Regular Paper

Communications of the CCISA
Vol. 26 No. 3 Aug. 2020

電子化醫療資訊系統的安全策略與隱私權保障

許寬宏[1]、黃耀民[2]、吳鎮宇[3*]、陳澤雄[4]
[1]國立台灣大學附設醫院骨科部
[2]國立交通大學管理科學系
[3]國立澎湖科技大學資訊管理系
[4]東海大學資訊管理系
[3]zywu@gms.npu.edu.tw

摘要

網路發展經年，應用面向日漸繁複，相關技術也趨於多樣化，相對於醫療的應用，資訊技術的意義在於擴大醫療資訊的臨床輔助功能。數位化醫療所涵蓋的範圍，包括電子病歷、電子處方箋、醫療資訊系統等，各種相關系統的資料處理結構與格式的研究雖趨於成熟，但整合性不足，因此，本研究提出一個整合醫療資訊系統，使跨醫療院所之間的電子病歷交換可以安全的進行，並且透過密碼機制的設計，保障病患與醫師的隱私權，但也提供主管機關的查核追蹤機制。藉此，醫療資訊系統或可發展為全面性的功能，免除人工單據的傳遞，維持病患就醫資訊的安全性，因此可以降低、甚或免除後續護理、藥劑、技術人員等可能的人為失誤，不但可以改善醫療品質，同時也是醫務管理上不可或缺的基礎設施。

本系統達到下列相關功能：強化健保 IC 卡的功能及其與整合式醫療資訊系統的相容性、建置功能完整的電子處方箋系統及其與醫療資訊系統的整合、保障病患與醫師的隱私權，並且從架構的設計上，根本解決病患就診紀錄儲存方式，提供代領藥物的機制設計以及維護醫師與病患的隱私權。

關鍵字：電子醫療、電子病歷、電子處方箋、醫療資訊系統

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 26 No. 3 Aug. 2020

Security Policy and Privacy Protection of Electronic Medical Information System

Kuan-Hung Hsu[1], Yao-Ming Huang[2], Zhen-Yu Wu[3*], Tzer-Shyong Chen[4]
[1]Department of Orthopedic Surgery, National Taiwan University Hospital
[2]Department of Management Sciences, National Chiao Tung University
[3]Department of Information Management, National Penghu University of Science and Technology
[4]Department of Information Management, Tunghai University
[3]zywu@gms.npu.edu.tw

Abstract

With the development of the Internet, the application orientations have become complicated as well as the relevant technologies have become diverse. Contrary to the application of medical treatments, the significance of information technology is to expand the clinical supports in medical information. Digital medical treatments cover the areas of electronic patient records, electronic prescriptions, and medical information system. Furthermore, studies on the data processing structures and the formats in various relevant systems have become mature, but the integration is still insufficient. For this reason, this project proposes an integrative medical information system to securely exchange electronic patient records among medical organizations, to guarantee the privacies of patients and doctors with the design of passwords, and to provide authorities with verification and tracking mechanisms. By doing so, the medical information system can be developed with comprehensive functions to dispense the transfer of manual documents and maintain the security of medical information so that the possible human errors, such as the follow-up nursing, medical preparation, and technical staff, can be reduced or even avoided. Not only can it improve the medical quality, but it can also become one of the inevitable fundamental facilities in medical management.

This project aims to strengthen the functions of National Health Insurance IC card and the compatibility with the integrative medical information system, to establish a full-functional electronic prescription system and the integration with medical information system, and to guarantee the privacies of patients and doctors. From the architectural design, it further aims to solve the problem of storing patients' treatment records, provide the design of helping draw medicine mechanisms, and protect the privacies of doctors and patients.

Keywords: Electronic medical treatments, Electronic patient records, Electronic prescriptions, Medical information system

壹、緒論

網路發展經年，應用面向日漸繁複，相關技術也趨於多樣，日常生活數位化儼然已蔚為現代科技發展的一大趨勢，常見的電子商務、電子醫療、網路銀行、電子化政府、網路社群應用等，都屬於網路應用的成果。

相對於醫療的應用，資訊技術的意義在於擴大醫療資訊的臨床輔助功能，所涵蓋的技術面，包括健保 IC 卡裝置[6]、醫學應用中的數位憑證與簽章、電子病歷、電子處方箋等[11][24][27][28]。將資訊技術導入醫療系統的應用，在醫務管理上獲得明顯的績效，但醫療資訊系統的開發與維護成本，所費不眥，發展之初，只在大型醫學中心試行，例如台大醫院、榮民總醫院、長庚等，而且僅止於單向式的資訊饋入，而非互動式的資訊回饋，例如以內建的醫療專業知識協助醫療人員，提供教學、諮詢、輔助、警訊等功能。1995 年全民健保實施之後，為了因應變動頻繁的健保給付申報作業，加速醫療資訊應用普及於中小型醫療院所的趨勢。新穎且成熟的系統開發技術不斷產生，透過新技術的應用，開發程式更為迅速，更有彈性，也更易維護；在提供醫師直接操作的應用之後，醫療資訊系統發展為全面性的功能，不但可以免除人工單據的傳遞，使用者饋入的資訊可以獲得即時的更正，維持資料庫資訊的及時性，跳脫傳統批次處理作業中資訊更新的時間差問題，因此可以降低、甚或免除後續護理、藥劑、技術人員等可能的人為失誤。在改善醫療品質的同時，資訊系統也成為醫務管理上不可或缺的基礎設施之一。

健保 IC 卡與數位憑證的資料結構、電子病歷與電子處方箋的資料格式等研究成果，已相當成熟。至於跨醫療院所電子病歷格式的統整[7][25]、跨院所的安全病歷資訊交換協定[2][8][12]、遠端視訊醫療，以及照護人身分驗證機制等[10][16]，則仍有亟待突破的努力空間，這些都屬於跨醫療院所電子病歷格式交換協定及醫療資訊系統傳輸格式的研究。

醫療資訊系統的強化與整合，有助於醫療品質與效率的提升，其中功能與技術的整合，更是醫療資訊化是否得以落實的關鍵，茲就本研究說明如下。

其一，強化健保 IC 卡的功能及其與整合式醫療資訊系統的相容性。一般所使用的健保 IC 卡都以晶片卡為主，記憶體容量不大，運算功能不佳，無法支援實際應用中的數位簽章或加解密需求，對於電子病歷、處方箋、檢驗單或收據的驗證與取得，相當不便，其重要性由此可見一般。健保 IC 卡的儲存媒介與晶片材質的挑選，例如，ROM、RAM、或 EPROM 等，都須經過謹慎考慮，根據其特性，配合系統運用。再者，卡片的內建資料可依據資料的重要性分級，或依照急診等緊急用途的必要與非必要資訊區隔。此外，內建資料的讀取方式與安全機制，也必須透過事前良好的規劃與設計落實。

其次，建置功能完整的電子處方箋系統及其與醫療資訊系統的整合。從電子病歷的快速進展，處方箋目前傾向電子化的趨勢[28]。以目前的醫療體系及健保制度而言，若能輔以數位簽章技術，則藥局與病患不但能夠驗證電子處方箋內容的正確性、完整性與不可否認性，藥局同時也可以透過網路的驗證機制，完成申報健保幾付作業功能，有助

於提升整體醫療資訊網絡的完整性，也是未來非常值得發展的研究目標。

其三，保障病患與醫師的隱私權[1][20]。醫療行為中的保密職責是建立良好醫病關係的基本要件，病人有要求個人醫療資訊保密的權利，醫師也有尊重病人醫療隱私的義務。在法律本質上，隱私權是一個受限制的權利，被動地受制於平衡公共衛生利益、第三人利益及個人隱私利益的衝突問題。此外，在目前轉診、會診、健保 IC 卡的醫療制度下，醫療分工與醫療團隊不但是趨勢，將是維護病人隱私的最大挑戰。因此，授權取得病歷資料的模式，可以落實醫病雙方隱私權的保障[14][23][26]。

整合式醫療資訊系統應該是安全且便利的完整系統，包含下列特性：

1) 近期就診紀錄的可攜性

將病患最近週期內的就診紀錄登入健保 IC 卡，透過認證程序，醫師可以從卡片讀取患者在其他醫療院所的就診資訊，快速取得患者病史，盡快做出正確的診斷，有助於提高醫師診斷的正確性與效率。

2) 藥物代領功能

該功能著重於病患領藥時的便利性，其作法為將代理人(Agent)身分與認證資訊與醫療資訊系統整合，並且登錄於病患的健保 IC 卡。當患者本身無法或無暇親自領藥時，特別是身心殘障或行動不便的患者，即可透過授權機制，委託合法的代理人代領藥物。

3) 連結性與隱私權保護

在數位化醫療制度中，病患與醫師的醫療隱私權，是相當受到重視的議題。系統開發之初，即應擬定以下四點需求：

3.1) 匿名性：在整合式醫療資訊系統中，病患與醫師皆應以假名行事。

3.2) 病患身分連結性(Linkability)：只有健保申報單位可以取得病患的真實身分，藥局對於病患身分的連結性，僅止於電子處方箋持有者身分的同異，但無法據此得知其真實身分。

3.3) 醫師身分連結性(Linkability)：只有特定的公正醫療公會可以掌握醫師的真實身分，健保局對於醫師身分的連結性，僅止於處方箋開立者身分的同異，但無法據此得知其真實身分。

3.4) 醫師身分的非關聯性(Non-Linkability)：藥局無法從電子處方箋內容連結開立醫師的身分。

4) 預防病患重覆領藥

衛生科學與技術全面電子化之後，電子處方箋的取得，或許比手寫處方箋的取得更為容易。為了避免患者持電子處方箋複本在不同藥局之間重覆領藥的

違法行為，造成醫療資源浪費，健全的整合式醫療資訊系統應具備防止類似行為的功能。

5) 防範藥局浮報藥品

在醫藥分業的主流下，經常可見藥局浮報藥品及價錢的情形。例如，藥局與納保人共謀，令其四處看診，取得醫師處方；納保人雖未領取藥品，但仍交處方箋交予藥局，供其浮報藥品與藥價。因此，整合式醫療資訊系統應結合電子簽章技術，透過健保申報單位，嚴格控管同一納保人的領藥明細與數量，杜絕合謀圖利之行為。

