行政院衛生署

九十三年度

「確立及推廣醫療資訊安全與隱私保護之政策」

政策執行與推廣建議書

用 印 欄	投 標 機 構 章	負 責 人 章

呈交者: 台灣醫學資訊學會

中華民國九十三年七月二十一日

主持人: 楊哲銘, 聯繫電話:29307930 Email: cyang@tmu.edu.tw
聯繫人: 王博彥, 聯繫電話:0968718848 Email: alexwang@tmu.edu.tw

目錄

壹. 計畫緣起

1.1. 背景

電子簽章法於民國九十年十一月十四日由總統頒布，並六個月內公佈細則，以推動電子商務為方向，加速知識經濟的推動。

本案為知識經濟發展方案－「網路健康服務推動計畫」之子計畫「委託研修相關法規」，所擬辦理之公開評選「確立及推廣醫療資訊安全與隱私保護之政策」案，期藉由制定並推廣相關隱私保護法案，得以確實保障醫療資訊的安全及私密性，並適時適度的解除民眾對醫療資訊電子化應用的疑慮。

有鑑於國內社會大眾對於保障醫療資訊安全與病歷隱私的意識日漸抬頭，且愈發重視，因此，除本計畫第一、二期期程內，已彙整分析相關議題，協調各方意見，輔助政策形成與推動工作之外，第三期計畫更將制定一套規範指引，並草擬「醫療資訊安全與隱私保護綱領」。基於提昇醫療服務品質、保障資料所有者權益及個人健康資訊安全的前提下，規劃建立我國醫療資訊安全及隱私權保護相關的法制規範，並促使醫療資訊流通、安全及隱私權保護間能共同取得平衡點。

1.1.1. 民眾與社會觀點

個人資料保護是一個常用但是內容卻不是很精確的『新創字』，常使人誤認為是以『資料』為保護的標的；然而眾所公認真正保護的法益，以德國說法是『隱私領域』(Private spare)。其內涵亦如美國學者 Westin 所說的資料隱私權，個人對

自身資訊的控制與決定之權；個人有權決定傳遞自身資訊時機，對象與方法，同時有權決定所欲傳遞資料的範圍以及用途。

所謂的個人資料保護，亦即對於以任何形式涉及或反應個人人格的所有資訊，指其蒐集、儲存或散佈的方式會與某特定個人產生關聯的資訊。

電子病歷之建置、導入與交換，都必須基於大眾接受，也就是符合社會個人隱私認知可接受的前提下，方可進行應用。

「隱私權」一詞在我國現行憲法或民、刑法相關法律中並未出現，對於隱私權的相關規定也付之闕如，僅在大法官會議於八十一年三月十三日所做出之釋字第二九三號解釋中，首次提到隱私權的保護：「銀行法第四十八條第二項規定『銀行對於助課之存款、放款或匯款等有關資料，除其他法律或中央主管機關令有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權」。

隱私權是大多數民眾耳熟能詳的名詞，隱私權的保障也成為人人所要求的基本權利。隱私權究竟屬於民法上的權利，抑或是憲法所保障的基本人權？在釋字二九三號解釋的不同意見書中可略窺端倪：「隱私權亦為人格權之一種，依民法第十八條第一項規定：『人格權受侵害時，得請求法院除去其侵害』憲法對此雖無直接保障之規定，但依憲法第二十二條規定『凡人民之其他自由及權利…均受憲法之保障。』」依此推論隱私權應屬憲法保障之基本人權纔是。

隱私權是什麼呢？各家說法不一，本研究對隱私權有如下之定義：「隱私權是指公民享有的私人生活安寧與私人資訊依法受到保護，不被他人非法侵擾、知悉、搜集、利用和公開等的一種人格權。」針對隱私權的保護，歐美先進國家的腳步走在我們前面，他山之石可以攻錯，我們應該瞭解人權保障的先進者做了什麼樣的努力與規範：

《世界人權宣言》第 12 條

任何人的私生活、家庭、住宅和通信不得任意干涉，其榮譽和名譽不得加以攻擊。

人人有權享受法律保護，以免受這種干涉或攻擊。

《公民權利和政治權利國際公約》第 17 條

（1）任何人的私生活、家庭、住宅或通信不得加以任意或非法干涉，他的榮譽和名譽不得加以非法攻擊;(2)人人有權享受法律保護，以免受這種干涉或攻擊。

《歐洲人權公約》第 8 條

（1）人人有權使他的私人和家庭生活、他的家庭和通信受到尊重；(2）公共機關不得千預上述權利的行使，但是依照法律的干預以及在民主國家中為了國國家安全、公共安全或國家的經濟福利的利益，為了防止混亂或犯罪，為了保護健康和道德，或爲了保護他人的權利與自由，有必要進行干預者，不在此限。

《美洲人權公約》第 11 條

（1）人人都有權使自己的榮譽受到尊重，自己的尊嚴受到承認；(2）不得對任何人的私生活、家庭、住宅或通信加以任意或不正當的干涉，或者對其榮譽或名譽進行非法攻擊；(3）人人都有權受到法律的保護，不受上述干涉或攻擊。在美國，隱私權是指任何法律主體所享有的"與他人毫不相干的權利"。

目前，美國已經形成較為系統、完備的隱私法律保護體系。最主要的法徑有 1967 年的《資訊自由法》、1973 年的《犯罪控制法案》、1974 年的《隱私權法》和《家庭教育及隱私權法》、1976 年的《稅收修正法案》和《公平信用報告法》、1978 年的《財務隱私權法》以及 1986 年的《電子通信隱私權法》等。另外，美國各州還制定了眾多保護本州公民隱私權的法律，例如：紐約州的《個人隱私保護法》、加利福尼亞州的《隱私與有線電視法》，還有伊利諾斯州的《通訊客戶隱私權法》等。

反觀國內，對於個人隱私保護相關法案，殆屬「電腦處理個人資料保護法」較為周延，但是缺乏其他相關法令的配合，是否能在瞬息萬變的現代社會中發揮其保

護隱私權之作用，尚有許多可議空間。「電腦處理個人資料保護法」第七條規定：公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合下列情形之一者，不得為之：一、於法令規定職掌必要範圍內者。二、經當事人書面同意者。三、對當事人權益無侵害之虞者。

在眾多隱私權的內容中，醫療隱私原本就較不容易保護，此乃因醫療行為牽涉到較複雜的專業知識，英文書寫的病歷與處方，讓一般民眾在這一方面無法有較好的掌握能力；再加上一般人與醫生或醫療院所的關係並不對等，病患往往居於劣勢。在這樣的情形下，配合我國「電腦處理個人資料保護法」為基礎來看健保 IC 卡，對於個人隱私的保護不得不有所擔憂。

健保ＩＣ卡登錄醫療資訊是有法源依據的，但是，需經被保險人（民眾）書面同意或對民眾權益無侵害之虞。可是全民健保為唯一且強制性的保險，民眾根本沒有說「不」的權利，在毫無選擇的情況下，人民所能期待的是有完善的法令及保護措施，因此政府相關單位更需要加緊立法的腳步，以求病患醫療資訊隱私權的確保，以及在個人隱私與公共衛生利益中找到平衡點。否則透過國家機器的強制性將全國人民的各種醫療相關資訊蒐集起來，又沒有足夠之法令、相關配套技術措施，只能將病患隱私權的保護建構在醫療暨行政體系相關人員的「道德」上，很顯然這將會是另一場浩劫的開始。

1.1.2. 技術與安全觀點

以國內外訂定的安全與電子簽章建議為基礎，本團隊將訂定能保障資料完整性，保密性，以及可用性的**管理程序、實體防護、技術安全軟硬體、技術安全機制**。以 HIPAA 為例，包含下列各子項目：

A. 保障資料完整性，保密性，以及可用性的管理程序
包括憑證，一連串信任夥伴合約，意外事故計劃，處理病歷正常機制，資訊存取

控制，內部稽核，個人隱私，個人存取權限，安全調控管理，回顧與測試隱私功能，安全事件程序，隱私管理程序，系統中止程序，訓練等。

B. 保障資料完整性，保密性，以及可用性的實體防護

隱私權限與責任歸屬，媒體控制，實體控制管制，工作站使用時的政策指引，隱私觀念訓練等。

C. 保障資料完整性，保密性，以及可用性的技術安全軟硬體

存取控制稽核控制，授權控制，資料授權，實體授權等。

D. 保障資料完整性，保密性，以及可用性的技術安全機制

傳輸與網路控制，數位簽章等。

1.1.3. 醫療行政觀點

健保ＩＣ卡的使用代表電子病歷必須快速導入,這意謂著醫療單位之病患的醫療資訊全面數位化。對病患而言，個人所罹患的疾病、或整形美容等醫療資訊，如果被不當外洩，可能造成病患工作、交友、結婚、保險等權利受到重大影響，以及個人身心、名譽與權益受到傷害。醫師法第二十三條亦規定，醫師對於因業務而知悉他人祕密，不得無故洩漏。不過，這些規則對病患醫療隱私的保障有限，因為病人通常不是由一個醫生負責，權責上接觸病患醫療資訊的機構（例：健保局、醫療資訊外包的電腦公司）與非醫療人員（例：資訊部門人員、網路駭客）越來越多。

