RDEC-PLN-091-002（委託研究報告）

隱私權保障機制：

以健保 IC 卡計畫爲例

研究主持人：　劉靜怡　副教授

共同主持人：　王大爲　副研究員

研 究 助 理：　蔣婉萍　鄭詩瑜

黃麗紅

行政院研究發展考核委員會編印

中華民國九十二年十月

目次

目　次……Ⅰ

提　要……Ⅲ

第一章 前言……1

第一節　研究主旨……1

第二節　研究主題背景與相關研究之檢討……2

第三節　研究方法與過程……12

第四節　研究內容大綱……13

第五節　研究預期發現與對相關施政之助益……13

第二章 全民健保 IC 卡計畫之內容與主要爭議所在……15

第一節　全民健保 IC 卡計畫之歷史沿革……15

第二節　健保 IC 卡計畫的爭議焦點……16

第三章 比較法制之介紹和探討：以美國法制爲重心……23

第一節　身份識別系統之建置及其利弊得失簡述……23

第二節　健康醫療資訊電子資料庫化趨勢下的 HIPAA 規範……28

第三節　HIPAA 之重要性及其檢討……44

第四節　德國與法國健保 IC 卡制度之比較經驗……55

第四章 現行全民健保 IC 卡制度應修正改進之處……61
第一節 法制面的補強……61
第二節 資訊安全如何確保的疑慮澄清……73
第三節 資訊隱私如何確保的疑慮澄清……81

第五章 結論與建議……87

附錄一 座談會紀錄（九十二年三月三日）……94
附錄二 座談會紀錄（九十二年三月四日）……104
附錄三 期末報告座談會紀錄（九十二年七月九日）……116
附錄四 Health Insurance Portability and Accountability Act of 1996 ……127
附錄五 Standards for Privacy of Individually Identifiable Health ……155

參考書目……272

提要

本研究係鑑於行政院衛生署中央健康保險局推動「中華民國國民健保卡實施計畫」（以下稱健保 IC 卡計畫）以來，在涉及人民隱私權保護的法律層面、科技層面和其他制度層面均引發不少爭議和辯論，爲了釐清政府在此一前所未有的重大政策的推動和執行過程中，可能出現的盲點和缺失，以確定此一政策需要及時修正和補強之處，本研究針對健保 IC 卡計畫內容中未臻周全之處，進行分析，並且分就健保 IC 卡的法制面補強措施（法律依據和契約相關事宜之分析），資訊安全疑慮的澄清，以及資訊隱私的保護等幾大部分，提出本研究計畫認爲就目前情形而言仍屬可行的調整和修正方向。

本研究的對象主要在於「資訊隱私」的保護機制如何形成和運作的問題，除了資料來源包含中文及外文的相關期刊與書籍之外，本研究計畫主要將分成法律層面和科技層面兩方面深入探討健保 IC 卡計畫的主要爭議，進而針對科技層面和法律層面做出具體之原則性建議。並且，本研究計畫以專家學者座談和焦點團體座談的方式，充分釐清健保 IC 卡目前遭遇的主要疑慮所在。

一、文獻分析法：從文獻中，引介國外相關法律和科技經驗，建立本研究之理論基礎。至於本國文獻方面，雖然目前搜尋所得有限，誠本研究亦將儘量在研究所需範圍內，予以援用參考。

二、專家座談法與焦點團體座談法：擬由從事相關領域研究學者專家，以及相關民間團體的座談中，對健保 IC 卡計畫和本研究計畫內容提出檢討與建議，以期在引介國外相關經驗後，一則檢視本研究計畫之架構和內容是否充實完備，再則進一步理解台灣社會在推行健保 IC 卡時所忽略的盲點和缺失。並嘗試藉此描繪適當的隱私權保護機制建構模式與運作機制。

本研究的內容，就文獻分析部分而言，分爲兩個部份。首先爲理

論層次的建構探討；其次則爲整理、分析國外文獻和法制相關經驗，進一步檢討其與我國相關制度建置的異同。接著，本研究計畫將參酌學者專家座談會和焦點團體座談會的意見，修正本研究計畫之架構和理論基礎，以提出較爲周延之政策建議。

本研究之發現包括：國外資訊隱私權保障相關機制和法制之主要內容、健保 IC 卡計畫的主要爭議和缺失所在、健保 IC 卡計畫之建置和營運契約內要內容分析、行政院在決定健保 IC 卡政策最終走向時應注意之處等等，相信研究計畫上述的分析和政策建議，對於行政院在針對此一健保 IC 卡計畫做成最終決策時，將有具體之貢獻可言。而且，綜合這些預期發現，將使行政院、研考會和衛生署將來在針對數位化業務的資訊隱私保護層面思考評估時，有所依循和參考。

爲了充分說明健保 IC 卡計畫在理論層面和執行層面可能遭遇的問題和阻礙，本研究自比較法制的觀點，說明身份識別系統和醫療資料所衍生的問題，至於說明分析的對象，則以本研究團隊比較熟悉的美國法制爲重點。

由於健保制度的差異和資訊隱私保護立法體制的不同，討論有關健康醫療資訊隱私的問題，美國制度的內容和經驗不見得能夠完全援用，是此處值得注意之處。所以本報告亦以簡要的方式，針對法國和德國兩國健保 IC 卡制度的主要內容，做了說明。

就本報告之結論而言，首先，在立即可行的建議方面，我們的建議如下：

一、加強健保 IC 卡之健保憑證意義和身份辨識證件兩者之間的意義區隔，澄清民眾的混淆所在

以健保憑證之本質來說，僅應被賦予確認健保身份的功能，不應

該轉而成爲身份證之外的另一身份辨識文件，進而衍生出身份辨識文件可能衍生的僞造變造或濫用等困擾，也不該以健保憑證之持有與否爲依據，越俎代庖地決定病患有無就診的權利。但是目前由於健保 IC 卡計畫宣傳中所謂照片卡可以免去攜帶身分證就診麻煩的說法，已經導致民眾混淆，有澄清之必要。同時，既屬健保憑證性質，其中所記載之事項和內容，即不應逾越憑證功能之所需，以免滋生資訊隱私不保的流弊。

主辦機關：衛生署；協辦機關：內政部

二、適當汲取比較法制的經驗，並且慎重分辨實行健保 IC 卡制度的國家和我國現狀不同之處

美國 HIPAAH 此一規範體制的擬定和辯論過程中所突顯出的問題，對於目前相關法制極爲欠缺的我國來說，極具價值，我們建議衛生署和健保局在制定配套措施和相應規範時，應該列爲重要參考依據。其次，當我們討論德國和法國的健保卡經驗時，必須區辨社會和制度脈絡不同之處。例如，因爲法國的保險申報方式，和美國的申報方式大致相近，是由被保險人先付款之後，再向保險公司申報退費。因此在使用 IC 卡做爲健保卡之前，無論是個人、醫療院所和保險機構往往爲了處理紙張形式的申報表，需要耗費大量的人力物力，而引進 IC 卡的目的，便是爲了減低這項行政成本。然而，與法國健保制度相較之下，我國目前的申報方式與法國截然不同，因此，我們的醫療院所與個人缺乏像法國制度背景下那樣的誘因。這或許也是爲什麼 IC 健保卡制度著手推行以來，不少醫療院所怨聲載道的原因之一。

主辦機關：衛生署

三、強化個資法等相關法令之規範密度和規範強度，儘速確立健保 IC 卡計畫的相關法律基礎

綜合前章所論，我們認爲目前我國規範個人電腦資料處理相關事宜的個資法以及相關的典章制度和組織文化，對於健保 IC 卡可能引發的個人資料保護問題，規範密度強度皆有不足之處，應儘速加強之。

其次，我們認爲，當健保憑證 IC 卡化和健保 IC 卡全面上線之後，健保憑證已經不再只是單純的健保憑證，而是在憑證功能之外，透過卡片儲存和網路傳輸等作用，開拓了增添不少憑證以外功能的無限空間；其所涉及者，是人民資訊隱私權是否能夠受到合法適當保護的問題，同時也涉及人民的資訊隱私權在何等情況下應該妥協，受某種程度之拘束或限制的問題；既然是涉及人民權利義務的事項，依據法治國家的法律保留原則，便應該透過立法的模式，透過全民健康保險法相關規定的修訂，或是訂定仿照美國特別法的方式，明訂健保 IC 卡的法律定位，徹底解決法源依據的問題；甚且，我們也認爲應該針對健保 IC 卡涉及醫療資訊的部分，修訂醫療法中和醫療資訊有關的規定，不應該繼續因陋就簡，以法規層級甚低的「全民健康保險憑證管理與使用須知」，做爲健保 IC 卡之法律依據。而是應該轉而思考以完整的法制架構和內涵，落實保護人民健康醫療資訊隱私的工作。

主辦機關：衛生署；協辦機關：法務部、研考會

四、健保 IC 卡建置計畫契約中相關權利義務事項規定的修正和加強

如同前章所述，檢視健保 IC 卡建置計畫契約之後，我們發現契約中對於資訊安全事項和資訊隱私保護相關之權利義務事項規定，不是模糊不清，便是付諸闕如。因此，我們建議，契約雙方應在可行之範圍內，儘速予以修正和加強，以落實健保 IC 卡計畫在保護人民資訊隱私方面的正當性。

主辦機關：衛生署；協辦機關：公共工程委員會

其次，在中長期建議方面，則可以區分成以下幾點：

一、以資訊安全透明度強化資訊安全

根據我們的觀察結果，我們認爲健保 IC 卡計畫應該追求以資訊安全透明度強化資訊安全的目標。首先，儘量公開資訊安全技術文件，針對認爲不該公開的文件，並應公開說明部分文件無法公開的理由；其次，亦應公開資訊安全相關委員會之成員執掌和相關活動之紀錄。我們之所以主張應該公開這些資訊，主要事基於符合政府資訊公開法制之立法精神、符合資訊安全原則、避免因爲對事實認知的不同造成的歧見與誤解、以公開資訊證明該項資訊之品質保證、以及有利於資訊安全的長期維護等幾個主要理由。同時，我們也建議在資訊安全方面，應該廣邀和廣納社會各界的參與和意見，避免過度的專業獨裁導致不必要的猜測。再者，和健保卡有關的所有建置計畫，其資訊安全規劃事項應該一併處理，不應過度切割，以免造成難以預測和彌補的漏洞。

主辦機關：衛生署；協辦機關：研考會

二、以強化資訊自主控制落實資訊隱私之保護

我們認爲，秉持資訊自主控制原則，是保護個人資訊隱私的不二法門，因此，就健保 IC 卡計畫而言，應該排除成見和既有規劃，研究最適當的資料分割方式，來滿足個人資訊自主控制的要求；當然最有彈性的作法是讓被保險人對每一項資料都可以決定是否要讓醫療人員讀取，但這樣的作法可能會造成卡片應用程式很大的負擔，需要研究適當的平衡點爲何。其次，健保 IC 卡過去至今的決策分析品質過份粗糙，在分析利弊得失的時候並沒有仔細的評估可能遭到的困難，今後似有修正改進的空間。例如，IC 健保卡減少醫療浪費的功能，必須在

第二第三階段階段實施後才可能發揮，但是在計畫初期，就可以預見這些敏感資料的存放必定引起大眾的疑慮與人權和社會團體的反彈。我們認爲，未來若能追求更加公開透明的決策過程，或者以設立隱私委員會的方式來處理資訊隱私相關問題，而不是將這類問題直接交由衛生署的醫療倫理委員會，做成可否的決策，可能是比較完備而且能夠服人的修正方向。至於有關未來個人資訊自主控制的規劃方面， 健保局應仔細分析評估如何在尊重個人意願與隱私的條件下將 IC 健保卡的功能發揮到最大。例如在充分尊重個人意願的情形下，在個人具有完全控制的條件下，將醫療相關資訊載入卡中。

主辦機關：衛生署；協辦機關：研考會

三、健全資訊稽核制度的建立和加強資訊倫理教育訓練

我們發現，在健保 IC 卡整體計畫中，無論是機關或機構之內部或外部，對於相關之資訊稽核審查制度，均未有充分的考量，我們建議應該仿照美國相關法制和措施，做完整之規劃，方足以確保健保 IC 卡計畫安全而順暢的運作，例如，醫藥衛生事務主管機關衛生署和健保局兩者，做爲全民健保制度運作的監督者和全民健保制度中唯一的給付者，應該善用醫療法和全民健保法中所規定的醫療機構監督權，在健保 IC 卡制度正式上路之前，全面建立上述機制，至少應該嚐試在醫療法和全民健保法兩項法律中尋找或儘速建立授權依據，設計出相應的細緻管制手段，要求健保 IC 卡制度下所涉及的醫療衛生機構建立此一資訊蒐集和處理事務的自我審查機制，以便大幅減少未來因健保相關資訊之蒐集和處理可能引起的反彈。同時，在健保卡計畫參與人員和醫療院所人員的資訊倫理教育訓練方面，目前之規劃也嚴重不足，就確保資訊安全和保護資訊隱私來說，也還有相當大的改進空間。

