個人化電子病歷之權限控管

施岳勳 Yueh-Hsun Shih[a]、連中岳 Chung-Yueh Lien[a]、朱唯勤 Woei-Chyn Chu[a]、
蕭嘉宏 Chia-Hung Hsiao[b*]、陳長輝 Wesley Chen[c]

[a] 國立陽明大學醫學工程研究所
[b] 慈濟大學醫學資訊學系
[c] 赫連網路股份有限公司

[*]通訊作者：蕭嘉宏Chia-Hung Hsiao, chhsiao@ym.edu.tw

摘要

本研究根據個人健康記錄(personal health records，簡稱 PHR)的概念為基礎，利用網際網路普及性，讓醫療人員、病患以及其他相關人員得以透過網路，登錄至網頁平台，即可以瀏覽相關病歷資訊。在高度透明化的網際網路環境下，任何人皆可以透過網路，進入個人健康紀錄平台瀏覽所需資訊。如何有效的管控人員是否有權限瀏覽平台內的資訊、保護使用者重要的隱私安全，為本研究重點所在。

關鍵字：personal health records、個人健康紀錄、權限管理

1、緒論

1.1 研究背景

台灣現行的醫療制度，是將民眾就診的病歷資料存放在各別的醫療院所的病歷系統中，若是病患下次就診前往不同醫院時，則病患的就醫記錄與病歷將會在新的醫院重新被建立。因此，個人的就診紀錄分散在各大醫療院所而無法有效的串聯，病歷資訊不能整合，因此無法詳細記載個人病史，這種儲存病歷的模式稱為「以醫院為基礎(hospital-based)」的病歷儲存方式。這種模式的病歷儲存方式，醫生僅有醫院內所儲存的病患資訊，在沒有充分的個人病史資訊下，診斷前來就診的病患。另外，病患可能在缺乏足夠的醫療知識下，做出「逛醫院(hospital shopping)」的行為。因此，在醫療資訊不對等的情況下，民眾自覺無法獲得預期之結果或顯著之改善，轉而求助於其他之醫療方式所形成醫療資源的浪費。

另外一種儲存病歷的方式稱為「以病患為基礎(patient-based)」的病歷儲存方式，其作法是此以病患為導向，有關所有病患的病歷都集中儲存，或是病患為搜尋的關鍵藉此找到資料。例如：病歷索引中心，或是病患自行管理。無論病患到任何一家醫院看診，透過web-based系統瀏覽病歷。這種病歷隨著病患帶著走(carry-to-go)的想法便是個人健康記錄(personal health records，簡稱PHR)的概念。

關於病患的健康資訊通常在醫院或診所本地建檔後，得向醫事人員輸入相關訊息以及各項檢查資料後，儲存於在本地資料庫中。由於安全機制的考量，設計上僅限於院內區域網路(region network)使用。若是資訊需要跨院交換時，例如：轉診或轉檢，病患必須再一次描述病史、重複檢驗。不僅麻煩、費時、更浪費醫療資源。因此如何有效率的使用個人的健康資訊用於跨院的資料共享上，成為未來健康管理的一個重要議題。另一方面，國內醫療體系逐漸往社區醫療群制度的發展，醫院之間互動及醫療資源之整合顯得格外重要，電子病歷交換也成為趨勢。現行醫療作業環境下，許多實際的需求(醫療保險、轉診及轉檢等)以及先進的應用(遠距會診、網路學習、行動醫療等)皆有病歷交換的需求。

1.2 研究目的

透過建置個人健康紀錄(personal health records、簡稱PHR)平台的應用，讓使用者得以掌握自身的健康資訊，提升健康資訊的可攜性。另一方面，建立完善的權限控管機制，依照需求設定不同角色瀏覽此病歷的權限。在我們的系統當中建置一包含各醫院樹狀組織結構的入口網站，因此病歷擁有者可設定樹狀結構當中醫護人員瀏覽此病歷的權限。近年來政府致力推行病歷資訊化，於未來，使用者擁有自身之電子病歷為主要趨勢，故有效的權限管控機制發展相對重要，需要加以嚴格控管 如Figure 1所示，以維護使用者隱私保密。