6) 醫師與病患或藥局合謀圖利

醫師與納保人或醫師與藥局共謀圖利，始終是醫療保險制度無法徹底杜絕的問題。舉例而言，納保人與醫師合謀，誆稱醫療事實，前者藉此領取非健保幾付或非醫療用途之保健藥品，後者則詐取看診費用；或以醫師與藥局共謀為例，醫師以一己之私利，浮濫開立昂貴藥品，並指使病患至特定藥局領藥，藉以高單價藥品圖利於藥局，謀取暴利。

7) 緊急醫療的急迫性

當發生緊急情況時，需即時取得病患的基本資訊，才得以在治癒前瞭解患者的身體狀況，但若病患是處於昏迷又無預警的狀態被送至醫療院所，對於一無所知的患者就必須先作各項檢查，以瞭解其身體狀況，如此將使患者的生存機率降低。在健全的系統中應避免這樣的情況發生，藉由透過電子病歷交換取得患者的資訊，並透過生物特徵身分驗證及簽章方式確保其安全性，這樣可提升患者的治癒率。

本研究提出全方面的醫療資訊整合系統，結合上述三大重點以及七項特性，除讓醫療資訊更佳完整，亦讓醫療交流更加快速，然而，除在技術面的突破之外，我們系統的建置，亦必須依賴政府公權力的介入，設置可信任的第三公正單位(Trusted Third Party，TTP)，專司異常醫療交易行為之監控與調查，以徹底杜絕違法行為。

剩餘章節將介紹如下：第二章介紹建構系統所用到的設備以及技術；第三章介紹「整合式醫療資訊系統」，包括系統的操作步驟、與使用者間的溝通模式，並搭配醫療看診環境加以模擬；第四章介紹研究成果；最後，第五章為結論以及未來展望。

貳、技術分析

整合式醫療資訊系統結合多種電腦科學技術，例如：智慧卡(Smart cards)、電子病歷(Electronic Medical Records)、公開金鑰密碼系統(Public-key Cryptosystems)、數位簽章(Digital Signature)以及指紋辨識(Fingerprint Identification)。數位簽章可延伸為群體簽章(Group Signature)或代理簽章(Proxy Signature)，並且運用於論文不同區域。敘述如下：

2.1 智慧卡

智慧卡(Smart Card)又稱為智能卡，最早是在 1968 年由德國發明家 Jurgen Dethloff 與 Helmut Grotupp 所提出，是一種嵌入 IC 晶片的 ISO 標準尺寸塑膠卡，並利用讀取晶片上的資料，以達成記憶、識別、加/解密與傳輸等多項功能的卡片[32][41]。由於智慧卡提供了簡易的電腦運算的功能，因此我們可以透過卡片儲存個人資料，例如：藥物、身分資料、金鑰、公開憑證、電子病歷、藥單等，多種相關的個人診斷紀錄[31]。在資料的傳輸加密處理上，則透過中央處理器讓資料更佳安全；在記錄資料的部份我們可以藉由記憶體作儲存；最後再透過輸出入的介面將資料透過讀卡機傳輸。

在本文提出的醫療資訊系統中，將會使用由智慧卡衍生應用的醫事憑證 IC 卡與健保 IC 卡。

醫事憑證 IC 卡又稱醫師卡，目前在醫療院所使用的 IC 卡有三種：醫事人員卡、醫師卡和醫事機構的附卡，透過這三張卡可讓醫事機構內的醫生或醫療人員發揮功能，每張卡片的功能不盡相同，持有醫事人員卡者可看到醫療相關的資料，卻看不到病患的個人資料；而醫師卡則可看到病患的資料及就診紀錄[31][52]。

醫師卡在本系統中扮演著極重要的角色，醫師卡即代表醫師，系統的使用過程需透過醫師卡內的群體簽章金鑰調閱電子病歷，而在領藥及保險的部分需透過醫師卡進行簽章以示負責，如此，發生醫療糾紛時便能即時找出當初簽章的醫師。

健保 IC 卡於九十三年一月一日正式上線使用，過去長期使用的健保紙卡也隨之被淘汰，為了因應時代的潮流，健保保險憑證也邁入電子化的時代[42][50]。

健保 IC 可以說是一張功能完整且多用途的健保卡，除了取代原有的健保紙卡，其他如兒童健康手冊、孕婦健康手冊、重大傷病卡等具有健保保險憑證功能的資料，均已整合於卡片內。所以可不管病患的身分別，就醫時只需攜帶健保 IC 卡即可順利看診，而且五至七年不用換卡，省去原本紙卡需更換卡片的不便與資源的浪費[30][42][50]。

健保 IC 卡的可擴充性極佳，有助於醫療資訊系統的功能整合，包括醫療資訊可攜性、避免重複領藥與浮報藥價等不法的醫療資源分配問題等問題的解決方法。因此，針對健保卡片的設計，本計劃採取層級架構，根據卡片儲存資料的重要性與機密性，區分為 4 個層級，分層負責醫療過程中的某些功能，每一層級的組成元件、使用者以及使用者權限，不盡相同，分述如下。

(一) 機密階層(Confidentiality Level)

用以存放該持卡人加解密或簽章使用的私鑰，元件之儲存設備為唯讀記憶體(ROM)。利用唯讀記憶體(ROM)的特性，一旦金鑰寫入後，就無法以其他技術再行更改、擷取或複製，甚致包括持卡人也無法取得，以確保私鑰絕對安全。

(二) 安全階層(Security Level)

用以存放病患最近幾次就診的醫療紀錄，包括電子病歷(E-Prescription)，個人健康電子紀錄(E-Patient Records)和個人診斷紀錄(Personal Diagnostic Records)。最大存放資料量視記憶體容量大小而定，儲存格式為具有先進先出特性的有序串列—佇列(Queue)，在佇列前端加入資料、佇列後端刪除資料，因此，每當新的一筆資料寫入時，最先加入的一筆資料就會被覆蓋，並從卡片中刪除，所以儲存元件之設備採用電子抹除式可複寫唯讀記憶體(EEPROM)。利用該元件的特性，當存取該區資料時，病患與醫師雙方的身分都必須經過驗證，以確認此次之存取確實得到病患之授權，同時也紀錄負責看診醫師之身分。

將病患的醫療紀錄寫入 IC 卡的用意在於實現行動醫療，現今大部分診療紀錄的保管權屬於院方所有，即使是病患本人，也必需經過重重手續，方能取得片段紀錄，耗費大量時間及人力資源，目前雖有諸多醫療院所，以醫療資訊化為發展目標。但資訊的取得，還是必需透過病患申請，再輔以電子簽章及數位憑證認證程序，中間或許仍有些程序還是需要病患親自到醫院，才能完成跨院所間的病歷資料交換。因此，將病患的醫療紀錄載入 IC 卡的做法，或是透過本系統從建保局取得醫療紀錄，對於取得資料與達成行動醫療的效率而言，不啻為最簡之道。

(三) 代理階層(Proxy Level)

此階層最主要的目的在於賦予 IMIS 具備代理領藥的功能，對於行動不便、或無法親自領藥之病患，可以經由授權之方式，委託代理人代為領藥。因此，存放的資料為病患未領取藥物之處方箋編號，儲存格式仍以佇列串列設計，同樣取其先進先出之特性，所以儲存設備也是採用電子抹除式可複寫唯讀記憶體(EEPROM)。

(四) 公開階層(Open Level)

此階層用以存放病患之公開金鑰憑證，用來驗證病患之簽章，除了可驗證病人的真實性外，還能驗證該病患是否有具給付健保費用的能力。

智慧卡在系統中扮演著最大媒介的角色，透過智慧卡儲存病人及醫師的金鑰和簽章認證，將能隨時的驗證病人身分、調取病患病歷、領取及核對藥物等，使得本系統得以順利運行。

2.2 電子病歷(Electronic Medical Records)

病歷為醫療機構的工作人員於從事醫療業務時，對於病人所做的各項檢查、診斷、治療、照護等過程中所產生的醫療業務文書(醫療法第 48 條)。其中內容包含病歷記錄、證明同意書、檢查記錄表、護理記錄等相關的資料。隨著各家醫院不同的存放方式，造成病歷資料零散且不易分享與交換，導致效率不彰而耗費醫療資源。為了改善此情況，紙本病歷逐漸發展成電子病歷，以方便將資料整合與更新，必要時也能夠在各家醫療院所流通使用，目前有多家醫院正朝著電子病歷在努力[34][35][38]，且依據醫療法第 69 條之法令規定「醫療機構以電子文件方式製作及儲存之病歷，得免另以書面方式製作」，如此，將能促使環境生態的保育。美國電子病歷協會(Computer-Based Patient Record Institute, CPRI)將電子病歷描述為「以電子方式儲存個人一生的健康狀況及醫療照護的資訊」，以取代紙本病歷作為主要的醫療照護紀錄[33][40][47]。表 1 為相關電子病歷之定義。

美國國家科學院國立醫學研究院(Institute of Medicine, IOM)更進一步指出電子病歷必須能夠提供完整且精確的數據，以及臨床決策及醫學相關研究[2]。美國病歷學會(Medical Records Institute, MRI)將電子病歷定義為個人一生相關於健康狀態及醫療照護的電子化資訊，並且將電子病歷系統的發展區分為五個階段，分別為自動化病歷(Automated Medical Record, AMR)、電腦化病歷(Computerized Medical Record, CMR)、醫療提供者為主的電子病歷系統(Provider-based Electronic Medical Record, EMR)、電子病歷(Electronic Patient Record, EPR)及電子健康紀錄(Electronic Health Record, EHR)[34][35][47][50]。