主辦機關：衛生署；協辦機關：研考會

四、非常之緊急狀況下不應亂求藥方，誤將健保 IC 卡當做醫療衛生政策之萬靈丹

政府行政和立法兩個部門，在檢討此次 SARS 疫情蔓延原因的過程中，數度提及健保 IC 卡可以有效預防疫情擴散，我們認爲此種主張有混淆之虞，充其量只展現出國人習於在非常緊急狀況下亂求藥方的陋規，才會誤將健保 IC 卡當做醫療衛生政策之萬靈丹，甚至可能將使各界更輕忽防疫真正關鍵問題。我們只要稍微回頭檢視感染擴大的原因，便可了解目前 95%的 SARS 感染都發生在醫院中，釐清導致各家醫院院內感染的根源。而經過歸納，SARS 疫情擴大原因可能包括：一、病人不知已遭感染，仍到急診室求診；二、醫師因爲各種原因對病情判斷有誤；三、病人疑似感染仍四處看病；四、醫療人員防護不足；五、醫院管理階層擔心收容 SARS 病患影響生意或導致封院，隱匿可能病例或將其轉院；六、疑似感染者隱身社區不願就醫；七、居家隔離執行令鬆散等。

想要解決前述第一與第二項癥結，必須從民眾公衛教育與醫療人員再教育著手。第三至五項則牽涉全國標準化的可疑病例後送與照護程序，避免病患成爲「人球」，同時得改善醫療院所過度商業化問題，否則，醫院將以考慮營運成本和效益爲優先，不願通報病例或未告知轉診醫院病患可能罹患 SARS，也可能爲了節省成本，要求前線醫護人員繼續使用可能已污染的防護設備，問題或病患刻意隱匿病例均非 IC 卡可解之問題。基本上病人就診史本可從紙卡背面戳記得知，並不需以健保 IC 卡達到此目的，病患倘若有意隱匿病史，也恐怕根本不願出示健保卡，甚或以其他特殊的就醫行爲來迴避。更詳細的確認病例亦應由胸腔 X 光、RT-PCR 檢測處理，不應指望記錄各種隱私資料（懷孕、經期、各種篩檢與疾病）的健保 IC 卡在此發揮此功效。

至於病患不願就醫，根源在於害怕疾病嚴重污名與歧視，這牽涉到官方、大眾與媒體對傳染病的了解與理性程度不足；居家隔離配合度問題，則與民眾教育與公民成熟度和官方配套措施之完備程度有

關。上述兩者其實都與 IC 卡均無關聯。試想，既然目前大家都已經知道 SARS 是足以快速致死的傳染病，既然願意上門求診，就代表求診者本來便具有恢復健康以便做長遠人生規劃的誘因，亦即應該有告知醫護人員主要接觸史和病情病史，以便及早獲得妥善治療的誘因，才能增加自己真正的福祉，因此，究竟是何種原因導致求診者決定「損己又損人」地隱瞞病情，就足堪玩味了：是不是錯亂的 SARS 相關資訊和社會不斷製造污名化的結果，造成求診者做出愚蠢的判斷和決策？是不是錯誤的醫療衛生體系設計使得病人有意無意地逛醫院和隱匿病情？甚至，我們是否更該深究到底是個別病人隱匿或是醫院控管粗糙，才是疫情擴散的主因，才更具科學說服力？

甚至，我們可以稍嫌武斷地指出，問題不在於要不要用 IC 卡，而是要有嚴謹的法規和正確的誘因機制，明確規範醫療院所和醫護人員及時回報的義務。

我們只要稍加分析，便可發現政府想透過健保 IC 卡解決的醫院通報問題，可以用更簡單方式解決：醫師診斷出可疑病例，即時以電話、傳真、網路報告衛生署，再由主管機關每天數次彙整通報病患資料給所有醫療院所。這些通報彙整，牽涉行政部門的效率整合，即使有了健保 IC 卡系統，也必須要有相關規劃配合，基本的醫療院所監督工作沒有做好，健保 IC 卡上的就醫紀錄記載得再多也無用。

病毒細菌與人類永遠共存，未來新興疾病只會更多，甚至可能引發更令人感到可怖的緊急狀態，我們認爲政府相關部門應該引此次 SARS 疫情擴散爲殷鑑，徹底檢討傳染病防治策略，而不是以病毒爲藉口，過度誇大健保 IC 卡的效能，反而導致社會各界對資訊隱私和公共利益如何平衡的看法更加偏離焦點分歧的不良結果。

主辦機關：衛生署；協辦機關：研考會

第一章 前言

本研究計畫之主旨，乃是希望針對我國目前推動實施中之健保 IC 卡計畫所涉及隱私權爭議，進行研究，並針對現況提出具體建議方向。從宏觀的角度來看，由於社會文化發展脈絡不同和基本法制建立時間較遲等緣故，和歐美國家相較之下，我國隱私權保障基本機制的建立，應該可以說是尚未真正步上正軌，而健保 IC 卡此一計畫，因爲涉及層面相當廣泛，則可視爲我國隱私權保障機制建立過程中的重要案例。

本章爲第一章，是本研究報告之前言，主要內容爲針對本研究之研究主旨做一說明，並且就本研究計畫之研究主題背景做一簡要之鳥瞰，進而說明本研究所使用之素材和研究方法，期能對本研究之整體架構和內容做提綱契領式的說明。

第一節 研究主旨

本研究係鑑於行政院衛生署中央健康保險局推動「中華民國國民健保卡實施計畫」（以下稱健保 IC 卡計畫）以來，在涉及人民隱私權保護的法律層面、科技層面和其他制度層面均引發不少爭議和辯論，爲了釐清政府在此一前所未有的重大政策的推動和執行過程中，可能出現的盲點和缺失，以確定此一政策需要及時修正和補強之處，乃接受行政院研究發展考核委員會之委託，以隱私權保障機制之建立爲研究主題，期能協助強調在民主憲政體制下既追求數位時代的效率，又能充分保障人權的政府，更加明確掌握健保 IC 卡計畫所涉及之主要爭

議，做出更爲明智而且可長可久的決策。

本研究雖然是屬於任務型性質的計畫，但是仍然希望在理論層面進行必要的探討，以便能夠對我國隱私權保障機制工程的基礎建立工作，有所貢獻。在理論基礎方面，本研究是以個人資訊保護和個人資訊自主爲前提，針對其如何和其他偏重行政和管理效率性質的諸般考量，儘可能達成平衡的假設出發，進行研究。綜合以上所述，本研究之目的有四：

一、引介國外健康及醫療資訊相關立法和制度的內容。
二、說明健康資訊及醫療資訊保護的理論基礎。
三、分析和評估中央健康保險局健保 IC 卡計畫的主要內容和影響。
四、討論健保 IC 卡計畫應有之隱私權保障機制之建構模式和運作機制。
五、政策建議。

第二節 研究主題背景與相關研究之檢討

自從全民健康保險（以下稱全民健保）開辦以來，無論是在節制醫療浪費，或者是在健保財務預測和監控方面，都受到不少質疑和檢討。中央健保局的健保 IC 卡計畫，規劃經年，健保局認爲，健保 IC 卡計畫建置之主要目的，除了要促進醫療資訊的整合、提升人民醫療照護的周延性和完整性之外，其實就是從考量目前台灣醫療環境及民眾就醫行爲的立場出發，希望能夠藉助健保 IC 卡的系統建置，達到對於重複就診、重複檢驗及重複檢查等醫療行爲，施以有效工具管控的目的，健保 IC 卡是爲有效之工具。並且，藉由健保 IC 卡之及時資料傳輸，立即有效地瞭解整體財務環境，推估醫療服務品質，降低醫界之經營風險，維持財務穩定，使全民健保之整體醫療服務供給不致扭

曲。

根據中央健保局的既定規劃，健保 IC 卡計畫目前已經開始進行全國性發卡作業。爲使全國民眾及醫療服務人員能逐漸適應並充分運用卡內資料，健保 IC 卡卡片存放資料採三階段逐步增列上線，各階段時程如下：

第一階段：九十一年七月至九十二年十二月，本階段開放使用之欄位內容，僅限於取代紙卡原有功能，以利民眾熟悉健保 IC 卡之使用，並利醫界調整醫療服務流程。

第二階段：九十三年一月至九十三年十二月，本階段將啓用醫師卡並開放費用資料欄位、長期處方箋與重要醫令如 CT、MRI 之登載。

第三階段：九十四年一月起，本階段配合本署國家健康資訊網路建置，以 IC 卡作爲病人授權醫師網路醫療資訊交換之憑證，提升醫療服務效益與品質。

由於健保 IC 卡計畫目前最受質疑者，乃是對人民的資訊隱私權保護是否周密的問題，因此，健保 IC 卡的存放資料內容，便值得特別說明。根據中央健康保險局的資料，首先，在卡體資料方面：健保 IC 卡外觀如名片大小，正面載明姓名、身分證字號及出生年月日三項個人資料，並依個人選擇印上個人照片，卡片左下方則有卡片流水號。一張健保 IC 卡片具備一般紙卡、重大傷病免自行部分負擔證明卡（以下稱重大傷病卡）、兒童健康手冊以及孕婦健康手冊等健保就醫憑證之功能，耐用五至七年，不需換卡。其次，在晶片資料方面：健保 IC 卡正面所嵌之 IC 晶片爲資料儲存區，計有「個人基本資料」、「健保資料」、「醫療專區」及「衛生行政專區」等四種資料存放區段，各區段預定存放內容如下：個人基本資料區所存放者爲「卡片號碼、姓名、身分證號或身分證明文件號碼、出生日期、性別、發卡日期、照片、卡片註銷註記」等資料。健保資料區所存放者爲「保險對象身分註記、

卡片有效期限、重大傷病有效起迄日（本項目前保留不實施）、就醫可用次數、最近一次就醫序號、新生兒依附註記、就醫類別。新生兒就醫註記、最近六次就診日期時間（本項目前保留不實施）、補卡註記、就醫序號、醫療院所代碼、安全簽章、就醫累計次數、保健服務(兒童、成人預防保健、婦女子宮頸抹片)、孕婦產前檢查」等資料，並將增列重大傷病代碼、主次診斷、醫師身分證號、就醫費用、部分負擔等，待實施健保資料段全部內容，即增列個人保險費資料。在醫療專區方面，存放者爲「門診用藥、重要醫療項目 CT、MRI」等，未來則將增列「門診檢查、治療及手術、住院重要檢查治療或手術、過敏藥物成分名稱」等。在衛生行政專區，則記載預防接種資料項目、器官捐贈資料項目。

在記載方式上，究其實際，上述各資料區段，所有欄位均屬健保業務資訊，均具有資訊隱私保護的意義，其中重大傷病註記與最近六次就醫紀錄則是目前較爲敏感且外界疑慮最深的資訊。目前中央健保局對於引起討論之重大傷病註記及簡易最近六次就醫紀錄，決定在第一階段中均不登錄，但顯然此並非根本解決問題之道，仍有待我們自資訊隱私保護機制的原始問題點上去釐清。另外，目前規劃定案之健保 IC 卡容量有 32K 位元，IC 晶片存放內容除上述各區段外，其餘晶片空間存放晶片應用程式及相關資訊安全管控程式，約占 10K 位元。除姓名爲中文顯示，其餘皆爲英數字。健保資料區之重大傷病註記及主次診斷碼均以 ICD-9-CM 代碼輸入；醫療專區之用藥紀錄及醫令，則以「全民健康保險支付標準代碼」輸入，並與健保資料專區「最近六次就診日期時間」紀錄連動。健保資料區及醫療專區有關醫療專業訊息之讀寫，則是均需配合「醫師卡」方可實施。因此，衛生醫療院所和醫護人員在醫事倫理和資訊倫理方面的素養如何，亦相當程度決定人民醫療和健康資訊隱私受到保護的周全程度，似乎也是政府在推動健保 IC 卡計畫時應該一併考慮檢討的重要周邊制度，但是目前衛生署在這方面的研究和規劃，則似乎未見具體可行之方案。同樣地，在日常及非常兩種時期的危機處理及應變計劃方面是否周全，也該是一併考量的重點。

其次，由於根據目前國內相關健保法令規定，健保卡之功能僅屬於「就醫憑證」，和人民享有全民健保服務的權利並無直接之關係，所以，目前規劃進行中之健保 IC 卡是否會成爲另位一種身分證件，最終甚至成爲電子病歷卡，也受到相當多的質疑。如前所述，根據中央健保局的資料和說明，健保 IC 卡卡片存放資料將採三階段逐步增列上線，IC 晶片內共有「個人基本資料」、「健保資料」、「醫療專區」及「衛生行政專區」等四種資料存放區段，而健保 IC 卡之個人專用安全機制，則可經由輸入個人密碼（PIN）方式產生進一步之保護效果。持卡者如設定個人密碼，將可使健保資料區及醫療專區等區段鎖碼。由於個人基本資料區和健保資料區內所登載之資料，多少仍然具有資訊隱私層面之意義，所以，即使如此規劃，是否便符合充分保護人民健康及醫療資訊隱私的理論要求，其實仍然不無探討空間。

另外，中央健保局指出，爲平衡病患隱私權與醫護人員之權利，未來亦將考慮重大傷病註記可由病患選擇是否登載，如不登載者，配套方式則可能是重大傷病患者須至特定醫療院所看診才得免部分負擔。然而，如此是否充分保障人民在全民健保制度下所應享有的就醫權利，是否達到不以不合理的差別待遇對待選擇不願暴露自己醫療健康資訊隱私的人民此一目的，此種規劃是否對部分疾病仍有影響，是否會導致醫療院所醫護人員的醫療專業判斷產生盲點，都應該進一步深入探討。

