

設計 IHE 基礎的醫療資訊安全系統：以旅遊業為例**Designing a Medical Information Security System Based on IHE for Tourism****蔡思玟**ssu-wen tsai
長庚大學資管所

B9144047@stmail.cgu.edu.tw

簡伶臻lin-jen jian
長庚大學資管系

B9344226@stmail.cgu.edu.tw

陳少鈞shau-jiun chen
長庚大學醫學系

cooldigi@gmail.com

蔡榮隆rung-lung tsai
長庚大學資管系

rtsai@mail.cgu.edu.tw

摘要

為確保病人隱私權，在跨醫院機構的電子病歷交換時，醫療資訊安全問題不容忽視。然而，資訊技術日新月異，資安的解決方法又層出不窮，致使醫療資訊安全方案無法落實。為達到異質系統間互通性，應要考慮標準化，以及資訊技術的可得性(availability)與可再用性，本論文乃提出一個機制來整合醫療療程(IHE)、資訊技術(Web Services)、及滿足在 PKI 及 SSO 等領域的安全需求。這套機制是以 IHE XDS 系統架構《ebXML 的註冊與儲存庫架構為規範》為基礎，結合 WS Security 去設計一套醫療資訊安全系統架構，並應用至保險資訊系統。使在旅遊時，當意外發生就醫時，臨床醫師即為有正確醫療資訊，使得就醫民眾獲得最高的醫療品質，並且降低醫療錯誤的發生機率。未來希望醫療院所與保險業者合作，使銀髮族及慢性病患得以參加旅遊產業，達到「玩得老，活得快樂」的境界。

關鍵字：IHE、XDS、Web Services**Abstract**

In order to ensure that patient privacy is protected, medical information security issues must be at the forefront when considering exchanging electronic medical records among different medical institutions. However, because the information technology advances very quickly, and new "solutions" in information security appears all the time, it becomes difficult to construct a concrete medical information security project without

being tempted into alternatives. To enhance interoperability among heterogeneous systems, it is important to consider the establishment of standards, the availability of the technology, and the re-usability of these technologies. This paper proposes a mechanism to integrate IHE, Web Services to satisfy the security needs in PKI and SSO. Based on IHE XDS system framework which is deployed in registration and repository functions of ebXML under the WS security constraints, this research also designed a medical information security system for travel and insurance services. When a traveler requires medical attention during a trip, through this system a medical service provider may examine the patient's medical record immediately, thus the quality of medical service may improve while reducing potential medical errors. This system provides a cooperative infrastructure for medical service provider, insurance agent and travel industry. Thus, the seniors and chronic disease patients may travel confidently to enjoy their lives.

Keywords: IHE、XDS、Web Services.**1、前言**

由於時代的變遷，社會風氣的轉變，現代人已不再像以前一樣在同一個地區出生、求學、成家立業甚至於終老一生。現代人往往因為求學、工作的調派、出差...等因素，而離開故鄉去外地生活，加上現代人愈來愈重視精神層面的享受，進而帶動國人從事休閒旅遊活動風氣的盛行，我們可以由統計資料發現去年國人全

年至少從事一次國內旅遊的比例為 87.6%，旅遊活動顯然已成為現代國人生活中不可或缺的一部分。

然而過去在醫療資訊尚未整合的階段，病患在外地或是不熟悉的醫療院所就醫時，往往可能會發生由於醫師不了解病患過去病史而使得診斷錯誤或是用藥錯誤的機率提高；加上病歷尚未共享，而且台灣民眾往往有「多看幾家醫院比較好」的觀念存在，以致於往往病患可能在 A 醫院照過 X 光之後，到 B 醫院又重覆照了一次 X 光，這樣的重覆檢查往往會造成整體醫療成本提高和不必要的醫療浪費；而在急救過程中，時間往往是最重要的關鍵，如何在黃金第一急救時間內做出最正確的急救處理，這往往除了依靠急救人員本身的醫療品質之外，相信如果能擁有更多病患相關醫療資料的話，會對急救處理的判斷上有更大的幫助。

