電子病歷之真確性保護機制

黃景彰
長庚大學資訊管理學系

周淑羚
長庚大學資訊管理學系

葉怡鎮
交通大學資訊管理研究所

蔡榮隆
長庚大學資訊管理學系

摘要

在本文中，我們以傳統病歷具有的循序記錄、檢驗記錄逐件加入的特性為基礎，以系統流程的角度思考，設計適用於電子病歷的漸增式複合式文件架構，並依此架構發展出真確性保護機制。本文提出的真確性保護機制是以新增單元文件為常態，只須對新增的單元文件計算檢查碼，並用以更新文件整體的檢查碼，原有眾多單元文件的檢查碼不需要重新計算，因而能有效率地更新複合式電子病歷的檢查碼，以進行真確性的維護與查驗。利用本研究所提出之複合式電子病歷架構與真確性保護方法，除了能保護電子病歷文件的真確性外，同時也能確保病歷中關於診斷流程先後順序的真確性，可以避免病歷資料遭到未經授權的變更，進而達到提升醫療品質的目的。

關鍵字：複合式文件、電子病歷、資訊真確性、真確性檢查碼

Protecting information integrity for electronic patient record

Jing-Jang Hwang
Department of Information Management, Chang Gung University

Shu-Ling Chou
Department of Information Management, Chang Gung University

Yi-Jen Yeh
Institute of Information Management, National Chiao Tung University

Ron-Lon Tsai
Department of Information Management, Chang Gung University

Abstract

We present a compound-document model for structuring the electronic patient records, based on the current practices of collecting the paper-form patient records in a hospital. We further devise a method for protecting information integrity to utilize the structural feature of the compound-document model. Through the the proposed compound-document model and integrity protection method, medical institutions can maintain document with integrity inspections more efficiently and thereby enhance the quality of medical care.

Keywords: Compound document; Electronic patient record; Information integrity; Integrity checking code.

壹、前言

病歷記錄為醫療照護過程中所產生的重要資訊，其內容包含病人之個人資訊、診療記錄與檢驗資料等，使之成為實行各項醫療行為的基礎，因此病歷記錄的好壞將會影響醫療照護的品質。隨著醫療資訊系統的發展，傳統紙本形式的病歷記錄逐漸被數位形式的電子病歷所取代(Smith & Eloff 1999)，藉由醫療資訊系統與電子病歷的相互輔助，達成縮減病患就醫時間、降低儲存成本與增進醫療資訊交換與共享的效率等功用，進而提升醫療照護的品質(Kaihara 1998)。除了院內醫療品質的提升外，電子病歷以網際網路作為傳輸媒介，將可突破時間與空間的限制，促進醫療機構間資訊交流與整合機會，使得跨院性的醫療照護行為得以有效率的進行，而對管理人員與研究人員來說，數位化的病歷記錄也可以減低資料收集與分析的困難，增進管理與研究工作的效率。

雖然電子病歷具有多項優點，但由於所記錄的資訊涉及使用者隱私以及重要的醫療資訊，加上數位化的資料型態與網路的開放環境，致使電子病歷有安全上的疑慮，一旦遭到盜用、竄改或是發生錯誤，將會造成病人與醫療院所的損失，甚至危及病人的生命安全。因此，電子病歷的醫療資訊安全議題便陸續浮現，而相關的研究文獻對此議題也多所著墨。藉由文獻整理得知，電子病歷的資訊安全應考量下列因素(Bakker et al. 2000; Haak et al. 2003; Barber 1998)：

(1) 機密性(Confidentiality)

(2) 真確性(Integrity)

(3) 鑑別性(Authentication)

(4) 應負責任性(Accountability)

(5) 可用性(Availability)

在這些資訊安全議題當中，電子病歷的真確性相對的重要。所謂的真確性表示資料具有真品性(Authenticity)及正確性(Correctness)，且資料未遭到未經授權的破壞，一旦真確性被破壞，即表示病歷內容遭到變更，其結果將使得病人受到錯誤的醫療照護，小則輕傷重則死亡(Barber 1998; West Midlands Regional Health Authority 1992)，有鑑於此，我們必須對電子病歷之真確性進行妥善的保護，以維護醫療照護的品質。

進一步檢視目前紙本形式的病歷記錄，可以發現傳統的病歷資料是循序記錄每次就醫記錄，而相關的檢驗記錄亦逐件加入病歷資料中，形成以病人為核心的完整病歷記錄，所以在設計電子病歷架構時必須將循序增加單元文件與可逐步擴展的特性納入考量，才能符合醫療與管理上的需求。因此，本文的目的即在探討傳統病歷記錄的特性，以系統流程的角度思考，配合文件可逐漸擴展的特性為基礎，設計適用於電子病歷的複合式文件架構，並依此架構發展出真確性保護機制。本文提出的真確性保護機

制是以新增單元文件為常態，只須對新增的單元文件計算檢查碼，並用以更新文件整體的檢查碼，原有眾多單元文件的檢查碼不需要重新計算，因而能更有效率地更新複合式電子病歷的檢查碼，進而完成真確性的保護，避免病歷資料遭到未經授權的變更，以達到維護醫療品質的目的。

貳、文獻探討

一、電子病歷具有複合式文件的特性

複合式文件(W3C 2005)有別於一般常見的文件格式，能夠在一份文件中儲存其它應用程式所產生的物件；此處所稱的物件，泛指在軟體設計的概念中，描述特定功能的一段可獨立運作之程式或程式產生的結果；並依需求不斷地增加文件內容，而這些物件仍可被原始的應用程式處理、更新。常見的應用如以 Microsoft Office Word 應用程式來製作報告，並在報告中插入由 Excel 所產生的數據、圖表；另外，廣泛應用於全球資訊網路的 HTML（Hypertext Markup Language）文件也是一個典型的例子。

複合式文件可組成不同的文件架構，如 XML 文件的階層式架構或是超連結文件的索引式架構，以因應不同的需求，除此之外複合式文件還具有可擴展性，以及可儲存多個不同格式的其他物件等特性，所以我們亦可將一份複合式文件看作具有多個從屬子物件的大型物件，而組成一份複合式文件的個別子物件，則可具有不同的產生來源或分屬不同的使用者。由此，可以複合式文件之概念實現的應用不勝枚舉，一個典型且成功的複合式文件的應用例子即為 eCheck 電子支票系統(Anderson 1998)。

由於傳統病歷具有以下的特性：一份病歷內的每一部份均具有相關性、病歷記錄循序增加新的文件或資訊、病歷內容可不斷增加、以病人為主軸等，在本質上與複合式文件完全相同，因此可利用複合式文件的概念，設計符合傳統管理與操作需求的電子病歷。