醫療服務在數位化的潮流下，在資訊科技大量引進與發展方面，一向居於各領域的領先地位，不論是電子病歷、網際網路醫療資訊服務、遠距醫療等，透過資訊科技與網路傳遞，加強醫療訊息之交換，均有助於追求醫療服務的最大效益與治療的完整性，並確保民眾得以獲得較高品質之醫療照護。然而，健保 IC 卡的發展與使用乃是朝可離線作業亦可連線作業的模式設計，幾乎已可稱爲一個攜帶型的小電腦。但是，在沒有讀卡設備的普遍化和資訊素養的提升等充分配套措施輔助下，個人對這部小電腦的控制程度，究竟如何，才能做到資訊自主控制的地步，卻是個極爲重要的問題。當醫療院所或醫護人員將

診斷及重要的檢查及用藥登載到健保 IC 卡上時，讓個人可以攜帶這些重要的結果或資料，是否就等於個人擁有自己的就醫紀錄，可以自己支配資料，自己可以決定資料流向，確保了醫療人權，其答案卻不見得是肯定的。更重要的是，依照目前中央健保局的規劃，健保 IC 卡系統乃是由承包廠商負責營運，在營運過程中，究竟中央健保局和承包廠商之間的互動關係和監督關係如何，目前既有的契約文件內容中是否已經充分考量到所有可能衍生爭議的情況，做了法律上的風險承擔和責任歸屬的適當安排，甚至，在實際考量醫療必要性時，究竟健保 IC 卡制度之有無可能帶來何種對基本人權保護和資訊交易成本所產生的影響，都將是本研究計畫中極爲重要的分析對象。

國內對於如何保障醫療資訊隱私和安全的的社會意識，最近逐漸進入萌芽階段，然而，和其他醫療資訊隱私與安全保護系統的先進國家相較之下，台灣在政策和法規此一基礎環境方面，卻仍然相當凌亂且欠缺。對一個積極籌劃進入醫療和健康資訊數位化的國家而言，此一現象對於公共利益和個人隱私的平衡來說，絕對是不利的。本計畫認爲，蒐集與整理國內外有關制定及推動「醫療資訊安全與隱私保護法」之重要發展趨勢與相關資訊，並且針對其內容進行分析和研究，對目前國內之相關政策和法規走向做出具體建議，將是當務之急，也是本計畫在法規研究部份應該著力之處。

相較於國內電腦處理個人資訊保護法和醫療資訊相關法規的不全和執行不力，健康和醫療資訊保護的問題在不少歐美國家長久以來早已是備受矚目的焦點，在法制建構上也已經努力甚久。以美國的發展爲例，二〇〇一年四月十四日，布希總統簽署了「可辨識個人之健康資訊隱私標準」(Standards for Privacy of Individually Identifiable Health Information)。這個行政命令是由美國國會先前通過的「一九九六年健康保險可攜性和責任法」(Health Insurance Portability and Accountability Act of 1996，簡稱 HIPAA)的授權而制定的，該法的主管機關則是「健康和人類服務部」(Department of Health and Human Services，簡稱 HHS)。這個法律的重要性在於其爲美國在健康資訊領域中第一個全國

性且系統性的法律，在此之前的相關法律，性質上都是屬於州層級的法律，至於總統簽署的此一行政命令，則是更進一步詳細地規定該法的實際運作模式。

在此必須特別說明的是，雖然美國目前並未如我國一般實施全民健康保險制度，但是在健康醫療資訊保護的學術討論上卻一直佔有相當重要的角色，而且，美國國內對於如何透過資訊的有效率運用，達到減少相關保險詐欺事件和提高醫療品質的討論，亦相當豐富，所以，美國雖然不足以做爲我國實施健保 IC 卡制度的高度參考指標，但是，從制度面和法律面來看，美國法制經驗卻依然具備高度之參考價值。至於其他具有全民健康保險制度的國家，在健保憑證方面究竟採取何種模式，是否發行及使用 IC 卡，如果未發行，其考量爲何？如有使用，其對其個人隱私權之保障機制爲何？這些問題本是本研究的重點之一，在必要的範圍內，本研究將搜尋分析美國的經驗，做爲論述的佐證。同時在主客觀條件可能與可行之範圍內，將相關法律文件、立法例、政府出版品等文件列爲本研究報告附錄之方式呈現之，以收法制對照比較之效果。

上述這個美國新近的法律之所以會出現，主要原因在於美國當時既存的法律對於健康醫療資訊所提供的保護不足，亦即既存的法律保護體系衍生出許多問題，不但在法律規定方面不適當，而且有彼此分割且不一致的現象。就憲法層次而言，在實際運作上幾乎只要是能夠舉出要追求的公共目的，也對健康醫療資訊提供看似合理的防護措施，就不會被判定爲違憲。同時，更重要的是，聯邦和各州憲法對隱私權侵犯的約束，也只限於政府的行爲，不及於私人的行爲，這就目前社會裡健康和醫療資訊處理的複雜程度而言，顯然是相當不充分的法律。至於在普通法體系的保護方面，美國州法（包括普通法和制定法）規定醫師、護士等人有要求保密的義務，否則會有民事責任。不過，在以下三種情況，亦即爲了保護第三人可識別的傷害、爲了公共健康的目的去報告資訊，還是可以未經個人同意而揭露該人資訊。雖然保密義務是傳統的隱私權保護架構和現代隱私權理論的先驅，不過

這種建立在醫病關係之間的義務，似乎已經過時了，因爲，現代健康資訊的蒐集，不限於臨床的醫病關係，且能夠取得健康資訊的人不只醫師而已。

簡言之，針對健康醫療資訊的保護，美國聯邦法律和州法的共同缺點，至少可以歸納出以下幾點：一、管制對象限於政府；二、未針對醫療記錄自動化之後的衝擊作規範；三、只保護特定的健康資訊；四、只規範特定的機構；五、某些資訊特別保護，某些則完全不保護；六、未有效地平衡個人隱私和公共利益；七、雖然有些州規定要告知後同意才可揭露資訊，但是例外卻太多。

在 HIPAA 中，國會在立法之初自己立下時限，亦即必須在一九九九年八月二十一日以前通過資訊保護立法，結果卻未能通過，只好由 HHS 的秘書處自行發布行政命令，也就是我們現在要討論的「個人可辨識健康資訊隱私標準」。該行政命令將於二〇〇三年的四月十二日開始生效。此一標準的主要內容，可以大致歸納如下，而這些內容，對於本計畫在歸納分析國內相關政策法規的問題時，想必亦能提供相當程度的參考和啓發作用：

首先，就該標準的規範範圍而言，在受保護的健康資料（protected health information，簡稱 PHI）方面，包含了所謂的「可辨識的個人資料」，也就是所謂的 PHI，任何可以辨識出該人身分的特徵，包括姓名、社會安全號碼、駕照號碼、指紋和「基因連結」（genetic link）等。HHS 在定義 PHI 時，包含了所有形式的資料，除了電子形式以外，書面和口語儲存的都算。在這一方面，可以說是具有爭議性的，因爲 HIPAA 並未明確授權給 HHI 保護電子形式以外的資料。

其次，就受規範的機構而言，包括健康計畫、健康照顧中心和健康服務提供者。健康計畫包括民營的（例如健康保險公司）和公營的（例如 Madicaid、Medicare），而健康照顧提供者則是指有連結到電子醫療資訊的醫師和醫院。同時，此一標準也包含了被規範機構的商業

代理人，包括律師、會計師等。雖然 HHS 無從管制律師和會計師的行爲，但是卻可以規範上述機構，如果上述機構知悉自己的商業代理人有洩漏 PHI 的情形，而不加以制止，則可以依法處罰被規範機構。不過，上述規範範圍似乎仍有闕漏。例如，針對人壽保險公司、勞工賠償保險公司等常常會接觸 PHI 的人，卻未能充分規範。

最重要的是，在同意使用和揭露 PHI，本規則有具體的規定，亦即在使用和揭露 PHI 前，必須得到本人同意。另外，也採取所謂「最小揭露標準」，意即在揭露或使用時，只能爲了達到使用目的而揭露最低的資訊量。不過，書面同意卻有實施上的問題。首先，書面同意書必須以簡明的文字書寫、告知 PHI 會被用在哪些地方、告知個人可以撤回該同意、告知個人可以要求被規範機構限制其使用範圍。不過，究其實際，上述書面同意制度其實並不是真的告知，也不是真的同意。一方面病人在接受治療前根本不知道記錄裡會有什麼資訊就簽署同意書，他也不知道到底未來這些資訊會被使用在哪些地方。另外，由於健康服務提供者往往會以病人的同意做爲治療的條件，造成實際上病人是被迫同意的此一結果。對服務提供者來說，是成本與效率的問題。

針對與健康照顧無關的資訊，本規則所提供的保護也相當週全，一樣也要讓個人同意授權。在同意書上對使用者、使用方法、使用目的得交代更爲清楚，甚至比健康資訊還要嚴格。

值得注意的是，本規則所規定的個人同意例外，其實便是爲了達成公共利益和個人隱私的平衡目的。首先，就法律執行方面而言，如果政府執行法律有需要時，不需要得到個人的同意。甚至，爲了發現犯罪真實，可以不經法院的同意，就揭露相關人的資訊，該規定也未給予法院任何裁量的判準。在司法程序和行政程序方面，此一例外同樣也未給予法院任何裁量的判準。其次，就未成年人而言，父母可不經未成年人同意，得知其子女的健康醫療資訊，至於其他重要的相關親友（Significant Others），其他與特定個人有關的親友（家人、朋友、管理人），在關於病人的治療、健康狀況的事項，可以毋庸得到病人的

同意就告知之。再者，因爲日常的公共醫療活動而揭露資訊，不需要得到病人的同意。例如，通知配偶其先生有傳染病，或者因爲商品有害而追蹤之行動，均屬之。

在醫療健康相關研究方面，原先大部分美國聯邦政府所贊助的研究計畫，都受到一稱爲「Common Rule」的規定管制，此一規定中要求設置審查委員會此種機構，審查計畫是否有「妥當地保護研究對象的隱私」。不過，此一 Common Rule 卻無從管制私人贊助的研究計畫。而此一新規則則是將管制對象擴大至私人贊助的研究計畫。亦即委員會若覺得研究計畫不會傷害到個人隱私，則可以揭露該資訊，不需要個人的同意。另外，就市場行銷領域而言，爲了進行市場行銷，不論是面對面的行銷，或是否與健康產品有關，都可以不用得到個人的同意。

歸納以上內容，我們可以發現這個規則的幾種例外彼此之間所追求的價值似乎有所矛盾，而以下幾個面向的檢討，或許可以提供給我們一些思考線索：首先，此一立法體制的目的，是要促進健康照顧，然而，以上所述的執行法律、司法和行政程序、市場行銷等三種例外，似乎與促進健康照顧無關。其次，以個人利益爲考量重心，也是此一立法體制的主要價值所在，是讓父母可以知道自己未成年小孩的醫療情況（例如懷孕或變性）的例外，卻可能導致因爲小孩可能擔心受罰，而不去就醫的結果，反而不利於小孩的利益。因執行法律和司法程序而揭露，若是使用上不受限制，也對個人不利。再者，在促進公共健康時應該儘量減小對隱私的傷害，同時，醫療產業的商業利益，似乎也不該是考量重心：醫療相關產業可能會主張，必須得到病人的 PHI，好讓他們得知與他們健康有關的產品服務訊息。但是即使如此，是不是應該立法明文成爲例外，還是有其他機制可以達成同樣目標，似乎仍有相當寬廣的討論空間。

被規範機構的資訊隱私和安全政策應該如何釐訂，也是本研究計畫在法規制度方面的研究對象之一。我們認爲，美國法制有其可取之

處，亦即被規範的機構必須制定隱私和安全政策，以保護健康醫療資訊。同時病人有權質疑這些政策，並且提出告訴，而上述機構則不可以要求病人放棄權利，以獲取治療。此一目的，必須透過相關制度要求受規範者應該從事公正的資訊活動來達成，亦即賦予病人被通知權，以及閱覽受保護的健康資訊的權利、修改受保護的健康資訊的權利、要求對揭露活動進行清查等權利。

最後值得一提的是，在保護健康醫療資訊隱私方面，法律可以在系統建置方面介入多深，方屬適當的問題。以智慧財產權的保護爲例，美國憲法第十七條保護智慧財產權，故對智慧財產權在法律上的保護，一直多過隱私的保護。另外，智慧財產權的當事人，也有比較多的經濟誘因會使自己尋求保護，甚至集合起來尋求保護，我們可以從歷史上找到許多實例。但是相對地，隱私權所有人卻沒有什麼經濟誘因去尋求保護。也由於交易成本和集體行動的問題，隱私權所有人通常不會於事前跟侵害人締約。另外，從利益團體理論的角度來看，少數利益集中的大企業，不希望有太多的資訊隱私保護，但是多數的小市民，卻沒有集中的力量與之抗衡，故而出現對隱私的法律保護很少的現象。除了上述標準所規定的原則之外，集體訴訟和建立健康醫療資訊安全港這兩種作法，可能是解決隱私保護不足問題的可行方法。不過，值得附帶說明的是，像音樂生產者那麼大的集團，要求法律保護是那麼容易，卻仍然覺得法律不夠用，更別說是醫療隱私權所有人的處境有多困難了，我們在討論分析比較法的內容和進行我們應該如何立法的考量時，或許更該注意此一問題。總之，在醫療服務數位化的潮流下，如何確保健保 IC 卡登載之內容資料與使用符合電腦處理個人資料保護法之規範，甚至進一步加強目前醫療法等相關法規的修訂，使其得在資料流通和使用管道極端複雜化的環境中，仍然能夠符合個人資訊隱私保護的理想，將是極爲嚴酷的挑戰，可惜目前國內無論是實務界或學術界，在此一方面的研究都只能算是處於起步階段而已，因此，本研究計畫在隱私保護機制建立的研究方面，可以努力空間仍然相當廣大，我們也期待此一短期研究能夠達到提出具體政策建議的目的。

