中談到電子病歷的建構，不但可改善紙本病歷記載的缺點與提供完整的教學研究資料，對於院際間的合作及整合有莫大的助益。黃章銘在榮民醫療資訊網計劃一文中，提及榮民醫療照護系統內電子病歷的建構。

隨著技術進步使醫療影像影像電子化的發展更快速，PACS系統所帶來的效益像是讓病患縮短等候時間、影像品質可調整、重照率降低、提高治療意願與時效、替遠距醫療及跨院區轉(會)診創造了便利性與

彈性等。相對的，在無片化環境中，各式醫療影像資訊傳送管理之安全性則是受到網際網路盛行伴隨著資訊安全屢遭挑戰。同年黃興進等人[3]也提出以識別碼、密碼、IC卡、申請書的審核、資料加密、資料交換的時間可追蹤等方式來解決。

衛生署為了加強醫療資訊安全的防範措施，建立以公開金鑰(Public Key Infrastructure, PKI)為基礎的醫療電子認證機制[4]，且已完成建置「醫療憑證管理中心」(Healthcare Certification Authority, HCA)，並開始並推廣使用『醫事機構』及『醫事人員』憑證 IC 卡，其主要目的除確實用來保障民眾就醫所產生的私密性或敏感性資料外，並確保醫療資訊電子化的作業安全與規劃電子病歷等相關醫療資訊化應用。

我們發現雖然大家已相當注重電子病歷（文件）的安全性，但是對於電子病歷（文件）的制作（或產生）過程中，是從具有醫療憑證中的誰來制作或是誰有權制作？這個角色目前卻少有人討論，站在權利與責任的立場而言，讓每個制作或使用的人都可以完全追蹤，以釐清應有的責任，這是醫療服務電子化中另一項重要的課題。

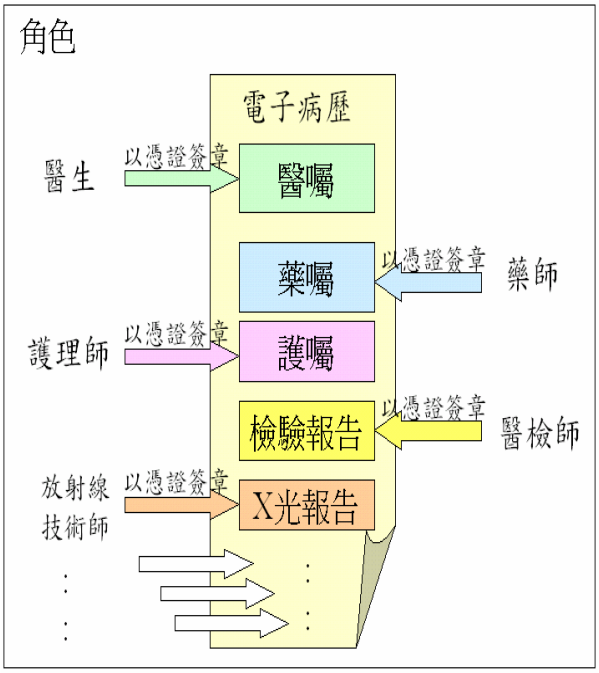
材料與方法

在醫療流程中導入醫療憑證時必須考慮各醫療人員之任務以決定病歷文件中簽章人員的角色類別，例如住院醫囑單即包含主治醫師、住院醫師與護士等角色，因此醫療憑證導入電子病歷時必須先將持有憑證之人員分類，依據各種電子病歷文件之需求，考量電子文件產生的時機與特性，決定應用憑證的種類與規劃簽署的角色類別與時機，並且透過PKI的安全機制期使醫療資訊在擷取、交換與儲存的過程中能確保安全。

本研究在探討以角色為基礎時醫療憑證的導入與安全認證機制如何運作。重要元件說明如下：

憑證種類：HCA 負責簽發醫療憑證，包括：醫事人員、醫事機構、伺服器應用軟體等三種用戶憑證。醫事機構憑證宛如醫療院所之關防，代表醫療機構法人之行為，醫事人員憑證如同個人印鑑，代表醫事人員個人行為，而其所謂醫事人員包括醫師、中醫師、牙醫師、藥師、醫事檢驗師、護理師、營養師、物理治療師、職能治療師、職能治療生、藥劑生、醫事檢驗生、護士、助產士、物理治療生等。[5]