二、電子病歷之真確性議題

資料真確性具有兩項意涵，即資料的正確性與資料的真品性(黃景彰 2001)。資料的正確性是指資料必須是正確而且是沒有錯誤的，而資料的傳輸與處理也必須預防過程中有所遺漏；資料的真品性則是指資料的產生必須是正當的、經過授權的、不是造假的，而資料的傳輸必須有合法的來源，不是惡意的重複傳送。因此，真確性保護機制必須要能克服國際標準 ISO/IEC 10181-6 所定義的五項破壞資料真確性的操作(ISO/IEC 1996)，包括未經授權的資料修改、未經授權的資料刪除、未經授權的資料創造、未經授權的資料增加與未經授權的資料重複使用。除了一般的資料真確性保護，加拿大醫療研究文獻對於電子病歷的真確性保護做了下列的詮釋(CPSA 2004)：

(1) 電子病歷內的診療內容資料之真確性必須被維護。

(2) 電子病歷中的診療流程順序資料之真確性必須被維護。

換言之，電子病歷除了要保護原有病歷記錄的真確性外，還必須進一步保護病歷記錄中醫療照護流程資料的真確性，即醫療過程中的每一項診療與檢驗記錄都有其順序上的意義，電子病歷必須維護各項單元文件的順序性，才能確保醫療照護的品質，因此電子病歷之真確性保護，也必須將病歷記錄中的各項資料的順序加以記錄，以確保病歷中各項記錄未遭受順序上的變動。

在了解電子病歷真確性的定義後，我們可進一步了解可能破壞電子病歷真確性的操作並加以預防，Bakker(1998)舉出了可能危害電子病歷真確性的五項操作，分別為程式錯誤、硬體故障、通訊問題、操作設備上的人為疏失，與授權或未經授權使用者的惡意變更。

三、相關的電子病歷真確性保護方法

現今電子病歷的真確性保護方法，多半是使用傳統密碼學技術附加足以代表原始訊息的檢查碼，例如，先以單向赫序函數計算訊息摘要(Kaihara 1998)或是以私密金鑰計算數位簽章(Haak et al. 2003; Bakker et al. 1998; Brandner et al. 2002)，然後將訊息摘要、數位簽章附加於原始文件之後，對單一筆資料進行保護與檢驗，然而，這樣的做法不適用於會不斷增加資料內容的病歷記錄，所以需設計出滿足漸增資料之真確性保護需求，並且有高運算效率的方法，才能達成本研究的目標。為了探討漸增資料之真確性保護方法，下文將介紹的兩個真確性保護的概念，作為我們所提出方法的參考。

(1) 以連結方式建立之真確性保護

Gropper 及 Doyle (2003)兩人所發明的方法，用來建立可透過電子方式傳送之文件的架構及方法，而且，在這份文件內仍保有與其他相關文件連結之標記且不破壞原始文件所提供之真確性。讓使用者能將與主要文件相關的所有附件整合或重新組織在一份檔案中，使相關資訊的呈現更為完整。

在這個方法中，需將要傳送之資訊的型態改變為具有文字及末端節點兩獨立部份的格式，其中，末端節點內含用來連結與文字部份視為同一檔案內容的連結資訊以及其他相關檔案的連結資訊，並由末端節點前的提示資訊告知系統該文件檔案的結束。另外，為了達到不破壞各相關文件原來即已具備的真確性，當使用者成功整合多個相關檔案於一份文件後，系統仍會呈現原用於連結各相關檔案的連結標記。

藉由此法，一個或多個部份的文字報告將能夠與相關資訊連結在一起並直接呈現於終端展示設備上，而不須修改報告所提供之內容。應用於電子病歷可讓醫師將一次診療期間中，所有的診療相關檔案整合成一次完整的記錄，並保有原始文件所提供之真確性。此方法為針對一個診療歷程之資料，以連結方式整合成完整的病歷資料，並且不破壞該資料真確性的方式。

(2) 序列資料之真確性保護

Debiez、Hughes 以及 Apvrille(2003)三人，針對序列資料的真確性保護需求，提出一個有效的方法。此方法使用與輸入資料之個數相同的一系列連續的單向赫序函數之組合，設計資料真確性保護及檢驗值的計算方法，並且在某一資料區段及其對應的單向赫序函數值遭到替換時，亦能偵測出資料被改變。

此法將儲存媒體中存有的許多資料，視為一系列的循序資料區段，並當作系統的輸入值，循序地輸入至相對應的序列單向赫序函數中，具有與輸入的資料區段相同之次序的單向赫序函數內進行運算，並且，除了第一個資料區段之計算外，在計算每一資料區段的檢查值時，將前一次運算中取得的檢查值引入，作為該次運算的第二個輸入值。在循序完成每一資料區段的檢查值運算時，將該資料區段與其檢查值連結，則整個流程完成後，便能以由資料區段連結相對應之檢查值所產生的一個序列資料，作為檢驗全部資料之真確性的依據。

進行檢驗時，須使用與產生序列資料檢查值之流程中相同的次序，重新計算用於檢驗的序列資料檢查值，並與原始檢查值比對，以確認資料是否受到保護；當有任一資料區段或檢查值遭到竄改或替換，則在進入下一次的運算時，便能由未經竄改的正確資料檢驗得知。

此方法可應用於一系列之電子病歷的真確性保護，但由於其檢查碼的運算會涉及前次運算的結果，使得檢查碼間都具有順序性，無法依照電子病歷不同的需求組成特定的檢查碼，會造成使用彈性上的限制。

參、複合式文件之真確性保護方法

在說明電子病歷真確性保護方法之前，本文先提出適用於一般複合式文件的真確性保護方法。本研究所提出的複合式文件之真確性保護方法，是將針對單一訊息來源所設計的檢查碼運算方法加以改良，使其能適用於可不斷增加內容的複合式文件。此方法之原理是將複合式文件中同層文件的檢查碼連結為一暫存記錄，再計算此暫存記錄的檢查碼作為其上層文件的檢查碼，依此類推，循序完成該複合式文件內每一層文件的檢查碼計算，即可獲得整份文件的檢查碼。

根據前述原理實施時，會將一份具有二層架構的複合式文件所包含的每一成員文件之真確性檢查碼，連結為一份暫存記錄，再對此一記錄進行產生檢查碼的運算，獲得足以代表整份複合式文件的檢查碼，即可使整份文件獲得適當的真確性保護。

以此方法計算整份複合式文件之真確性檢查碼的理由，是因為檢查碼在資訊安全領域具有足以代表原始訊息的能力，而一份複合式文件是由其所含括之所有成員文件組成，全部成員文件的內容正是該複合式文件的內容，因此，以所有成員文件的檢查碼之連結值，替代整份複合式文件的內容，完成真確性檢查碼的運算，是一個合理的設計。

這樣的設計還可獲得另一個好處。由於每一層文件的檢查碼是以固定順序連結產生暫存記錄，因此當同層文件間之次序受到改變，或者是其中的部份文件遭受未經授權的刪除，則連結產生的暫存記錄就會改變，由暫存記錄計算獲得的檢查碼亦將改變，而能迅速檢驗出更動文件次序或是部份刪除的破壞行為。前述說明請參閱圖1 中的第一個敘述式，且可表示如下：