第三節　研究方法與過程

本研究的對象主要在於「資訊隱私」的保護機制如何形成和運作的問題，除了資料來源包含中文及外文的相關期刊與書籍之外，本研究計畫主要將分成法律層面和科技層面兩方面深入探討健保 IC 卡計畫的主要爭議，進而針對科技層面和法律層面做出具體之原則性建議。並且，本研究計畫以專家學者座談和焦點團體座談的方式，充分釐清健保 IC 卡目前遭遇的主要疑慮所在。

爲達此預期成果，擬以下列研究方法達成研究目的：

一、文獻分析法：從文獻中，引介國外相關法律和科技經驗，建立本研究之理論基礎。至於本國文獻方面，雖然目前搜尋所得有限，誠本研究亦將儘量在研究所需範圍內，予以援用參考。

二、專家座談法和焦點團體座談法：擬由從事相關領域研究學者專家，以及相關民間團體的座談中，對健保 IC 卡計畫和本研究計畫內容提出檢討與建議，以期在引介國外相關經驗後，一則檢視本研究計畫之架構和內容是否充實完備，再則進一步理解台灣社會在推行健保 IC 卡時所忽略的盲點和缺失。並嘗試藉此描繪適當的隱私權保護機制建構模式與運作機制。

此一部份的座談，乃是以蒐集民間反對健保 IC 卡制度之主要理由，例如 IC 卡遺失遭到冒用、目前電腦系統安全性堪慮、個人資料遭竊層出不窮的情況下 IC 卡登錄之個人就診記錄極有可能外洩，懷疑個人隱私權可能經由健保 IC 卡承包商手中外洩，以及健保 IC 卡等數年前一度規劃推動之國民 IC 卡之異同等等爲主要目的，換言之，在此一部份，本研究希望能夠深入發掘健保 IC 卡此一制度所涉及之各種利害相關團體或關係人，如健保局、民間得標承辦機構、醫療人員、被保險人、被保險人家屬、法院及一般民眾等所持的意見和立場，針對其

所提出之不同利害得失及考量重點，進行分析俾供政策決議取捨。

第四節　研究內容大綱

本研究的內容，就文獻分析部分而言，分爲兩個部份。首先爲理論層次的建構探討；其次則爲整理、分析國外文獻和法制相關經驗，進一步檢討其與我國相關制度建置的異同。接著，本研究計畫參酌學者專家座談會和焦點團體座談會的意見，修正本研究計畫之架構和理論基礎，以提出較爲周延之政策建議。

第五節　研究預期發現與對相關施政之助益

本研究之預期發現包含有：國外資訊隱私權保障相關機制和法制之主要內容、健保 IC 卡計畫的主要爭議和缺失所在、健保 IC 卡計畫之建置和營運契約主要內容分析、行政院在決定健保 IC 卡政策最終走向時應注意之處等等，相信研究計畫上述的分析和政策建議，對於行政院在針對此一健保 IC 卡計畫做成最終決策時，可以有具體之貢獻。而且，綜合這些預期發現，將使行政院、研考會和衛生署將來在針對數位化業務的資訊隱私保護層面思考評估時，有所依循和參考。

第二章 全民健保 IC 卡計畫之內容與主要爭議所在處

本章的主要目的，是針對全民健保 IC 卡計畫的內容，以及歷來所引發的討論，進行簡要的整理和歸納，以便能夠釐清爭議焦點所在。

第一節　全民健保 IC 卡計畫之歷史沿革

如前章所述，全民健保 IC 卡之緣起，和原來準備於 1998 年開標建置的國民卡計畫互有淵源，國民卡計畫推出當時便受到不少出自於人民資訊隱私保護層面的質疑，國民卡計畫當時雖然因爲議約不成而停擺，但是，針對電子病歷系統和健保 IC 卡建置計畫，衛生署和健保局則是一直持續進行，並未中輟。自 2002 年七月開始發卡至 2003 年三月爲止，健保 IC 卡已經發行了一千萬張左右的卡片，雖然此一計畫預計要在 2003 年六月完成，但是社會大眾對此一計畫和相關措施仍然有所質疑。

換言之，由於預算執行進度之故，全台目前已經有三分之一左右的人口拿到健保 IC 卡，而本計劃的承包廠商則是交由東元企業集團旗下的東元科技股份有限公司負責。在承作廠商方面，之所以會引發爭議，是因爲在東元科技股份有限公司的規劃中，未來將發展相關的電子商務業務，同時亦規劃前往中國發展類似業務，所以，承作廠商是否會將其透過業務運作而得以接觸的人民個人資料，以不當的方式進行商業層面的應用，甚或做出對人民資料所涉及的國家安全事宜有害的事。同時，除了懷疑主管機關衛生署和健保局的監督能力和監管措施是否充分之外，東元科技股份有限公司的軟硬體的工作人員，是否

也在該公司良好嚴密的監督下從事相關業務的實際執行工作，以確保資訊安全和個人隱私的保護，也是眾所關切的重點所在。大體上來說，目前健保局是透過與東元科技股份公司訂定契約的方式，依照契約中所規定的權利義務事項，來控管東元科技府份有限公司的行爲。根據這份契約的內容，要求東元科技公司必須提出安全企劃書，並且成立安全防護小組，專門負責健保 IC 卡業務執行過程中的安全防護作業。

第二節　健保 IC 卡計畫的爭議焦點

即使健保 IC 卡在目前既有的建置下，並不是全然欠缺保護機制，但是依然受到不少質疑，而且每個質疑彼此之間皆環環相扣。再者，就醫療服務所涉及的資訊問題來說，個人所關心的問題往往與醫療院所所關心的問題不同，這些差異相當容易引發問題及衝突。人民所關心的是資料放在該處的安全與否，會不會遭駭客竊取或被不當利用等外部入侵與內部管理問題，及個人本身對其資料的控制管理權問題，對於資料的審核或授權，是應採分階段同意制或者是全面授權制。而醫院所關心的是相關費用的支出，例如讀卡機成本由誰負責，及如何降低成本。

歸納起來，則可以整理成以下幾個部分的主要爭執重點：

一、　個人資訊隱私權保護爭議

依據健保局的說法，目前健保 IC 卡已發行一千萬張以上。而整個健保 IC 卡計畫目前是第一階段，資料內容就相當於現在的紙卡內容，沒有納入任何病歷資料。其他資料在第二階段〈93 年 1 月起〉才陸續

納入，但是健保局也指出第二階段以後是有彈性的，該放什麼資料，是要經過對談和討論才決定內容。因爲 IC 卡的容量只有 32K，無法詳細紀錄任何醫療過程，同時也不如外界所擔心的，其實並未放入病歷資料，也沒有家族病史或 DNA 圖譜等資料。

健保局指出，第二階段的蒐集仍以健保業務相關的資料爲主，亦即希望有助於醫師的診療，並且可以作跨院的整合。IC 卡的好處在於卡面看不出卡別、醫院紀錄，並可節省換卡的時間成本和換卡據點等社會成本。健保局承認 IC 卡的確有其風險，其防範措施則是使用 pin code，並且要透過健保局的讀卡機才能讀出。同時也承認某些疑慮如個人資料是否會被盜用、個資法到底有沒有完善保護的問題等等，有其正當性。健保局指出，上述問題並非新問題，由於現在很多醫院都已電子化，醫院資訊也有可能會外洩，IC 卡並非引起上述問題的源頭，而是全面涉及隱私權考量、醫學倫理和科技資訊等等因素的問題。

批評健保 IC 卡計畫者，對於健保 IC 卡整體計畫是否有防禦外來危險的機制？政府是否有良好的技術與配套措施解決個人資訊隱私在健保 IC 卡計畫下可能遭遇的不當甚或不法暴露問題？例如，對於愛滋病友團體而言，立場上應該是屬於支持全民健保制度的，但是對於健保 IC 卡計畫，則持有不同的意見。其意見主要可以歸納成以下幾點，而且，在反對健保 IC 卡計畫的個人團體中，也甚具代表性：第一，第三階段之後會使病患隱私嚴重曝露，關於放入何種資料和放入多少資料的問題，在健保局的文宣和廣告上少有說明。同時，即使放入的資料是使用代碼，也同樣可以間接推出其意義；並且，健保 IC 卡計畫其實將放入大量的資料，例如可以放入 60 筆用藥紀錄，這樣的數量幾乎可以是一個人一生的用藥量了，更重要的是，60 筆用藥紀錄更是意味著使用了某些藥物之後，有可能必須再累積 60 筆紀錄才會消掉該紀錄，這樣很容易暴露病人隱私並且爲某些病人貼上標籤。例如愛滋病患者便可能一再地被貼標籤，以目前 AIDS 的防治而言，大概只有一半左右的病患就醫，主要是因爲既有的醫療制度威脅人民的隱私，如今使用 IC 卡極可能使問題加劇。第二，雖然健保 IC 卡計畫內的資料

並非全然完整，但是已經足已探知人民隱私了。卡片上 32K 的容量可放 16000 字，容量其實十分地大，而且是由別人寫入，病人自己對於寫入內容爲何，也無從知悉，值得擔心。第三，健保局強調健保 IC 卡內簡單的註記可以幫助醫師做判斷，但是這其實應該是利用轉診制度的落實就已經足夠，無須再疊床架屋。第四，IC 卡並非健保局所宣稱的一般方便，因爲每就診六次還是要再刷一次，拿藥還要再寫入紀錄，對病人來說是多出一道手續。現在的醫療制度已經有許多的漏洞，使用 IC 卡可能只是再多增添複製漏洞罷了。最後，健保 IC 卡計畫不應該被看成是單一的健保 IC 卡個案，而是整個國家科技政策的問題，我們應該思考爲什麼國際潮流走向保護隱私之際，台灣還是決定採取會對隱私造成高風險的作法？

另一方面，對健保 IC 卡持比較正面態度的人，則是指出：第一階段的 IC 卡只紀錄原本健保紙卡的資料，這是比較沒問題的，而第二和第三階段，可能較具爭議性，包括就醫紀錄和病歷資料等。由於人民的醫療紀錄並非是由健保局紀錄，而是由醫生直接在爲病人看病時，直接紀錄在 IC 卡內，而健保 IC 卡的記憶容量並不大，只有 32K，所以資料能放的並不多，而且存放的是疾病碼並有經過加密的處理，並不能被隨便讀取，只能用由健保局所製作的 IC 卡讀卡機才能讀出〈讀卡機是由承包廠商東元科技公司製造提供〉。同時，之所以要在 IC 卡中紀錄某些病歷資料，如重大傷病代碼，目的就是爲了要免除病人的部分負擔費用，是有益於病人的。所以，目前健保 IC 卡計畫第一階段的工作已經結束，正要展開第二階段和第三階段的工作，而可以想見的是隱私權的爭議會愈加嚴重，但是當務之急是要培養國人的資訊保護概念。同時，由於最有爭議的是病歷史是否要放入健保 IC 卡內，如果放入會產生什麼問題與風險，那麼，更該讓人民充分認識到其本身資料放與不放的問題及風險所在，了解後自己選擇並承擔風險。舉例而言，在美國可以上網看病歷，但全都可以留下紀錄，以便於進行稽查。同時，贊同者認爲雖然民眾可以選擇使用 PIN CODE 保護自己的資料，但也應讓其了解這種方式是否仍具有風險，風險何在，以及如果未來發生緊急醫療救護的需求時，因爲自己無法言語或語言不清致

使無法讓醫療人員使用過往資料時，可能導致何種風險也必須了解。贊成者認爲在美國有 break glass 機制，只要有經過授權，在人命危急的前提情況下，可以去存取病歷資料，目的就是要讓個人即使在簽署個人資料保護協定之後，也不要因此而造成遲延，犧牲生命。

贊成者認爲第二和三階段的資料建構仍然是不可偏廢的，但是可以保留某程度以上的資料或是敏感性資料。然而，因爲涉及醫護人員的責任，這些資料可能就具有重要性，如果病人保留某些資料未讓醫療人員得知，而使得醫療人員誤判，則責任歸屬於誰？所以醫療人員到底能不能詢問病史？能不能建檔儲存？甚至上傳至健保局？或是就儲存在健保 IC 卡內？這些都是值得深思和做細部分析的問題。

針對上述正反意見，健保局的態度似乎是，第二和第三階段的計畫執行工作，要等待社會共識充分形成之後，再決定要放入哪些具體的資料。目前健保局認爲有三種方案可以選擇（一）放入資料，用 pin code 保護；（二）某些資料完全不考慮放入；（三）預留空間，讓人民自己選擇是否放入。這三種方案都必須有配套措施，而且要分別討論放入與不放入所可能涉及的風險。

針對上述官方立場，對健保 IC 卡計畫持比較保留的態度者指出，雖然健保 IC 卡可以使用的範圍相當廣泛，但是基於各種和隱私保護相關的原因，仍要加以限縮。不過，要以資訊保護爲由，阻礙科技發展及應用的作法，終歸會失敗，因此有建議應將批評健保 IC 卡計畫之相關資訊分爲三類來處理：（一）無爭議性的資料，亦即目前紙卡就已經有的資料；（二）較具爭議性但有用的資料，例如病歷，這類資料可以考慮在配套措施做好之後再放入；（三）絕對不應該放入的資料，就不應該考慮放入。