全民健康保險往往只提供民眾最基本的醫療保障，然而現今也有許多保險業者也紛紛推動醫療保險，像是安泰人壽所提出的日額型意外傷害住院醫療保險，以及南山人壽所推出的各種醫療保障專案等等。而當民眾有能力去另外投保其他醫療險，就是希望能補足健保之不足的地方並得到更好的醫療品質，但是這些民眾往往在就醫時並不是完全清楚在那當下是否有其他更好的選擇，而醫師也往往僅會開立健保上所允許的用藥，而不會主動告知民眾有其他更好、更有療效的藥物可供選擇，使得民眾無法得到最好的醫療品質。而本研究希望提出一套機制去對以上幾點做一個改善的動作

在這邊我們可以舉一個案例做為說明：李爺爺為一血管性失智症患者，平常即服用抗血小板凝集藥物做治療，家人也為其投保安泰人壽意外傷害住院醫療險，某一天，李爺爺卻在一次旅遊中出了車禍，急救人員在做急救時因為並不清楚李爺爺的日常服藥習慣，所以在處理上花費了比一般還久的時間去止血，而在醫院時也花費了將近一天的時間在等待空的病房。

如果我們已經使用了一個改善的機制在上述的案例裡的話，急救人員可在第一時間內得知李爺爺的日常服藥習慣，知道他平常有服用抗血小板凝集藥物的習慣，如此一來才可以在最快的時間內對李爺爺做最適當的止血及急救動作，而在醫院內也因為知道李爺爺

有另外保醫療險的部分，保險可給付非健保房的住院費用，所以就不用在花費時間在等待病房上，而醫師也因為了解李爺爺的身體狀況而為其做了最適當的醫療診斷動作，以達更高的醫療品質。

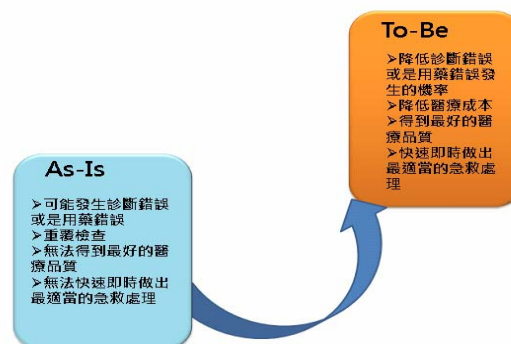


Figure 1 As-Is & To-Be Model

所以本研究以保障個人健康安全為出發點，提出了一個預先註冊機制，希望能結合醫療和保險的概念，達到讓國人在外地生活或是旅遊時也能讓個人健康安全有所保障的目的。

2、文獻探討

下面就本研究所應用到的相關技術做文獻上的探討。

2.1 IHE (Integrating the Healthcare Enterprise)

IHE(Integrating the Healthcare Enterprise)為美國北美放射醫學會(Radiological Society of North America, RSNA)與健康資訊管理系統協會(Health Information and Management Systems Society, HIMSS)於1999 年共同進行的一項為期五年的醫療企業整合測試計畫。目的在於解決醫療產業之軟硬體溝通的問題，以整合軟體與硬體的技術提供流程導向的標準架構，使不同的造影儀器製造商、系統廠商、醫院等彼此間能夠經由一套共通的語言，在現有標準協定的基礎上，根據不同功能的造影儀器在醫療環境中扮演的角色，要求各家廠商開發的各項造影儀器設備與醫療資訊系統間皆提供IHE 之介面，使各項軟硬體於醫療資訊環境中皆能「隨插即用(plug and play)」，並且，希望透過profiles 如工作流程排程機制的導入，使整體業務進行時更為順暢，強調醫療業務之流程最佳化設計，提高效率與效能，最終目的為為病患提供更專業、更有效率及更符合

合成本效益的照護方式[1]。

IHE 推廣組織的版圖已由美國向其他國家擴展，並相繼成立 IHE-Europe(包含德、法、義等等)、IHE-Japan.. 等等，台灣於 2003 年 11 月 8 日在中山科學院 IHE 研究團隊與 HL7-Taiwan、DICOM- Taiwan 等學會組織的共同合作下成立 IHE-Taiwan。