目前病患的醫療記錄多為數位化資訊,雖然數位化資訊為醫療院所帶來療程的效率，但是醫療資訊的管理亦帶來諸多問題，例如：病患的醫療記錄只有醫護、行政人員會接觸到，但是醫療資訊數位化的啟用，資訊科技人員（IT 人員）因為工作職掌的原故亦有接觸的場合,甚至連網路上的駭客亦有機會接觸個人的醫療記錄。醫護人員、行政人員、IT 人員（醫院內部、健保局等資訊中心）、駭客等四種身份，若以醫療資訊外洩的觀點來檢視這四種身份，可以簡分為二類：一類

是小單位的資訊外洩，例如：與病患接觸最直接的醫、護人員，可能洩漏少數幾位特定人士的醫療資訊；另一類是大單位的資訊外洩，例如：IT 人員、駭客因為深暗資訊科技的技術，最有機會、亦最能直接取得大量的個人醫療資訊，對個人隱私權的傷害是更直接、更強烈。有關電子監控的範疇，以及電子監控與隱私權保護之間的關係說明如下：

一、電子監控的範疇

Conger（1995）與 Straub and Collins（1990）的研究指出，IT 人員未經許可的情況下，瀏覽、公開、轉送他人之資料檔案，是侵犯個人隱私權的行為，例如：IT 人員利用電腦來監督員工的工作，公開、瀏覽或轉送他人之電腦檔案資料，以及追蹤或偷窺電子郵件等行為，是使用資訊科技侵犯隱私權經常發生的例子。換言之，醫院與健保局的 IT 人員因為工作職掌的原故，與個人醫療資訊的接觸不僅是最直接、也是最大單位管理者之一。在保障個人隱私權的立場，若以醫院為中心，其電子監控的範疇可區分為醫院內部、外部兩個單位。相關的電子監控範疇說明如下：

（一）醫院內部

Ernst and Yung （1993）與 Negron（1992）研究認為員工監控活動可被視為制止員工不當行為的利器。然而，為保障病患醫療資訊的隱私權，醫療單位在進行電子監控之前，應事先告知醫院內的組織成員，並取得組織成員的同意，以避免侵犯醫療單位之組織成員的隱私權。本研究認為醫院內部有權接觸病患醫療資訊的人員，例如：醫護人員、醫療行政人員與 IT 人員等，均為醫療資訊的監控範疇。電子監控方式有實體監控、電子監控兩類（Welch, 1997），通常管理單位使用電腦、攝影機與錄音機監控員工的活動（Kidwell and Kidwell, 1997）。依據病患醫療資訊的輸出型態，本研究認為醫院內部人員可以劃分為三種程度：

1. 醫護人員

醫師與護理人員的工作較偏重於臨床醫療行為，病患醫療資訊的接觸較偏向特定人士，病患醫療資訊的輸出型態偏重於記憶、紙張列印，可能接觸到的輸出量較

小。

2. 醫療行政人員

一般行政人員的工作偏重於病患醫療資訊的行政管理，例如：週報表、單位報表等，病患醫療資訊的輸出型態偏重於紙張列印，可能接觸到的輸出量較大。

3. IT 人員

大多數醫療院所均設有資訊單位，IT 人員協助醫療院所管理、維護所有病患的醫療資訊，病患醫療資訊的輸出型態偏重於數位化型態，可能接觸到的輸出量最大。

醫療院所之病患醫療資訊系統的擷取、查詢、更新功能除了應以電腦系統內電子監控功能避免不當的使用，同時亦應思考以實體監控方式來減少醫院內員工危害病患醫療資訊的不當行為。本研究認為接觸病患醫療資訊的輸出量越多、資訊技術能力越高的電子監控程度應該越嚴密，例如：IT 人員。然而，不管醫院採行何種型態的監控，醫院內部員工隱私權的維護亦是管理單位應重視的議題。

（二）醫院外部

除了醫院內部的組織成員以外，某些醫療院所亦可能將資訊系統的建置與維護工作外包給資訊公司，醫療院所在行政程序上亦應該對外包的 IT 人員有所要求，以確保病患的醫療資訊安全。另外，醫療院所在上傳資料給健保局時，對網路駭客的防範亦是醫療院所應該注意。除此之外，本研究認為健保局本身對全國民眾的醫療資訊，應該以最高的資訊安全標準來維護全國民眾的醫療資訊，保障個人的隱私權。

1.2. 國內外隱私與安全相關法規之探討

衛生署曾於七十九年二月七日衛署告字第 857431 號函規定，「醫療機構使用電腦製作病歷者，於輸入電腦時，應隨即將紀錄內容列印，並由診治醫師簽名，以依法建立實體病歷資料，並依規定年限保存，對於電腦保存之病歷，亦應妥善管理，

善盡法令所規定之保密義務」。多年來這種作業模式，除了需雙重作業管理保存紙本與電子病歷記錄相關資料外，亦需足夠的空間及設備以儲存病歷資料，在醫界已造成相當多的討論與爭議。

目前醫療法修正案中增列第六十六條「醫療機構以電子文件方式製作及貯存之病歷，得免予以書面方式製作，其資格條件與製作方式、內容及其他應遵行事項之辦法，由中央主管機關定之。」乃為保障民眾健康資訊權和推動醫療產業資訊化所必備之要件，除了病歷記錄之電子化外，X 光等影像資訊之數位化，均可直接在電腦上判讀、傳送。

美國於 1996 年 8 月 21 日公告 HIPAA 法案後，我國衛生主管機關旋即於八十五年十二月四日公佈「醫院電腦處理個人資料登記管理辦法」，其中:

第十一條 「醫院保有之個人資料檔案，應指定專人依相關法令辦理安全維護事項，防止資料被竊取、竄改、毀損、滅失或洩漏」。

第十二條「醫院個人資料檔案安全維護計畫，其內容應依本法施行細則第三十四條之規定，包括資料安全、資料稽核、設備管理及其他安全維護等事項」。第十三條「醫院應定期或不定期實施資料安全防護教育訓練及其他必要措施」。均明白揭示醫院應對個人資料檔案有一全面之管理政策與措施，

1.2.1. 國內相關法律

個人資料保護法

民國八十四年八月所制定之電腦處理個人資料保護法，其目的在於規範電腦處理個人資料之行為，以避免人格權受到侵害，並促進個人資料之合理使用。惟該法立法之初，其目的在於規範單純電腦處理個人資料之型態，並未考慮到要規範網路上電腦處理個人資料之保護。

按該法所規範之對象可分為公務機關以及非公務機關，其中之非公務機關依據該法第三條第七款之定義，共可分為以下之三大類：

A. 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。

B. 醫院、學校、電信業、金融業、證券業、保險業及大眾傳撥業。

C. 其他經法務部會同中央目的事業主管機關指定之事業、團體及個人。

電子簽章法的通過正式的賦予了電子病歷的法律地位。綜觀我國與眾多電子簽章法國際立法例，可歸納整理以下三大重要立法原則：

A. 技術中立原則：任何可確保資料在傳輸或儲存過程中之完整性及鑑別使用者身分的技術，應皆可納入使用，並不以「數位簽章」為限，以免阻礙其他技術應用發展。制定法律應採「電子簽章」（Electronic Signature）法為立法方向，而不以「數位簽章」（Digital Signature）法為限，以利日後諸如生物科技等電子鑑別技術之創新發展。也就是任何電子技術製作之電子簽章及文件，只要功能與簽名蓋章、書面文件相當，皆可使用。

B. 契約自由原則：對於民間之電子交易行為，宜在契約自由原則下，由交易雙方當事人自行約定採行何種適當之安全技術、程序及方法作成之電子簽章及文件，作為雙方共同信賴及遵守之依據，並作為事後相關法律責任之基礎；是以，不宜以政府公權力隨意介入交易雙方契約關係；交易雙方應可自行約定共同信守之技術作成電子簽章及文件。另憑證機構與其使用者之間，亦可以契約方式規範雙方之權利及義務。但此項原則是否適用於醫療界中之電子病歷有待各方共同討論。

C. 市場導向原則：政府對於憑證機構管理及電子認證市場發展，宜以最低必要之規範為限。今後電子認證機制建立及電子認證市場發展，宜由民間主導發展各項電子交易所需之電子認證服務及相關標準。

國外立法例因為賦予安全電子文件電子簽章極大推定效力，所以相對亦規範甚嚴謹符合程序，以配套實行之。例如規範

A. 需為經過主管機關認可之認證機構所發，

B. 經當事人約定並具可資信賴（有效）之技術等等程序要求。

而要符合（A）需為經過主管機關認可之憑證機構所發部份，制度規範上便必須對於憑證機構設計更多嚴謹之技術審驗及管理程序，技術層次上甚為繁瑣（相對而言，主管機關之審驗負擔責任便為相當龐雜），而此部份技術審驗安全標準相關規範，是不可或缺的配套措施，短期間內要完全制定出來是一項相當浩大工程；並且國外制定有「安全電子文件電子簽章」的立法例中，可看到均是以更嚴格縝密之憑證機構管理機制互為配套措施而為實施，衛生署對於憑證機構之管理之實施管理細則的訂定，將是決定我國順利推動電子病歷之主要因素。

1.2.2. 國外相關法律

國外電子簽章法運行數年，歐美澳日東南亞均有相關法令，其中以歐盟的數位簽章法以及美國數位簽章準則及 HIPAA 等最具有代表性，茲列出相關代表法案如下。

A. 歐盟指令(Proposal for a European Parliament and Council Directive on a common framework for electronic signatures)，2000 年 1 月 19 日公佈，全文共 15 條，其立法目的在降低使用電子簽章（electronic signature）之困難，並提供其法律承認地位（legal recognition）。在秉持科技中立架構（A technology-neutral framework）之下，歐盟對於使用不同形式科技的電子簽章（例如非對稱性加密或生物特徵辨識），不因科技的形式而予以法律上歧視，藉以保留科技創新空間。歐盟所制定的電子簽章法並不規範相關會員國或共同體法律所規範契約的締結與效力或其他法律責任；且不影響就文件使用之規定與限制。歐盟僅提出電子簽章一般性規範，對於醫療上使用電子簽章亦無另行制定排外條款或推行細則。