另外一個問題則是涉及程序的問題，在醫療資訊的使用上，IC 卡只是冰山一角，如果衛生署第一關都無法把關，那麼身爲個資法法務部就很難接著設計進一步的規範。同時，醫療資料庫的使用必須嚴謹

且絕對要用正確的方法爲之，尤其是如果要將醫療資料庫與其他資料庫（例如財稅資料庫）作交叉運用的話，更應該要有透過法律層級的程序，做爲規範依據，方得爲之。

最後，亦有批評者指出，健保 IC 卡計畫原意不該限於抑制健保浪費，而是也希望解決弱勢的就醫問題，例如在偏遠的山區，因爲沒有病史，常常會延誤診療時機，所以弱勢團體應該樂見 IC 卡能解決病歷傳輸的問題；不過，在人民權利保護方面，卻因爲衛生署和健保局絕大多數情況下只諮詢醫療院所和醫師的意見，導致和民間社會團體溝通不良的結果，醫療專業霸權當道的結果，反而忽略了健保 IC 卡的目的是爲了在便利人民就醫和節省成本之餘，對人民盡最高的權利保護義務。也忽略了是否應該考慮政府的善意（good intention）不必然帶來良善後果（good consequence）的問題。

二、 健保 IC 卡計畫所涉及的各方當事人間權利與義務問題

健保 IC 卡計畫所涉及的各方當事人，彼此之間究竟應該是具有怎樣的權利與義務關係，也是關心健保 IC 卡計畫者經常提及的問題。首先，健保 IC 卡計畫究竟具有什麼樣的法律保護規定和科技保全機制，以確保健保 IC 卡持卡人的資訊隱私安全。例如，在全民健保的強制納保體制下，雖然健保 IC 卡上的照片是被保險人自願放進去的，但是在要求被保險人提供照片當初，是否出現告知不清甚或半哄半騙要求人民繳交照片的情況，反對者認爲是有質疑空間的。健保 IC 卡讀卡機設備的費用由誰負擔，也曾是爭議之一。此外，政府公權力在健保 IC 卡計畫中的角色，也值得討論。根據個資法的規定，健保 IC 卡計畫所涉及的資料隱私問題，似乎沒有任何清楚負責的主管機關，當初中研院資訊所即曾討論過否應該交由健保局或衛生署負責，但是由涉及個人資料處理業務主管機關本身來擔任監督者，其結論則是認爲這種作法很可能是球員兼裁判，似乎難免終歸失敗。

其次，質疑健保 IC 卡計畫者指出，我國的健保制度是採強制加保的方式，人民沒有選擇要或不要的權利，那麼要人民如何能信任健保局呢？同樣地，健保 IC 卡也是強制的，雖然法律依據仍有疑慮，但是在實務操作上，人民幾乎沒有選擇的機會，即使主管機關很難令人信賴，結論也無兩樣。舉例而言，雖然北區健保局經理因不配合警調單位偵查而被控妨害公務的罪名移送，但是北區警調單位不也移送了兩名健保局員工，該員工竊取人民的醫療資料之後再轉賣給保險公司，而移送法辦的是兩名員工，處罰的也是兩名員工，健保局高層都未因此而受到處罰，則高層又如何會關心要加強保護資料隱密性呢？倘若連信任中央健保局的安全維護機制都不容易，何況是民間機構？所以未來應該強調參與健保 IC 卡計畫各個當事人之間信任機制何在和如何建立的問題，同時也該針對訓練人員素養和安全防護措施等事項加強。同時，在健保 IC 卡使用之後，是否會改變個人的就醫行爲，也是值得附帶處理的問題。

最後，質疑者也指出，由於保險憑證是由健康保險法授權而來的，而健保 IC 卡所涵蓋的範圍已經超過健康保險法中所授權的範圍，因此就產生了兩個問題：第一就是健保局是否適宜就健保 IC 卡相關的資訊管理與搜集？第二就是這樣做，對民眾的利益爲何？而且，第二和三階段的資料以健保局的說法是可以方便資料流通，以及節省資源浪費，但是其中仍有些問題，舉例來說，倘若病人已作了 MRI 的治療，醫療過程上是不該重複做的，那麼法律上的配合及醫療行政上是否清楚？最重要的是第二和三階段的資訊揭露，也涉及到各個醫療院所的病歷移轉信任關係，如果甲病人曾在 A 醫院看病，病歷儲存在健保 IC 卡中，之後，甲再到 B 醫院看病，B 醫院的醫師是否信任 A 醫院的醫師所載入的病歷資料？出了錯又應該由誰來負責任？如果又因病人本身自己保管 IC 卡不當，致使資料出錯，又該誰來負責任？

第三章　比較法制之介紹和探討：以美國法制爲重心

爲了充分說明健保 IC 卡計畫在理論層面和執行層面可能遭遇的問題和阻礙，本章將自比較法制的觀點，說明身份識別系統和醫療資料所衍生的問題，至於說明分析的對象，則以本研究團隊比較熟悉的美國法制爲重點。

第一節　身份識別系統之建置及其利弊得失簡述

健保 IC 卡在我國法律定位上是屬於全民健保就醫憑證，出示健保 IC 卡時便等於具有某種程度的身份辨識功能，然而，在進行身份辨識之際，可能出現哪些減損身份重要性的問題，或者爲身份辨識帶來負面的影響，以下即簡要分析美國學者所做的相關論述，做爲參考。

根據美國邇來研究身份識別系統和各種人民個人資料庫的著名學者 Richard Sobel 的看法，美國目前正積極討論整合全國性身份號碼（national identification numbers）、資料庫和身份證件（identity cards）的全國性身分識別系統，違背了憲政精神及民主政府的哲學基礎，然而，九一一事件卻加速了這個趨勢的發展。[1]

Sobel 認爲，無論是以哪種身分識別資料爲核心的身份識別系統，全國性身分識別系統〈national identification systems，簡稱 NIDS〉比較

---

[1] Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37 (2002).

適於解決封閉社會的問題，如果是在一個開放自由的社會裡實行這種制度，則極可能會破壞開放自由社會的核心價值—強調選擇與機會〈options and opportunities〉的社會基本價值。NIDS 等於是將個人特質〈personhood〉由每一個本來具有特質的個人本身抽離出來，代之以數字量化測量，由卡片代表，或者是由電腦資料庫記錄，因而弱化(degrades)了個人的意義。Sobel 認爲，NIDS 的發展會使原先強調個人特質的美國人，不再是美國人，只有一個訴諸威權主義〈authoritarian〉的社會，才可能經由身份號碼與相關憑證來否認個人獨特的身份認同與機會(identities and opportunities)。[2]

簡單地說，美國這一兩年來因應特殊需求所發展出來的 NIDS，是由號碼資料庫與身份辨識要求(ID requirement)發展而來的，細究之下，則可以分成幾個層面來觀察美國目前主要的 NIDS：

一、 Immigration Reform and Control Act of 1986 (IRAC)

要求雇主令受僱人提供其爲美國公民或政府允其工作之證明。受僱人必須在證明表格（I-9 verification form）上填寫並簽名後，提出政府核發之身分證件，例如護照。雇主每僱用一次不符上述資格的外國人，將被處以高達一萬美元的罰金；且若該雇主從事上述行爲，還可能須入監服刑，至多可達六個月。[3]

---

[2] *Id.* at 38-40.

[3] *See generally* Jack L. Runyan, *A Summary of Fed. Laws and Regulations Affecting Agric. Employers: Immigration Reform and Control Act of 1986,* U.S. DEP'T OF AGRIC., ECON. RESEARCH SERV., AGRIC. INFO. BULLETIN NO. 652 (AUG. 1992).

二、 Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA)

此一立法嚴厲處罰「以詐欺方式使用政府所核發之文件」(fraudulent use of government-issue document)的行爲。倘若違犯該法所規定之其他更爲嚴厲的條款規定，最高甚至可能被判刑 25 年。同時，此一立法也規定了一個五個州(five-state)的「關於工作資格證明的試驗計畫」(Pilot Program for Employment Eligibility Verification)，該計畫允許以資料庫審核社會安全號碼。並且授權提供經費給愛荷華州的「機器可讀取文件試驗計畫」(Machine-Readable-Document Pilot Program)和「外國犯罪者身份系統」(Criminal Alien Identifycation Syatem)進行試驗計畫。

IIRIRA 的立法意旨，是希望能夠統一各州的出生證明及駕照，並且藉此發展出標準的社會安全卡雛型(development of prototype counterfeit-resistant social security cards)；在 IIRIRA 的規範下，雇主不再能夠憑著檢查其受僱者的美國公民證、歸化證或未過期的外國護照等等方式，來證明其受僱者具有被允許工作的資格，而是必須檢查其美國護照、綠卡(resident alien card)或外國人紀錄卡(alien registration card)才算盡到義務。[4]

三、 Personal Responsibility and Work Opprtunity Reconciliation Act of 1996 (Welfare Reform Act)

本法以立法方式明文授權設置一聯邦層級的資料庫，以便能夠紀錄和追蹤新進受聘的人員。此一資料庫記錄了自 1997 年 10 月 1 日後受雇的人員姓名、住址、社會安全號碼和薪水等資料。這些資料由州

---

[4] IIRIRA, Pub. L. No. 104-208, 404, 110 Stat. 3009-664 to 3009-665 (1996) (codified as amended at 8 U.S.C. 1324a (2000)).

收集後之傳輸(transmitted)到附屬於 Department of Health and Human Services(HHS)的一個全國性資料庫中。

此一立法的最初意旨，在於協助聯邦與州政府，針對個人的工作轉換和在各州遷徙的情形，追蹤那些未能妥善扶養其子女的父母，然而，此一立法授權資料庫的結果，實際上卻影響到了所有的新進受僱者，並且將隨著時間的經過而擴及其影響到所有勞工階層。[5]

四、 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

本法授權發展出一套「特定（獨一無二）的健康身份識別」(unique health identifier)，其目的在於使追蹤病人、健康照護提供者、醫療計畫、以及追蹤由公共與私人經費所給付的健康照護費用等等，變得更爲容易。由於此一立法之部分目的在於使健康保險能夠隨著個人轉換工作而移轉，所以其也就授權針對個人健康照護資料，建置一個全國性的電子化資料系統。此一立法授權結果，使得病人轉換醫療人員時，此一資料庫也能發揮監控病人的健康、協助病人取得其舊有資料、並且得以協助成本分析與研究的功能。同時，所有病人的醫療資訊，即使是自費給付的相關資訊，都會被囊括入這個資訊系統當中。[6]

五、 FAA ID requirement and Computer Assisted Passenger Screening system (CAPS)

美國聯邦航空總署（Federal Aviation Administration，簡稱ＦＡＡ）要求航空公司必須要求國內線的乘客出示政府所核發之附有相片的識

---

[5] Welfare Reform Act, Pub. L. 104-193, 111, 110 Stat. 2105 (1996) (codified as amended at 42 U.S.C. 405 (2000)).

[6] *See* Sheryl Gaye Stolberg, *Health Identifier for all Americans Runs Into Hurdles,* N.Y. TIMES, July 20, 1998, at A1.

別證，表明自己的身份。爲了避免恐怖事件的發生，CAPS 則是針對進行 check-in 程序的乘客，予以完整掃瞄描繪(profiled)下來，符合某些描繪條件者，就會被徹底搜查其行李及身上的隨身物品。依據描繪結果，有一些從被檢查過的行李當中挑出的行李，也會被要求強制施以 X 光檢查。

六、 其他公共或私人的資料庫與身份辨識要求

其他公共或私人的資料庫與身份要求，也助長了 NIDS 的趨勢。例如，Department of Transportation(DOT) 和 Social Security Administration（SSA）便要求將駕照和社會安全卡列爲身份辨識證件，並且責成 DOT 去要求將駕照聯邦化(federalize)，而聯邦化之後的駕照，則將列有駕駛人姓名、住址、電話號碼、生日、照片和社會安全號碼等資訊。1966 年 DOT 即要求各州於 2000 年 10 月 1 日之前將社會安全號碼列於駕照上，例如喬治亞州州議會則是於 1996 年 4 月通過將指紋列於駕照中的法律，以爲回應，至於加州、科羅拉多、佛羅里達、夏威夷等州則是在此之前便採取類似措施。

其次，想要取得或更新美國護照者，必須提供納稅人識別號碼(通常就是社會安全號碼)，否則就必須繳交 500 美元的罰款給國稅局〈IRS〉。這種作法雖然是用來檢查要離開美國國境的外國人或者公民是否有納稅，但是卻是由核發護照給居住於美國的公民的政府部門執行。此一法律因而長期被批評爲有違反公平資訊(fair information)原則。

由於 NIDS 會讓每個個人具有一個獨一無二的國民身份號碼(national identity number)，資料庫也就可以經由此一由政府所發給的數字，以從搖籃到墳墓的方式，來追蹤每一個人。同時，這個 ID number 也可以被使用在許多不同的目的上，甚至，爲了追求效率起見，電腦系統除了收集相關資料之外，也可以透過這個 ID 號碼與教育、社會安全、稅賦、醫藥資訊等資料庫互相通連。只要每個人在出生時會被發