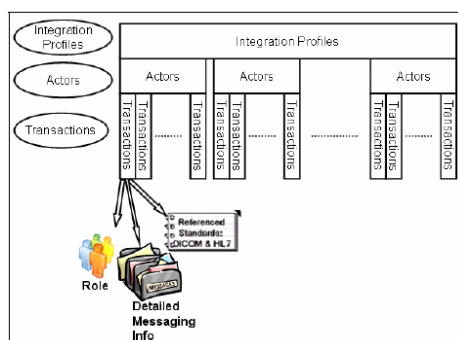


Figure 2 IHE 技術架構[7]

Figure 2 為 IHE 技術架構示意圖，分為三大層次，分別為[7]：

(1) Transactions：

為基本的資料存取模型，使用 DICOM 以及 HL7 等通用的醫療資訊交換標準，整合呈現出如病人、就診、醫囑...等的醫療相關資料。

(2) Actors：

提供既有系統一個通用性並且不侷限於特定產品的機器溝通介面，Actors 可以提供並且相互交換資料，並且，Actors 甚至可以整合多個既有系統形成一個完整的服務，對外開放。

(3) Integration Profile：

一個組織內的醫療資訊相關功能常分散在不同的系統中，要完成一組完整的醫療資訊服務工作，需要整合多個分散的功能，亦即需要多個 Actors 讀取 Transactions 層次的資料。在此，IHE 提出 profile 的概念，針對不同的醫療資訊服務行為，訂出不同的 profile，如此，實際需要執行服務時，僅需要依據 profile 與各個相關的 Actors 逐一互動，便可完成任務。

雖然 IHE 著重於醫療器材之間的軟硬體的配合互動，由於一個組織內的資訊互動可視為跨機構環境的縮影，IHE 提出的概念，在完成了機構內的資訊交換整合後，將可拓展至醫事機構間的資訊交換[5]。

2.1.1 IHE XDS (Cross-Enterprise Clinical Documents Sharing)

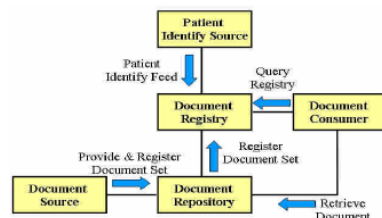


Figure 3 XDS 架構圖

IHE XDS (Cross-Enterprise Clinical Documents Sharing) 是其中一個 Integration Profile，目的在協助 IHE 進行整合時更容易達到分享跨醫療院所的電子臨床病歷 (electronic clinical documents)，並且能夠保留原來的病歷內容及文件架構。由下列 actor 組成：

(1) Document Source：產生和發佈臨床文件的單位，可以視為系統間任一資訊交換機構。

(2) Document Repository：永久儲存一份文件的單位。

(3) Document Registry：管理每一份已經註冊的臨床文件其 metadata，包含每份臨床文件的儲存庫連結位置資訊。

(4) Document Consumer：相當於 Client，向 Registry 執行查詢醫療資訊工作，可以視為系統間任一資訊交換機構。

(5) Patient Identify Source：提供每一位病人的唯一 identifier，並且維護一些人口統計資料以及加快病人在 Registry 的驗證。

它主要的重心是放在提供一個標準基礎的規範讓我們可以管理醫療院所 (healthcare enterprises) 間分享的病歷，並使醫療院所快速的分享電子病歷[6]。

2.2 Web Services

Web Services 是以 SOAP、XML 與 HTTP 為基礎而發展的技術，在運作程序上，應用軟體可以透過網際網路尋找並連結其他的服務，並且是一個去中心化(decentralized)、鬆散的關聯結構(loosely coupled)與協同作用的網路建構模式。在 Web services 的架構中，有服務提供者(Service Provider)、服務要求者(Service Requester)、與服務登錄(Registry)資料庫等三種基本角色而形成市場運作機制[5]。其運作關係如 Figure 4 所示：