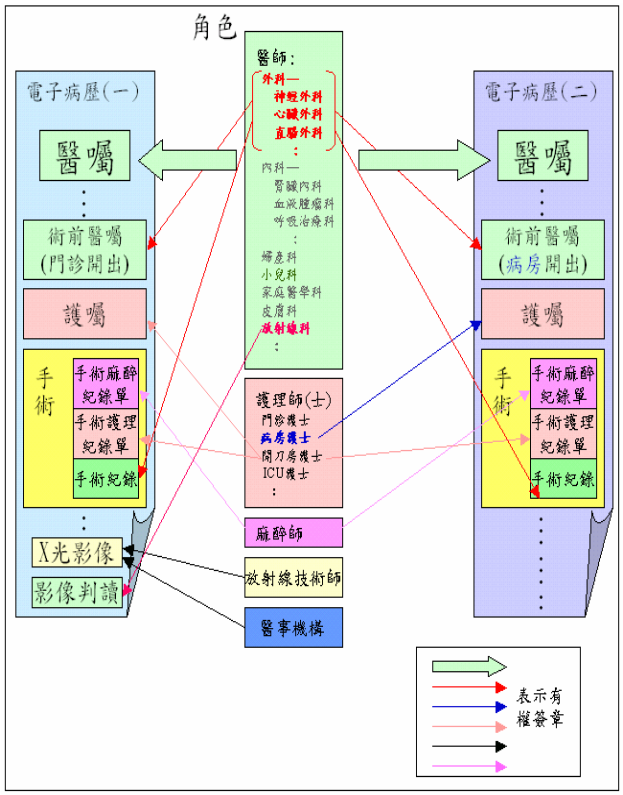
角色分類：在規劃流程導入的過程，以憑證種類與醫事人員之專業為角色，並規範各式醫囑、藥囑、護囑、檢驗報告及檢查等電子文件應該簽署的角色，如圖一所示，因此可以分為醫事機構、醫師(含西、中、牙醫師)、藥事人員(含藥師及藥劑生)、護產人員(含護理師、護士及助產士)、醫事檢驗人員(含醫事檢驗師、醫事檢驗生)及其他醫事人員(含醫用放射線技術師(士) 、鑲牙生、營養師、物理治療師(生)及職能治療師(生))等。其中醫療人員所作之醫療紀錄以其專業角色類別簽署，醫療儀器產生之資料以機構之角色簽署，當醫療記錄需要交付給病人或院外機構時，則視該文件屬於醫事人員個人行為或醫院行為決定應簽署之角色類別。



圖一、以角色的專業作分類

說明：一份電子病歷（文件）中，醫生的診斷與處方是屬醫囑部份，應由醫師完成醫囑後以其個人醫事人員 IC 卡產生電子簽章，並儲存於簽章伺服器之資料庫，以維持醫囑部分資料之完整與不可否認性，同理類推其他醫事人員。