給一個全國性的身份識別號碼（national identification number），鍵入資料庫，此後其一生的住址、健康記錄、學校記錄、工作紀錄都會被追蹤。當其年紀大到足以就學或工作時，其就會被發給全國性的身份識別證件（ID card），以攜帶至外地使用。資料庫中包括個人的駕駛記錄、健康照護使用記錄、政府服務的使用記錄。此外，此種系統既適用於合法移民者，也適用於可辨識出身份的非法移民及短期旅客（temporary visitors）。此一資料庫因而能詳細地描繪每一個個人的習慣和偏好，無論此種描繪所達到的後果是否完全準確與安全。換言之，從美國社會運作常軌的觀點來看，一個人若是沒有 ID number，就等於沒有政治認同身份（political identity），也無從行使政治權利。該資料庫等於是創造了一個紙上的，可被塑造出來的電子人(electronic person)。尤其是在九一一事件發生後，有許多整合各種資料庫的呼聲開始此起彼落。此一整合，將構成一行政、刑事犯罪、國家安全資料和程序的合併。這種整合一開始可能會告知人民而且是自願的，可是到後來，很可能會發展成爲半強制性的，甚至必定會要求人民隨身攜帶整合之後的身份證，全面建立全國性身份辨識系統。

第二節　健康醫療資訊電子資料庫化趨勢下的 HIPAA 規範

除了上述全國性身份識別系統的相關辯論和本研究報告的討論分析有關之外，美國近幾年來討論得相當熱衷而頻繁的健康醫療資訊電子化和資料庫化趨勢，也相當值得重視，同時也和本研究報告的討論主題健保 IC 卡計畫所涉及的健康醫療資訊，具有最爲直接密切的比較參考關係。

放眼歷史，我們可以發現美國在過去的十五年當中，對於個人財

務隱私立法做了相當豐富的法制辯論[7]，至於醫療健康資訊隱私的辯論，則繼之而起，也成爲眾所關切的焦點。以下本研究計畫便針對美國醫療健康資訊法制的背景，圍繞在美國醫療健康資訊法制周圍的辯論，以及目前的發展趨勢，做一鳥瞰式的介紹和分析。

一、背景與概述

一九九六年國會通過的「健康保險可攜性和責任法」（Health Insurance Portability and Accountability Act of 1996，簡稱 HIPAA））[8]，可說是當代美國最具爭議性的健康照護相關法規之一。這項內容廣泛的立法，其立法目的主要是爲了簡化健康醫療繁複的行政程序，以及增加健康照護體系的效率。爲了達成上述目的，該法內容不但包括和醫療詐欺（fraud）和相關濫用行爲的規定，也處理健康醫療資訊隱私權的範疇，要求提升健康醫療資訊的安全性。

根據 HIPAA 的規定之下，國會在該立法通過之後，有三年的時間去完成執行資訊隱私權保護的相關立法工作，以符合 HIPAA 所規定的標準。但是，因爲上述其無法在一九九九年如期完成，這項工作乃由「健康與人性服務秘書處（Secretary of Health and Human Services，簡稱 HHS）」接手。「健康與人性服務秘書處（HHS）」在一九九九年的十月二十九日發佈法規命令[9]，隨即收到超過五萬兩千份以上的評論意見[10]。歸納這些意見之後，我們可以發現，隱私權的捍衛者希望能對健康照護相關資訊，賦予更爲嚴格的保護措施；相對地，健康照護產業

---

[7] Mike Hatch, *National Health Information Privacy Regulations under HIPAA: Commercial Interests Win Round Two,* 86 MINN. L. REV. 1481, 1481-83 (2002).

[8] Public Law 104-191 (104th Congress).

[9] 65 Fed. Reg. 82461 (December 28, 2000).

[10] U.S. Department of Health and Human Services, HHS Fact Sheet (January 22, 2002).

人士則是相當擔憂這些法規命令會妨礙他們對病患所做的醫療照護，同時也表達出他們對實際執行上述規範時可能涉及的繁雜手續與鉅額成本的憂心[11]。

無論如何，根據上述法令，「個人可辨識健康醫療資訊之隱私權標準」（Standards for Privacy of Individually Identifiable Health Information）也隨之制定，這是由「健康與人力服務部（Department of Health and Human Services，以下簡稱 DHHS）」所發佈的，也象徵了第一次全國性和系統化的健康醫療資訊隱私保護法之誕生。上開法律規範之對象爲所有的「受規範機構」（cover entities），其範圍包含健康照護的提供者、健康保險計畫、健康照護的資料蒐集中心，以及和這些單位具有交易關係的「商業組織」（business associates），從律師、會計師、理賠聲明處理人員、到帳務管理中心，以及資料分析人員等等，皆屬之。本法所保護的對象，則是任何形式之個人可辨識的健康醫療記錄，無論是口頭形式、書面或電子記錄，皆包含在內。至於其保護之具體內涵，則包括取得資訊的權利、使用與揭露資訊的限制、正當的資訊處理方式，以及隱私與安全的政策。

由於全國健康資訊基礎建設的建置在美國逐漸趨於穩固的結果，使得美國最近的醫療記錄的保存形式也逐漸從紙本轉爲電子記錄，資料的擴散和取得變得更加常見普遍，也連帶使得醫療資訊隱私權如何保護的問題，成爲益形重要的全國性問題。根據民意調查的結果顯示，許多美國人相當關心自身的健康醫療資訊隱私，並認爲其資訊隱私遭到侵犯的程度相當嚴重[12]。但是，另一方面，爲了達成公共利益的目的，在某些必要的情況下，必須針對個人健康醫療資訊進行揭露和共享的行爲，例如基於維護健康的目的，醫療研究的目的，公共衛生目

---

[11] *See generally* Susan M. Gordon, *Privacy Standards for Health Information: The Misnomer of Administrative Simplification,* 5 DEL. L. REV. 23 (2002).

[12] The Gallup Org., Inst. for Health Freedom, Public Attitudes Toward Medical Privacy 2 (2000).

的等等；或者是基於非健康的目的如司法程序和法律執行的必要等等，都包括在內，所以也不乏主張個人資訊隱私權與公共利益間應該有所平衡，而反對個人資訊隱私權至高無上的觀點者；事實上，後者觀點也反映在目前美國健康醫療資訊隱私的實定法規範中，在隱私權標準裡，DHHS 便指出應該「在個人的需要與社會的需求兩者間求取平衡」。[13]

換言之，如何不再將傳統上將「個人自主權」(individual autonomy)視爲是具有主宰地位要素的模式奉爲唯一的可能性，而試圖將個人隱私與真正的公共利益等量齊觀，同時，更爲細緻的作法，可能就是該援引比例原則的模式，衡量資訊揭露和分享將對個人產生傷害的機率和該傷害的大小，相乘之後與公共利益目的的強度相較，若後者的強度較高，那麼個人恐怕便不可拒絕資訊的使用、揭露和分喜；反之則不然。因此，在分析架構上，或許是應該考慮如何同時極大化「個人資訊隱私權」與「公共利益」兩者，而不應該將兩者視爲必然對立。基於此項前提，健康醫療資訊的取得、使用或揭露，可以歸納成都必須符合以下幾個原則：(1) 除非極爲特殊的例外必要情形，否則應限縮於個人資料蒐集的原始目的內；(2) 二次揭露資訊應獲得個人的授權，不可隨意爲之。這樣的主張雖然降低了傳統上自主權的重要性，但卻能讓整個社會的成員因爲醫療研究、公共衛生等公共利益的增進而間接獲益。以下所述，便是美國根據 HIPAA 規定基於上述原則所訂定出來的標準中，主要的規範內容：

二、交易標準（Transaction Standards）

交易標準的規範對象，乃是醫療資訊與帳務資訊交換所需的標準形式。國會認爲，建立行政管理與醫療照護資訊的電子化交換標準，

---

[13] Charles A. Welch, *Sacred Secrets - The Privacy of Medical Records*, 345 NEW ENG. J. MED. 371 (2001).

具有其必要性，因爲可以藉此增進健康照護體系的效率與實效性。根據 HHS 估計，目前美國有大約四百種不同的健康照護保險索賠格式，倘若能夠建立出全國性的標準，美國境內的醫療照護提供者，就能夠以特定格式提交交易紀錄給任何健康醫療保險計畫（health plans），而所有健康保險計畫，也可以藉由此種更有組織和效率的方式，將匯款通知與轉診授權送交給健康照護提供者[14]。

三、隱私標準（Privacy Standards）

上述規範中所訂定的隱私標準，所規定的內容包括：在何種條件之下，個人健康醫療資訊（簡稱 PHI），才能夠在沒有經過病患同意或者授權的情況下被利用或揭露；以及病患可以在何時、以何種方式取得其受到隱私保護的健康醫療資訊[15]。各個健康照護機構達成上述隱私標準的最後期限，與交易標準所的要求期限則是相同的[16]。

（一）適用範圍

隱私標準規定的規範對象（covered entities）範圍，包含健康保險計畫[17]、健康照護的資料處理中心[18]，以及用標準電子格式傳遞健康醫

---

[14] 65 Fed. Reg. 82461 (December 28, 2000).

[15] 65 Fed. Reg. 82766 (Dec. 28, 2000).

[16] 45 C.F.R. §164.534.

[17] 所謂「健康保險計畫（Health Plan）」指的是：任何提供、或支付醫療照護費用的計畫，例如團體或個人的健康計畫、販售醫療保險的公司、醫療維護組織（HMO）、醫療保險計畫（Medicare）、CHAMPUS 或雇員的福利計畫。

[18] 「健康照護的資料處理中心（Health Care Clearinghouse）」指的是將未標準化的健康醫療資訊轉換爲標準化的健康資訊的單位。健康照護的資料處理中心的資料處理中心會收到提供者、健康計畫、其他健康照護的資料處理中心、或是上述單位的合夥機關所提出的的交易資料，其職責就是把這些資料轉換成是接收單位可以接受的格式 *See* 65 Fed. Reg. 82488.

療資訊的健康照護提供者[19]。此一隱私權標準所保護的資料，包含任何足以彰顯出個人身份的健康醫療資訊。目前所通過的規定只針對電子化記錄，不過最終應該也會將書面紀錄也含括在內。

（二）一般性規定（General Rules）

根據隱私標準的一般性規定，原則上是禁止取得個人健康醫療資訊的，可以獲得允許使用 PHI 的情況，一般而言可以區分成以下三類：

（1）爲了提供治療、支付或者是健康照護的執行（use and disclosure for treatment, payment, and health care operations）；

（2）在個人授權的情況下使用和揭露個人健康醫療資訊（use and disclosure with individual authorization）；

（3）在無個人授權的特殊情況下使用和揭露 PHI，例如依法律規定、或爲司法與行政訴訟而揭露資訊（use and disclosure without authorization for specified purposes, such as disclosures required by law and disclosures for judicial and administrative proceedings）。

（三）最低限度的資訊使用與揭露（Minimum Necessary Use and Disclosure）

爲了落實個人健康醫療資訊保護的立法意旨，美國聯邦 Department of Health and Human Services （簡稱 HHS）起草了一項規範使用和揭露 PHI 的標準，要求受規範的對象必須對 PHI 提供合理的保護，以避免最低限度以外的資訊揭露與使用行爲出現。

---

[19] 「健康照護的提供者（Health Care Provider）」指的是對健康照護服務的供應、付款或是接受付款的單位或個人，*see also* 45 C.F.R. 160.103。但此處應該注意的是，只有用標準電子格式傳遞健康醫療資訊的健康醫療照護提供者，才是本法的規範對象。

在此一規範中，HHS 針對最低限度的資訊使用和資訊揭露兩者加以區分，所謂的「使用」(use)，所指的是在特定健康醫療照護組織內所進行的資料運用行爲，至於所謂的「揭露」(disclose)，則是指向健康醫療照護組織以外的個人或機構提供資訊[20]。受到規範的組織，則必須在遵守一定的政策和程序之後，才能對需要 PHI 的對象提供個人的健康醫療資訊，包括特定個人身份的揭露、PHI 範圍的特定、以及提供資訊的條件等等[21]。同時，如果是非屬於常態性質的資料要求的話，那麼受規範者則必須事先建立起合理的審核標準，並且以「逐案審查」(case by case) 的方式，一一審查是否應該對其揭露個人健康醫療資訊。此外，上述審查過程和審查通過的理由，都必須做成書面[22]。同時，HHS 也認爲每一位受到健康照護組織診療的個人，都可以依據既定程序，取得其所有的健康醫療記錄[23]。

（四）針對治療、支付和健康照護之執行所爲的同意（Consents for Treatment, Payment and Health Care Operations ）

美國政府所制定的最終版本管制規定，也要求醫療照護單位必須在使用或揭露 PHI，以達成診療、給付或是健康照護等目的時，先取得個人的同意。但如果是在「間接醫療關係（indirectly treatment relationship)」時，就不需取得同意[24]。所謂的間接醫療關係，所指的是醫療單位根據另一個醫療機構的指令提供診療，並且將診療結果回報給該單位[25]。至於「直接醫療關係」，所指的則是面對面的診療關係；例如病理學家做檢測就是間接醫療關係，而醫生將病人轉診時，則會創造出新的直接醫療關係。

---

[20] 65 Fed. Reg. 82544 (2000).

[21] 45 C.F.R. §164.514(d).

[22] 45 C.F.R. §164.514(d)(3)(ii).

[23] 65 Fed. Reg. 82544 (Dec. 28, 2000).

[24] 45 C.F.R. §164.506.

[25] 45 C.F.R. §164.501.