在資料格式上由美國國家科學院國立醫學研究院(Institute of Medicine, IOM)認定應至少包含六種不同的格式，也就是文字(Text)、圖形(Graphics)、影像(Images)、數字(Numerical)、聲音(Sound)及影片(Full-motion Video)。因此，電子病歷系統乃是應用上述儲存資料的方式所完整建製起來的一套機制。IOM 說明：「此機制是由人員、資料、規則、程序、處理、儲存設備、通訊及技術支援所組成的系統，該系統提供病歷記錄的獲得、使用、儲存與擷取等機制」[34][45]。

表 1、電子病歷定義

提出者	名詞	定義
Dick,Steen, &Detmer, 1997	CPR	存在於資訊系統中的電子化病歷記錄,該系統支援使用者正確及準確使用資料的能力,提供臨床決策支援,可和醫學知識及其他輔助系統相連結。
Raghupathi, 1997	EPR	利用識別碼儲存個人的健康資訊，並能夠蒐集、儲存、擷取、傳輸及使用病人的相關資料，包含管理及個人基本資料等。
CPRI, 1998	CPR	個人終其一生的健康狀態及電子化的醫療照護資訊。電子病歷，不只是紙本病歷的自動化格式，更包含了所有健康資訊的範疇，如：醫學記錄、藥物記錄、各種檢驗及檢查結果還有 X 光影像等。
CPRI, 1998	EPR	在進行診療的過程中產生文件的檔案,包含手寫病歷記錄的影像檔、歷史性的資料及其他由紙本文件產生的記錄。
	EMR	CPR、EMR 加上醫學影像處理能力。
HIMSS-Electronic Health Record(EHR), 2005	EHR	取自於許多不同來源,並以電子化形式維護的資料,內容為每個人終其一生與健康狀態及醫療照護有關的資訊。
ISO, 2005	EHR	電子健康紀錄儲存病患的健康狀態,並且可以透過電腦修改內容。
	ICEHR	整合醫療照護的電子健康紀錄,可透過電腦處理、儲存、傳送的健康狀態紀錄，並且可安全的給予不同使用者存取。主要目的在於支援連續性、有效率且品質整合性的醫療照護，並且包含可追溯過去、現今及未來可預測的資訊。
Venkatraman et al., 2008	EMR	電子病歷系統是臨床數據自動化的系統,包括病患相關病史、人口統計資料、臨床醫師指示、藥物資訊、電子處方診斷及檢驗相關表單。
Ayers et al., 2009	EMR	造就無紙化病歷,由醫務相關人員將病患的資料輸入電腦系統，以代替紙本病歷。

近年來資訊科技蓬勃發展，各式各樣雲端應用服務應運而生，其中雲端帶來許多方便性及不少好處，像是有利於集中管理、節省儲存空間以及方便分享給其他使用者，但這樣的方便卻造成很大的問題，有可能造成資訊遺失或病人的隱私遭到竊取甚至濫用，因此將電子病歷存放於雲端業者存在著相當的風險[51]。所以本研究將電子病歷存放於

健保局中，各式的醫療業務將由健保局承包，且在傳輸的過程中透過安全有效率的加密技術，用以保障病人病歷的安全。

2.3 密碼學與加密系統

個人的病歷資料儲存於健保局，並且透過電子病歷及醫療資訊系統進行傳輸，只要稍不注意，病人的隱私將會暴露，除了對病人造成嚴重傷害外，還可能對整體的醫療環境造成重大的破壞，導致整個醫療體制面臨無法挽回的風險。因此，在資訊傳遞的保護上必須降低其風險，我們可利用加解密系統來實現，並確保資料的完整性及保密性還有可用性。以下將介紹基礎密碼學與加密系統。

(一)基礎密碼學

密碼學是門將資訊透過特殊的方法，處理成無法直接解讀的訊息，如：透過數學式的變化，使資訊變得不規律，讓他人無法讀取訊息的內容，並可透過數學式還原成原先的資料。因此，加解密演算法可說是密碼學重要的學問，主要分成加密(Encryption)及解密(Decryption)，我們可以透過加密(Encryption)演算法的技術，將訊息從明文變成密文以保護重要的訊息。同理，我們也可透過解密(Decryption)演算法的技術，將訊息從密文變成明文以讀取資料。

(二)公開金鑰密碼系統(Public-Key Cryptosystems)

公開金鑰密碼系統(Public-Key Cryptosystems)又稱非對稱式密碼系統（Asymmetric Cryptosystem）或雙金鑰密碼系統（Two-Key Cryptosystem），是由 Diffie 和 Hellman 於 1976 年首次提出。此密碼系統在加解密的過程中分為公開金鑰(Publickey, PK)及私密金鑰(Secretkey, SK)，公開金鑰是用來加密(Encryption)及解簽署文，另一把私密金鑰是用來解密(Decryption)及簽署；其中，私密金鑰是由訊息傳送方和訊息接收方各自擁有，而公開金鑰則是人人皆可取得的金鑰。通常，密碼學運用於網路傳輸資料上，且需避免違法的第三方竊取及篡改。因此在訊息的傳遞上，傳遞者需先把收件者的公鑰對訊息加密成密文，當密文訊息被傳送至接收者後，訊息接收方則可透過自己的私密金鑰，將密文解密成明文以便讀取，在此我們也能確信該訊息是由接收方所讀取，另外，除非收件者的私鑰被盜取，否則不可能經由違法的使用者開啟[39][44][49]。

自從 Diffie 和 Hellman 提出公開金鑰密碼系統後，多位學者接連提出各種類型的公開金鑰密碼系統，常見的公開金鑰密碼系統有 RSA[21]、ElGamal[9]及 Elliptic Curve[15][17]等。因此，目前在設計系統上為了顧慮到資訊安全，其設計原理大多採用公開金鑰密碼系統。

2.4 數位簽章(Digital Signature)

數位簽章最初源自密碼學，功能在於提供簽署文字訊息的機制，確保資料得以完整安全地傳送到目的端[9][19][21]，一般而言，搭配單向雜湊函數(One-way Hash Function)使用。單向雜湊函數是數學演算法的一種，可以任何長度的文字訊息為輸入值，得到固定長度的輸出值。雜湊函數的主要功能，在於避免第三者從輸出值推得輸入值[22]。

綜合上述，簡要說明產生數位簽章之方式如後。假設以公開金鑰系統為基礎，傳送端先使用單向雜湊函數將電子文件轉換成固定長度的文字訊息，稱之為訊息摘要(Message Digest)[19]，然後使用個人的私密金鑰對此訊息摘要進行簽署，產生數位簽章；接收端收到訊息與簽章後，使用傳送端的公開金鑰驗證簽章的完整性，確認是否與經過雜湊函數運算的訊息內容符合；若比對不一致，表示接收的訊息已經遭到竄改；若比對一致，表示接收的訊息為有效文件。藉此，使用者可以確認資料傳送的完整性與安全性。

(一)群體簽章(Group Signature)

D. Chaum 與 E. van Heyst 於 1991 年提出的群體簽章概念，屬於數位簽章相關應用之一，群體成員皆以群體名義對訊息進行簽署[3]，簽署者形同以匿名方式簽署，只有當爭議發生時，責付特定的公正第三方查核簽章，追蹤真正的簽署者。群體簽章通常使用於一個群體發佈的訊息，簽章的生成，可以經由群體中任一成員使用個人私鑰產生，驗證則只需透過一把公開的群體公鑰。在邏輯上的認定，群體簽章可歸類為多簽章私鑰對單驗證公鑰的簽章機制[5]。以病歷文件的傳遞為例，一名患者在同一個門診時段，可能掛入數個不同科別的門診，病歷在傳遞的過程中，或許可能產生失誤，因此，可以藉由群體簽章查核科別的可驗證性及建立簽署者身分的不可連結性，或在醫療紛爭發生之際，透過具有公信力的第三方，以私鑰追蹤簽署者的確實身分。如圖 1 及圖 2 所示[37][43]。

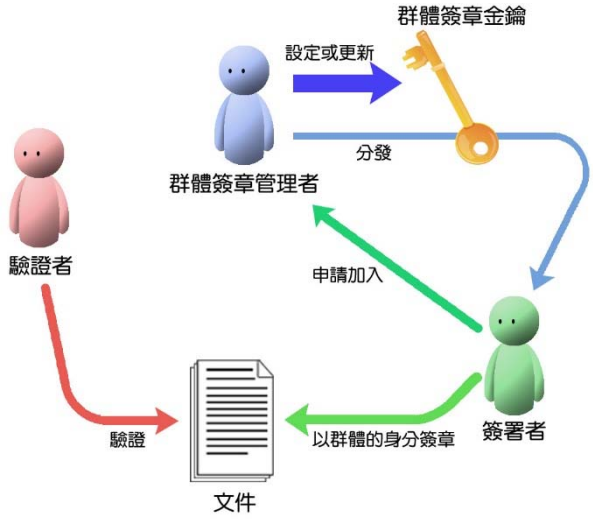

圖 1：群體簽章流程

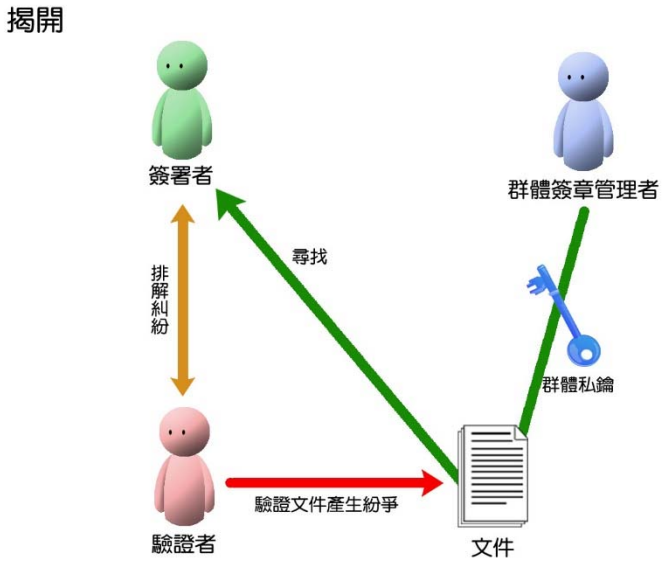

圖 2：群體簽章流程(揭開)