然而，醫事人員只以其專業來劃分角色還不夠，我們認為應加上其從事的職務類別再做細分才行，如圖二所示



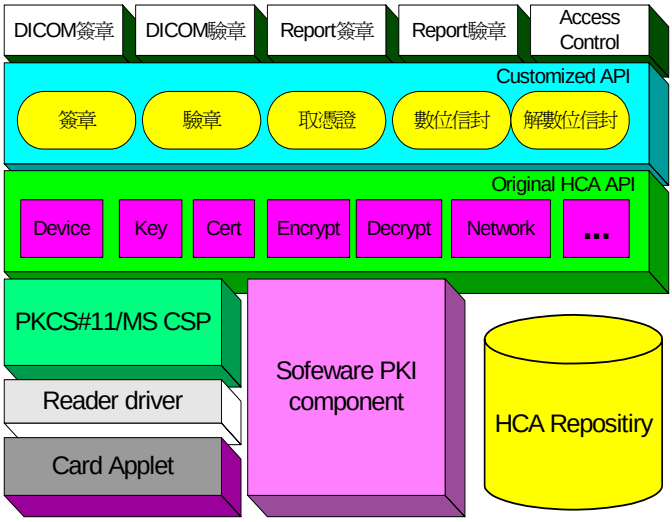
圖二、以角色的專業與職務作分類

以紙本病歷而言，一般醫生皆可開立醫囑，但像是術前醫囑基本上只有外科醫師才能開立，病房開出的術前醫囑由病房護士完成護囑，而門診開出的術前醫囑卻由開刀房護士完成護囑，另外像是 X 光的影像判讀須由放射線科的醫師做判讀與簽章，這些皆與其從事的職務類別有關，雖然法律上目前並未明文規定手術的醫囑只能由外科醫師開立，但是實際上依健保給付、依常理來說卻是如此。我們希望電子病歷也能有如此的機制以避免未來不必要的糾紛。

醫療影像PKI系統介面架構：公開金鑰基礎建設（Public Key Infrastructure，PKI）是以公開金鑰密碼學為基礎而衍生的架構，在電子訊息傳遞與交換過程中，PKI是唯一可以符合下列五項數位安全要求的機制：身分辨識（Authentication）、不可否認性（Non Repudiation）、資料完整性（Integrity）、資料隱密性（Private）及存取控制，為了符合這些安全需求， PKI 是一項非常有效的工具，提供在 Intranet、Extranet 及 Internet網路環境間交換資訊的信任基礎。

PKI包含了一支公開金鑰（Public Key）與一支私密金鑰（Private Key）；前者公諸於大眾，而後者由使用者獨自持有保管。這一對金鑰是具相對應關係的數位密碼，其中一把對訊息進行「加密」後，進行訊息傳輸，使傳輸過程中訊息不會落入他人之手而遭到破解或修改；另一支金鑰則作為「解密」用途，以獲得原始訊息內容。

由於大多數PACS系統並未提供憑證功能，為了不因導入 PKI 應用而影響 PACS 系統線上作業，以不變更現有 PACS 之架構為前題，可用外掛系統作業模式，進行系統之建置。而依據現有 PACS之 DICOM 影像與 RIS 檢查報告產出與查調作業程序導入 PKI 技術，相關服務共分為五大個服務元件，其於整體系統之相關位置圖如圖三所示



圖三、醫療影像PKI整體系統之相關位置圖

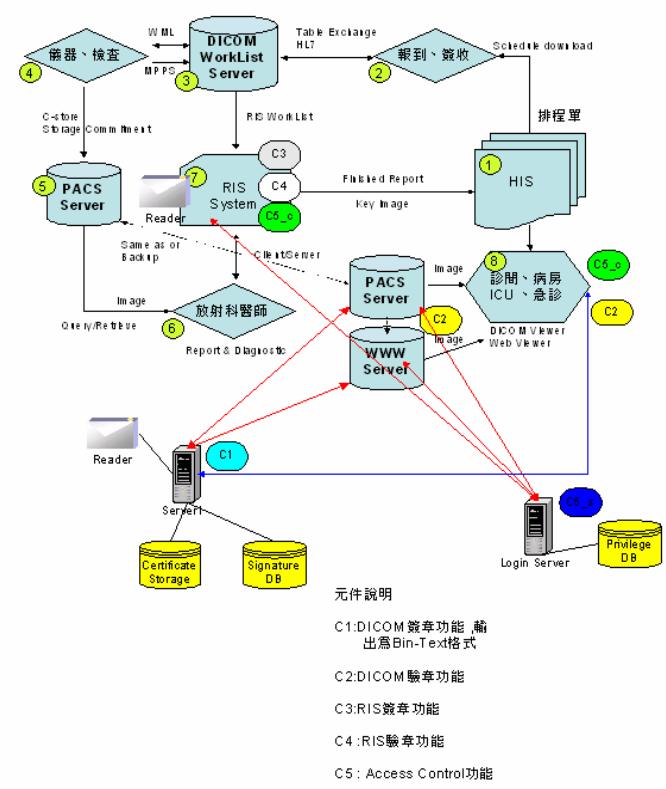
研究結果

醫療影像主要來自醫院放射部門，放射部門之資訊系統一般稱為放射科資訊系統(Radiology Information System, RIS)，RIS的功能包括放射科之報到、檢查排程、報告、管理統計的資訊系統，應用此套系統可縮短病患等侯的時間，且增進技術師和醫師之工作效率，檢查作業結合排班、醫師工作清單、報告等自動化系統。