B. 美國數位簽章準則，分為五大部分，分別對於數位簽章之相關名詞定義，基

本原則，憑證機構，憑證註冊者以及憑證驗證者。在名詞定義方面共列有37項數位簽章中的特有名詞，堪稱相當完整，是美國各州制定電子簽章法參考的主要法律。其中值得注意的是法規中對於器官捐贈統一法(Uniform anatomical gift act)中之相關書面同意行為，以及醫療決定統一法(Uniform Health-care decision act)中之相關書面同意行為之負面表列。

C. 美國醫療保險簡便性與責任法案，於1996年8月由柯林頓總統宣示後通過，並於1999年12月發布。HIPAA對健康資訊的定義，泛指所有關個人過去、現在以及未來的各種生理及心理狀態，經由口頭、書面以及任何形式之媒體紀錄。該法適用於所有醫療相關機構：健康照護機構、健康計畫機構、公共衛生單位、雇主、保險公司、學校、大學或其他會交換健康資訊的單位。HIPAA立法的目的在於：1、增進健康保險之保障。2、降低資料之偽造與濫用。3、簡化行政事務。４、病患資料的保護。５、提升行政事務之效益HIPAA已擬”電子文件資料(EDI)”、”安全與電子簽章(Security & Electronic Signature)”、”隱私(Privacy)”、”標準識別(Standard Identifier)”，其中與本報告有關的安全與電子簽章及隱私部份均尚未通過，經數次專家會議及相關研究，本學會亦發現 貴署電子病歷法的訂定無法全然引用HIPAA所訂定之相關規定及準則，僅能節錄部分探討程序以及行政管理規定(列於本章節後)。HIPAA估計將花費達60億至600億美金於建置相關基礎設施，對於違反法規者亦罰款從美金$100到$250,000，因營利、個人目的、惡意而故意散佈病患個人資訊者將會處以十年有其徒刑，除此之外，機構也將會提高他們失去評鑑與名譽的危機。HIPAA的影響是全面性的，而且於今年(2002年)開始，除了小型健康計劃提供者之外必須全面實施，也因此有專家預言由於過度龐大的社會資源以及大部分的單位尚未準備完全，有可能會發生反立法(React)也就是延後或背棄HIPAA法案的其中一些部分。然而HIPAA的制定以及相關規模之大影響之遠，還是讓美國成為世界訂定電子化醫療相關規定的重要先趨者。

國際社會對隱私權的法律保護

全球性保護

依據《世界人權宣言》第 12 條規定："任何人的私生活、家庭、住宅和通信不得任意干涉，其榮譽和名譽不得加以攻擊。人人有權享受法律保護，以免受這種干涉或攻擊。"

《公民權利和政治權利國際公約》第 17 條規定："1、任何人的私生活、家庭、住宅或通信不得加以任意或非法干涉，他的榮譽和名譽不得加以非法攻擊。2、人人有權享受法律保護，以免受這種干涉或攻擊。"

區域性保護

《歐洲人權公約》第 8 條規定："1、人人有權使他的私人和家庭生活、他的家庭和通信受到尊重。2、公共機關不得干預上述權利的行使，但是依照法律的干預以及在民主國家中爲了國家安全、公共安全或國家的經濟福利的利益，爲了防止混亂或犯罪，爲了保護健康和道德，或爲了保護他人的權利與自由，有必要進行干預者，不在此限。"

《美洲人權公約》第 11 條規定："1、人人都有權使自己的榮譽受到尊重，自己的尊嚴受到承認。2、不得對任何人的私生活、家庭、住宅或通信加以任意或不正當的干涉，或者對其榮譽或名譽進行非法攻擊。3、人人都有權受到法律的保護，不受上述干涉或攻擊。"

《非洲人權和民族權憲章》第 4 條規定："人是神聖不可侵犯的，每個人的生命和整個人格權均有權受到尊重。任何一個人均不得被剝奪此項權利。"第 5 條規定："每個人的固有尊嚴有權受到尊重，其合法地位有權得到承認。"第 6 條規定："每個人均有權享有人身自由與安全。"第 16 條規定："人人有權享有能夠達到的最佳的身心健康狀況。"第 18 條規定："家庭是社會的自然單位和基礎。它應當受到國家的保護，國家應當關心它的物質上和精神上的健康。"

各國的保護

在美國，隱私權是指任何法律主體所享有的"與他人毫不相干的權利"。目前，美國已經形成較爲系統、完備的隱私權法律保護體系。最主要的法律有 1967 年的《資訊自由法》、1973 年的《犯罪控制法案》、1974 年的《隱私權法》和《家庭教育及隱私權法》、1976 年的《稅收修正法案》和《公平信用報告法》、1978 年的《財務隱私權法》以及 1986 年的《電子通信隱私權法》等。另外，美國各州還制定了衆多保護本州公民隱私權的法律，如紐約州的《個人隱私保護法》、加利福尼亞州的《隱私與有線電視法》，還有伊利諾斯州的《通訊客戶隱私權法》，等等。其中，1974 年制定的《隱私權法》是一部全面保護個人隱私權的專門立法。該法就不同的資料用戶對屬於隱私權範圍的個人資料的收集、保存及取用都作了較爲詳盡的規定。依照該法，聯邦政府在收集有關資料時，凡對個人有害或不利的資料必須向有關的個人直接收集。在取得資料的過程中，應向被收集者表明其收集資料所依據的權利、收集資料的性質、資料的用途以及不提供資料的法律後果等。任何聯邦機構只能收集與其本身職責有關的，或者與現行法律所賦予的任務有關的資料。各機構所保存的資料記錄必須做到"精確、相關、完整和公平"。未經與資料有關的本人同意，不得任意公開資料。允許公民查對和更正與本人有關的資料。1976 年的《公平信用報告法》規定，任何人向客戶報告代理機構提出請求時，該機構都有義務將自己的文檔中有關該個人的資料

資訊（涉及該人的醫療情況資訊除外）披露給該人。如果被存儲了檔案的個人認爲代理機構所存儲的資訊不準確， 該代理機構即有義務重新調整並修改所存儲的文檔。該法還要求一切客戶報告代理機構採取有效措施，確保所持有的資料安全可靠。

據統計，目前已有近 20 個國家制定了個人資料保護方面的法律。如，瑞典在 1973 年制定了《資料庫法》，規定建立瑞典資料監督局，未經該局批准，任何人不得非法擁有他人的個人資料，並對有關資料庫資料的收集、利用和保管等方面進行了規範。西德於 1976 年制定了《聯邦資料保護法》，規定了何種資料得以儲存、處理和傳送。並規定，在儲存、傳遞、修改和刪除個人資料時，禁止對這些資料加以濫用；資料需經本人同意或法律上的授權方可處理；個人可以請求獲取資料庫中關於本人的資料，除非這對資料庫的功能有所妨害；個人有權查詢、更正本人的有關資料；個人有權清除有關自己的某些資料。法國於 1978 年通過了《資料處理、檔案與自由法案》，規定收集和處理、使用個人資料，不得損害個人資料主體的人格和身份以及私生活。規定資料庫必須公佈其搜集資料的授權、目地和種類等。1984 年英國制定了《資料保護法》，規定不允許以欺騙手段從資料主體那裏取得資訊，取得個人資訊必須經過有關的個人同意；只有爲特定的和合法的目的，才能持有個人資料；使用或透露個人資料不得與持有資料的目的相衝突；必須採取安全措施，以防止個人資料未經許可而被擴散、更改、透露或銷毀；對於用戶遺失、毀壞有關資料，或者未經許可而透露有關資料的，資料主體有權請求賠償。《加拿大人權法案》規定，政府每年需公佈其資料庫的名稱、資料內容和使用情況，個人有權查詢並更正本人資料中不正確的部分。日本也於 1990 年實施了《關於保護行政機構與電子電腦處理有關的個人資料法律》。

一些國家雖然沒有隱私權或個人資訊保護的專門法律，但在憲法、民法等法律

中體現了對公民隱私權的保護。如，《土耳其憲法》第 20 條規定："每個人都有要求個人生活和家庭生活受到尊重的權利，個人生活和家庭生活的秘密不受侵犯。"《荷蘭憲法》第 10 條規定："每個人都有私生活受到尊重的權利，但須遵守議會法令的限制。議會法令制定有關記錄和公佈個人資料的規定，以保護個人的私生活。個人有權詢問被記錄下的有關本人的資料、資料的使用情況和修正錯誤資料。"《法國民法典》第 9 條規定："任何人有權使其個人生活不受侵犯。""法官在不影響賠償所受損害的情況下，得規定一切措施，諸如對有爭議的財產保管、扣押以及專爲防止或停止侵犯個人私生活的其他措施。在緊急情況下，法官得緊急下令採取以上措施。"

1.2.3. 資訊隱私與安全之議題

一般而言，在資訊隱私與安全的議題下，大多數的民眾均聯想到電腦駭客以及主機的管理，茲整理如下：

影響資訊安全因素

- 未經授權者（駭客）侵入電腦系統，竊取或更改資料甚至更動原系統設定，造成系統無法正常作業。
- 合法使用電腦人員有意或無心，造成資料的毀損、竊取或系統破壞。
- 未作資料備份儲存或毀損後無法復原。
- 未作系統備援設計，以致影響業務正常運作。
- 資料在傳輸中途被截取、竊窺或變更。
- 電腦感染與傳遞病毒。