(二)代理簽章(Proxy Signature)

1996 年，Mambo 等提出代理簽章[18]，運作機制包括原始簽署者、代理簽署者與驗證者等三方。在原始簽署者的授權下，代理簽署者可代為決行；授權模式可區分為完全授權、部分授權與授權書授權三種，其中以授權書授權模式為最常見[4][13]，授權書載明原始簽署者的識別碼、代理簽署者的識別碼、以及代理期限等資訊，可使用於代領藥物功能之設計上，使行動不便或無法親自領藥的病患，以簽章授權的方式，委託代理人領藥。

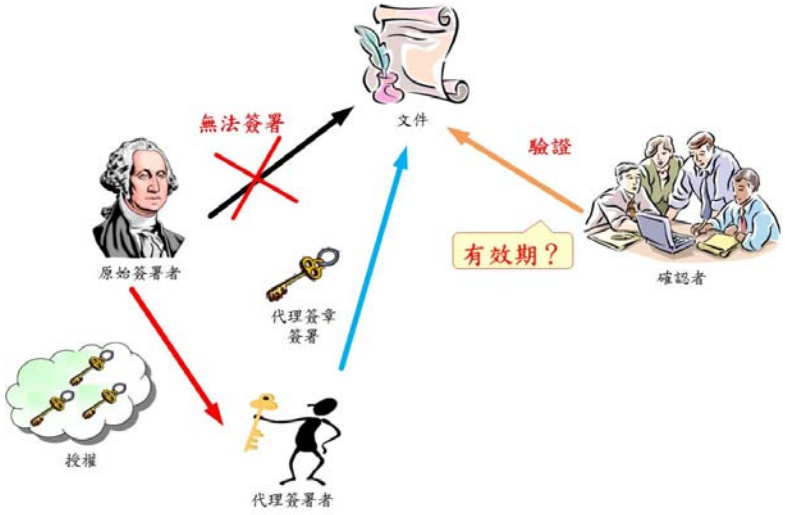

圖 3：代理簽章

2.5 使用者身份認證指紋辨識

隨著科技與網路的發展，大多數的使用者都能透過網路取得需要的資訊，但在取得服務之前，使用者需要先經過身份認證以確保其為合法者。其中，使用者身份認證(User Authentication)是用來識別是否為合法的系統使用者，以防止不法的使用者入侵系統取得重要資訊。

指紋辨識在千年前就已被中國人所使用，如在紙張上簽名或蓋上手印。19 世紀人們發現指紋是終生不變，且每個人的手指紋路皆不相同，因此成為已生物特徵達到身份辨識的效果[48]。

指紋辨識的過程，大致上可分成四個步驟，分別為指紋特徵建檔程序、擷取指紋影像、影像處理與特徵抽取、特徵比對等步驟，如下所示[29][46]：

1) 指紋特徵建檔程序：指紋特徵建檔程序是最重要的步驟，使用者事先將指紋特徵建檔於資料庫中，作為日後進行身分和身份識別的依據。
2) 擷取指紋影像：指紋影像是由指紋的突起與凹陷紋所構成的結果，將可利用光學式指紋讀取機擷取指紋，擷取的方式為透過手指按壓於指紋讀取機器，稱之為活體指紋影像。
3) 影像處理與特徵抽取：指紋影像的品質優劣對於指紋辨識系統的辨識率影響甚大，因此，這一個步驟需要透過影像處理去除雜訊和增強指紋的資訊及特徵，才能取得正確的指紋特徵點。
4) 特徵比對：將已建檔的指紋進行比對，藉以評估錯誤接受率(False Acceptation Rate)及錯誤拒絕率(False Rejection Rate)。

透過指紋辨識確保身分的識別，當病患昏迷或無攜帶健保卡時，即可利用指紋辨識替病患調閱歷史病歷，以避免延誤就醫的情形。雖然已有研究利用浮水印結合指紋辨識提升安全性，但缺乏完整性及不可否認性。該研究將欲傳送出去的指紋檔案加入浮水印保護，接著經過身分驗證取得電子病歷後，卻沒有作驗證紀錄，日後發生問題時將無法作糾紛排解，且各家醫院的浮水印不盡相同，在調閱病歷時會有辨識上的困難[36]。

參、研究方法

本章節介紹我們提出的 Integrated Medical Information System (IMIS)，包含架構、實體機構以及執行程序。IMIS 整合個人健康電子紀錄(E-Patient Record)和電子病歷(E-Prescriptions)，因此簡化原本複雜及費時的醫療流程，包括看診、檢驗、領藥、急診、保險給付；甚至運用密碼學技術，如：加解密、數位簽章保障病患及醫師的隱私權，並防止違法獲益行為發生；此外，當發生醫療糾紛時，由系統中的公正的第三方檢視訊息與簽章，平息紛爭。

IMIS 的架構與運作流程如圖 4 所示，可將整個機制分成四個階段，註冊階段(Registration Phase)、診斷階段(Diagnosis Phase)、領藥階段(Collecting Medicine Phase)和補助階段(Subvention Phase)。主要實體機構包含保險公司、健保局、藥局、病患、醫生和代理人。健保局負責全國之醫療業務，也就是從醫師至病人領藥都囊括在內，一開始會給予病患醫療所使用的健保卡(National Health Insurance IC Card)以及醫師和藥局的諮詢及醫藥認證，包含收集、保管與更新全國病患之電子病歷與處方箋，並協助驗證代理者是否有資格代理領藥；此外，亦負責補助藥物費用以及診查與治療病患之部分或全額費用；並核發每位醫師診治病患所使用之群體簽章與憑證，同時亦協助處理藥局、保險公司、醫生和病患之間可能發生的醫療糾紛；藥局負責驗證處方箋及藥單裡簽章之正確性並提供藥物給病患或代理人；病患、醫生和代理人在 IMIS 中各扮演著重要的角色。

基於保護病人和醫生的隱私性，在註冊階段，病人需向健保局(Bureau of National Health Insurance, NHI)辦理一張具有匿名特性的健保卡(National Health Insurance IC Card)，而醫生則需向健保局申請個人的群體簽章私鑰及醫師卡；藉由群體簽章的特性，滿足匿名的要求。此外，IMIS 中有代領人協助病人領藥功能，代理人使用的代理簽章私鑰也會存入卡中。

診斷階段(Diagnosis Phase)，當病患持健保卡(National Health Insurance IC Card)就醫時，醫師首先將醫師卡及健保卡插至機器，並將病人資料傳送至健保局，以驗證病人簽章，當確認病患的確為持卡本人，接著該名病患之基本資料、歷史就診紀錄、以及卡中的最近幾次診療紀錄，將會顯示於醫師電腦螢幕上，有助於醫師了解患者近來的身體狀況與就醫情形。

看診完成後，醫師會更新病患的病歷資料並填寫處方箋與藥單讓病患至藥局領取藥

品；這些動作，醫師都必須使用個人的群體私鑰做簽章，以示對當次診療負責。此外，醫師會把當下的診療紀錄與處方箋資料寫入病患的健保卡(National Health Insurance IC Card)中。

若病人需向保險公司申請保險時，只要請醫生將此次的診治內容轉成申請保險需要的診斷證明書，並連同醫師本人做群體私鑰簽章以示負責，最後將其診斷書傳至保險公司，即完成保險與醫療完整結合的環境。

當病患處於昏迷被送至急診時，為避免因蒐集病患的血液或為了解病患身體狀況而導致延誤治療，需先採集病患的指紋，接著醫師將醫師卡及採集到的病患指紋資料傳至健保局，並透過病患的指紋取得病歷資料，當健保局藉由指紋資料確認為患者後，便會把病患之基本資料、最近的診療記錄、歷史就診紀錄顯示於醫師電腦螢幕上，當病患脫離危險後，將會轉至其他科別及病房，其餘的處理皆和門診相同。

領藥階段(Collecting Medicine Phase)，病患將持健保卡(National Health Insurance IC Card)前往藥局(Pharmacy, PH)領取藥物。藥劑師首先會藉由比對卡中與醫師所傳來的資料是否相符來驗證患者身分，若無錯誤，則發給藥品給病患，並作已領藥的註記。若患者不便或無暇自行取藥，可由通過授權的代理人授權代領。

患者在完成領藥、簽署具結的程序後，藥局即可憑藉病患或代理人的簽章向健保局申報藥費補助，病患也能夠依據自己的投保狀況和保險公司領取理賠金，完成由病患與醫師、醫師與院方、院方與藥局、保險公司與病患所構成的醫療流程。