$CC_D = CCF(CCF(M_1)||CCF(M_2)||CCF(M_3)||\cdots||CCF(M_n))$；

其中，CC_D 表示整份複合式文件的檢查碼(Checking Code of a Compound Document)；CCF 表示檢查碼函式(Checking Code Function)；M_n 表示第 n 份成員文件(nth Member Document)，n 是一個由壹開始循序遞增的正整數；而“ || ”符號則代表數學運算中的連結。

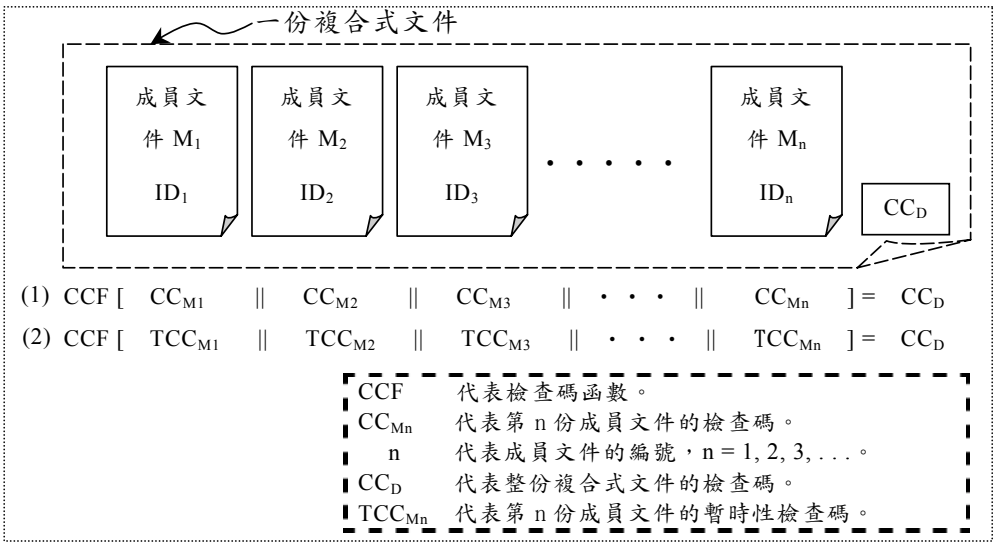

圖 1：一份複合式文件及其檢查碼運算方法之示意圖

由此，一個有效率且能提供整份複合式文件足夠之安全性的真確性保護方法，可以如此實施：先對每一成員文件進行單向赫序函數運算，求其訊息摘要做為檢查碼，接著將每一成員文件之檢查碼連結為一暫存記錄，以此暫存記錄代表整份複合式文件，並對其進行一次單向赫序函數的運算，再以求得的訊息摘要進行金鑰密碼學運算，獲得整份複合式文件的檢查碼。

上述方法的實施理由，是因為金鑰密碼學的運算負荷遠高於單向赫序函數運算，且成員文件的數量可不斷增長，若採用金鑰密碼學技術，將會有很大的運算負荷，因此，在成員文件的檢查碼計算上，採用運算效率較高且負荷較輕的單向赫序函數，而在計算整份複合式文件之檢查碼時，為了能有較高程度的保護，所以採用金鑰密碼學方法，如此，可確實保護複合式文件的真確性，也可提升檢查碼運算時的效率。

這個方法，雖然對每一成員文件採用安全保護程度較低的訊息摘要做為檢查碼，最後並不會減損本研究所提之方法的真確性保護能力，這是因為每一成員文件的檢查

碼亦會受到複合式文件之檢查碼的保護，任一成員文件的內容或檢查碼受到未經授權的變更，都可由複合式文件的檢查碼檢驗得知。此方法可表示如下：

$CC_D = KC(H(H(M_1) \| H(M_2) \| H(M_3) \| \cdots \| H(M_n)))$；

其中，KC 表示使用金鑰密碼學之檢查碼函式(Cryptographic Function)；H 表示單向赫序函數(One-way Hash function)；其它表示符號則如前述。由於使用金鑰密碼學函式進行檢查碼運算時，實務上會搭配單向赫序函數使運算具有效率，因此，本表示式實際上與前述的原始表示式相同。

另外，由先前的敘述可以發現，本研究所提之方法以每一成員文件的訊息摘要之連結值，取代所有成員文件之原始內容作為複合式文件的內容，再對此一連結值進行單向赫序函數的運算，以求得之訊息摘要當作整份複合式文件並執行真確性檢查碼運算。訊息摘要在資訊安全領域具有足以代表原始訊息之能力，而一份複合式文件是由其所含括之所有成員文件組成，全部成員文件的內容正是該複合式文件的內容，因此，以所有成員文件的訊息摘要之連結值，替代整份複合式文件的內容，完成真確性檢查碼的運算。

而且，在先前的運算中，已取得每一成員文件之訊息摘要，這些函數值均可代表用於產生該函數值之原始訊息，因此，將每一訊息摘要連結為一暫存記錄，則該暫存記錄亦將具有代表所有成員文件連結後之訊息的效力，也就是說，這個訊息具有可代表整份複合式文件的功能。此外，一個訊息摘要通常僅為一百多個位元的大小，遠小於產生其之原始訊息，在連結為暫存記錄後，亦將遠小於原始訊息之連結值，所以在訊息摘要的計算上，將更具效率。

為了使本研究所提之方法可讓個別的成員文件具有檢驗其本身之真確性的功能，在實施時可以如此執行：先對每一份成員文件進行單向赫序函數運算，再對每一份成員文件的訊息摘要使用金鑰密碼法求取檢查碼，接著將前一步驟獲得的訊息摘要連結為一暫存記錄，並對此記錄進行單向赫序函數運算，再以金鑰密碼法對獲得之訊息摘要進行運算，求取複合式文件的檢查碼，即可達成有效保護成員文件及複合式文件的目標。可如下表示：

$CC_{Mn} = KC(H(M_n))$；

$CC_D = KC(H(H(M_1) \| H(M_2) \| H(M_3) \| \cdots \| H(M_n)))$；

其中，所有的表示符號均如前述。由於使用金鑰密碼學函式進行檢查碼運算時，實務上會搭配單向赫序函數使運算具有效率，因此，本表示式實際上亦僅為前述原始表示式的延伸。

另由上式可以看出，每一成員文件之真正的檢查碼是由使用金鑰的檢查碼函式計算而得，但如前所述，搭配單向赫序函數可以使整體之運算效率更佳，而且，單向赫序函數值即已具備足以代表原始訊息之特性，因此在計算複合式文件之檢查碼時，改採用成員文件的訊息摘要取代真正的檢查碼。

此外，還可延伸出另一個實用的概念。由於上式使用的訊息摘要為計算真正的檢查碼之前置步驟，且同樣具備檢驗文件之真確性的功能，因此稱其為暫時性檢查碼。

另外，只要不是真正當作該文件之檢查碼，且具備檢查碼之特性與功能——足以代表原始訊息而能檢驗訊息真確性的數值，都可將其稱為暫時性檢查碼。因此，暫時性檢查碼可如前述，是一個計算檢查碼之前置步驟所產生的數值，也可以是檢查碼的衍生值，例如，檢查碼與該訊息之序號的連結值。由此，可修改上式之表示為：