要確保資料安全除資訊主管部門訂定週密作業規定外，最重要的還是使用者的配合。使用者若能依照規定的程序使用資訊裝備，對於部門資料安全的維護，必定具有相當正面的效果。

建立資料安全稽核制度，定期或不定期抽檢、抽測各項資訊安全防護作業，並追

蹤督導改善缺失。

電腦主機系統安全注意事項

- 主機系統應有專人負責管理，並配合門禁管制禁止無關人員進入。
- 系統參數必須以密碼設定保護，責由專人維護或異動。
- 主機系統內儲存之資料，須每日予以備份，以維資料安全；備份作業方式與使用之媒體，應研擬作業規定妥善保管。
- 建立使用紀錄檔，並經常檢視稽核，防杜異常狀況發生。
- 主機系統應考量災害防治（水、火災或地震等）及環境因素（溫度或溼度），並作好應變措施及防災演練。

應用系統及資料庫管理

- 指定專人負責管理應用系統及資料庫，並落實版本控管工作。
- 軟體系統應有完整備份，以確保系統正常運作；備份使用之媒體，應依備份管理作業規定，分別存放於不同處所，妥善保管。
- 建立完整系統維護作業，並於發生異常狀況時立即處理。

電子簽章(Electronic Signatures)

組織將需要一些方法去產生、證明、傳送及管理產生出來的 public key，另外，他們也需要決定去建立一個 PKI 或者去買這樣的服務‧企業流程、工作流程及應用程式將需要修改，以配合數位簽章這項新機制‧公開金鑰的證明還無法完全的在所有電腦中交互運作，而且在健康照護方面也沒有一個標準存在，所以造成了標準無限期的延期‧

醫療機構資訊安全

非常少的健康照護組織有安全標準建立方面的需求‧實行安全標準必須改變企業

的流程、工作程序、人員安排、公司文化、實體設備及建立資訊科技的基礎建設。讓大家都有安全的意識將是管理上的一大挑戰。在老舊系統中提供 end-to-end 的責任機制將是技術上主要的挑戰。額外的處理程序監督將造成系統額外的負擔。統一及分析從各系統得到的資訊在現行上並不可行。最後的安全標準仍未公開，大部份的組織不太願意去建置這類不確定的需求。

隱私

隱私標準將明顯的影響到組織的行為，其中即代表一個主要的文化挑戰。隱私標準也將明顯影響組織的運作及與客戶的互動。資料庫管理系統一般使用在臨床資料的需求上面，而其卻缺乏對於顧客隱私政策上該有的安全保護。一般來說，將客戶的規則轉換成技術上安全的措施也將是一項重大的挑戰。

1.3. 歷年研究成果

醫療資訊學會在早期即發現醫療資訊隱私與安全的重要性，歷年來已舉辦多場主題為醫療資訊隱私與安全研討會，並承蒙　貴署醫政處以及資訊中心抬愛，承辦電子病歷使用電子簽章法研究計劃，以下列出相關執行成果。

1.3.1. 研討會與專家論壇

本團隊曾辦理以下與醫療資訊隱私與安全直接相關之研討會及專家論壇。

- **電子病歷下之隱私權保護研討會** 2002/10/24 – 台北市立衛生局計劃贊助

主題：電子病歷實施對個人隱私權之衝擊、醫療資訊數位化的社會影響、資訊安全之市場趨勢。

- **電子簽章法實施對電子病歷推動影響系列活動**，包括研討會 2001/12/26、電子簽章法實施對電子病歷推動影響專家論壇第一次 2001/12/06 以及第二次 2001/12/20 論壇 – 衛生署計劃贊助

請參考附錄一、二、三。

- **健康資訊隱私與安全研討會** 2001/6/26

目的：因應 21 世紀基因文明以及電子病歷時代來臨，個人基因特性、病歷、保健等資訊將直接衝擊到個人的醫療服務、工作權和相關的保險範圍。例如，HIV 帶原者就醫時是否可以不告訴醫師？雇主是否可以要求調閱員工的病歷？或因員工有某種疾病而招不同待遇？諸如此類問題爭議，將隨著科技發展和電腦網路的普遍而日益頻繁。本研討會將探討國外健康資訊趨勢、HIPAA 法案的影響、以及在兼顧個人資訊之隱私與安全權的原則下、醫療院所應如何建構醫療資訊系統，一方面可以確保個人病歷資訊的安全，另一方面又可提供醫療服務及保險機構方便的使用以上的資訊。

1.3.2. 研究計劃

■ 建置醫療資訊交換中心研究(2000)

MIEC 是 Medical Information Exchange Center 的縮寫，主要是為了在衛生署 HIN2.0 的大架構下，提供醫療人員一個安全，高效率、易用且精確的醫療資訊流通系統。為了要實現這個需求，必須先訂定一系列系統架構和規格。而這些系統架構和規格必須在現今技術上能實行、讓使用者能充足信賴這些資料、對醫院不能造成太大的衝擊和讓合格的授權者容易取得及使用。

MIEC 的主要目的是：(1) 能透過醫療資訊的交換達成連續性的醫療照顧，(2) 減少重複性的檢驗和檢查，(3) 改善醫療照顧的品質。

MIEC 主要分為兩大部份：中樞系統和週邊系統。中樞系統係由五個伺服器和兩個應用界面所組成。伺服器有 MIEC 主網頁伺服器、索引用伺服器(IS)、稽核用伺服器(Audit Server)、使用登入伺服器(Access Server)、通行和驗証伺服器(CA)。應用界面分別醫師 (醫師工作站－Physician Workstation－PW) 和病人 (病人導向索尋中心－Patient Centered Retrieval－PCR)兩種 。週邊系統主要由資源服伺者 (Resource Server－RS) 和 gateway 所組成。這兩個系統藉著網際網路而串通。當使用者通過 HIN2.0 並透過我們的 CA 伺服器註冊之後，當使用者登入使時其動作將會被登錄在我們的稽核伺服器內。稽核伺服器者的目的是避免任何預使不到的事件發生和駭客的侵入使作追蹤。針對個人安全和隱私，MIEC 的中央系統並沒有保留任何使用者之臨床資料。索引伺服器只保存一些基本資料病和就診醫院及試驗項目名稱的資料。中央系統伺服器只扮演仲介者，透過週邊系統的 RS 尋取病患臨床資料，並在使用者使用結束後自動把資料抹去。在週邊系統中 gateway 主要扮演著資料轉換的角色。

RS 是寄附在 HIS (Health Information Management System 醫院醫療資訊系統)的極小伺服器。透過一個定義完整的 RS 統一格式及政策的規定，Gateway 把部份資

料轉換成 RS 格式，而醫院有自己的權利和政策作各種調配和訂定，例如：資料機密程度之界定，預分享查詢的檢驗項目和時間的間隔等。RS 資源伺服器不會帶給醫院太多的衝擊，只需一個小型的伺服器及資料轉換系統，不會影響醫院醫療系統(HIS)的正常運作。在晚上或某商議的時間 RS 將送資料到 IS (索引伺服器)，或 IS 向 RS 索取資料，所以在那些資料更新時將不會影響或阻礙醫院系統的基本運作。

MIE 完成數項工作，包括 RS 和 Gateway 資料轉換的設立、RS 的運作、患者導向健康資訊查詢表單(Patient Request Form－PRF)界面的建立、醫院查詢表單(Hospital Request Form－HRF)界面、XML 格式的醫病記錄（病歷）

■ 電子簽章法實施對電子病歷推動影響研究(2001)

本案為行政院衛生署醫政處委託醫學資訊學會擷取國外經驗，針對電子病歷可能的施行細則從學術面、法律面、技術面、社會面各個觀點加以分析，邀集各界專家集思廣益，以作出具體能促進醫療產業知識經濟之建議。

本學會共邀集二十餘名政界、學術界、法律界、資訊界、醫療院所以及產業界專家學者，開立兩次專家會議；並經由兩次會議所得到之建議與結論辦理一次大型研討會。透過相關專家會議、研討會以及非正式的訪談討論中我們發現，運用電子簽章法推動電子病歷無論是適法性或技術性均為可行，並且可能對於推動健康產業知識經濟有一定之助力。因此本學會提出了一套電子病歷試辦要點以及推動建議供各界訂定細則之參考。

電子病歷試辦要點部分，本學會建議以成立電子病歷委員會方式代替建立冗長無彈性的細則。電子病歷的實施類似藥品人體試驗之管理，難以單憑法律管制，取而代之的應該是一個常設的機構以及具彈性的機制，以因應變化快速的資訊科技。

電子病歷試辦要點推動建議部分，提出病歷委員會、試辦單位、電子簽章方式、加密技術、民眾宣導等建議，以補足試辦要點不足之部分。

■ 醫院資訊系統白皮書建置計畫(2003)

從 2003 年初起，台灣醫學資訊學會提出行政院衛生署資訊中心提出建構醫療資訊系統白皮書的企劃案，並進一步進行多次的簡報，終於在八月一日起由行政院衛生署資訊中心以及醫政處以部分補助的方式成立 92 年度白皮書建置計畫並開始執行。透過行政院衛生署的補助以及產官學研專家學者的投入，計畫有了初步成果。在短短五個月內，徵求了醫療院所與資訊廠商系統規格書，開立三次技術指導委員會議以及二十餘次技術委員會議，並建立了龐大的知識管理平臺，產生千餘頁文件、近六百 MB 資料，都可作為未來醫療院所執行醫療資訊系統時的有用資源。整個規範大致可分為臨床資訊系統、支援資訊系統以及共通資訊系統三大塊，茲明列如下:

- 臨床資訊系統

包括第七章醫令，第九章檢驗，第十章影像與放射，第十一章護理，第十二章手術與麻醉以及第十三章重症照護。

- 支援資訊系統

包括第二章財務行政管理，第六章健康保險以及第八章藥品衛材。

- 共通資訊系統

包括第三章訊息與編碼標準，第四章病患安全以及第五章隱私安全。

貳. 概述

電子簽章法於民國九十年十一月十四日由總統頒布，並六個月內公佈細則，以推動電子商務為方向，加速知識經濟的推動。然而電子簽章法通過至今，雖然衛生健康相關資訊未以排除適用方式執行，卻也尚未提出運用細則。

本案為知識經濟發展方案－「網路健康服務推動計畫」之子計畫「委託研修相關法規」，所擬辦理之公開評選「確立及推廣醫療資訊安全與隱私保護之政策」案，期藉由制定並推廣相關隱私保護法案，得以確實保障醫療資訊的安全及私密性，並適時適度的解除民眾對醫療資訊電子化應用的疑慮。

有鑑於國內社會大眾對於保障醫療資訊安全與病歷隱私的意識日漸抬頭，且愈發重視，因此，除本計畫第一、二期期程內，已彙整分析相關議題，協調各方意見，輔助政策形成與推動工作之外，第三期計畫更將制定一套規範指引，並草擬「醫療資訊安全與隱私保護綱領」。基於提昇醫療服務品質、保障資料所有者權益及個人健康資訊安全的前提下，規劃建立我國醫療資訊安全及隱私權保護相關的法制規範，並促使醫療資訊流通、安全及隱私權保護間能共同取得平衡點。

本案將以本團隊開立的多次研討會與執行委辦計劃經驗，決心導入 HIPAA、BS7799 將『合法的電子病歷』具體化，並初擬建立「醫療資訊安全與隱私保護綱領」，期待在政策全力衝刺推廣病歷電子化的同時，提供醫療院所在病歷電子化時，建構隱私與安全環境之有效參考。並於本期結案前辦理五次專家論壇，四次大型研討會，並建置與維護「醫療資訊安全與隱私保護」全球資訊網站供產官學研與民眾參考。

參. 計畫架構

本章節將敘述本計劃書執行與推廣目標，以及工作內容分期敘述。

3.1. 計劃目標

本團隊在委辦計劃中決心將『合法的電子病歷』具體化，並初擬建立『健康資訊隱私與安全環境之因應對策與指引』，期待在政策全力衝刺推廣病歷電子化的同時，提供醫療院所在病歷電子化時，建構隱私與安全環境之有效參考。主要目標如下:

- 參考 HIPAA、BS7799，具體化『合法的電子病歷』
- 建立『健康資訊隱私與安全環境之因應對策與指引』

3.2. 工作內容

本計畫實施期程自九十三年八月至九十三年十二月，共五個月，工作內容包含下列事項。

A. 蒐集與研讀本計畫前二期制定及推動「醫療資訊安全與隱私保護法」之發展趨勢與相關資訊，並邀相關專家學者請益。

國內外與「醫療資訊安全與隱私保護法」相關的趨勢與資訊在本計畫前二期專案中已經有過研讀與蒐集，包括美國 HIPAA、歐盟指令、澳洲日本東南亞等地的電子簽章法。本團隊於本期工作之開始著眼於如何將先前蒐集與研讀後的資訊轉換成淺顯易懂的摘要，公佈給予本計畫後續使用、產官學研各界與民眾參考。

B. 成立「醫療資訊安全與隱私保護法」起草專家小組

邀請國內對於「醫療資訊安全與隱私保護」議題具有深入研究之法律學者、資訊

安全專家以及醫療院所管理人員，共同組成「醫療資訊安全與隱私保護法」起草專家小組。

C. 舉辦「醫療資訊安全與隱私保護法」專家座談會。

本計劃將比照本團隊 91 年計劃 –「電子簽章法的實施對電子病歷推動之影響」研究，以及 92 年計畫「醫院資訊系統白皮書建置計畫」，邀集專家學者以工作小組會議模式，進行 5 次專家座談會。

D. 研擬「醫療資訊安全與隱私保護綱領」草案

透過本計畫核心團隊成員，以及專家學者所組成「醫療資訊安全與隱私保護法」起草專家小組 1-2 次座談會，本計畫將產生「醫療資訊安全與隱私保護綱領」草案，並放置「醫療資訊安全與隱私保護」網站供各界參考。

E. 提出「醫療資訊安全與隱私保護綱領」

根據專家學者工作小組座談會議成果，本會將提出「醫療資訊安全與隱私保護綱領」。

F. 舉行醫療院所與民間團體代表之實務醫療資訊安全與隱私保護座談會

本會擬於台北開設「確立及推廣醫療資訊安全與隱私保護之政策」研討座談會。時間初定於民國 93 年 12 月。由於在開立研討會以前將會開立五次的專家論壇，因此研討會邀請對象主要著眼於醫事機構以及民眾，預估約 100-200 人，務必讓各界關心醫療資訊安全與隱私保護人士有機會提出不同意見。

G. 維護「醫療資訊安全與隱私保護」專屬網站之運作

配合計畫執行進度，維護更新網站內容、線上論壇，提供醫療資訊安全與隱私保護相關議題討論之園地，網址為 http://privacy.doh.gov.tw/plan.html。本會除了維

護網站之內容連結正確(目前 http://211.20.178.26/icct/health_web/policy.html、http://211.20.178.26/icct/health_web/dis.asp 為錯誤連結)之外，也將註冊本網址於各大入口網站，並將相關討論/座談會簡報、會議內容放置網站上，提供更完整資訊。

H. 期末報告撰寫

除具體提出「醫療資訊安全與隱私保護綱領」之外，本團隊亦將研究執行過程以及方法論等資料彙整撰寫結案報告，並產生對主管機關醫療資訊政策之建議，供貴署及社會大眾參考。

肆. 實施策略與方法

本章節將敘述本執行與推廣計劃的實施策略，執行方法，以及具體的實施步驟。

4.1. 實施策略

本章節將探討本計劃之必須的實施策略，並以前瞻的眼光觀前顧後，參考過去發生的發生的事件並研擬因應之道，以增加本計劃的可行性。

4.1.1. 前車之鑑

國民卡:

行政院研究發展考核委員會於民國 86 年 7 月 21 日設立「IC 卡規劃及推行小組」，其目的為「加速推動 IC 卡在政府部門之整合運用，以提高行政效率、加強便民服務及促進國內 IC 卡產業之發展」。經一年研議，此小組於今年 6 月 10 日公布「國民身份健保合一智慧卡（簡稱國民卡）」專案徵求建議書，以整體委外(out sourcing)之方式，公開徵求資訊業者承作「設計及製發符合現行國民身份證、健保卡、電子簽章機制等應用需求之 IC 卡，並建置相關作業程序及軟、硬體環境，其他約定營運項目由承作業者提出建議」。

國民卡計劃引發各界的反彈聲浪。在監察院於民國 88 年 1 月對研考會提出糾正案後，行政部門趨於保守謹慎，重新思考相關措施，從 BOO(Build, Operate, Own) 方式改為政府編列預算，不再擁有電子商務功能，最後計劃停擺，身分證，健保卡也採個別發卡方式辦理。從相關報導看來，反對最力的是立法委員及學界專家。

健保 IC 卡:

在國民卡案停擺後，由行政院衛生署中央保險局參訪歐洲德國、捷克等國家做

法，以及根據 86 年 7 月澎湖地區的健保 IC 卡試辦計劃，於民國 88 年 5 月研擬接續健保 IC 卡計劃，並預計於 90 年換發健保 IC 卡取代紙卡。

健保 IC 卡因有國民卡的前車之鑑，較為公開政策的研擬以及廠商評選的過程。然而各界依然引發在病患隱私權、資料安全性相關疑慮未解和補助措施未確定之前，不宜草率上路的聲浪。再加上醫界認為導入健保 IC 卡的使用必須加裝 50 億元的獨卡機以及系統修改費用，使得健保 IC 卡上線計劃由原先的 90 年，延至中期的三階段計劃(第一階段 91 年 7 月~92 年 5 月為試辦、第二階段 92 年 5 月~93 年為全面上線、第三階段為 93 年加入過敏藥品等個人性健康資訊)，目前看來第一階段亦已延後。

本學會與醫院協會、健康保險行政協會共同合作健保 IC 卡最佳化流程業務委辦計劃，開立多次健保 IC 卡醫界研習會，並且與醫界多所接觸，發現健保局亦缺乏與各界之互動，並且決策時程非常緊湊，也造成各界反對的聲浪。雖然目前看來健保 IC 卡仍會進行，然而卻已耗費極大的社會成本。

省思：

在上述兩計劃中，相關政府官員以及產業人士政策研擬的過程中，缺乏與民意代表以及學界專家的互動，即貿然制定決策，是計劃失敗或延誤的最大主因。可見的**資訊的揭露**，以及**取得各界學者專家的共識**，在政策推動的過程中之重要性。