本研究計畫，目的在於建置完善個人健康記錄(PHR)整合平台，結合病患疾病資訊、權限管控機制、以及病歷儲存系統，作為日後個人使用。

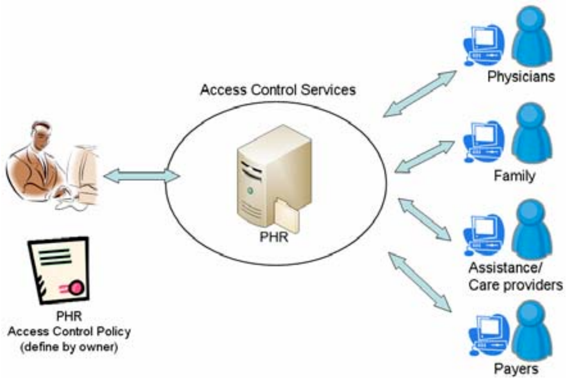

Figure 1 個人健康記錄管理系統（PHR） 應用示意圖

2、文獻探討

2.1 個人健康記錄概念

個人健康記錄(personal health records，簡稱 PHR)中，主旨為提供「以人為本(patient-orientation)」的健康資訊平台，使用者得以自行編輯相關資訊。包含基本資料、症狀描述、健康紀錄、檢驗結果與診斷資料，並給予其他人員對於此病歷資訊是否有行使動作的權限。引用 Markle 基金會報告中提到 PHR 的定義為：

”An electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment.” [1]

由上述可知，於實現個人健康紀錄應用平台，最重要的必需因素有三：「隱私」、「安全」、「共享」。從 1994 開始，美國哈佛大學、MIT 與波士頓兒童醫院合作，開始全球第一個個人病歷管理系統(Personal Internetworked Notary and Guardian，簡稱 PING)的開放平台[2]，以此作為開端。

個人健康記錄，其歸納特點如下：

1、 節省醫療資源運用：

當醫生為病患診斷時，若需要的檢驗資料於健康記錄中已經存有紀錄，則醫生可以依照其資料是否合適用於目前症狀診斷，決定參考或是重新檢驗，避免重覆檢查，節省醫療資源。

2、 紀錄病患生涯病程：

讓醫療人員得以徹底了解病患，對於病患有足夠疾病知識背景以後，方能達到準確的診斷，提升疾病的治癒率。

3、 以網際網路為基礎(web-base)：

不管病人在何處就醫，亦或是醫生、病人以及其他健康照護者都可以便利地透過網際網路，存取個人健康記錄。

2.2 Role-Base Access Control

Role-Based Access Control（簡稱 RBAC）[3, 4]，是本研究使用權限控管之基礎概念。根據 RBAC 中，權限之於角色、角色之於使用者之架構。 RBAC 主要有三種元素，使用者(User)、角色(Roles)、及權限(Permissions)。在不同系統或體制下，其規範決定且制定一角色所擁有的可行使之權力。權限之於角色、角色之於使用者之架構如 Figure 2 所示。

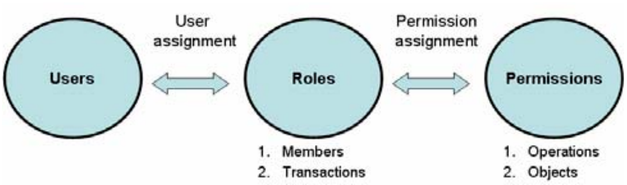

Figure 2 RBAC 架構圖

RBAC 擁有以下之特性：

1、 簡單以及容易管理：

當系統或體制下，制定出一套關於權限政策後，只需要一次設定角色所對應的權限內容，即可管理所有對應其角色之人員的權限。

2、容易改變、有彈性：

當一個角色的權限有所改變時，僅需要更改其角色的權限內容，其相對應的人員權限將同時一併更改。另一方面，當人員的權限有需要改變時，僅需將其設定至相對應權限的角色下即可。