$CC_D = CCF(TCC_{M1} \| TCC_{M2} \| TCC_{M3} \| \cdots \| TCC_{Mn})$；

其中，TCC_{Mn}則是第 n 份成員文件的暫時性檢查碼(Temporary Checking Code of nth Member Document)；而其他表示符號均如前述。如此，便與圖2 中用於描述暫時性檢查碼之應用的第二個敘述式相同。

此外，每一份成員文件可能還會具有一個唯一序號，這個序號可以是依照文件產生時間，或是該文件在複合式文件中之次序而產生，通常具有識別文件之功能，因此稱其為識別碼(identifier)。在產生複合式文件之檢查碼時，便可利用將每一成員文件的識別碼與其訊息摘要、或保護封條、或數位簽章連結，產生一個足以代表全部成員文件之暫存記錄，再對此記錄進行檢查碼運算，即可獲得複合式文件之檢查碼。

其中，前述的識別碼與其訊息摘要、或保護封條、或數位簽章之連結值，也同樣具有檢驗文件之真確性的功能，是暫時性檢查碼之另一例，而其亦可以圖1 中描述暫時性檢查碼的第二個敘述式來表示。

因此，總結暫時性檢查碼之應用，其將每一份成員文件實際附加的檢查碼、求得檢查碼之前置步驟的產出值、或前述兩者與文件識別碼的連結值，當作複合式文件檢查碼的運算來源；而在資訊安全的領域中，上述各項數值均具有足以代表原始訊息的性質。

以這些數值所產生之暫存記錄計算而得的訊息摘要，可代表全部成員文件——即整份複合式文件——的內容，並再次進行產生檢查碼的運算，獲得足以代表整份複合式文件的檢查碼，使各成員文件可獲得完善的真確性保護，且使產生整份複合式文件之檢查碼的運算更具效率。

肆、複合式電子病歷記錄架構

本研究同時提出創新設計的複合式電子病歷記錄架構，用於將病患在同一醫療機構內，產生的全部就醫記錄整合為同一病歷檔案，而其執行方法，是將一位病患之電子病歷內應存放的每一病歷記錄，以複合式文件的概念聚合為一份完整的檔案。另外，進一步參照醫療機構日常營運時，對病歷記錄的操作及管理方法，可以發現，一般是以一次診療歷程做為記載相關醫事記錄的區隔基準，亦即每次產生的診療相關記錄會經由醫師撰寫或審閱後，歸在同一診療歷程中，再以醫師簽章作為診療結束的依據，該簽章值還具有區隔醫療責任的功能。在設計電子病歷記錄架構時，亦應將此管理需求納入，使電子病歷能真正符合醫療機構的營運架構，獲得更完善的真確性保護功能。

因此，可將一位病患的整份電子病歷視為具有至少三個層級的複合式記錄，此三個層級分別為第一層級的醫事文件層、第二層級的診療層及第三層級的病人層。屬於

第一層級之醫事文件層記錄可從屬於第二層級之診療層記錄，或可直接從屬於第三層級的病人層記錄；而第二層級之診療層記錄則從屬於第三層級之病人層記錄。

第一層級記錄之檢查碼，由其本身內容透過檢查碼函數計算獲得；第二層級記錄的檢查碼，是由第一層級記錄的檢查碼透過本研究所設計之方法運算而得；第三層級記錄的檢查碼，則由第二層級記錄之檢查碼或再加上第一層級記錄之檢查碼，作為本研究所設計之方法的輸入值，透過本研究所設計之方法運算獲得。其中，醫事文件層的定義與前段相同。此三層式複合式電子病歷架構，如圖2 所示。

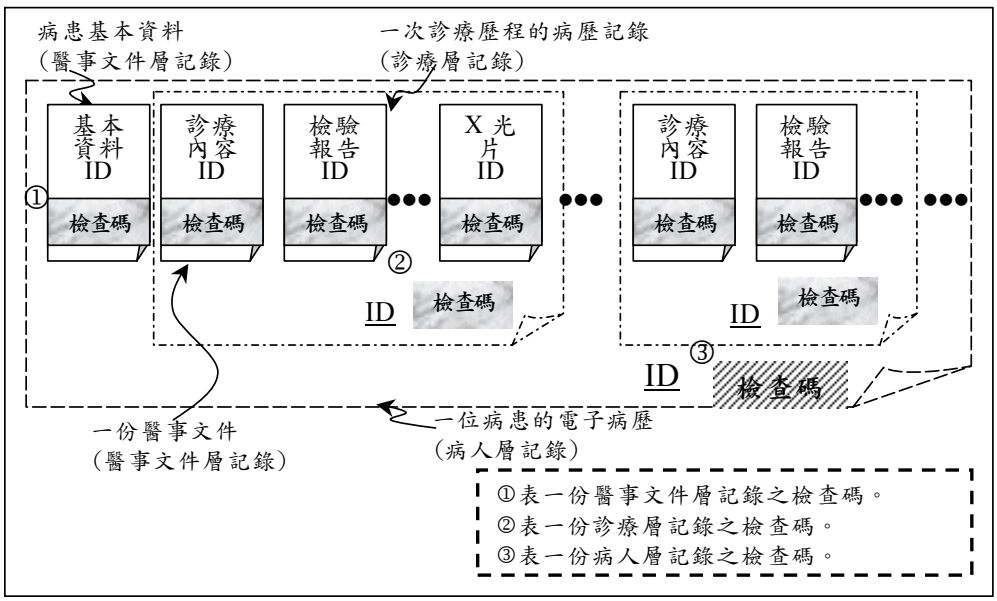

圖 2：三層複合式電子病歷架構示意圖

一、複合式電子病歷之層級定義

（一）醫事文件層

醫事文件層的每一份記錄描述著一份診療相關之醫事記錄，是構成整份病歷檔案的基本元件，此記錄可經由醫療機構內部的電子病歷系統產生，或透過病歷資料交換機制由其他醫療機構提供，記錄中會包含一個識別碼(identifier)以及由記錄內容產生的檢查碼（checking code），其中，識別碼即為系統用於識別其之唯一序號，而檢查碼將作為檢驗該份醫事文件層記錄之真確性的依據。

（二）診療層

診療層所描述的內容，由同一診療歷程中所產生的每一醫事文件層記錄所組成，為一份複合式記錄，記錄中亦應包含一個識別碼以及用於保護該記錄的檢查碼，因此，該檢查碼須以診療層記錄之全部內容進行計算而得，以作為檢驗該份診療層記錄真確

性的依據，其中，從屬於診療層記錄的醫事文件層記錄可能是一份診斷記錄、數位化的 X 光片資料或經由醫療造影技術產生的醫療影像資料，如電腦斷層掃描(CT)、核磁共振(MRI)等技術所產生的影像記錄。