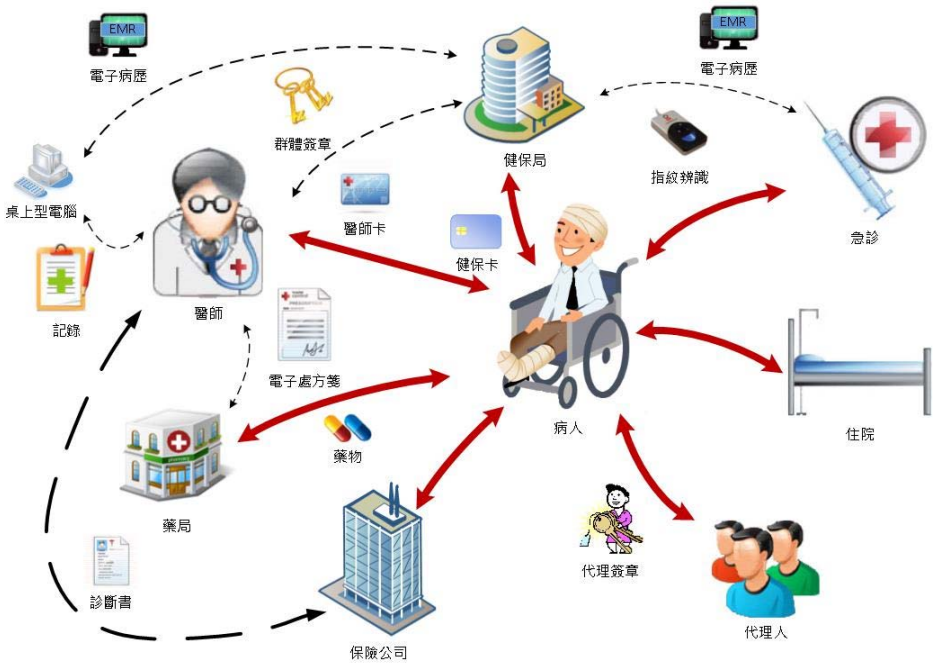

圖 4：IMIS 的流程圖

3.1 註冊階段(Registration Phase)

在初始步驟，基於保護病患(Patient, P)的隱私，必須向健保局(Bureau of National Health Insurance, NHI)辦理一張具有匿名特性的健保卡(National Health Insurance IC Card)，並將私鑰及相關資訊儲存於健保卡中。因此，病人將對健保局提出辦理的要求 R_P，其表示式如(1)所示，內容包含申請健保的細節項目 Req、看診時所需使用的代理人公鑰 PK_{AP}，及 Req 和 PK_{AP} 透過自己使用的私鑰 SK_P 所做的簽章，並附加此金鑰憑證 $Cert_P$ 經由安全通道一併傳送給健保局。

$$P \rightarrow NHI: R_P = \{Req, PK_{AP}, Sig_{SK_P}(Req, PK_{AP}), Cert_P\} \quad (1)$$

當健保局接收到 R_P 後，會運用包含在 $Cert_P$ 裡的公鑰資訊 PK_P 來驗證簽章 $Sig_{SK_P}(Req, PK_{AP})$ 之正確性，若無誤，則隨機選擇一個流水編號 PID_P 給病人，在此 PID_P 算是病人的假名，往後無論看病、領藥或申請給付都使用該 ID，除了健保局外，任何人均無法從其他資訊，包括金鑰或病歷資料中得知所對應之病人真實姓名。另外，$Data$ 為病人已給付健保費用之相關證明資料，藉此告知此病人是合法且有能力給付醫藥費用的。最後，加上病人所傳的代理人公鑰 PK_{AP}，還有病人的公鑰 PK_P，透過自己的私鑰 SK_{NHI} 簽章產生公鑰憑證 $PCert_P$，其表示式如(2)所示，最後再將儲存資料的健保卡交給病人，當然裡面除了存公鑰憑證 $PCert_P$ 外病人還需將自己的私鑰 SK_P 儲存於健保卡內，如圖 5 所示。

$$NHI \rightarrow P: PCert_P = \{PID_P, Data, PK_{AP}, PK_P, Sig_{SK_{NHI}}(PK_{AP}, PK_P)\} \quad (2)$$

圖 5：病人與健保局註冊

保護醫生隱私方面，醫師(Doctor, DR)需向健保局申請醫師卡及個人的群體簽章私鑰，並將群體簽章私鑰儲存於醫師卡中，如圖 6 所示。藉由群體簽章的特性，除了健保局可透過簽章得知為哪位醫生簽署外，任何人皆只能利用群體簽章公鑰 PK_{GK} 來驗證其正確性及完整性，而無法得知為何人所簽署，滿足匿名與保護隱私之特性。因此，醫師將自己的身份 ID_D 運用私鑰 SK_D 簽章後，包含金鑰憑證 $Cert_D$ 藉由安全通道一併傳給健保局，做為申請群體簽章的要求 R_D，其表示式如(3)所示。

$$DR \rightarrow NHI: R_D = \{ID_D, Sig_{SK_D}(ID_D), Cert_D\} \quad (3)$$

圖 6：醫師與健保局註冊

當健保局驗證其簽章正確性後，會用群體簽章的 *Master Key (MK)*，結合醫生的 ID_D，藉由公式 F_{GK} 產生醫生看診所使用的群體簽章私鑰 K_D，其表示式如(4)所示，最後再將儲存資料的醫師卡交由醫師，完成產生簽章金鑰之過程。

$$NHI \rightarrow DR: F_{GK}(MK, ID_D) = K_D \quad (4)$$

此外，因 IMIS 中具備代領人(Agent, A)協助病人領藥之功能，因此若有必要，當健保局確認代領人的合法性後，病人與代理人間可運用病人私鑰 SK_P 與代理人的私鑰 SK_A 藉由公式 F_A 產生代理人簽章私鑰 SK_{Ap}，其表示式如(5)所示，最後再把代理人簽章私鑰 SK_{Ap} 儲存於代理人的健保卡中，如圖 7 所示。

$$P \leftrightarrow A: F_A(SK_P, SK_A) = SK_{Ap} \quad (5)$$

圖 7：代理人與健保局註冊

3.2 診斷階段(Diagnosis Phase)

(一)門診

本階段病人將攜帶健保卡(National Health Insurance IC Card)前往醫院看病，流程如

下所述：

首先，病人前往醫院櫃台掛號，需先將健保卡插入掛號機內，並用健保卡內自己的私鑰 SK_P 對電腦中簽署近期的戳章 TS，此時醫院櫃台可查驗該病患的給付健保費用之相關證明資料 $Data$ 是否合法；接著，等候輪流看診；於看診中，醫生和病人需把醫師卡及健保卡插入讀取的機器中，並利用健保局的公開金鑰 PK_{NHI} 對近期的戳章 TS 及公鑰憑證 $PCert_P$ 資料加密(E)後傳送，其表示式如(6)所示。

$$P \rightarrow DR: E_{PK_{NHI}}(TS, Sig_{SK_P}(TS), PCert_P) \quad (6)$$

此時，機器連線至健保局的系統，健保局將解密(D)，於是利用自己的私鑰 SK_{NHI} 及病人的公開鑰匙 PK_P，即可解開 PK_{NHI} 並驗證簽章 $Sig_{SK_P}(TS)$ 之正確性，其表示式如(7)所示。

$$DR \leftrightarrow NHI: D_{SK_{NHI}}(E_{PK_{NHI}}(TS, Sig_{SK_P}(TS), PCert_P)) \quad (7)$$

一旦驗證無誤，亦確認為病患本人後，會將群體簽章公鑰的驗證結果保存於健保局的本機端，以確保將來有醫療糾紛時能夠調查，則該名病患之基本資料、歷史就診紀錄、以及卡中的最近幾次診療紀錄 $OtherRC_S$ 將顯示於醫師電腦螢幕上，其表示式如(8)所示，以供醫生方便了解病人身體狀況。

$$NHI \rightarrow DR \quad OtherRC_S \quad (8)$$

當醫生對病人診療完畢後，會將此次的診治內容 $NewRC_S$ 新增於病患的病歷紀錄，其表示式如(9)所示，同時更新此病患存於健保局資料庫之病歷內容，最後將其連同醫師本人群體簽章 $Sig_{K_D}(NewRC_S)$ 上傳至健保局做為對此病人病歷紀錄的整合，其表示如圖 8 所示。

$$DR \rightarrow NHI: NewRC_S, Sig_{K_D}(NewRC_S) \quad (9)$$

圖 8：一般門診

另一方面，醫生需填寫該次服用藥物所遵照的處方箋 R_X，包含編號 R_X_ID 及藥單成份內容 MR_S，同樣，藉由醫師本人的群體私鑰 K_D 做簽章，以示負責。將所有資料，包含病人的公鑰憑證 $PCert_P$，運用病人所指定領取之藥局(Pharmacy, PH)的公鑰 PK_{PH} 加密(E)後傳送，其表示式如(10)所示。

$$DR \rightarrow PH: E_{PK_{PH}}(R_X, R_X\_ID, MR_S, Sig_{K_D}(R_X, R_X\_ID, MR_S), PCert_P) \quad (10)$$

並更新病人健保卡上最近的診療資料，其表示式如(11)所示，並附上這次領藥所需的處方箋編號 R_X_ID，以供病人在領藥時做驗證與簽章使用，如圖 9 所示。

$$DR \rightarrow P: NewRC_S, R_X\_ID \quad (11)$$

圖 9：醫師開藥

當病人需向保險公司(Insurer, I)申請保險時，只需請醫生將此次的診治內容 $NewRCS$ 轉成申請保險時所需要的診斷證明書 MC_S 及費用相關資料 EP_S，最後將其連同醫師本人群體私鑰 K_D 做簽章以示負責，並做為對此病人保險紀錄的整合，如圖 10 所示；最後將所有資料，包含病人的公鑰憑證 $PCert_P$，運用病人所指定領取之保險公司(Insurer, I)的公鑰 PK_I 加密(E)後傳送，其表示式如(12)所示。

$$DR \rightarrow I: E_{PK_I}(MC_S, EP_S, Sig_{K_D}(MC_S, EP_S), PCert_P) \quad (12)$$