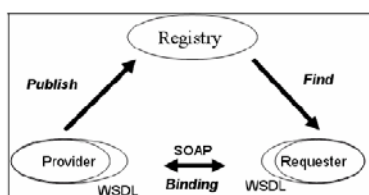


Figure 4 Web Service 三種角色關係圖

(1)服務提供者(service provider)：

負責提供服務讓要求者使用，透過WSDL 描述該服務的功能。WSDL 是為Web Services 的介面定義語言(IDL)。當服務提供者欲對外公佈其提供之Web Services，必須以WSDL 來建置描述檔案，描述內容包括：伺服器所提供的各種Web Services、在個別Web Service上可進行的諸多Operations、傳輸協定、參數定義...等。

(2)服務登錄資料庫(service registry)：

即UDDI，讓服務提供者能將服務內容公告出來，並讓服務要求者能找到該服務。

(3)服務要求者(service requester)：

服務要求者先送SOAP 訊息傳遞查詢指令給UDDI 登錄資料，之後根據查詢到的服務提供者資訊獲得需要的服務。

2.2.1 Security Assertion Markup Language (SAML)

以網際網路為基礎的協同合作時代，一個終端要求者所要求的資料往往可能擷取自許多不同的服務，在資訊安全議題的考量下，各個服務必須要經過「登入」

(Sign-On)的程序，如果每到了一個服務，必須由使用者親自登入一次，這樣的作法耗時費力，勢必降低使用者的使用意願。另一方面，各個服務的帳號管理系統無法一致，同一個使用者在不同的服務實體中的帳號不盡相同，凡此種種，造成了 SOA 中登入動作的困難度。如果將帳號密碼直接存放在訊息內，必須承擔相當大的風險，尤其許多駭客的攻擊方式[4]都是以此為出發點。因此，本研究引進了 SAML，透過類似「換證」的機制，將取得的通行證(assertion)加掛在訊息表頭，經過的每一個服務，僅需查驗該通行證，便可決定是否放行。因此而達到單一簽入(Single-Sign-On, SSO)的目的[5]。

Figure 5 是為 SAML 運作循序圖，使用者 U 的目的地是 D 網站，但是使用者先到認證網站 S 登入，S 儲存資訊後，回應一的通行證(assertion)給瀏覽器 B，並要求 B 轉址(redirect)到 D 網站，D 網站遇到有一個使用者要進入，D 取得了 assertion 後，詢問 S 網站，是否已經過登入程序，若為已登入，則允許 U 進入取得服務。

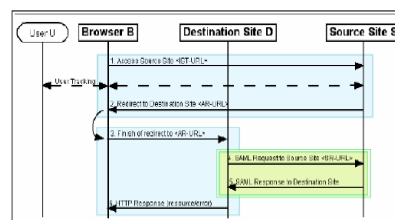


Figure 5 SAML 運作架構[8]

3、研究方法

3.1 系統概念

根據前面所描述到的情節，我們規劃了一個預先註冊機制的系統概念(如 Figure 6)，將個人以往就醫紀錄以及所投保之相關醫療險的部分儲存起來。當民眾在外地發生意外事故時(如旅遊意外)，在送到當地醫院急診時，可藉由健保 IC 卡去辨別民眾身份，並透過健保 IC 卡在我們預先註冊機制中得知病患相關病歷資料和所投保醫療險中關於用藥給付的部分。

在病歷資料的部分包含了病患就醫紀錄，記錄著病患所曾就醫的醫療院所資料，方便當地醫師可以快速調

閱病患的相關病歷資料；也包含了病患可能和意外發生有關的資料，例如病患是否有腦血管方面的疾病？是腦出血還是腦阻塞？這二者所用的治療方式大不相同，用藥不小心很可能造成二度意外發生，而這份資料可以幫助醫師在第一時間內對病患做出最適當的意外處理。