（三）病人層

病人層所描述的記錄為一複合式記錄，此記錄由病患在同一醫療機構接受診療而產生的每一份醫事文件層記錄所組成，也具有識別碼，因此，一份病人層記錄即代表著一位病患的完整電子病歷記錄，而用於保護該記錄的檢查碼，應由記錄內的全部內容作為計算來源而產生，此檢查碼亦將作為檢驗該份病人層記錄之真確性的依據。

二、識別碼的應用

承前所述，每一層級文件均具有唯一的識別碼，供系統辨別之用。在病人層記錄中，識別碼可以是一個足以代表該病人層記錄之主體——病患——的唯一序號，例如，病人的病歷號碼。

診療層記錄之識別碼則可由病人層記錄之唯一序號，連結一屬於診療層的有序號碼所組成。而醫事文件層記錄的識別碼，可由病人層記錄之唯一序號，連結診療層記錄之有序號碼，再連結一屬於醫事文件層的有序號碼組成。

因此，在存取病患病歷時，可依照該病患之病歷號碼，將整份病歷檔案取回，或再額外加上一些限制條件，例如，就診科別、就診日時...等，將特定的部份病歷記錄取回，提供診療醫師進行判斷。

伍、複合式電子病歷之真確性保護方法

根據前述關於複合式文件之資料真確性保護方法，所設計的檢查碼產生方式，可以衍生多種產生一份電子病歷記錄之檢查碼的實施方式。實施方式之一敘述如後。對每次醫療行為產生之醫事文件層記錄以醫師金鑰進行簽章運算，簽章值作為該記錄的檢查碼，而簽章值運算之前置步驟所產生的訊息摘要，則依序連結為一份暫存記錄，作為整份病歷檔案的代表值，接著以醫療機構之秘密金鑰對該值進行保護封條的運算，以獲得的保護封條值作為病歷檔案的檢查碼存於系統，即可達成對病歷檔案的保護目標。

其中，以每一訊息摘要連結產生的暫存記錄代表病歷檔的全部資訊，是使用訊息摘要在密碼學領域具有足以代表原始訊息之特性，加上複合式記錄是由成員記錄組成之性質，所設計出的表示方法，符合密碼學的理論以及實務應用所需的效率。

承上所述，將改良後的三層級複合式電子病歷記錄架構，與複合式文件之資料真確性保護方法結合，則可如下實施。

請參閱圖3。由醫事文件層記錄所組成之診療層記錄，將透過檢查碼函數運算之計算，獲得足以代表該記錄的檢查碼，在這個例子中，檢查碼的函數運算以數位簽章

做說明，亦即，將屬於同一診療層的每一醫事文件層記錄之檢查碼連結成一份暫存記錄，再以此記錄進行單向赫序函數的運算，獲得足以代表該份診療層記錄的訊息摘要，並以醫師的私密金鑰對其進行簽章計算求得數位簽章，儲存於電子病歷資料庫中，做為檢驗及保護診療層記錄之真確性的依據。

其中，上述足以代表診療層記錄的訊息摘要之表示式如下：

hash(診療層記錄 #1) = hash(Y)；

其中，hash( )是一個廣泛用於檢查碼計算的單向赫序函數； Y 代表所有從屬於該診療層記錄之醫事文件層記錄的數位簽章連結值，例如，Y = signature(醫事文件層記錄 #1) || signature(醫事文件層記錄 #2) || ・・・|| signature(醫事文件層記錄 #n)，符號“||”代表數學運算中的連結之意；而 n 代表該診療層記錄中的第 n 份醫事文件層記錄，在接著介紹的例子中，同時具有表示該記錄為最後一份醫事文件層記錄之意。

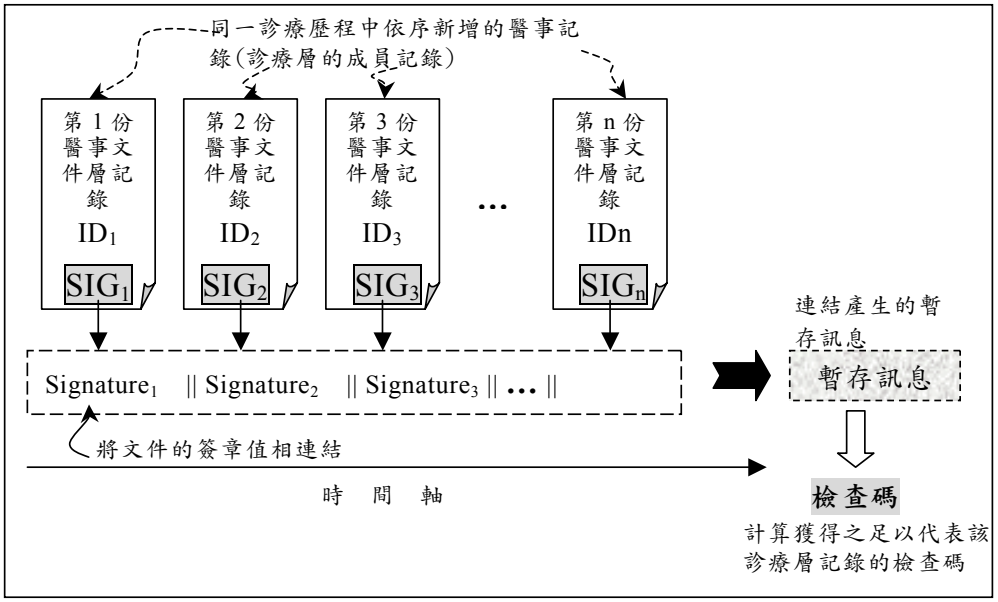

圖 3：計算足以代表診療層文件之檢查碼的一個實施方式

承圖3，請參閱圖 4。在病人層記錄中所儲存的內容，為一位病患在同一醫療機構就診的完整病歷資料，按照本研究所提之方法，是以從屬於該病人層記錄的醫事文件層記錄，及診療層記錄所組成，因此，當計算病人層記錄之檢查碼時，需將從屬的每一醫事文件層記錄及每一診療層記錄之簽章值，相互連結成一份暫存記錄，再以此記錄進行單向赫序函數的運算，獲得足以代表該份病人層記錄的訊息摘要，接著以系統的秘密金鑰對其進行運算求得保護封條，儲存於電子病歷資料庫中，做為檢驗及保護該位病患之電子病歷真確性的依據。

上述足以代表病人層記錄之訊息摘要的表示式亦可表示如下：

hash(病人層記錄) = hash(S)；

其中，S 代表所有從屬於該病人層記錄的醫事文件層記錄(以病患基本資料為例)，及診療層記錄(以門/急診病歷為例)之數位簽章的連結值，例如，S = seal(病患基本資料) || signature(診療層記錄 #1) || signature(診療層記錄 #2) ||・・・|| signature(診療層記錄 #n)。