圖 10：申請保險開立診斷書

(二)急診

本階段為病人經救護車送往醫院急診，因發生重大傷亡導致病患處於無意識狀態，流程如下所述：

首先，病人被送至急診室，因病人命危處於昏迷狀態，醫護人員需利用指紋辨識機器取得指紋FS，醫生需把醫師卡插入讀取的機器中，並對指紋FS做群體簽章$Sig_{K_D}(FS)$，接著利用健保局的公開金鑰PK_{NHI}加密(E)後傳送，其表示式如(13)所示。

$$DR \rightarrow NHI: E_{PK_{NHI}}(FS, Sig_{K_D}(FS)) \quad (13)$$

此時，機器將連線至健保局的系統，其表示式如(14)所示，健保局將透過自己的私鑰SK_{NHI}解密(D)，並利用群體簽章公鑰PK_{GK}，驗證(V)醫生傳送的群體私簽之正確性，同時把醫師卡及指紋FS資料帶入健保局的資料庫查找病人資料，並將群體簽章公鑰的驗證結果保存於健保局的本機端，以確保未來有醫療糾紛時能夠調查。

$$DR \leftrightarrow NHI: \begin{array}{l} D_{SK_{NHI}}(E_{PK_{NHI}}(Sig_{K_D}(FS))), \\ V_{PK_{GK}}(Sig_{K_D}(FS)) \stackrel{?}{=} FS \end{array} \quad (14)$$

一旦驗證無誤，亦經由指紋確認為病患本人後，則該名病患之基本資料、歷史就診紀錄、以及最近幾次診療紀錄$OtherRC_S$將顯示於醫師電腦螢幕上，其表示式如(15)所示，以供醫生方便了解病人身體狀況，如圖 11 所示。

$$NHI \rightarrow DR: OtherRC_S \quad (15)$$

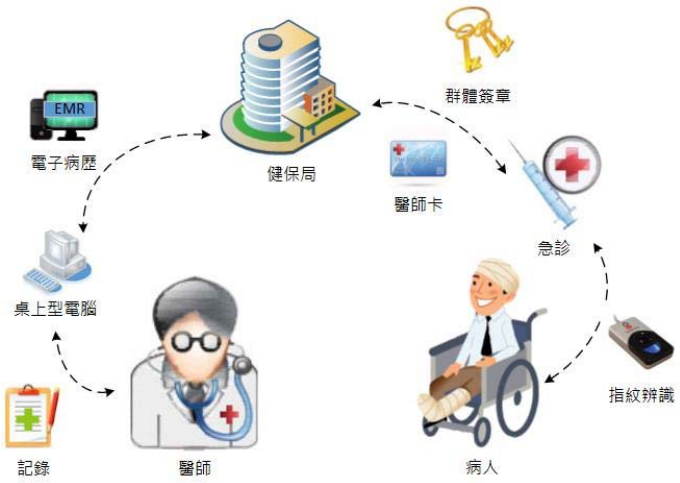

圖 11：急診

3.3 領藥階段(Collecting Medicine Phase)

本階段藥局將透過個人私鑰 SK_{PH} 解密 (D) 即取得醫師簽署的群體簽章 $Sig_{K_D}(R_X, R_X\_ID, MR_S)$，其表示式如(16)所示，並根據健保局公布的群體簽章公鑰 PK_{GK}，驗證 (V) 醫生傳送的處方箋資料之正確性，此驗證結果將被保存於藥局的本機端，以確保將來有醫療糾紛或金錢爭議時，可請健保局協助解決。

$$PH \leftrightarrow NHI: \quad D_{SK_{PH}}(E_{PK_{PH}}(Sig_{K_D}(R_X, R_X\_ID, MR_S))),$$
$$V_{PK_{GK}}(Sig_{K_D}(R_X, R_X\_ID, MR_S)) \stackrel{?}{=} R_X, R_X\_ID, MR_S \quad (16)$$

接著，病人攜帶健保卡至藥局領藥；病人將健保卡插入藥局的機器中，其表示式如(17)所示，可藉此判斷儲存於病人卡中的處方箋編號 R_X_ID 是否符合醫生所傳的編號，藥局可以確認是否為病人本人領藥，若正確無誤，則藥局將請病人用自己存在健保卡內的私鑰對編號簽章，以成為藥局向健保局申請藥費補助的依據；最後，藥局將藥物給予病人，並標記其處方箋編號為已領取藥品，完成整個流程，如圖 12 所示。

$$P \rightarrow PH: \quad Card(R_X\_ID) \stackrel{?}{=} R_X\_ID, Sig_{SK_P}(R_X\_ID) \quad (17)$$

圖 12：領藥

另外，若病人行動不方便或有突發情形產生，則代理人可依規定幫其病人領藥。上述得知，代理人可在註冊階段取得協助領取藥物的代理私鑰 SK_{AP}；因此，當代理人使用自己健保卡內的代理私鑰對其處方箋編號做簽章 $Sig_{SK_{AP}}(R_X\_ID)$ 後，其表示式如(18)所示，即可至藥局領藥。

$$A \rightarrow PH: Sig_{SK_{AP}}(R_X\_ID) \quad (18)$$

藥局會運用病患公鑰與代理人的公鑰 PK_P 和 PK_A，其表示式如(19)所示，藉由公式 F_A 還原代理人的代理公鑰 PK_{AP} (證明確實由病人授權代理)來驗證(V)處方箋簽章之正確性，一旦無誤，則保留簽章成為申請藥費補助之依據，與病人領藥流程相同，如圖 13 所示。

$$A \leftrightarrow PH: \ PK_{Ap} = F_A(PK_P, PK_A)\ V_{PK_{Ap}}(Sig_{SK_{Ap}}(R_X\_ID)) \stackrel{?}{=} R_X\_ID \quad (19)$$

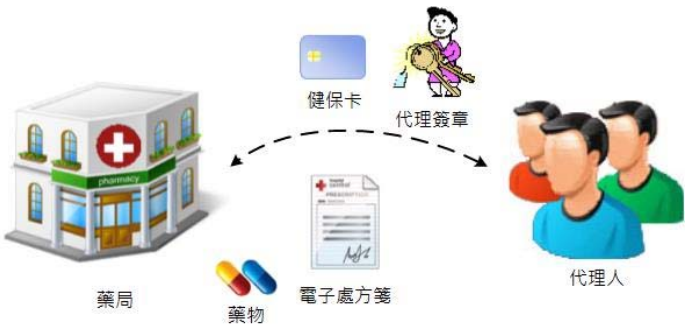

圖 13：代理人藥局領藥

3.4 補助階段(Subvention Phase)

當藥局欲向健保局申請藥費補助時，需提供兩項簽章以茲證明，其表示式如(20)所示。第一個為醫生簽署的群體簽章 $Sig_{K_D}(R_X, R_X\_ID, MR_S)$，第二個為病人簽署的處方箋編號之簽章 $Sig_{SK_P}(R_X\_ID)$ 及代理人公鑰 PK_{Ap} 或代理人簽署的處方箋編號之簽章 $Sig_{SK_{Ap}}(R_X\_ID)$。如此，可證明該位病人確實結束在某醫生的診療並已領取藥物。藥局會將這兩個簽章及驗證資料還有代理人公鑰，藉由健保局的公鑰 PK_{NHI} 加密(E)傳送給健保局，如圖 14 所示。

$$E_{PK_{NHI}}(R_Y, R_Y\_ID, MR_S, Sig_{K_D}(R_Y, R_Y\_ID, MR_S),\ Sig_{SK_P}(R_Y\_ID), PK_{AP})$$
or
$$E_{PK_{NHI}}(R_Y, R_Y\_ID, MR_S, Sig_{K_D}(R_Y, R_Y\_ID, MR_S),\ Sig_{SK_{AP}}(R_Y\_ID)) \quad (20)$$

圖 14：健保補助

在健保局接收資料之後，會運用私鑰 SK_{NHI} 解密，並一一驗證每個取得的簽章之正確性及完整性，一旦沒有錯誤，即回送給藥局和醫師具有健保局簽章的電子支付明細*(E-Payment)*，其表示式如(21)、(22)所示，供其藥局及醫師收取補助款。

$$NHI \rightarrow PH:\ EPayment, Sig_{SK_{NHI}}(EPayment) \quad (21)$$

$$NHI \rightarrow DR:\ EPayment, Sig_{SK_{NHI}}(EPayment) \quad (22)$$

本階段為病人欲向保險公司申請保費補助時，保險公司需先從醫生傳至的診斷書透過個人私鑰 SK_I 解密*(D)*，其表示式如(23)所示，取得醫師簽署的群體簽章 $Sig_{K_D}(MC_S, EP_S)$，並根據健保局公布的群體簽章公鑰 PK_{GK}，驗證*(V)*醫生群體簽章之正確性，此驗證結果將被保存於保險公司的本機端，以確保將來有金錢爭議時，可請健保局協助解決，如圖 15 所示。

$$I \leftrightarrow DR:\ D_{SK_I}(E_{PK_I}(Sig_{K_D}(MC_S, EP_S))), V_{PK_{GK}}(Sig_{K_D}(MC_S, EP_S)) \stackrel{?}{=} MC_S, EP_S \quad (23)$$

圖 15：保險補助

在保險公司接收資料之後，並一一驗證每個取得的簽章之正確性及完整性，一旦沒有錯誤，即發送給病人簽章的電子支付明細*(E-Payment)*，其表示式如(24)所示，供其病人收取理賠款。

$$EPayment, Sig_{SK_I}(EPayment) \quad (24)$$

肆、功能分析

我們提出的醫療系統需完整且方便並符合安全，必需符合以下特性：醫藥記錄的行動性、緊急醫療的急迫性、代領藥物的功能、保護連結功能和安全、避免藥物衝突和衝突問題。以下將一一敘述，並且證明我們的系統已滿足以上需求。

(一) 醫藥記錄的行動性(Mobility of Medicine Records)