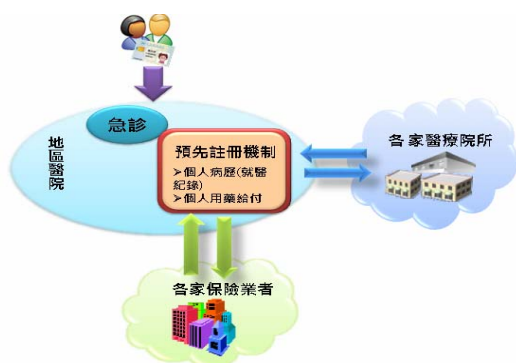


Figure 6 系統概念圖

另外在用藥給付的部分，則是紀錄病患所投保的醫療險中在用藥的部分所負責給付的範圍。因為一般在無特殊保險只有健保的情形下，醫師所開的用藥都是在一般正常健保所規定的標準內，像是住院時的病房，在一般情形之下都是住健保房(三到六人一間房間)，健保房大部分情況下都要排隊等候空房，但是如果投保其他醫療險的話，醫師就可透過系統中所顯示的用藥給付資訊中，告知病患在保險給付的範圍內另有其他病房選擇供病患做參考，同樣地，除了病房之外，在用藥部分，由於更高級的藥品，健保是不予給付，而是要病患自行負擔的，所以大部分醫師在開藥時都以健保給付為標準去開藥，除非病人的病情無法使用在健保給付範圍內的藥品，醫師才會再去開立其他需要病患自行負擔的藥品給病患。而醫師可透過此機制，去得知有那些更好的藥品是在病人所投保其他保險中所能負責的範圍，而去主動告訴病患另外的選擇，以供病患做最好的用藥選擇。

3.2 系統架構設計

本論文在系統架構設計的部分，根據前面所提出的 Business Model，以 ebXML 的註冊與儲存庫架構為規範的 IHE XDS 系統架構[2](如 Figure 7)為基礎，設計一套結合醫療及保險業者的系統架構(如 Figure 8)。

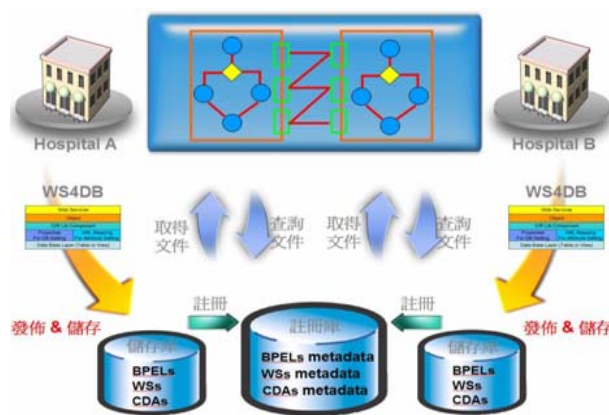


Figure 7 IHE XDS 系統架構[2]

醫院的病歷資料會透過 Web Services 發佈並儲存在儲存庫中，同樣地，保險業者也會將客戶關於醫療險部分的資料透過 Web Services 的方式發佈並儲存在儲存庫中，而註冊庫則是定義這些資料的相關屬性資訊，以協助這些資料的搜尋。希望醫師能透過預先註冊機制去查詢並取得病患相關醫療資料，以供醫師在診斷用藥上的參考。

而在預先註冊機制的部分，我們強調 One-Step 功能，民眾只要在預先註冊機制下做註冊的動作就好，而醫院即可透過此機制在民眾就醫時配合健保 IC 卡去查詢並取得病患相關醫療資料。

在資訊安全部分，我們除了結合健保 IC 卡，醫師才能做病患相關資料的存取之外，我們還採用 WS-Security 來解決 Web Services 安全性的問題，除了 WS-Security 基本的加密簽章機制之外，並參考前面 2.2.1 小節所提到的 SAML 標準來完成本研究對於 Web Services 的安全性需求。