4.2. 執行策略

綜合以上討論，本團隊將擬以下列方式作為主要計劃進行的依據，以避免醫療資訊隱私與安全政策執行上的反對與衝突。

- 根據 91 年初本會承辦之電子病歷使用電子簽章法研擬計劃，以及 92 年本會

承辦醫院資訊系統白皮書建置計畫執行經驗，將主動邀請政府單位(包括貴署資訊中心與法規會及各處、健保局、司法部、法務部)；學界研究單位(包括資策會科法中心、中央研究院資訊科學所與社會所等資訊隱私與安全研擬之主要學者專家等)；參與學協會(包括醫院協會、區域/私立/教會/地區醫院協會、醫師/牙醫師/中醫師公會、醫事法律協會、醫管學會、台灣人權協會、醫療人權協會等)；以及合理數量的醫院代表及其他人民代表參與專家論壇。

- 邀請電子病歷試辦計劃執行的八家醫院團體，包括臺大醫學院附設醫院、長庚醫院、台北榮總、台中榮總、高雄榮總、慈濟醫院、高學醫學大學附設中和醫院、成大醫學院附設醫院等，共同參與並於試辦期間加入本計劃實施成果測試與回饋。
- 將醫療院所電子化普查計劃成果加以分析，納入本案醫療資訊隱私與安全未來推廣以及所需耗費的社會成本考量。
- 邀請　貴署資訊中心 – 健康憑證(HCA, Health Certification Authority)委外執行計劃承辦人與廠商加入本計劃討論並將成果測試與回饋。由於 HCA 預計發放時程為今年年底，與本研究計劃時程有整合之可能性，因此本團隊將與 HCA 計劃承辦人與廠商保持良好的互動，並確立研擬的技術、標準、醫事人員卡等確為可行。

4.3. 本團隊執行優勢

由於確立及推廣醫療資訊安全與隱私保護之政策是一項仰賴高度專業，以及高度協調能力與國際觀的工作，本會具備執行本計劃的以下能力。

- 曾於 91 年初執行電子病歷使用電子簽章法可行性研究計劃，最為具體了解醫療資訊隱私安全法規與細則的訂定過程，並深知訂定過程中極需醫界、法界、資訊產業、社會人文各界討論參與。

- 本會擁有醫療、法律與倫理與資訊專業與良好的人脈關係，能有效整合政府單位、學界、醫界與資訊產業，進一步含括民眾參與。
- 本會擁有『醫資分析師』與『醫資管理師』兩種證照，有能力研擬並執行在未來可能需要的『醫資安全管理師』證照，有效推動資訊隱私與安全觀念與層級，解決醫事人員不了解醫資安全的困境。
- 本會為國際醫學資訊協會(IMIA, International Medical Informatics Association)的正式學術會員，並為亞太醫學資訊學會(APAMI, Asia Pacific Association for Medical Informatics)理事長國，每年組團赴美、歐參與國際性的生物醫療資訊研討會，與國際醫療資訊產官學關係良好，以本會於今年 9 月初籌組的美國醫學資訊學會年會(AMIA, American Medical Informatics Association Annual Symposium)為例，即邀請 Philip 與 CA 等公司的 HIPAA 研究單位人員擔任本團隊的顧問，能有效適時導入國際經驗。

4.4. 研究方法

本會參考 W3C 以及 HIPAA 之做法，以徵求意見(Call For Comment)為主軸，配合管理領域常用之會議審議方法論，試圖產出一套最小化批評與挑戰之規範。。本團隊擬導入 HIPAA、BS7799 等不同指引作為參考，並以不同的推廣策略輔助以促成本計劃順利執行。

4.4.1. 建立醫療院所『最佳化醫療隱私/安全作業準則』

依據下圖準則建立程序，以證據導向(Evident-based)的方式建立實際有用的隱私/安全作業準則，提供醫療院所評估自身是否合乎最佳化，以及應在哪一個部分加強。

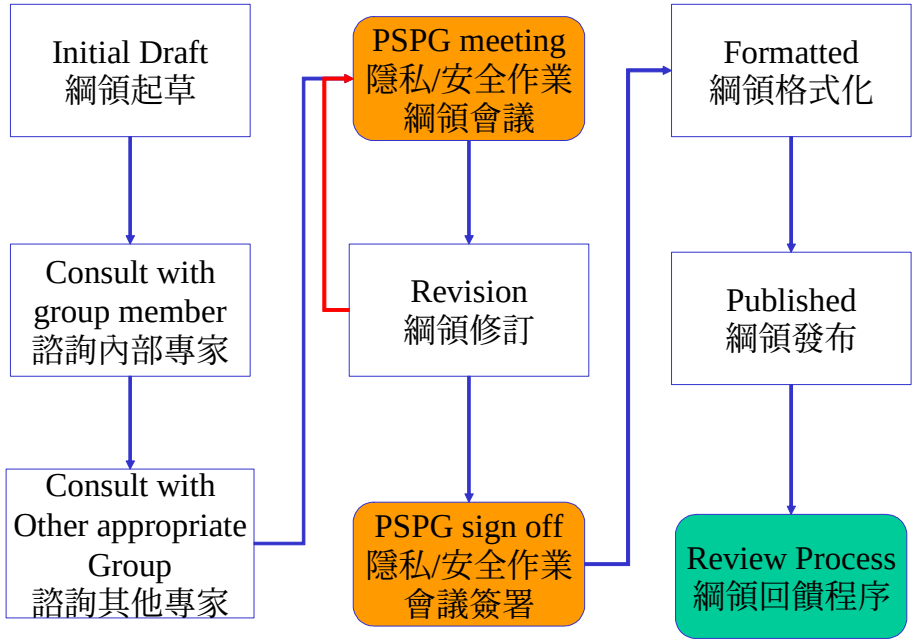
程序一. 由本研究之人員從國內外蒐集的資訊以及腦力激盪成果起草綱領。
程序二. 將起草完成的綱領提出給予本研究列名顧問評估。
程序三. 將起草完成的綱領提出給予本研究未列名之外部顧問評估。
程序四. 開立隱私/安全評估綱領會議，邀請座談討論綱領修訂事宜。

程序五. 重複程序四，五直到隱私/安全綱領會議簽署修訂完畢。

程序六. 將綱領格式化。

程序七. 公佈綱領。

程序八. 不斷評估，回饋綱領，以促使綱領達到最佳化。



圖表 1 隱私與安全綱領專家審議圖

4.4.2. 導入 BS7799 與 HIPAA 比較國內外隱私與安全建構情形

BS7799

BS 7799 是一套英國國家標準，由英國國家標準協會所制定，此項標準之主要目的在於定義及提供組織作為保護自身或客戶關鍵資訊之機密性（Confidentiality）、完整性（Integrity）及可利用性（Availability）的管制方法。機密性的定義是確保只有獲得授權的人才能取得資訊。完整性的定義是確保資訊和處理方式是正確和完整的。可利用性的定義是確保獲得授權的使用者在需要時可以取得資訊，並使用相關資訊資產。以波士頓的 Harvard Vanguard 為例，共撰寫了 31 頁，近四萬字，分成 7 個部份的文件。並以下列表格檢核。

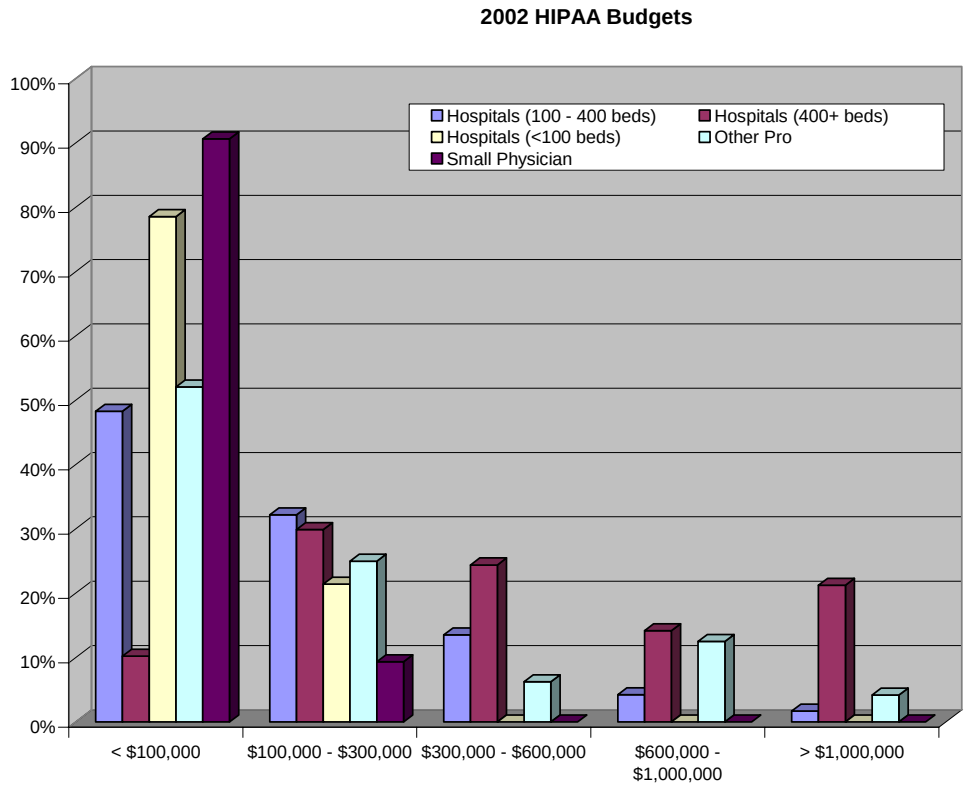
控制項	控制措施	評分	備註
4.1.1.1	資訊安全政策文件	3	每位 Harvard Vanguard 管理員與監察員應繼續加強負責教育他或她的部屬這些政策,以及遵守這些政