3、可延伸的：

在成長中的系統或體制下，當有新的權利政策產生時，只需新增新的角色即可，不需要將所有權限重新設定，隨著政策的制定，依循的成長角色的數量，增加權限管理的範圍。

3、研究方法

3.1 架構說明

本論文研究權限控管採用階層式架構，以此定義並存取不同醫療院所規範中所制定的人員以及對應的權限，如 Figure 3、4 所示。

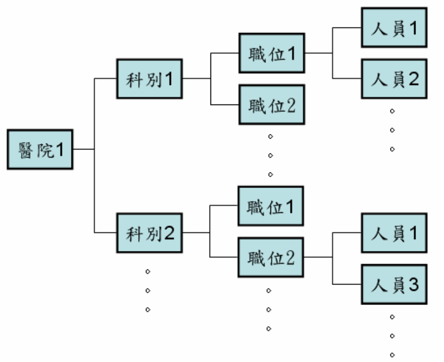

Figure 3 人員 階層架構圖

由 Figure 3 所表現之意義，人員 1、2 擁有在「醫院 1」裡的「科別 1」底下的「職位 1」的執行權限。故人員 1、2 於系統中，則以「醫院 1➔科別 1➔職位 1」代表其權限並存取。另一方面，人員 1 同時也擁有「醫院 1➔科別 2➔職位 2」的執行權限。所以，人員 1 得以允許兩項權限所能執行的功能。

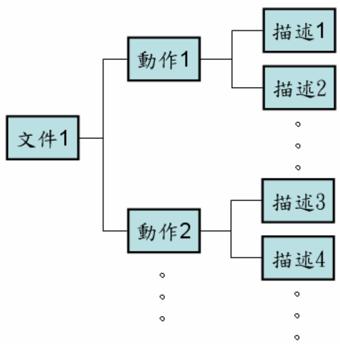

Figure 4 可執行權限 階層架構圖

由 Figure 4 所表現之意義，資料庫將記載，允許哪些群組或是人員在「文件 1」中可執行的動作。「描述」所記載的，是允許執行的人員或是群組的樹狀路徑，以方便人員欲動作時可以提供對照的機制。

3.2 使用情境

使用者登錄個人健康紀錄伺服器後，欲瀏覽屬於其他人的健康紀錄時，將會有一請求至伺服器中的 Web Service，驗證是否有其權力執行使用者欲做的動作，如 Figure 5 說明：

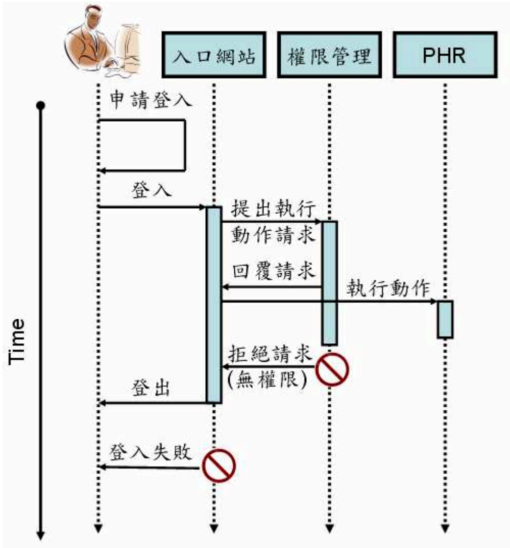

Figure 5 時序圖

3.3 資料庫說明

3.3.1 建立人員階層樹

建立時，需要三個資料表如 Figure 6 所示。

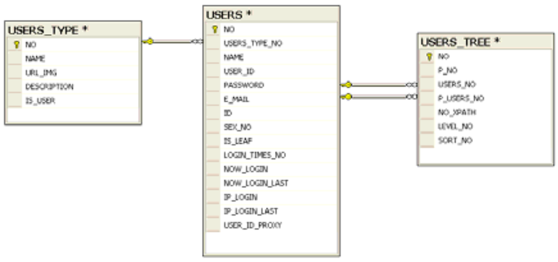

Figure 6 階層樹所需資料表

USERS Table：

將各醫院、科別、職位、人員…等，每一項目依照不同規定所對應之角色，存入此資料表中，不同的階層定義於 USER_TYPE Table，給予 USERS 每一欄位所對應的階層說明。

USERS_TYPE Table：

依照 USERS Table 中不同項目所扮演的角色，定義出不同階層分類。譬如：系統管理者、醫院、科別、職位、人員…等等。

USERS_TREE Table：

主要紀錄醫院或是網站中的階層政策，以樹狀結構方式存於此資料表中。其中 NO_XPATH 紀錄到此子節點之前，所經過的父節點的紀錄(其格式為 NO1-NO2-….)，方便驗證時比對權力是否符合。呈現方式如 Figure 7：