或者，也可以使用之前介紹的應用暫時性檢查碼的方法。將屬於同一診療層的每一醫事文件層記錄之識別碼(以 ID 表示)，連結其檢查碼(此處亦使用簽章值，signature)後，再連結成一份暫存記錄，並以此記錄進行單向赫序函數的運算，獲得足以代表該份診療層記錄的訊息摘要，再以醫師的私密金鑰對其加密求得數位簽章，儲存於電子病歷資料庫中，做為檢驗及保護診療層記錄之真確性的依據。其中，上述足以代表診療層記錄的訊息摘要之表示式如下：

hash(診療層記錄 #1) = hash(Y)；

其中，hash( )是一個廣泛用於檢查碼計算的單向赫序函數；Y 代表所有從屬於該診療層記錄之醫事文件層記錄的識別碼及其數位簽章的連結值，例如，Y = 醫事文件層記錄 #1 的 ID || signature(醫事文件層記錄 #1) || 醫事文件層記錄 #2 的 ID || signature(醫事文件層記錄 #2) || ・・・|| 醫事文件層記錄 #n 的 ID || signature(醫事文件層記錄 #n)，符號“||”代表數學運算中的連結之意。

因此，檢查碼的表示式可列為：

$CC_D = ID_1||Signature_1||ID_2||Signature_2||ID_3||Signature_3||\ldots||ID_n || Signature_n$；

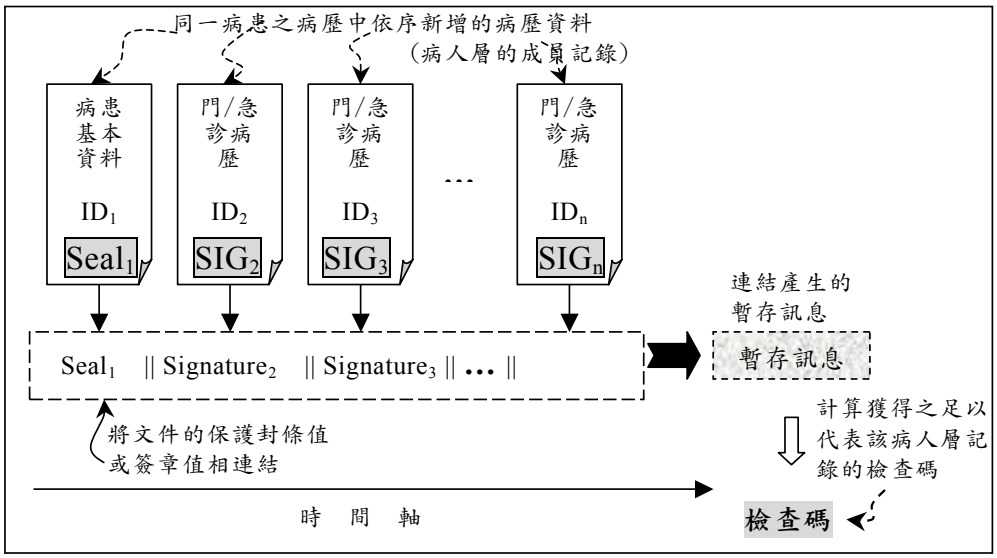

圖 4：計算足以代表病人層文件之檢查碼的一個實施方式

相同地，接著需對病人層記錄進行檢查碼的更新。在病人層記錄中所儲存的內容為一位病患在同一醫療機構就診的完整病歷資料，按照本研究所提之架構，是以直屬

於該病人層記錄的醫事文件層記錄及診療層記錄所組成。因此，當計算病人層記錄之檢查碼時，需將從屬的每一醫事文件層記錄之識別碼連結其簽章值及每一診療層記錄之識別碼連結其簽章值後，相互連結成一份暫存記錄，再以此記錄進行單向赫序函數的運算，獲得足以代表該份病人層記錄的訊息摘要，並以秘密金鑰對其進行運算求得保護封條，儲存於電子病歷資料庫中，做為檢驗及保護該位病患的電子病歷之真確性的依據。

上述足以代表病人層記錄之訊息摘要的表示式亦可表示如下：

hash(病人層記錄) = hash(S)；

其中，S 代表所有從屬於該病人層記錄之醫事文件層記錄的識別碼及檢查碼，與診療層記錄的識別碼及檢查碼的連結值，例如，S = 病患基本資料的 ID || seal(病患資料記錄) || 診療層記錄 #1 的 ID || signature(診療層記錄 #1) || 診療層記錄 #2 的 ID || signature(診療層記錄 #2) ||・・・|| 診療層記錄 #n 的 ID || signature(診療層記錄 #n)。

因此，檢查碼的表示式可為：

$CC_D = ID_1 \| Seal_1 \| ID_2 \| Signature_2 \| ID_3 \| Signature_3 \| ... \| ID_n \| Signature_n$：

當然，檢查碼或暫時性檢查碼的應用方式，可以依上述例子進行適當的改良，例如，在產生診療層記錄或病人層記錄的檢查碼時，使用各成員記錄的識別碼連結訊息摘要，再相互連結成暫存記錄，再對該記錄進行適當的檢查碼運算；或者，分別以不同方式產生診療層或病人層記錄的檢查碼，都可正確並有效率地完成檢查碼的產生流程。

最後，根據前述真確性保護方法的運作說明，以及對醫療機構病歷處理流程的觀察，本研究所採用的各層級記錄之檢查碼，可以確實在電子病歷遭受各項操作時，維護其真確性。這些可能破壞資料真確性的操作行為，已在前文中列舉，不再贅述。本研究使用的真確性保護方法可提供之效益，彙整如表 1。

表1：本研究成果採用的真確性保護方法之效益說明

破壞真確性的操作	檢驗及維護資料真確性的方法
非授權的資料創造	使用醫事文件層記錄的檢查碼
非授權的資料修改	使用醫事文件層記錄的檢查碼
非授權的資料增加	使用醫事文件層記錄的檢查碼
非授權的資料刪除	部份刪除：使用診療層記錄的檢查碼
	完全刪除：使用病人層記錄的檢查碼
非授權的資料重覆使用	無法僅依靠檢查碼，須額外加上唯一性或時效性資訊

陸、研究成果的運作效率分析

本研究的目標之一，是提出具有較佳效率的資料真確性保護方法；所提出的複合式電子病歷記錄運作機制，正具備提高整體運算效率的能力。接著以推論的方式，說明本研究成果可滿足此目標。

一、檢查碼更新程序

效率的好壞在檔案進行變更時最為明顯，以下舉一個增加病歷記錄內容的例子，來說明本研究所提之文件架構具有較佳的運作效率。

請參考圖5，圖中額外加上底色的圖示即為流程中被更動的資料。假設診療醫師要在就診病患的病歷檔案中，存入醫事人員為該病患拍攝的一份 X 光片記錄，他僅需先對增加的 X 光片記錄進行檢查碼的檢驗運算，再於診療層記錄中，新增一個用於儲存 X 光片資料的醫事文件層記錄，並將 X 光片的數位資料存入。