			策的必要性.
4.3.2.1	分類原則	1	在「臨床訊的機密性」僅提到：資訊歸為客觀（objectively）和敏感性（sensitively）文件檔,但未提到分類標準.
4.3.2.2	資訊標示和處理	3	在「臨床訊的機密性」的「醫療記錄內容」中說明：某些資訊被標明為敏感的,並加以標「限制」符號.
4.4.1.3	保密切結	3	「機密性的規範」的「機密性的安全保護」有描述.
4.4.2.1	資訊安全教育訓練	1	僅有提到做資訊安全的政策教育,但沒有說明.
4.4.3.1	安全事故的回報	3	「對於違反病患機密性的懲罰過程」的「程序」中,有說明違反機密性事宜時的報告處理方式.
4.4.3.5	懲戒程序	3	「對於違反病患機密性的懲罰過程」有詳細的描述.
4.7.7.1	事件日誌紀錄	2	「對於違反病患機密性的懲罰過程」的「程序」中說明：任何等級的錯誤,將記錄建檔.
4.7.7.2	監控系統的使用	1	在「機密性的規範」的「機密性安全保護」提到：自動化的醫療記錄系統須有一個「審核追蹤（audit trail）」的方式,顯示透過醫療記錄碼與密碼查詢的歷史記錄.
4.8.3.2	加密	1	「敏感性的醫療記錄」有說明敏感性的醫療記錄應以保護碼的形式來存檔.

HIPAA

HIPAA 訂定的安全與電子簽章建議書中共有四大部分，分別是保障資料完整性，保密性，以及可用性的管理程序、實體防護、技術安全軟硬體、技術安全機制(請參考附錄六)。

HIPAA 無疑的是全世界現有規範健康資訊的隱私與傳遞最完整的法案，然而根據美國健康資訊與管理協會(Healthcare Information and Management Systems Society, HIMSS)年初針對醫療院所 HIPAA 建構狀況的統計，今年度(2002 年)超過 21%的 400 床以上醫療院所預計將花費 3500 萬台幣(100 萬美金)以上來建構安全隱私相關軟硬體設施。因此一定程度的本土化是必要的工作。



圖表 2 2002 年醫療院所對於符合 HIPAA 法案預算比例圖

4.4.3. 政策推廣

整體計劃成果之推廣分為推力與誘因(Push and Poll)，推力包括:

A. 彙編與公開研發本計劃相關成果刊物

B. 參加國際醫療資訊研討會(Medical Informatics Symposium in Taiwan, MIST)，參加主題展覽並籌組一場醫療資訊隱私與安全論壇

C. 協辦其他分項計畫主辦的座談/說明會

D. 成果推廣暨媒體宣傳活動：透過舉辦一般民眾皆可參與的活動並搭配平面/電子等媒體的宣傳，推廣與教育民眾認識本研究成果

E. 提供各學術/應用單位相關文章：報導本分項計畫所舉辦各項活動提供相關課程講義及活動資料上網的訊息

F. 訓練推廣網站設置及維護：網站提供內容將包括推廣訓練相關活動訊息、活

動紀錄、課程講義等。

G. 成果推廣，包括技術之擴散、標準與規格之宣導

4.5. 預期進度

月次 / 工作項目	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	備註
1. 助理聘用及訓練								**X**					
2.蒐集與研讀前二期計畫成果								**X**					
3.成立起草專家小組								**X**	**X**	**X**			
4.舉辦專家座談會								**X**	**X**	**X**	**X**	**X**	
5.提出研擬草案								**X**	**X**	**X**			
6.提出綱領										**X**	**X**	**X**	
7.舉行座談會											**X**	**X**	
8.維護專屬網站之運作								**X**	**X**	**X**	**X**	**X**	
9.報告撰寫											**X**	**X**	
工作執行累計百分比	0%	0%	0%	0%	0%	0%	0%	24%	40%	60%	80%	100%	
經費執行累計百分比	0%	0%	0%	0%	0%	0%	0%	20%	40%	60%	80%	100%	

預定查核點說明

查核點編號	預定完成時間	查核點敘述	評估基準
3.	93 年/ 10 月	舉辦「醫療資訊安全與隱私保護法」專家座談會	繳交「醫療資訊安全與隱私保護綱領」起草專家小組會議成果報告書
5	93 年/ 10 月	研擬「醫療資訊安全與隱私保護綱領」草案	繳交「醫療資訊安全與隱私保護綱領」草稿初稿
6.	93/12/31 前	提出「醫療資訊安全與隱私保護綱領」	繳交「醫療資訊安全與隱私保護綱領」相關條文
7.	93/12/31 前	舉行醫療資訊安全與隱私保護之座談會	繳交醫療資訊安全與隱私保護座談會成果報告書
8	93/12/31 前	維護醫療資訊安全與隱私保護專屬網站之運作	繳交「醫療資訊安全與隱私保護」專屬網站維護紀錄

伍. 預期成果

5.1. 預期效益

■ 影響人次

透過與醫院協會、醫管學會等單位合作，以座談、說明會、公聽會、專題學習班、現場研討會、報刊發表、成果推廣暨網路與實體媒體宣傳活動等方式宣傳，預計直接影響超過 500 名醫事相關人員，民眾 1,000 名。透過公文之間接接觸更能達到國內所有醫療院所。

■ 影響醫院

透過座談、說明會、公聽會、專題學習班、現場研討會、報刊發表、成果推廣暨網路與實體媒體宣傳活動、公文發送等方式宣傳，預計影響層面將可達到所有醫療院所。

■ 標準作業程序與準則的回饋與更新

透過座談、說明會、公聽會、專題學習班、現場研討會、報刊發表、成果推廣暨網路與實體媒體宣傳活動等方式宣傳，預計將接受各界對於本研究成果標準作業程序以及準則之回饋與更新。

5.2. 預計之成果效益

■ 提交國內外「醫療資訊安全與隱私保護法」之重要發展趨勢與相關資訊

■ 建構「醫療資訊安全與隱私保護法」全球資訊網站

■ 產出醫學資訊隱私與安全成熟度模型

- 病歷電子化相關問題測試與回饋
- 影響醫事人員超過 500 人次以上
- 影響民眾人次超過 1,000 人次以上

貢獻以及對計劃人員之預期之訓練成效

- 此一計畫相關人員將可得到隱私與安全相關技術觀念
- 相關研習研討會可訓練提昇院所內部員工對於資料隱私與安全概念

陸. 人力配置及需求

6.1. 本計劃人力配置

ID	姓　名	現任工作	擔任職務	其他事蹟	學歷
1	楊哲銘	萬芳醫院核子醫學科主任 臺北醫學大學醫務管理系助理教授 醫院評鑑暨醫療品質策進會 TQIP 小組召集人	主持人	中華民國醫師證書 中華民國公職醫師高考及格證書 美國印第安那州律師證書 美國華盛頓特區律師證書 萬芳醫院副院長	臺北醫學院醫學士 美國印第安那大學法學博士 美國約翰霍浦金斯大學公共衛生學院醫務管理博士候選人
2	專任助理	兩名	TBD	TBD	TBD
3	兼任助理	兩名	TBD	TBD	TBD

柒.經費需求概算

項　　目	金　　額	說　　明
人事費	878,130	
專任研究助理薪資	318,000	31,800 元/月x2 人x5 月=318,000 元
兼任研究助理薪資	80,000	8,000 元/月x2 人x5 月=80,000 元
臨時工資	240,000	800 x 150 x 2=240,000 (進行網站修改、會議籌備雜務、計畫雜務等)
鐘點費	200,000	2000 x 20 x 5 = 200,000, 包括前述 PSPG 會議以及內外部顧問邀請鐘點費
保險費	40,130	4013(每月勞保 1425，健保 1400，退休金 1188)*2*5= 40,130
業務費	1,250,000	
文具、紙張、影印	100,000	文具、紙張、影印、及研討會辦理講義
郵電	100,000	研討會文宣資料郵寄、醫院配合作業文件郵件
印刷	150,000	研討會文宣資料、結案報告、論文出版、公函
資料收集費	200,000	資料檢索、文獻、期刊收集
台澎金馬區旅費	100,000	研究人員會議旅運費用 2,000x50 人次=100,000
租金與餐點費	300,000	大型研討會 200,000+五次小型討論會 x20,000
電腦處理費	300,000	資料彙編、流程輸入及分析及炭粉夾、光碟片、磁碟片、全球資訊網程式設計費與資料處理費
管理費	170,250	170,250 (8%)
合計	**2,298,380**	

捌. 主持人學經歷

附表一：研究人員學經歷說明書（每人填寫一份）					
類　別	（　　）主持人　（ √ ）協同主持人　（　　）研究員				
姓　名	楊哲銘	性 別	男	出生年月日	54.8.5

學　　歷（擇其重要者填寫）			
學　校　名　稱	學　位	起迄年月	科 技 專 長
台北醫學院	醫學士	72/9-79/6	
美國印第安那大學	法學博士	82/8-85/5	醫療衛生法暨行政
美國約翰霍普金斯大學	博士	85/8-92/5	醫務管理

經　　歷（請按服務時間先後順序填寫與現提計畫有關之經歷）		
服　務　機　構　及　單　位	職　稱	起迄年月
現任：台北醫學大學醫務管理學系	助理教授	92/6~
中華民國外傷防治協會	理事	87/10~
台灣醫務管理學會	理事	89-
曾任： 台北市立萬芳醫院	副院長	87/5-92/5
台北醫學大學	主任秘書	92/6~93-6