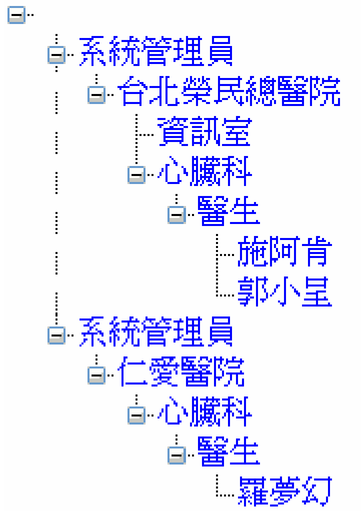

Figure 7 以樹狀結構呈現階層權限分布

若人員擁有不同身分，則將其加入至所對應身分節點下即可。

建立人員階層樹時，限制條件如下：

1、若節點為人員則必規定為子節點，不能變成其他節點的父節點。

2、A 群組若互為另一 B 群組的子節點時，則規定不能再為其子節點。

3.3.2 建立文件權力樹

建立時，需要四個資料表如 Figure 8 所示。

Figure 8 權力樹所需之資料表

RECORDS Table：

給予紀錄、附件各一主要索引欄位 NO，於資料庫中建立節點並儲存於伺服器中相對位置。

ACTIONS Table：

制訂使用者得以動作的選項。

參考 PING，其項目有：

1、新增紀錄

2、讀取紀錄

3、查詢紀錄

4、修改紀錄

5、刪除紀錄

6、新增、更新、刪除紀錄中的附件

RECORDS_TREE Table：

依照 ACTIONS Table 中的動作為父節點，為每個文件儲存同意有權使用，或是符合身分的使用者或群組為子節點，建立每一紀錄所擁有的權力樹。

存取方法有二種：

1、若同意有權使用或符合身分為指定的群組時，此資料表中在 USERS_NO_XPATH 欄位內，儲存此群組對

應到 USERS_TREE Table 的 NO_XPATH 欄位，此時 USERS_NO 欄位為設為 null。

2、若同意有權使用或符合身分為一人員時，在每個資料表中 USERS_NO 欄位中儲存此群組對應到 USERS Table 欄位中，表示此使用者的 NO，而 USERS_NO_XPATH 為 null。