醫療影像管理系統（Picture Archiving and Communication System, PACS）係指將各種醫療攝影裝備（Modality）攝得的影像數位化後儲存；並透過網路傳輸到各個終端機，使得診間、病房、開刀房、急診等，只要是有工作站的地方，皆可即時查詢就醫者影像，醫學影像儀器和軟體間，則使用DICOM（Digital Image Communication in Medicine）協定規

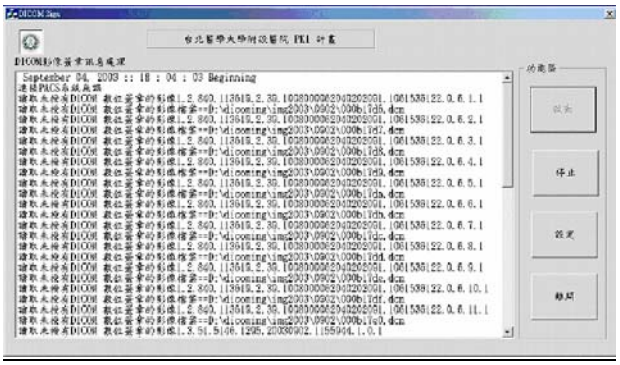
範。經由RIS結合HIS / PACS使得醫院的資訊作業流程更完整。

本研究將醫療憑證角色與PKI融入放射線科作業流程中，其架構如圖四所示。

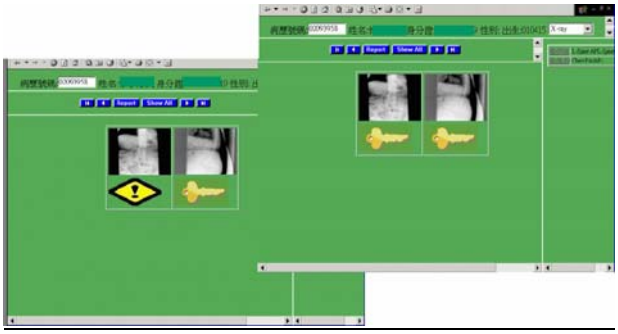


圖四 、放射線科作業流程架構圖

DICOM影像憑證角色與簽章產生作業：DICOM 影像由儀器端產生後，傳輸至 DICOM Server 儲存，其間 DICOM 影像之傳輸並未牽涉人工作業，因此DICOM影像之簽章作業由系統自動偵測影像檔案寫入時，立即使用醫事機構憑證產生數位簽章，儲存於簽章伺服器之資料庫，至於操作醫療儀器之醫用放射線技術師的憑證尚未發放，所以醫用放射線技術師之醫事人員角色憑證仍未使用，無法對操作人員作確認。未來如能整合並於儀器端送出影像或DICOM Server 接收影像時產生數位簽章，將更完善。(圖四之C1)



DICOM 影像驗證作業：輸入病人之 Patient ID之後，系統於顯示其所包含之 DICOM 影像小圖示時，自動進行影像簽章驗證作業，在影像調閱前於Server site驗一次，調閱後於Client site複驗一次，確保影像資料之安全。若比對結果不同時，可將有問題時之影像註記於小圖示下方，藉以提示使用者此張影像其資料完整性出問題。當使用者檢視完整 DICOM 影像內容時，系統另提供功能鍵，讓使用者可確認此DICOM影像之資料完整性，藉以防止網路傳輸時遭竄改資料之疑慮。（圖四之C2）