健康保險計畫或健康照護的資料處理中心，則不必一定要取得個人的同意。這些資料處理中心倘若未能取得個人同意，但是爲了診療、給付或健康照護等目的，必須揭露 PHI 的話，則必須根據資料處理的規定，負擔通知義務。但若健康保險計畫或健康照護的資料處理中心，主動請求個人同意，但是卻遭到個人拒絕的話，便不可以揭露上開資訊。

此外，值得注意的是，在以下三種例外的情況下，可以不必取得個人的同意，即可使用資訊：急診；法律規定必須揭露資訊；有語言溝通障礙，而醫療提供者主觀推定病患有接受診療的意願時。

同時，相關條文內也規定了「同意」所需具備的格式，格式要求可以歸納如下：

（1）必須以簡潔易懂的語言寫成書面；

（2）告知個人有關 PHI 會被使用或揭露，以達成診療、給付或健康照護等目的之事實；

（3）讓病患瞭解相關資訊隱私權保護規定存在的事實，並且告知其可在簽署同意書之前，審閱相關之告知文件；

（4）說明上述告知文件可能會被修訂，並且告訴病患如何取得最新版本的告知文件；

（5）向病患說明個人可以要求醫療機構在診療、給付或健康照護等目的下使用或揭露個人資訊時，應該受到某些限制。醫療機構不一定要受這些限制拘束，但是醫療機構一旦同意受該等限制之拘束，就必須遵守規定；

（6）向病患說明個人擁有以書面方式撤回同意的權利；

（7）病患之同意必須以親自簽名和加註日期的方式完成。

在上述規定發佈之後，出現許多醫療機構嚴重反彈的現象，認爲上述所規定的同意要件會妨礙個人取得醫療單位所提供高品質的醫療服務。

（五）個人的授權（Individual Authorizations）

根據隱私權標準的規定，就同意和授權（authorization）兩者做了相當明確的區分。所謂的同意，是指在診療、支付或健康照護等目的下所要求的當事人意思表示，至於若是基於其他非屬管制措施所承認的目的，則必須獲得授權[26]。例如供醫療行銷之用的資料使用，聘僱關係建立與否的決定，心理治療隨手紀錄等等，都是屬於此種類型[27]。

授權之取得必須和診療、支付和健康照護[28]在必須取得授權方得使用個人健康醫療資訊的情況下，醫療機構必須很清楚明確地敘明哪些個人資訊會被揭露，以及資訊揭露的對象爲何。同時，也可以透過書面方式約定授權的有效期間和條件，以及重新授權的相關規定，而且必須由授權人簽名和加註日期。

（六）病患表達反對利用或揭露資訊的機會（Use and Disclosure Requiring Opportunity to Object）

根據隱私權標準的規定，在兩種情況之下，病患應該要被賦予反對利用或揭露資訊行爲的機會。第一種情況是，由於醫院一般都會編輯病歷資料索引，在病歷資料索引中會包含病患個人的姓名、一般病況描述、甚至是其居住的區域等資料，此時院方必須以書面方式通知病患其有「選擇退出」（opt-out）病歷資料索引的機會，並且，在其未表示反對時，才可以揭露上述個人資料[29]。

第二種情況是，病患可以反對利用或揭露個人資訊給一些可能參

---

[26] 45 C.F.R. §164.508(a).

[27] 65 Fed. Reg. at 82514.

[28] 45 C.F.R. §164.508(b)(3).

[29] 45 C.F.R. §164.510(a).

與醫療流程的人，例如家人或朋友都包括在內。只有在病患已被明確告知其具有這項反對的權利後，並且沒有反對之意思時，方可使用或揭露資訊。

（七）其他可資允許的資訊揭露行爲（Other Permitted Disclosures）

根據隱私權標準的規定，在某些例外的情況下，仍然可以在沒有個人同意或授權時揭露個人健康醫療資訊。例外情形之相關規定簡述如下：

（1）法律所要求的揭露

例如法律明文規定，或者是法院的命令或經法院發佈的傳票等等，可以例外進行揭露。此時尚須符合法律的其他要件，例如必須沒有資料濫用的情形、沒有過失，或者是沒有司法權或行政濫權等行爲出現時；再者，資料的揭露也必須符合法律執行的目的[30]。

（2）公共衛生功能

基於法律規定，爲了防杜或控制疾病、傷害或身心障礙等情況之蔓延或惡化，主管機關得蒐集和取得個人醫療健康資訊資訊時，受HIPAA 規範的機構便必須依法揭露有關資訊[31]。

（3）揭露有關虐待、過失或家庭暴力等相關犯行的資訊

基於法律規定之義務，受 HIPAA 規範之機構可以揭露虐待、過失或家庭暴力受害人的個人健康醫療資訊給負責犯罪偵察之機關或相關

---

[30] 45 C.F.R. §164.512(a)(2).

[31] 45 C.F.R. §164.512(b).

主管機關。原則上，該揭露資訊機構並且必須告知被害人此一已經實現或即將實之現揭露事實，不過，假使揭露資訊之機構認爲上述資訊揭露的行爲會導致被害人之安全受到威脅，或者是揭露資訊機構已經將該個人健康醫療資訊報告給受害人之個人代表，而該個人代表有權處理上述犯行者，則不在此一告知的限制要求內[32]。

（4）揭露給監督健康照護體系的機關

當監督健康照護體系運作的相關機關，提出取得個人健康醫療資訊的要求時，受 HIPAA 規範的機構可以將 PHI 揭露給主管審計、民事、行政、或是刑事等事務的機關，以進行相關調查工作[33]。

（5）司法程序與行政程序層面的要求

基於司法程序和行政程序進行之必要，得要求揭露個人健康醫療資訊；換言之，相關機關可以基於法院命令，以及由法院發出之傳票、法院發現真實的要求或是其他透過合法程序而提出之要求，提供資訊[34]。

（6）基於執法目的所爲之揭露

基於執法目的時，即可不經當事人同意揭露個人健康醫療資訊，構成揭露 PHI 的例外，主要之執法目的包含以下數項：

a. 法律要求的揭露：例如根據州法規定、或者是依法要求出具有關之傷害報告等。
b. 法院的命令與行政的要求：也就是基於司法機關、陪審團或行政官員所發佈的傳票，可以揭露資訊。不過，若是由行政官員所發佈的

---

[32] 45 C.F.R. §164.512(c).

[33] 45 C.F.R. §164.512(d).

[34] 45 C.F.R. §164.512(e)(1)(i)；45 C.F.R. §164.512(e)(1)(ii).

傳票，則還必須符合其他更爲嚴格的要求，必須符合實質關聯性、合目的性和資訊之可辨識性[35]等三個判準。

c. 所在位置之資訊：爲了方便指認犯罪嫌疑人、在逃嫌犯、失蹤人口和被害人等的所在，執法機關可以要求提供特定的資訊。但是這些資訊不包括 DNA、齒模、血液分析等資料[36]。
d. 犯罪的被害人：除非執法單位認定該 PHI 的揭露對於犯罪偵察極爲重要，否則應取得犯罪被害人的同意才能揭露資料。
e. 已過世者：若有合理的懷疑，認爲死亡是肇因於某犯罪行爲時，偵查機關可以要求揭露已過世者的 PHI。
f. 營業場所的犯罪：若有合理的懷疑，認爲有足夠證據證明，某犯罪行爲發生在場所內時，則可以將 PHI 提交給司法單位。
g. 緊急情況：指對於犯罪偵查、確認嫌疑犯所在位置、或是指認犯罪者身份而言非常重要的資料。

（7）已過世者

若是有必要確認死亡者的死因時，可將已過世者的 PHI 揭露給犯罪偵查機關。

（8）器官捐贈推動事宜

受 HIPAA 規範者可以將 PHI 揭露給接受捐贈器官的單位，無須經過當事人的同意或授權的取得程序。

（9）研究用途

當個人健康醫療資訊的使用，是涉及研究用途時，那麼便應該由機構審查委員會（IRB，即 Institutional Review Board）或是隱私權保護

---

[35] 45 C.F.R. §164.512(f)(1)(ii)(C).

[36] 45 C.F.R. §164.512(f)(2).

委員會（Privacy Board）擔負起審核的工作，針對上述審查委員會的組成、運作和權責，則設有相當繁複的要求[37]。

（10）避免健康或安全的威脅

當避免個人或公眾健康或安全上的威脅此一需求出現時，可以例外允許揭露個人健康醫療資訊[38]。

（11）特定政府效能的履行需求

基於特定政府職能的需求，例如軍事國防和保護國家元首之需求等，可以例外揭露個人健康醫療資訊[39]。

（八）「去除辨識可能性」（de-identified）的資訊

有關 PHI 隱私保護的規定，不適用於已經「去除辨識可能性」的個人資料[40]，也就是只要無法從資料本身看出其所屬個人之身份者的資訊，不受個人健康醫療資訊隱私保護標準的規範。

（九）行銷

受隱私權標準所規範的機構，在以下幾種情況下，不需獲得授權即得揭露個人健康醫療資訊：（1）與個人資料所有者進行面對面的行銷溝通；（2）針對產品或者服務的一般價值所爲之溝通行爲；（3）針對該受規範的機構或者第三者所提供的健康醫療產品或服務所爲之溝

---

[37] 45 C.F.R. §164.512(i).

[38] 45 C.F.R. §164.512(j).

[39] 45 C.F.R. §164.512(k).

[40] 45 C.F.R. §164.514(b)(1).

通行爲，而且包含適當之資訊揭露在內者[41]。

（十）募款

若是基於自利性質的募款目的，那麼受隱私權標準規範的機構，不必取得個人授權，亦能使用和地理分布狀況有關的醫療紀錄，以便從事此類資金募捐的活動。不過，該機構必須在其既有的隱私聲明之外，針對此等事項另爲敘述聲明，說明其得基於資金募集事項接觸身爲資料所有者的個人，爲該機構募集經費；同時，在提供給個人的募集經費相關說明中，也應該詳實說明個人能夠以何等方式選擇退出（opt-out）該資金募集計畫的對象範圍之外[42]。

（十一）身份之確認

受 HIPAA 規範的機構，在依法揭露 PHI 之前，必須確認提出資訊揭露要求者的身份，以確定該等資訊之揭露，屬於合法之揭露行爲[43]。

（十二）個人受 HIPAA 保護的權利

在 HIPAA 的隱私權標準規範下，個人被賦予某些權利，以確保其資訊自主控制的權力，例如必須以書面方式通知當事人，並且告知當事人其有要求隱私權受保護的各種權利等等，歸納起來，這些權利大致上包含以下數項：

1. 資訊處理的告知（Notice of Information Practice）；
2. 要求施以限制的權利（Rights to Request Restrictions）；
3. 機密通訊的權利（Confidential Communications）；

---

[41] 45 C.F.R. §164.514(e)(2).

[42] 45 C.F.R. §164.514(f).

[43] 45 C.F.R. §164.514(h).

4. 個人取得其 PHI 的權利（Access to PHI）；
5. 修正資料的權利（Amendments）；
6. 估算被揭露資訊之多寡的權利（Accounting of Disclosures）。

（十三）行政的要求

根據 HIPAA 規定和隱私權標準，職司健康照護任務的機構必須符合相當嚴格的行政流程要求，才算達到隱私權保護的義務。首先，每個機構都必須設置負責隱私權保護的專責機關，以促進和實現隱私權保護所需的相關程序和政策[44]。再者，每個機構都必須對該機構內的人員提供隱私權方面的專業訓練，即使是志工人員，也不例外[45]。同時，各機構亦可考慮設置「守門員」此種機制，以確保個人健康醫療資訊的安全性[46]。同時，各機構必須設有專責單位，負責處理病患所提出之有關其隱私權受侵犯的申訴案件[47]。對於未能達到法規要求的雇員或附屬機構，受 HIPAA 規範的機構必須對其施以處罰措施[48]。即使是基於行政管理目的之要求，健康照護機構也必須盡量減低未經授權之資料使用或揭露行為所會帶來的傷害[49]。同時，健康照護機構本身也必須徹底遵守其所制定的隱私權保護相關政策和程序，例如確保資料揭露或使用的相關程序已被確實遵守等等[50]。

（十四） 商業組織

所謂商業組織使用個人健康醫療資訊，主要指的是個人或者機

---

[44] 45 C.F.R. §164.530(a)(1).
[45] 45 C.F.R. §164.530(b).
[46] 45 C.F.R. §164.530(c).
[47] 45 C.F.R. §164.530(d).
[48] 45 C.F.R. §164.530(e).
[49] 45 C.F.R. §164.530(f).
[50] 45 C.F.R. §164.530(i).

關，代表受 HIPAA 規範的某個醫療照護機構，使用或揭露 PHI，例如律師、會計師和顧問等所扮演的角色。這類商業組織和原醫療照護機構之間所簽訂的契約中，必須明訂資料揭露或使用的目的和範圍等[51]。

雖然 HIPAA 的規定範圍，原本無法適用在這些非屬醫療照護機構的商業組織上，但是，依照目前的發展趨勢來看，若是這類商業組織乃是以常態方式爲該醫療照護機構提供服務者，則最好能夠儘快依據 HIPAA 之相關規定調整其既有措施或作法。

（十五）法律適用關係

當州法與聯邦法規定衝突時，若州法的規定較聯邦法爲嚴格時，則優先適用州法之規定。

（十六）執行

民權局（Office of Civil Rights，簡稱 OCR）是本規定的主管機關。違反 HIPAA 規定者，最高每年可處美金兩萬五千元的民事罰鍰，亦可施予刑事處分[52]。

（十七）成本

根據美國政府本身所做的估計，倘若要達到 HIPAA 規定所設定的標準，在未來十年內將花費一百七十五億元的經費，這些經費包含政策宣導、人員訓練、修改醫療記錄和取得授權等等各項費用在內[53]。

---

[51] 45 C.F.R. §164.504(e).