待完成增加 X 光片資訊（標號(A)的圖示）的過程後，再將從屬於該診療層記錄之每一醫事文件層記錄的識別碼，與訊息摘要連結為一份暫存記錄（標號(B)的圖示），以該記錄代表整個診療層記錄，重新計算足以代表診療層記錄的訊息摘要（標號(C)的圖示），並利用如數位簽章的密碼學方法加以運算（標號(D)的圖示），即可獲得更動後的單一診療層記錄之檢查碼。此檢查碼將存於系統儲存設備中，做為檢驗診療層記錄之真確性的依據。

接著，請參考圖6。由於病歷檔案中的一份診療層記錄已修改（標號(E)的圖示），便須立即更新病人層記錄的檢查碼，更新的方法是將病人層內，每一醫事文件層記錄或診療層記錄的識別碼，與其訊息摘要連結成一暫存記錄（標號(F)的圖示），並計算該暫存記錄的訊息摘要（標號(G)的圖示），做為足以代表病人層記錄之訊息摘要，之後以如對稱式密碼法的密碼學方法運算，即可更新整個病人層記錄的檢查碼（標號(H)的圖示），如此便可達到整份病歷的真確性保護。

由前述內容可知，本研究所提之文件架構在增加病歷記錄的內容時，只需進行少量的真確性保護運算，接著，配合前例，以一個實際進行檢查碼運算時可能產生的結果進行說明。

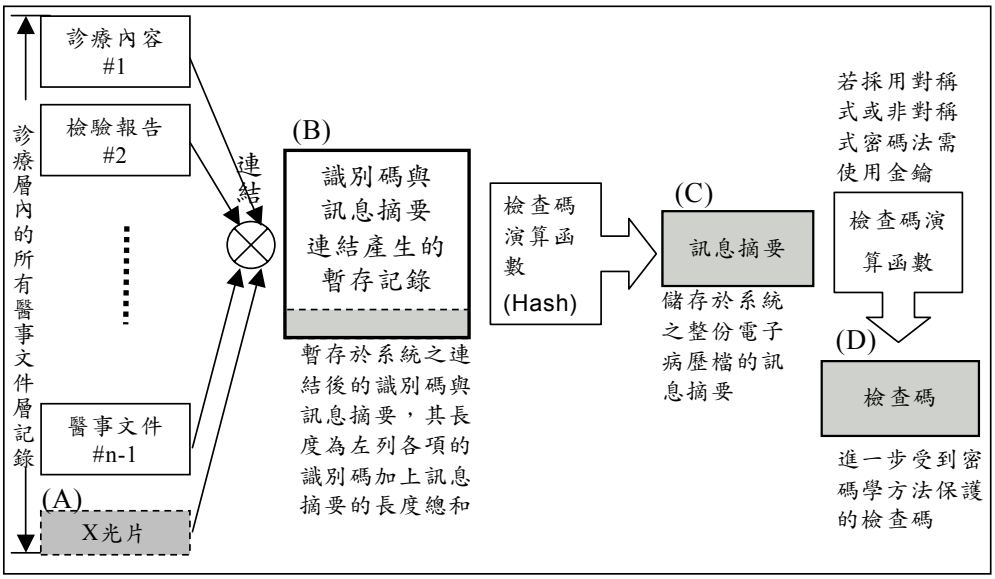

圖 5：檔案內容變更的說明圖示——診療層

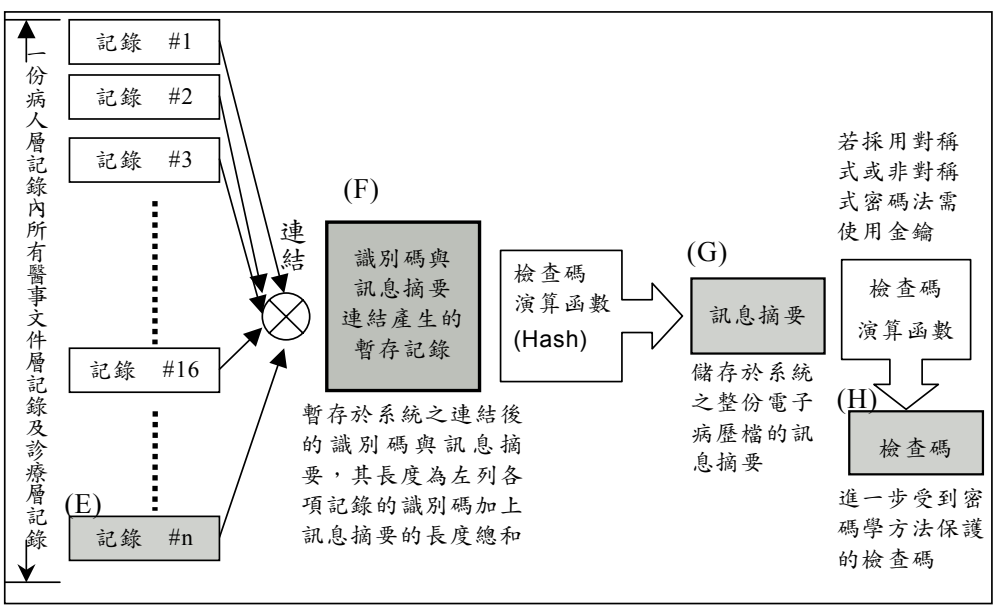

圖 6：檔案內容變更的說明圖示——病人層

二、檢查碼更新所需運算量

現假設某病患之病歷記錄具有一百次的診斷記錄，亦即具有一百個診療層記錄，並假設每個診療層記錄包含診療內容、檢驗報告及 X 光片三部份，若最後一份診療層記錄內的 X 光片需額外加上一些註記資訊，在本研究所提之電子病歷儲存架構中，僅

需新增一份用於撰寫補充病歷資料的醫事文件層記錄，儲存 X 光片所需的加註內容，並建立該醫事文件層記錄的檢查碼，更新代表該診療層記錄的檢查碼，更新系統儲存設備中的診療層記錄之檢查碼、更新病人層記錄的檢查碼，以及更新系統儲存設備中的病人層記錄之檢查碼。

假設以 SHA-1 赫序函數做為訊息摘要的運算函式，則每個訊息摘要將僅佔 160 bits，並假設每個識別碼佔 100 bits。每份醫事文件層記錄將以原始大小進行運算，並各自得到 160 bits 的訊息摘要，因此，該份加註資訊的診療層記錄僅需以(160+100)×4 bits（連結後的識別碼及訊息摘要，大小為 1040 bits）的資料量去計算訊息摘要。

而其他不需加註的診療層記錄，僅需以(160+100)×3 bits（連結後的識別碼及訊息摘要，大小為 780 bits）的資料量去計算訊息摘要；相同地，在病人層記錄的檢查碼運作中，亦僅需以 160+(160+100)×100 bits（屬於該病人層的全部醫事文件層記錄，與診療層記錄之識別碼及訊息摘要的連結值，大小約為 3.2 KB）的資料量，去計算病人層記錄的訊息摘要。