隨著行動裝置的普及，例如：智慧卡、手機，和 PDA，發展技術不斷地精進，無論在儲存空間、計算能力、記憶體大小都提升的情況下，欲實現行動性的醫藥記錄將不再是遙不可及的事情。就我們所提出的 IMIS 而言，其搭配使用的健保卡(National Health Insurance IC Card)將遵照文中提到的內容來設計，不僅能具備簽章、加密、解密的功能，同時亦可使得相關的醫藥記錄安全地存於卡中，且因卡片之可攜性滿足了行動功能。雖然現今社會的醫療體系已採用類似的智慧卡，但要取得相關的醫療記錄還是必須通過一些複雜的驗證；但假以時日，相信在電子醫療的應用上能有很大的發展空間，而類似我們所提出的智慧卡在電子醫療系統(E-Medical System)、個人健康電子紀錄(E-Patient Records)和電子病歷(E-Prescriptions)日漸普及的情況下必能在未來被實際使用，以實現行動性的醫藥記錄。

(二) 緊急醫療的急迫性

醫療可說是常與生死拼搏的一門技巧，儘管醫療技術的進步提升了治癒率，但在治

癒前需瞭解患者的身體狀況，病患卻是處於昏迷又無預警的狀態被送至醫療院所，對於一無所知的患者就必須先作各項檢查，以瞭解其身體狀況，如此將使得患者的生存機率降低，而要如何快速的了解病況將不再是費時之事。透過我們提出的 IMIS 搭配使用指紋辨識系統，將遵照文中提到的內容來設計，不僅能具備簽章和加解密的功能，同時能調閱到病患的病歷資料，不僅滿足緊急醫療的急迫性，同時在資訊上具備完整的保護。現今而言，雖然能夠作一些較簡單的檢查，但對於醫療上而言，越是精細的資料越能有效提升治癒率，未來類似於我們所提出的緊急醫療必能被實際應用，搭立新的里程碑。

(三) 代領藥物

代領藥物將給予病患在領藥時更大的便利性，尤其對於身心殘障或行動不便的患者，合法地委託代理人代領藥物，可保障藥物不致遺失或遭人冒領。特別地，在未來全面電子化的醫療體系，代領藥物可能不再像現今體系，只要將醫師簽署的藥單交給藥局領取藥物如此簡單而已，如何在充斥著有心人士或電腦駭客會惡意攔截或修改藥單資料的網路環境下，安全提供代領藥物的功能，是個重要的議題。因此，我們的 IMIS 引用代理簽章，其不僅授權代理人可代理簽署藥單，代領藥物之能力，同時亦讓簽署之數位簽章保有確認性、整合、避免偽造，不可否認等特性，讓驗證的第三方可清楚知道病患及代理人身份是合法的。如此一來，除了保證病患與代領人可安全、確實的領到藥，也讓醫療資訊系統可放心提供代領藥物功能。

(四) 保護安全性(Protection of Privacy)

關於保護安全性，我們表現 IMIS 藉由病患使用之假名與醫師使用之群體簽章確保文中提到的五項安全性的連結需求，分別是匿名性、不可共謀性(Coalition-resistance)、病患的可連結性(Linkability of Patients)、醫師的可連結性(Linkability of Doctors)、醫師的不可連結性(Non-Linkability of Doctors)。

由於匿名性，健保局提供的假名、真名及隱私不會被揭露。因此，除了確保患者的臨床資料隱私，同時也能無私地提供學術單位做研究，進一步地發現更好的治療藥物或方法。

由於不可共謀性，使得醫師和病患的真名及隱私不會被合法的使用者合作揭露。因此，可防範藥廠對同病症的患者施以試驗藥品，及藥廠壟斷該症狀的藥物，以便進一步有效運用醫療資源。

由於病患的可連結性，健保局提供患者假名後，只有健保局可辨認病患的真實身分和假名的關係，任何人(除了看診的醫師外)無法輕易得知。同時，藥局只能從相同的假名分辨不同的病歷出自同一患者，因此我們提出的 IMIS 可滿足病患的可連結性。

以醫師的不可連結性而言，因為 IMIS 中群體簽章的引用，使得只有公正的健保局可以追蹤每位醫師對診療結果簽署的簽章並得知醫師的真實身分，其他單位只能驗證此簽章為合法簽署，無法得知簽署醫師的真實身份。此情形下滿足藥局無法從病歷內容中

得知為哪位醫師所開立而滿足醫師的不可連結性。

(五) 避免各式衝突和謀取暴利

避免藥物衝突及謀取暴利，和發生在藥局、保險業者、醫生與病人之間的衝突問題，我們的系統會建立離線的健保局，並解決這些可能發生的糾紛，詳述如下：

1) 協助解決藥物衝突問題：

對醫生而言，不小心開錯藥物或是蓄意亂開藥物是有可能發生的。若病人在不知情的狀況下依舊照著指示服藥，則可能會發生無法挽回的悲劇。因此，為避免類似的事件發生，當藥局的藥劑師發現藥單所列藥物有怪異之處，如不適合服用或不能一起服用，則藥劑師可透過離線的健保局幫忙協助調查究竟為何醫生會開出此藥單。

2) 協助解決昂貴藥物問題：

對於想謀取暴利的醫生而言，連續開出一系列昂貴的藥材給病人並不是一件很稀有的事，當然，對於健保局而言，勢必就必需補助高額的藥物費用，因此，若離線的健保局對於某家醫院之補助金額感覺異常的突兀，可向院方提出合理的懷疑，請求調查連續開出昂貴藥材的原因。

3) 協助調查病人頻繁看病的問題：

醫生和病人可能會共謀做出不法的勾當。例如：即使病人沒有生病，仍舊前往醫院看診；一方面自己可領取保健藥物得到好處，一方面幫忙醫生謀取看診費用。因此，若離線的健保局發現病人看病次數實在過於頻繁，可直接對病人作調查，看是否病人真的需要醫療上的協助，亦或蓄意浪費醫藥資源。

4) 協助調查病人申請保險的問題：

醫生和病人可能會共謀作出不法的勾當，其詐領高額保險金。例如：即使病人沒病或輕傷，仍舊前往醫院看診，並請醫師開立重大傷害的診斷書；一方面除了自己可領取保健藥物，還能夠申請巨額保金，另一方面醫師仍可謀取看診費用及不實的診斷費。若保險公司發現病人申請的保險金異常，可請離線的健保局對醫師及病患作調查，看是否病人真的需要醫療上的協助，亦或蓄意浪費醫藥資源。

以上四點爭議，皆與醫生有密切關係，因此，離線的健保局可從醫師簽署的群體簽章中追溯出負責的醫生。健保局將藉由 *Master Key (MK)*與醫生所簽的群體簽章 $Sig_{K_D}(\cdot)$，利用 *function* F_{GK_T}得到醫生簽名使用的群體簽章私鑰 K_D，其表示式如(25)所示，再比對存於資料庫裡的醫生金鑰與真名對照表，即可得知其簽章為那位醫生所簽署。最後，健保局將請該位醫生與藥局或保險業者當面對質，協助解決以上可能發生的爭議。

$$F_{GK\_T}(Sig_{K_D}(\cdot), TK) = K_D \quad (25)$$

伍、結論

本論文提出安全策略與隱私權保障的醫療資訊整合系統,結合個人健康電子紀錄(E-Patient Records)、電子病歷(E-Prescriptions)、改良的智慧卡、指紋辨識系統、並運用代理簽章和群體簽章的結合，提出以下三點結論：

1) 個人健康電子紀錄(E-Patient records)可透過健保局在不同醫療院所交換,處方箋與藥單還有診斷書也可被整合與使用，透過個人健康電子紀錄及電子病歷能發揮巨大的綜效，病患、醫師、醫院、藥局和藥廠將能被完整的掌握，除了避免藥廠壟斷藥品的價格，及醫療院所為了賺取看診費而與病人勾結，節省醫療資源之外，還能夠對環境保育盡一份心力。

2) 藉由指紋辨識系統的媒介，將能把緊急醫療的急迫性發揮得淋漓盡致，可透過指紋辨識系統確定病人身分，調閱病患存於健保局的電子病歷，如此將能替重傷且意識不清的患者進行治療。

3) 透過代理簽章和群體簽章的功能，能創造醫師與病患安全的認證保護，對病患而言能避免因在醫療或隱私上的不安而放棄治療，如碰到罕見疾病將能立即進行研究，並在醫學上有所突破；對醫師而言將能精進自己的技術，在配藥時並無名醫的開藥資料參考，因此各類藥物將存在各種可能性，也可能因而發現某種藥物在治療該症狀時有較好的成效，將促使原本複雜及費時的醫療流程因而簡化。

透過本系統將能有效運用及節省醫療資源，並滿足醫藥紀錄的行動性、代領藥物的功能、安全性、避免藥物衝突、謀取暴利等因醫療機制不夠完全所產生出的問題，進而物盡其用，才能以最少的資源獲得最大效益。在電子化醫療逐漸受到重視且成為主流的未來，相信本系統的安全、便利，能夠適用於未來的醫療環境。

參考文獻

[1] Ateniese, G., Cutmola, R., Meideiros, B. de and Davis, D., “Medical Information Privacy Assurance: Cryptographic and System Aspects”, *Third Conference on Security in Communication Networks*, Amalfi, Italy, pp. 199-218, 2002.

[2] Ball, E., Chadwick, D.W. and Mundy D., “Patient Privacy in Electronic Prescription Transfer”, *IEEE Security & Privacy Magazine*, Vol. 1, No. 2, pp. 77-80, 2003.

[3] Chaum, D. and Heyst, E. van, "Group signatures", *In proceedings of Advances in Cryptology - Eurocrypt 1991*, Vol. 547 of LNCS, Springer-Verlag, pp. 257-265, 1991.

[4] Cao, F. and Cao, Z., "A secure identity-based proxy multi-signature scheme", *Information Sciences, Vol*. 179, No. 3, pp. 292-302, 2009.

[5] Chen, C.-L., Chen, Y.-Y. and Chen, Y.-H., "Group-based Authentication to Protect Digital Content for Business Applications", *International Journal of Innovative Computing, Information and Control*, Vol. 5, No. 5, pp. 1243-1251, 2009.