近五年內曾參與之相關研究計畫	計　畫　名　稱	計畫內擔任工作	計畫支援機關	起迄年月
	研究倫理審查可行性探討	主持人	省衛生處	87/6/1-88/5/31
	新世紀醫學倫理與醫病關係相關性之探討	協同主持人	國科會	89/8-90/7
	從病人醫療自主權看基因工程應用於人工生殖技術之倫理困境	主持人	台北醫學大學	90-91
	國家醫學倫理政策暨指導綱領之國際比較研究	主持人	衛生署	92/1-92/12
執行中之相關研究計畫	計　畫　名　稱	經　　費	計畫支援機關	起迄年月
	專業倫理教學方法之研究	59 萬	國科會	92/8-93/7

近五年相關之著作及研究報告名稱：（另紙繕附，不得超過兩頁）

研究人員簽章：　　主持人簽章：

附表二：研究人員最近五年已發表與計畫內容相關之學術性著作（每人填寫一份）

1. 「美國法官會議簡介」,司法周刊,八十四年三月二十二日。
2. 「都是冷凍胚胎惹的禍」,健康世界,二百四十七期,頁九十八至一百零三,一九九六年七月。
3. 「診斷關聯群論病例計酬制度之美國立法經驗」,公共衛生,第二十三卷第二期,頁七十九至頁八十九,八十五年七月三十一日。
4. 「誰是媽媽－代理孕母的法律問題」,法律與你[36],頁一六一至一六七,一九九六年十月。
5. 「老蚌應不應該生珠」,健康世界八月號,一百四十期,頁一百零一,一九九七。
6. 中央日報副刊：「死亡醫生卡布基」,「如何預防心動脈阻塞」。
7. 中央日報大千世界版「杏林札記」專欄。
8. 安樂死的陰陽界線，公共衛生,第二十五卷第二期,頁八十五至九十二頁,八十七年七月三十一日。
9. Twenty-first Century Genetic Ethics, NTJM 1999; 2:59-61.
10. 研究倫理審查制度建立之重要性探討(Submitted for review)

附錄一.醫療法與電子病歷有關之節錄

醫師法第十二條

醫師執行業務時，應製作病歷，記載病人姓名、出生年、月、日、性別、住址、職業、病名、診斷及治療情形。但在特殊情形下施行急救，無法製作病歷者，不在此限。前項病歷，應保存十年。

醫療法第四十八條

醫院、診所之病歷，應指定適當之場所及人員保管，並至少保存十年。病歷內容應清晰、詳實、完整。醫院之病歷並應製作各項索引及統計分析，以利研究及查考。

醫療法第五十條

醫院、診所因限於設備及專長，無法確定病人之病因或提供完整治療時，應建議病人轉診。但危急病人應依第四十三條第一項規定，先作適當之急救處置，始可轉診。前項轉診，應填具轉診病歷摘要，交予病人，不得無故拖延或拒絕。

醫療法第五十一條

醫院、診所診治病人時，得依需要，並經病人或其配偶、親屬之同意，商洽病人原診治之醫院、診所，提供病歷摘要及各種檢查報告資料。原診治之醫院、診所不得拒絕；其所需工本費，由病人負擔。

醫療法第五十二條

醫院對出院病人，應依病人要求，掣給出院病歷摘要。醫院對尚未治癒而要求出院之病人，得要求病人或其關係人，簽具自動出院書。

醫療法施行細則第四十七條

醫院、診所依本法第五十一條規定商洽原診治之醫院、診所提供病歷摘要及各種

檢查報告資料時，應以書面為之。前項所稱各種檢查報告資料，指報告單影本或檢查造影片拷貝。

衛生署規定醫療法「修正草案」中有關病歷記錄的新規定如下:

第六十四條

「醫療機構應建立清晰、詳實、完整之病歷。前項病歷，應包括下列各款之資料：一、醫師依醫師法執行業務所製作之病歷。二、各項檢查、檢驗報告資料。三、其他各類醫事人員執行業務所製作之紀錄。醫院對於病歷，應製作各項索引及統計分析，以利研究及查考。」(修正理由一、條次變更。二、現行條文第一項有關病歷保存之規定，移至修正條文第六十七條第一項規定。三、現行條文第二項前段移列為第一項，並酌作文字修正。四、由於醫療科技進步，國民知識水準提升，各項醫療作業日趨精細複雜，醫療作業紀錄應有明確之規範，以利診療參考，並提升醫療品質，爰增訂第二項規定病歷涵蓋之資料範圍。五、現行條文第二項後段移列為第三項，並酌作文字修正。)

第六十五條

「醫療機構應督導其所屬醫事人員於執行業務時，親自記載病歷或製作紀錄，並簽名或蓋章及加註執行年、月、日。前項病歷或紀錄如有增刪，應於增刪處簽名或蓋章及註明年、月、日；刪改部分，應以畫線去除，不得塗燬。醫囑應於病歷載明或以書面為之。但情況急迫時，得先以口頭方式為之，並於二十四小時內完成書面紀錄。」(修正理由一、本條新增。二、為強化醫事人員執行業務之責任規範，爰規定如上。)

第六十七條

「醫療機構之病歷，應指定適當場所及人員保管，並至少保存七年。但未成年者之病歷，至少應保存至其成年後七年；人體試驗之病歷，應永久保存。醫療機構因故未能繼續開業，其病歷應交由承接者依規定保存；無承接者至少應繼續保存六個月以上，始得銷燬。醫療機構對於逾保存期限得銷燬之病歷，其銷毀方式應確保病歷內容無洩漏之虞。」(修正理由一、本條新增。二、第一項由現行條文第四十八條第一項移列，並就病歷保存期限，因應需要酌作修正。三、第二項規定醫療機構因故未能繼續開業時，其既有病歷之處理原則。四、第三項規定對逾

保存期限病歷銷燬，仍應注意確保病歷內容無洩漏之虞。)

行政院衛生署 82.8.16.衛署醫字第八二五三０六四號函示

「說明： 一、復貴處八十二年七月二十二日八十二衛一字第０六二０三八號函。二、按醫療工作之診斷、處方、手術、病歷記載、施行麻醉等醫療行為，應由醫師親自執行，迭經本署函釋在案。因此，醫療機構有關處方箋之開具及病歷之記載，不論係採手寫、打字、或電腦製作，均應由醫師親自執行。 三、至於醫師親自開具處方及記載病歷以後，由其他人員將處方或病歷資料鍵入電腦系統，以利後續之調劑作業或病歷之研究、查考，尚無不可。

衛生署七十九年二月七日衛署告字第 857431 號函規定

「醫療機構使用電腦製作病歷者，於輸入電腦時，應隨即將紀錄內容列印，並由診治醫師簽名，以依法建立實體病歷資料，並依規定年限保存，對於電腦保存之病歷，亦應妥善管理，善盡法令所規定之保密義務」。多年來這種作業模式，除了需雙重作業管理保存紙本與電子病歷記錄相關資料外，亦需足夠的空間及設備以儲存病歷資料，在醫界已造成相當多的討論與爭議。

附錄二.HIPAA 隱私與安全規章節錄

HIPAA法案尚未通過之有關安全與電子簽章建議：
HIPAA訂定的安全與電子簽章建議書中共有四大部分，分別是保障資料完整性，保密性，以及可用性的**管理程序、實體防護、技術安全軟硬體、技術安全機制**。以下列出文中各子項目：

1. Administrative Procedures to Guard Data

Integrity, Confidentiality, and Availability

Certification

Chain of trust partner agreement

Contingency plan

- Applications and data criticality analysis
- Data backup plan
- Disaster recovery plan
- Emergency mode operation plan
- Testing and revision

Formal mechanism for processing records

Information access control

- Access authorization
- Access establishment
- Access modification

Internal audit

Personnel security

- Ensure supervision of maintenance personnel by authorized, knowledgeable person
- Maintenance of access authorizations record
- Operating, and in some cases, maintenance

Personnel have proper access authorization

- System users, including maintenance personnel, trained in security

Security configuration management

- Documentation
- Hardware/software installation & maintenance

Review and testing for security features

- Inventory
- Security testing

- Virus checking

Security incident procedures

- Report procedures
- Response procedures

Security management process

- Risk analysis
- Risk management
- Sanction policy
- Security policy

Termination procedures

- Combination locks changed
- Removal from access lists
- Removal of user account(s)
- Turn in keys, tokens, or cards that allow access

Training

• Awareness training for all personnel, including management
• Periodic security reminders
• User education concerning virus protection
• User education in importance of monitoring log-in success/failure and reporting discrepancies
• User education in password management

2. Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability

Assigned security responsibility
Media controls
Physical access controls be implemented
Policy/guideline on workstation use
Secure workstation location
Security awareness training

3. Technical Security Services to Guard Data Integrity, Confidentiality, and Availability

Access control (Procedure for emergency access must be implemented. In addition, at least one of the following features must be implemented, except encryption, which is optional.)
Audit controls
Authorization control

(At least one must be implemented.)
Data authentication
Entity Authentication (Automatic logoff and unique user identification must be implemented. In addition, at least one of the remaining features must be implemented.)

4. Technical Security Mechanisms to Guard Data Integrity, Confidentiality, and Availability

Communications/network controls
(If communications or networking is employed, the following features must be implemented: integrity controls and message authentication. In addition, one of either access controls or encryption must be implemented. If using a network, the following four features must be implemented: alarm, audit trail, entity authentication, and event reporting.)
Digital Signature