RECORDS_TYPE Table：

說明不同紀錄所屬的屬性，譬如：DICOM、病歷、ECG…等等。

3.4 權力樹初始值建立

使用狀況分為二種：

1、若為個人健康紀錄網路平台使用，使用者建立紀錄後，一開始沒有權力樹初始，等到紀錄擁有者同意給哪位角色執行所同意的動作後，才有權力樹的產生。

2、若為醫院使用，不同的科別建立的紀錄，則根據不同醫院內部擁有之規定，以此制定相關模組。此模組由另一樹狀結構存取，建立其紀錄最初的權力樹。

3.5 驗證流程

當使用者欲對於紀錄執行動作時，其驗證流程如 Figure 9 所示。

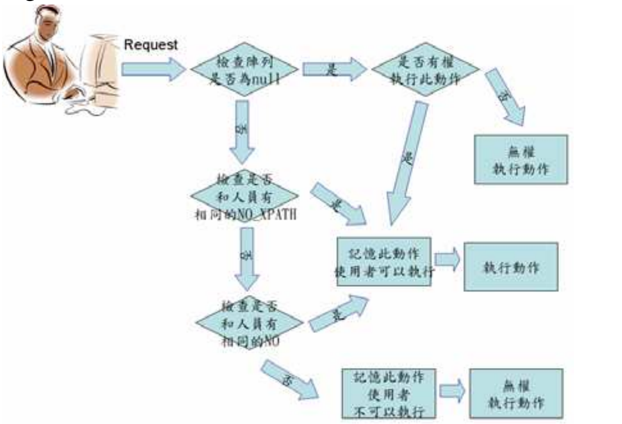

Figure 9 驗證流程圖

由上圖所示，當使用者瀏覽紀錄的同時，為了提升效率，當使用者選擇一動作執行時，將會記憶使用者對於此一紀錄的動作權力，離開後馬上清除。

若檢查尚無記憶說明使用者是否有權力執行此動作時，在驗證過程分成二種：

1、人員是否屬於在指定中有權力執行的群組裡。

2、人員是否被單一認定得以行使其動作之權力 。

如 Figure 10、11 所示。

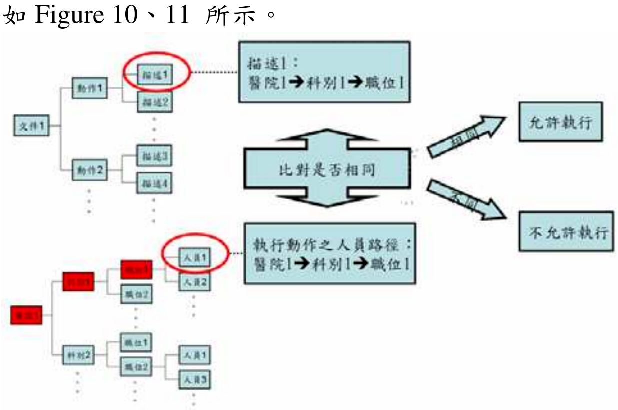

Figure 10 驗證人員是否屬於在有權力執行的群組

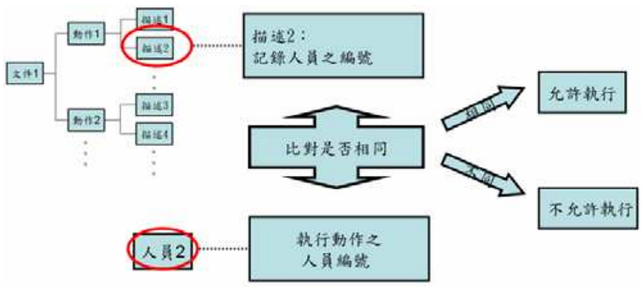

Figure 11 人員是否單一認定得以行使其動作之權力

經過此兩樣驗證後，人員方能依照結果，在文件中執行欲執行之動作。

4、討論

近年來提倡醫療行動化，讓使用者得以「無時無刻、無所不在(ubiquitous)」的完善醫療照護，並且隨著民眾醫療意識的增長，其自身健康資訊不僅僅只限於醫療人員，也有了解自身健康的權力。西元2005年，美國總統布希發表聲明，希望在10年內，要讓大部分的美國人都有電子健康紀錄。由此可見，個人健康紀錄(PHR)儼然成為未來趨勢所向。[5]

透過網際網路進入個人健康紀錄平台，如何有效保護使用者的隱私、並且可以有效控制其他人員的權限，為主要課題。在醫療院所裡，複雜的權限政策下，難以制定一套有效的權限控管的方法。本研究利用 Role-base Access Control 模組，制定權限管控方法。利用歸納出的權限政策，簡化複雜的政策內容，將權限管理權給予建立此病歷的主治醫生或是病患，以符合 PHR 的精神[1]，並以相對於不同階層的職位定義不同角色(Roles)的權力，再依照使用者(Users)所屬不同分配所屬的角色。除此之外，管理者得以依照政策所需求，新增、更改、刪除角色的定義，讓此權限控管機制得以靈活應用，提供所需要的要求，讓此權限控管日漸成長、完善。

5、結論

本研究提出個人健康紀錄平台之權限控管，為使用者之個人資料於高度透明化的網際網路中，保護其重要隱私，為此平台之第一防線。在現行醫學資訊安全的規範當中已包含身分驗證、傳輸加密、以及文件的電子簽章(參考 IHE IT Infrastructure) ，本研究之權限控管機制有潛力與 IHE 所提之安全機制搭配應用。 整個安全控管並可配合 IHE XDS 之病例儲存交和機制，建構一安全且便利之網路病歷使用機制，以利病患基本資料、疾病歷史、檢驗資料、以及醫學影像能透過網路方便地在不同醫療機構使用，作為日後行動化醫療的一個參考。期望於本實作測試完成後，將此權限控管機制延伸至醫療院所，解決更複雜的權利政策問題。

參考文獻

[1] Connecting for health: The personal health working group final report. 2003.

[2] W.W. Simons.,K.D. Mandl, and I.S. Kohan,”The PING personally controlled electronic medical record system: technical architecture.” The American Medical Informatics Association vol. 12,

Num. 1 Jan/Feb 2005.
[3] D.Ferraiolo,and R.Kuhn,”Role-Based Access Control.” 15th National Computer Security Conference, 1992.
[4] R.Sandhu, D.Ferraiolo,and R.Kuhn, “The NIST Model for Role-Based Access Control Towards A Unfied Standard.”,
[5] [cited; HSS News].Available from: http://www.hhs.gov/news/press/2005pres/20050606.html.