[6] Chan, A. T.S., Cao, J., Chan, H. and Young, G., "A Web-Enabled Framework for Smart Card Application in Health Services", *Communications of the ACM*, Vol. 44, No. 9, pp. 77-82, 2001.

[7] Dolin, R. H., Alschuler, L., Beebe, C., Biron, P. V., Boyer, S. L., Essin, D., Kimber, E., Lincoln, T. and Mattison, J. E., "The HL7 Clinical Document Architecture", *Journal of the American Medical Informatics Association*, Vol. 8, No. 6, pp. 552-569, 2001.

[8] Dolin, R. H., Rishel, W., Biron, P. V., Spinosa, J. and Mattison, J. E. (1998), "SGML and XML as Interchange Formats for HL7 Messages", *Journal of the American Medical Informatics Association*, pp. 720-724, 1998.

[9] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, Vol.IT-31, No. 4, pp. 469-472, 1985.

[10] Gritzalis, S., Lambrinoudakis, C., Lekkas, D. and Deftereos, S., "Technicl Guidelines for Enhancing Privacy and Data Protection in Modern Electronic Medical Environments", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 9, No. 3, pp. 413-423, 2005.

[11] Huston, T., "Security Issues for Implementation of E-Medical Records", *Communications of the ACM*, Vol. 44, No. 9, pp. 89-94, 2001.

[12] Huang, K.-H., Hsieh, S.-H., Chang, Y.-J., Lai, F., Hsieh, S.-L. and Lee, H.-H. (2010), "Application of portable CDA for secure clinical-document exchange", *Journal of Medical Systems*, Vol. 34, No. 4, pp. 531-539, 2010.

[13] Hong, X., "Efficient threshold proxy signature protocol for mobile agents", *Information Sciences*, Vol. 179, No. 24, pp. 4243-4248, 2009.

[14] Hsu, C. C. and Ho, C. S., "A new hybrid case-based architecture for medical diagnosis", *Information Sciences*, Vol. 166, No. 1-4, pp. 231-247, 2004.

[15] Koblitz, N., "Elliptic curve cryptosystems", *Mathematics of Computation*, Vol. 48, pp. 203-209, 1987.

[16] Le, X. H., Lee, S., Lee, Y.-K., Lee, H., Khalid, M. and Sankar, R., "Activity-oriented access control to ubiquitous hospital information and services", *Information Sciences*, Vol.

180, No. 16, pp. 2979-2990, 2010.

[17] Miller, V.S., "Use of Elliptic Curves in Cryptography", *Advances in Cryptology--Crypto '85 Proceedings*, Vol. 218 of LNCS, Springer-Verlag, pp 417-426, 1986.

[18] Mambo, M., Usuda, K. and Okamoto, E., "Proxy signatures: Delegation of the power to sign message", *IEICE transactions on fundamentals of electronics, communications and computer sciences*, E79-A, Vol. 9, pp. 1338-1354, 1996.

[19] National Institute of Standards and Technology, "*Digital signature standard*", Technical report, 1994.

[20] Rash, M.C., "Privacy Concerns Hinder Electronic Medical Records", *The Business Journal of the Greater Triad Area*, available at http://www.bizjournals.com/triad/stories/2005/04/04/focus2.html?page=all , 2005

[21] Rivest, R.L., Shamir, A. and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[22] Stallings, W., "*Cryptography and network security: principal and practices*", 6th Edition, Prentice Hall, 2013.

[23] Tsumoto, S., "Mining diagnostic rules from clinical databases using routh sets and medical diagnostic model", *Information Sciences*, Vol. 162, No. 2, pp. 65-80, 2004.

[24] Takeda, H., Matsumura, Y. and Kuwata, S., "Architecture for networked electronic patient record systems", *International Journal of Medical Informatics*, Vol. 60, No. 2, pp. 161-167, 2000.

[25] Um, K. S., Kwak, Y. S., Cho, H. and Kim, I. K., "Development of an HL7 interface engine, based on tree structure and streaming algorithm, for large-size messages which include image data", *Computer Methods and Programs in Biomedicine*, Vol. 80, pp. 126-140, 2005.

[26] Ulieru, M., Hadzic, M. and Chang, E., "Soft computing agents for e-Health in application to the research and control of unknown diseases", *Information Sciences*, Vol. 176, No. 9, pp. 1190-1214, 2006.

[27] Wang, D.W., Liu, D.R. and Chen,Y.C., "A Mechanism to Verify the Integrity of Computer-Based Patient Records", *The Journal of China Association for Medical Informatics*, No. 10, pp. 71-84, 1999.

[28] Yang, Y., Han, X., Bao, F. and Deng, R. H., "A Smart-Card-Enabled Privacy Preserving E-Prescription System", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 8, No. 1, pp. 47-58, 2004.

[29] 丁鎮權,"指紋辨識系統設計",*碩士論文*,淡江大學電機工程學系,台北市,2003 年。

[30] 二代健保,衛生福利部中央健康保險署,http://www.nhi.gov.tw/ ,2014。

[31] 王裕盛,"以平板電腦與健保 IC 卡為基礎之行動醫療資訊系統之研究",*碩士論文*,

立德管理學院應用資訊學系，台南市， 2006。
[32] 王鴻康，“探討電子智慧卡支付系統的採用決定要素與產品組合策略”，*碩士論文*，國立暨南國際大學資訊管理學系，南投縣，2007。
[33] 邱柏盛，“建構一個標準病歷文件整合平台- 以台灣醫療系統為例”，*碩士論文*，逢甲大學資訊電機工程學系在職專班，台中市，2012。
[34] 呂卓勳，“以醫師觀點探討電子病歷系統之效益評估”，*碩士論文*，國立中正大學資訊管理學系，高雄市，2006。
[35] 李依金函，“電子病歷交換與其對醫院績效之前因探討：雲端運算觀點”，*碩士論文*，國立中正大學醫療資訊管理學系，嘉義市，2013。
[36] 吳彥典，“結合浮水印與指紋辨識以提升電子病歷安全”，*碩士論文*，國立高雄應用科技大學電子工程學系，高雄市，2008。
[37] 吳一杰，“一個基於身分認證且沒有連結問題的群體簽章方法”，*碩士論文*，逢甲大學資訊工程學系，台中市，2006。
[38] 林玉玲，“我國電子病歷發展現況與趨勢的調查研究”，*碩士論文*，國立臺灣大學醫療機構管理學系，台北市，2001。
[39] 胡國新，“設計植基於自我驗證公開金鑰系統之安全線上電子拍賣機制”，*碩士論文*，大葉大學資訊管理學系，彰化縣，2000。
[40] 黃履州，“可攜式電子病歷之隱私安全保護措施”，*博士論文*，國立陽明大學醫學工程學系，台北市，2009。
[41] 黃勛隆，“便利商店 IC 儲值卡市場區隔之研究—以統一超 icash 卡為例”，*碩士論文*，國立交通大學經營管理學系，新竹市，2006。
[42] 黃志龍，“使用智慧卡建立複合式安全認證機制”，*碩士論文*，國立成功大學工程科學系專班，台南市，2005。
[43] 黃正心，“擁有撤銷機制的前進式群體簽章系統”，*碩士論文*，國立交通大學資訊科學學系，新竹市，2002。
[44] 陳哲豪，“遠端登入及無線射頻辨識技術下之認證機制”，*碩士論文*，朝陽科技大學資訊管理學系，台中市，2006。
[45] 許加樂，“影響採用電子病歷結合雲端運算跨院交換行為意圖之實證研究”，*碩士論文*，國立勤益科技大學研發科技與資訊管理學系，台中市，2012。
[46] 張勝偉，“指紋特徵合成方法應用於指紋辨識系統之多次按壓建檔程序”，*碩士論文*，國立清華大學電機工程學系，新竹市，2000。
[47] 張雅琦，“探討影響台灣醫院實施電子病歷之因素”，*碩士論文*，亞洲大學健康管理學系，台中市，1999。
[48] 賴郁仁，“指紋辨識改善之研究”，*碩士論文*，東吳大學資訊科學學系，台北市，2008。
[49] 賴溪松、韓亮、張真誠，*近代密碼學及其應用*，旗標出版公司，台北，2004。
[50] 劉建良，“健保 IC 卡與分散式電子病歷系統整合探討”，*碩士論文*，國立暨南國際大

學資訊管理學系，南投縣，2002。
[51] 戴靜瑤，“雲端儲存系統中個人健康紀錄之安全存取控制-使用屬性加密機制”，*碩士論文*，國立交通大學資訊科學與工程學系，新竹市，2013。
[52] HCA 一般問題，醫事憑證管理中心，http://hca.nat.gov.tw/Default.aspx，2014。

附錄一

論文使用參數表

人物名稱	私鑰	公鑰	其他
病人	SK_P	PK_P	$Cert_P$
代理人	SK_A	PK_A	
代理人 Key	SK_{Ap}	PK_{AP}	
健保局	SK_{NHI}	PK_{NHI}	$PCert_P$
醫師	SK_D		IDo
群體簽章	K_D	PK_{GK}	
藥局	SK_{PH}	PK_{PH}	
保險公司	SK_I	PK_I	
病人對健保局提出辦理的要求		R_P	
申請健保的細節項目		Req	
病人的金鑰憑證		$Cert_P$	
流水編號		PID_P	
病人已給付健保費用之相關證明資料		$Data$	
病人的公鑰憑證		$PCert_P$	
醫師的身份		ID_D	
醫師的金鑰憑證		$Cert_D$	
醫師對健保局申請群體簽章的要求		R_D	
病人簽署的近期戳章		TS	
最近幾次診療紀錄		$OtherRC_S$	
此次的診治內容		$NewRC_S$	
處方箋		R_X	
處方箋編號		R_X_ID	
藥單成份內容		MR_S	
診斷證明書		MC_S	
診斷費用相關資料		EP_S	
病人指紋		FS	
電子支付明細		$E\text{-}Payment$	