另外，由上述說明還可發現，本研究所提出之文件架構在錯誤檢驗上亦具有非常高的效率。由於系統儲存設備中，均存有醫事文件層記錄、診療層記錄及病人層記錄之識別碼及檢查碼，因此，當資料有缺失或錯誤，即可立即由所存的識別碼及檢查碼比對出異常的部份，而不需再經由額外的流程或計算以進行檢驗，相對地也減少了系統負荷，提升整體效能。

總的來說，本研究提出的方法僅在發生更動的層級中產生新的計算需求，已存在而不需更動的層級並不需要重新計算，其檢查碼仍可直接利用，因此，最後的運算量會比重新計算減少甚多。更重要的是複合式電子病歷之變更，以新增單元文件為常態，而舊的文件原則上是不允許變更的，變更屬於例外處理；故依此特色，本研究所設計的真確性保護機制相對的是具有高度效率的。

柒、結論

電子化為醫療機構帶來效率提升及成本節省，卻也使訊息更易於遭非授權的修改、刪除而破壞了真確性，且由於電子化資訊易於複製及散佈之特質，造成的資訊安全問題亦無法避免，因此需藉助其他機制以達成所需的安全保護。本研究即以複合式文件的概念重新設計電子病歷檔案架構，使病歷檔案內任一病歷記錄的真確性保護需求均可獲得滿足，特別是能以不同層級之檢查碼，確保電子病歷不會受到非授權的創造、增加、修改甚至是刪除的破壞行為，僅要再設計系統機制於病歷記錄中增加具有唯一性(uniqueness)及時效性(timeliness)資訊，便能確實維護電子病歷的真確性。

本研究所提之真確性保護功能，僅使用各醫事文件層記錄的檢查碼即可檢驗出『非授權的資料創造』、『非授權的資料修改』、『非授權的資料增加』；若是『非授權的資料刪除』之檢驗，使用診療層記錄的檢查碼可檢驗出資料的部份刪除，資料的完全刪除，亦可使用病人層記錄的檢查碼偵測；而『非授權的資料重複使用』，則無法僅由

任一層級記錄之檢查碼判斷，須於記錄中加上具有唯一性或時效性之資訊才能滿足檢查需求。

本研究在提出真確性的保護方法外，也提出符合病歷資料具有循序記錄、檢驗記錄逐件加入等特性的多層式複合式電子病歷架構，使之能以因應診斷流程與習慣上的需求，有效率的循序紀錄每個診療資料，除了可達成個別病歷與整體病歷資料的真確性保護外，亦能保護診療流程順序資料上的真確性，此為本研究於電子病歷真確性保護的創見，亦為本研究的貢獻之一。

此外，本研究所著重的議題為電子病歷記錄的真確性保護方法之改良，藉由設計一個多層級的安全保護架構，使病歷記錄具有高效率之運算及驗證真確性檢查碼的能力，但若缺乏其他安全機制配合，仍舊無法真正達到所需的安全性，因此，根據 Smith 及 Eloff(1999)二位學者對醫療資訊研究領域的分類，本研究的未來發展應可朝向資料庫安全及存取控管兩方向著手，使醫療機構內部所使用的資訊系統具備極高的安全性，並且有能力提出符合法律規範的證據以保障法律效益，同時，也唯有在醫療機構內部資訊能夠得到完善的安全保護之前題下，才能發展出真正具有安全保護能力的醫療資訊交換機制。

致謝

本研究承兩位匿名審查委員給予諸多寶貴的修正意見，並承行政院國科會研究計畫之補助，計畫編號：NSC94-2416-H-182-003 與 NSC93-2416-H-182-008，特此致謝。

參考文獻

1. 黃景彰，2001，資訊安全——電子商務之基礎，台北：華泰文化事業股份有限公司。
2. Anderson, M. M., “The Electronic Check Architecture Version 1.0.2,” 1998, Available at eCheck Organization web site: http://www.echeck.org/, Accessed Nov. 21, 2004.
3. Bakker, A., “Security in perspective; luxury or must,” *International Journal of Medical Informatics* (49), 1998, pp:31-37.
4. Bakker, A., Barber, B., Ishikawa, K., Takeda, H. & Yamamoto K., “Over conclusions and recommendations,” *International Journal of Medical Informatics* (49), 1998, pp:135-137.
5. Bakker, A., Barber, B. & Moehr, J., “Security of the distributed electronic patient record: conclusions, recommendations and guidance,” *International Journal of Medical Informatics* (60), 2000, pp:227-236.

6. Barber, B., “Patient data and security: an overview,” *International Journal of Medical Informatics* (49), 1998, pp:19-30.
7. Brandner, R., Haak, M. van der, Hartmann, M., Haux, R. & Schmucker, P., “Electronic signature for medical documents – integration and evaluation of a public key infrastructure in hospitals,” *Methods of Information in Medicine* (41), 2002, pp:321-330.
8. College of Physicians and Surgeons of Alberta (CPSA), “Transition to electronic Medical Records (EMR),” 2004, Available at CPSA website: http:// http://www.cpsa.ab.ca/publicationsresources/policies.asp, Accessed Nov. 12, 2005.
9. Debiez, J., Hughes, J. P. & Apvrille, A., “Data Integrity Check Method Using Cumulative Hash Function”, U.S. Patent 6,640,294 B2, 2003.
10. Dolin, R. H. et al., “The HL7 Clinical Document Architecture,” Journal of the American Medical Informatics Association (8), 2001, pp:552-569.
11. Eastlake, D. 3rd & Jones P., “US Secure Hash Algorithm 1 (SHA1),” RFC 3174, 2001.
12. Gropper, A. & Doyle, S., “Method And Structure For Electronically Transmitting A Text Document And Linked Information,” US Patent Application 2003/0177446 A1, 2003.
13. Haak, M. van der, Wolff, A. C., Brandner, R., Drings, P., Wannenmacher, M. & Wetter, Th., “Data security and protection in cross-institutional electronic patient records,” *International Journal of Medical Informatics* (70), 2003, pp:117-130.
14. Health Level Seven, “HL7 Clinical Document Architecture Release 2.0,” 2004, Available at HL7 website: http://www.hl7.org, Accessed Mar. 05, 2005.
15. ISO/IEC, “ISO/IEC 10181-6: Information technology — — Open Systems Interconnection —— Security frameworks for open systems: Integrity framework,” 1996.
16. Kaihara, S., “Realisation of the computerised patient record-relevance and unsolved problems,” *International Journal of Medical Informatics* (49), 1998, pp:1-8.
17. Smith, E. & Eloff, J. F. P., “Security in health-care information systems — current trends,” *International Journal of Medical Informatics* (54), 1999, pp:37-54.
18. W3C, “Compound Document by Reference Framework 1.0,” 2005, Available at W3C website: http://www.w3.org/TR/2005/WD-CDR-20051219/, Accessed Mar. 20, 2005.
19. West Midlands Regional Health Authority, “Report of the Independent Enquiry commissioned by the West Midlands Regional Health Authority into the Conduct of Isocentric radiotherapy at the North Staffordshire Royal Infirmary between 1982 and 1991,” 1992.