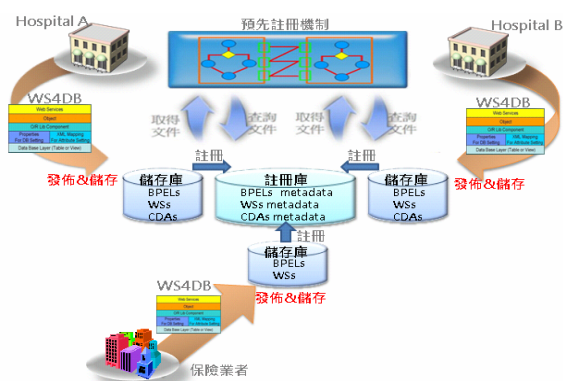


Figure 8 系統架構

3.3 系統實施的困難性與障礙

本論文所提出的預先註冊機制主要是結合醫療院所以及保險業者，而在這裡我們面臨到了一些問題：

- 1.如何取得醫療院所以及保險業者的合作和信任，讓病患獲得最佳的醫療品質以及最適當的保險給付。
- 2.如何使各醫療院所間彼此信任並交換彼此的病歷資料，使得醫師能夠完整掌握病患的身體狀況，降低醫療疏失的發生機率。
- 3.如何得到民眾的信任並讓民眾使用這套系統，且使其系統達到普及化。

從以上的問題中，我們可以發現這些都不是技術方面的問題，而是人為上的問題，如政策的關係甚至是利益上的關係，所以我們需要一個強而有力且足以讓大家都信任的機構來推動執行，如政府單位的大力推動；並希望能和旅遊產業做結合達到系統普及化。

4、結論

由於現代人的生活水準提升，生活習慣已和以前有很大的改變，雖然老化，依然外出旅行，達到「玩的老，活的快樂」的境界。資訊技術日新月異，異質醫療資訊系統間互通，使只在一處就醫習慣也改變，加上保險業為爭取客戶，提昇顧客滿意，乃日新月異推出的吸引人的醫療旅遊險。本研究基於保障個人健康安全為出發點，提出一個結合醫療及保險的預先註冊機制，希望可以使得就醫民眾獲得最高的醫療品質，並且降低醫療錯誤的發生機率。

這套預先註冊機制以 ebXML 的註冊與儲存庫架構為規範的 IHE XDS 系統架構為背後資料處理的基礎，希望透過此概念去達到病歷共享以及結合保險的功能，使得民眾在不熟悉的地區醫院內就診時，也可以讓醫師清楚病患的身體狀況、用藥習慣以及在醫療上保險所給付的部分，以供醫師做診斷上以及開藥時的參考。希望能夠透過這套機制達到降低診斷錯誤或是用藥錯誤發生的機率、降低醫療成本、快速做出最適當的急救處理以及得到最好的醫療品質。

未來希望能真正和醫療院所以及保險業者做實質上的合作，也希望可以將這個機制結合旅遊產業去做一個推廣的動作，以擴大民眾的使用率。並希望在安全議題的部分再做加強，達到病患資料保密以及保護個人隱私權。

參考文獻

- [1] 林怡君，What is IHE??何謂 IHE??，HL7 Taiwan IHE SIG，2003，
“<http://www.hl7.org.tw/viewforum.php?f=18>”
- [2] 陳威成、鄭心瑀、蔡榮隆，“The Design of A Interoperable Collaboration Process Architecture for Heterogeneous Healthcare System based on the IHE XDS”，MIST 2005 國際醫學資訊研討會，2005
- [3] 黃登揚，“以 IHE 為基礎設計個人健康資訊整合平台”，長庚大學資訊管理研究所碩士論文，2005
- [4] 黃景彰，“資訊安全-電子商務之基礎”，華泰文化事業公司，2001
- [5] 劉益成，“保障隱私的醫療資訊安全機制設計”，長庚大學資訊管理研究所碩士論文，2004
- [6] 鄭心瑀、吳昱儀、陳少鈞、蔡榮隆，“以物件導向概念設計長期照護系統-以腦中風病人為例 The Design of Integrated Long-Term Care Information System based on the Object-Oriented Technology- Using Stroke as Example”，第十七屆物件導向技術及應用研討會，九月，2006。
- [7] Christopher D. Carr, Stephen M. Moore, "IHE :a model for driving adapton of standard", Computerized Medical Imaging and Graphics 27, 2003
- [8] Thomas Gros, "Security Analysis of the SAML Single Sign-on Browser/Artifact Profile", 19th Annual Computer Security Applications Conference, 2003