RIS 檢查報告憑證角色與簽章產生作業：當放射科醫師於檢查報告撰寫完成時，點選該筆檢驗報告，並於健保讀卡機插入其醫事人員憑證 IC 卡，輸入IC卡之PIN Code（ 每次插卡只需輸入一次 ），系統以其IC卡產生數位簽章後，並儲存於簽章伺服器之資料庫。（圖四之C3）

RIS 檢驗報告簽章驗證作業：調閱病人之 RIS 檢查報告時，輸入病人之 Patient ID，系統於顯示檢驗報告同時，自動進行報告資料完整性檢查，同樣在調閱前於Server site驗一次，調閱後於Client site複驗一次，針對報告資料完整性有問題者，先顯示提示訊息告知使用者此檢驗報告其資料完整性出問題，若檢驗報告資料完整性檢查正確，於使用者查調檢驗報告畫面，同時顯示此檢驗報告撰寫醫師之簽章圖示，以確

認檢驗報告之撰寫者之身份不可否認性。(圖四之C4)

使用者系統登錄之權限控管作業：為了應用醫事人員憑證 IC 卡作為系統登錄之身份鑑別機制，院內醫事人員當領到醫事人員憑證 IC 卡時，需進行憑證登錄作業，系統藉由登錄作業將醫事人員之原系統之使用者代號與憑證進行連結作業，並建立完整使用者權限控管資料庫，以作為系統登錄作業之身份認證基礎。(圖四之C5_s)

當醫事人員於憑證登錄作業完成後，進入系統時，將醫事人員憑證 IC 卡插入健保讀卡機，輸入IC 卡之 PIN Code ，系統即可以其 IC 卡產生身份辨識資料送至應用系統伺服器，由伺服器端驗證其憑證身份，並對應原先系統所設定之使用者代號與系統作業權限，完成系統登錄之權限控管機制。(圖四之C5_c)

結論

目前雖說大家很注重醫療憑證與PKI的結合與運用，但我們希望能更加注意到醫療憑證中之角色與電子病歷（文件）的關係－誰可查調？誰有權簽章？誰該負責？醫療記錄本身即具有高度的私密性(Privacy)，並且醫療記錄之著作權與所有權的歸屬原本就存在著相當複雜的關係，因此醫療資訊在擷取、交換與儲存的過程中就必須更加謹慎地掌握存取控制(Access control)及認證程序(Authentication)的嚴密性與完整性。完整的醫學資訊安全管理必須以醫療記錄為基礎，輔以醫療活動為導向之安全存取控制真正解決醫療記錄的安全存取控制。亦即透過以醫療記錄為基礎才能保證具有不可分割性的醫療資料群之存取控制，能夠具有完整性與一致性；輔以醫療活動為導向才能管控醫療記錄權限取得與失去的時機，避免權限釋放後未能回收之漏失。是故，在規劃醫療服務電子化中，對於醫療憑證角色能更嚴謹來看待以避免未來不必要的糾紛。

參考文獻

1、簡文山、李友專、唐大鈿、胡俊弘著（1997）：建立臺灣醫療資訊交換中心之藍圖。醫療資訊雜誌，中華民國醫療資訊學會出版，第六期，民國八十六年十二月。

2、林俊龍、張顯洋、陳玉寧著（1999）：醫療資訊化與醫療管理品質。醫療資訊雜誌，中華民國醫療資訊學會出版，第九期，民國八十八年六月，p83-92。

3、黃興進、彭振興、連俊瑋著（2000）：國內發展 PACS 之回顧與展望。國際醫學資訊研討會論文集（2000），p170-176。

4、行政院衛生署醫療憑證管理中心　網站 http://hca.doh.gov.tw/HCA/default.jsp

5、醫事人員人事條例（1999.7.15）：第三條「本條例所稱醫事人員，指依法領有專門職業證書之醫師、中醫師、牙醫師、藥師、醫事檢驗師、護理師、營養師、物理治療師、職能治療師、職能治療生、藥劑生、醫事檢驗生、護士、助產士、物理治療生及其他經中央衛生主管機關核發醫事專門職業證書並任前條職務之人員。」

6、林玉玲（2000）：我國電子病歷發展現況與趨勢的調查研究。國立台灣大學公共衛生學院醫療機構管理研究所碩士論文。