[52] 42 U.S.C. §1320d-5.

[53] 65 Fed. Reg. 82761 (Dec. 28, 2000). See also Robert E. Nolan Company, Inc., ANALYSIS OF HHS COST ESTIMATES FOR THE FINAL HIPAA PRIVACY

（十八）受規範對象的準備措施

根據以上所述，我們可以發現，爲了確實落實 HIPAA 的相關規定，受規範之對象必須重新檢視其既有的隱私權政策、條款和相關契約等等的內容，同時也必須重新羅列出可以使用個人健康醫療資訊的商業組織的名單，甚至必須建置新的病歷資料系統。

第三節　HIPAA 之重要性及其檢討

如前所述，HIPAA 此一立法的出現，對於美國健康醫療資訊隱私法制而言，具有里程碑的意義，以下本研究報告將就 HIPAA 內容中具有特殊重要性而值得特別注意者，以及目前美國學界和實務界對於 HIPAA 和相關規範的檢討，進行歸納，並且選擇重要的面向加以說明和分析。

一、建構「個人資訊隱私權」與「公共利益」兩者均趨於極大化的分析架構

美國國會制定 HIPAA 的首要目的，就是要保障可資辨識出個人身份的健康資訊。這一方面是由於健康資訊被任意洩漏，使消費者逐漸對醫療照護體系喪失信心；另一方面，醫療單位內的資訊建置、以及醫療體系集中化的趨勢，也使得個人記錄的隱密性愈加受到挑戰。個人記錄在健康醫療服務之支付者（如雇員和保險人）、醫療健康服務提

REGULATION (March 2001).

供者（醫院）與醫療健康服務系統之支援者（如雇主、藥商）之間到處流傳，尤其加深了此一問題的嚴重性。如前所述，健康醫療服務的支付者與提供者，有可能基於某些公共利益目的（例如公共衛生）而揭露個人健康醫療資訊，也有可能基於商業目的（例如行銷需求）而揭露個人健康醫療資訊。甚至，爲了以更有效率的方式保存或傳遞健康醫療資訊，美國的政府與企業界也發展出許多方式，來達成此一目的，例如建置更爲複雜的資訊系統如電子資料庫等；但是，這種趨勢反而使病患更加擔心資料的外洩，例如因駭客入侵而導致資訊安全受威脅等問題[54]。以上這些疑慮，都是政府必須透過法律手段管制醫療健康資訊的蒐集、處理、使用和揭露，而且將重點放在保護「個人資訊自主權」上的主要原因[55]。不過，如何在上述保護個人資訊自主權的前提下，兼顧到系統性蒐集和使用電子化健康醫療紀錄所將帶來的益處，例如讓醫師在進行診斷時能夠儘量獲得充分的資訊，以及開出正確的處方。然而，爲了達成這些目的，卻都可能付出一些潛在成本，例如未經個人明示同意的資訊揭露，造成對個人資訊自主權的侵害；倘若個人醫療健康隱私被揭露給親朋好友得知，可能會導致個人受窘的感覺；甚至，雇主或保險公司若能取得個人健康醫療資訊的話，則可能會採取歧視性的手段。[56]

職是之故，目前社會上對於個人健康醫療資訊隱私權的嚴重關切，並非空穴來風。健康醫療資訊內可能包含相當敏感的個人資料，例如診斷結果、就醫記錄，至於諸如愛滋病或其他性病的紀錄，則更是敏感。醫療記錄裡可能也包含一些與健康無直接關係的個人資訊，例如辨識個人的方式（社會安全號碼）、人口數字（年齡、婚姻狀態、

---

[54] *See* Jennifer Kulynych & David Korn, *The Effect of the New Federal Medical-Privacy Rule on Research*, 346 NEW ENG. J. MED. 201, 201 (2002).

[55] *See generally* Lawrence O. Gostin, *Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations*, 127 ANNALS INTERNAL MED. 683, 684 (1997).

[56] *Id.*

子女數目）、財務狀況（保險等級、收入）、導致必須接受診療的原因（如暴力傷害），以及病患對於自身狀態的答詢紀錄等等，但是這些資訊也難保絕對不涉及個人隱私。

如前所述，個人隱私權保障與公共利益兩者之間並非處於絕對對立的狀態，兩者之間也可以維持相當程度的平衡關係。在某些情況下，可以既保障個人隱私又增進公共利益，例如藉此改善醫病關係和鼓勵個人協助公共衛生資料的蒐集等等。不過，更爲常見的情況是，過度的隱私保護會降低達成公共利益的可能性，例如當個人可以選擇不提供公共衛生資料時，那麼最後統計出來的樣本數和結果，就會出現偏差。既然個人隱私保護與公共利益兩者之間，具有上述抵換（trade-off）關係，那麼，如何建立起一個可以同時儘量極大化這兩項利益的架構，便該是規範健康醫療資訊的管制架構應該追求的目標[57]。過去一面倒地支持個人隱私或公共利益，卻未細緻地區別在何種情況下，何者應該成爲優先保護或追求目的的論述方式，應該重新檢討；同樣地，政府決策者經常認爲某幾項要素應該在健康醫療資訊系統中佔有特別重要的地位，但卻未充分說明原因的作法，也應該有所調整。

（一）基於公共目的而使用可辨識個人身份之健康醫療資訊

根據贊成對個人健康醫療資訊基於公共目的而使用可辨識個人身份之健康醫療資訊者的看法，適當使用個人健康醫療資訊的好處，可以歸納成以下幾項：

（1）增進行政效率和降低醫療成本

---

[57] *See, e.g.*, Charity Scott, *Is Too Much Privacy Bad For Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481 (2000).

就美國而言，無論是公私部門都在健康照護體系上付出相當高的成本，尤其是行政管理上的成本。所以，倘若能夠以電子化方式管理資料，應該可以大幅降低交易成本。根據美國官方統計，使用電子化的醫療健康資料交換方式，未來十年內將可省下兩百九十九億元[58]。

（2）促進醫療與健康服務之研究

不論是從事臨床、預防或診療等工作，或者是從事公共衛生的研究，龐大且完整的健康照護資料庫，有助於迴歸等統計方法的分析。然而，由於美國近來也不乏主張政府應該透過立法手段，賦予基因資訊財產權保護者[59]，論者以爲此一趨勢值得注意也有予以平衡的必要，因爲，倘若讓病患有選擇不揭露自己資料的機會，將會使得整個統計樣本出現「自體選擇的偏差」（self-selection biases）的問題[60]。

（3）發揮公共衛生守門員的角色

藉由追蹤總體人口中疾病流行的趨勢，以及良好嚴謹的帶原者管控模式，可以更有效率地降低公共衛生領域所關切的疾病威脅程度，以及減少個人醫療費用上的支出。不過，某些高度敏感性疾病的病史資料，例如愛滋病，則必須在高度警戒的前提下善加保存[61]。

---

[58] U.S. Dep't of Health and Human Servs., HHS Fact Sheet: Protecting the Privacy of Patients' Health Information (May 9, 2001), *available at* <http://www.aspe.hhs.gov/admnsimp/final/pvcfact2.htm>.

[59] LAWRENCE O. GOSTIN ET AL., NATIONAL CONFERENCE OF STATE LEGISLATURES, GENETICS POLICY AND LAW: A REPORT FOR POLICYMAKERS (2001).

[60] L. Joseph Melton, III, *The Threat to Medical-Records Research,* 337 NEW ENG. J. MED. 1466, 1467 (1997).

[61] Rene Bowser & Lawrence O. Gostin, *Managed Care and the Health of a Nation,* 72 S. CAL. L. REV. 1209, 1217-18 (1999).

（二）極大化個人利益與公共利益之際的判斷基準

根據美國相關學者的看法，就個人健康醫療資訊的管制架構而言，極大化個人利益與公共利益固然是最適當平衡的目標，但是在追求兩者同時極大化之際，應該先建立判斷基準，以資遵循，以下便是幾個重要的判斷基準：

（1）爲公共利益目的使用或揭露資訊

當揭露一項資訊所謂帶來的效益非常地大，對個人帶來傷害的可能機率卻很低（例如，經過嚴密成本效益分析和執行程序控管的健康照護、公共衛生、研究計畫等）時，應允許揭露個人健康醫療資訊。論者以爲，也正因爲這些資料的使用的目的，僅限於嚴格定義的具體公共利益目的，因此個人不必擔心其資料流爲他用，因爲濫用或誤用這些資料的機關都必須受到隱私權保護規定的規範。

以公共利益之目的爲由，使用或揭露個人健康醫療資訊的機關，必須依照下列程序爲之：(1) 證明所欲達成的是一項重要的公共利益目的；(2) 證明揭露或使用資訊是達到該目的之諸手段中，成本最低的一項；(3) 可能的話，應該儘量使資料與個人身份兩者分開，亦即應該做去辨識個人身份化的工作；(4) 執行隱私標準和安全標準，以確保只有在爲了達成公共目的之前提下，近用資料者爲了執行其職務或發揮其功能不可或缺時，才能近用資料；(5) 執行適當處理個人資料的規定（fair information practices）[62]。

（2）可能導致傷害發生的資訊使用或揭露

---

[62] Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule,* 86 MINN. L. REV. 1439, 1455-56 (2002).

當使用或揭露可辨識身份的個人健康醫療資料，因此可以達成的公共利益目的之可能機率很低，但卻很有可能對個人造成傷害時，就應該要特別彰顯隱私權保護的必要性。之所以必須遵守此一判斷基準，除了因爲揭露個人健康醫療資料的後果原本就堪慮之外，更是因爲不當揭露個人健康醫療資訊的後果，會因爲科技的發達而使以下四種危險更加嚴重：

1. 個人健康醫療資訊可以被用來做爲差別待遇甚或歧視的依據。例如在工作或保險事項上，潛在的遺傳缺陷(potential genetic deficiencies)可能被用來當做拒絕聘僱或拒絕承保壽險（life insurance）的原因。

2. 個人健康醫療資訊被洩漏之後，可能對造成個人的窘境。例如關於性病或憂鬱症相關醫療資料的揭露，都在此列。

3. 不當揭露健康醫療資料會招來藥商與其他醫療服務提供者的推銷。這些產品和促銷對於某些人而言可能很有用，但是這類推銷也可能令人感到困擾或不愉快。

4. 不當揭露個人健康醫療資訊的結果，將弱化病患對醫療系統的信任。無論從道德層面或法律層面來看，病患都預期其與醫療人員之間的溝通對話交流會被保密，倘若病患不能抱持如此期望，那麼很可能會採取對自己病情或其他相關資訊有所保留的策略，反而不利醫療行爲的順利進行。

二、HIPAA 的檢討及其啓示

從宏觀的角度來看，HIPAA 可以被看成是美國健康醫療照護體系邁入電子化時代之後，醫病關係（physician-patient relationship）[63]發展

---

[63] *See* Mark A. Hall et al., *Trust in Physicians and Medical Institutions: What Is It,*

與維持信任的重點所在，缺乏隱私不僅會對病人造成損害，也會不利醫療照護行爲和體系的進行和運作[64]。

個人健康醫療資訊的不當使用可能造成的負面影響，已如前述，然而，我們的確也很難否認個人健康醫療資訊的適當使用，有其正面意義，例如：

（1）醫療照護專業人員之間對 PHI 的共用行爲，例如醫師和藥劑師間就應該對病患所服用的藥物狀況有精確的了解，以避免藥物之間的交互作用，對病人造成不良影響。

（2）爲了研究與公共健康目的而使用 PHI，例如，HIPAA 允許以維護國家安全的重大理由，做爲保護病人資訊隱私權的例外事由[65]；同樣地，若是研究目的涉及重大公共健康目的，而使用個人健康醫療資訊，亦然。

（3）直接對消費者推銷藥物此一理由受 HIPAA 例外允許的價值雖然頗爲可疑，但是，HIPAA 目前的規定顯然認定直接對個人進行市場行銷仍然具有相當價值，因爲可以提供與病人之病況相應的醫療產品的知識，而這些知識原本很可能被忽略掉了，所以 HIPAA 也基於對病人福利的考量，例外允許行銷行爲。

Can It Be Measured, and Does It Matter?, 79 MILBANK Q. 613, 622 (2001); David Mechanic, *The Functions and Limitations of Trust in the Provision of Medical Care*, 23 J. HEALTH POL. POL'Y & L. 661, 671-72 (1998).

[64] Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L.REV. 1497 (2002).

[65] Peter P. Swire & Lauren Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515 (2002).

從正面意義來看，HIPAA 的通過，對於美國健康醫療照護體系保護病患資訊隱私權來說，的確提供了某些助力；至少，從表面上看來，HIPAA 的確對病人健康醫療資訊隱私的保護，提供了相當高程度的保護，其不但要求所有醫療照護提供者及健康保險計畫（health plans）必須保護其病患的 PHI，同時也要求醫療照護提供者及健康保險計畫必須制定一套周全的政策與程序，以保護 PHI 不會在未經同意的情況下被揭露。其次，HIPAA 的規定，也使得資料的收集與傳遞(collection and transmission)，在目前可能的範圍內，達到標準化的結果。藉由 HIPAA 此種規範模示，可以達成資料交換的效率（transaction efficiencies），並且使健康醫療系統內有關病人醫療情況的資訊出錯的比例儘量降到最低，並且易於在系統內傳遞，降低健康照護的行政成本。同時，HIPAA 也可能有助於促進醫療人員與病患的交流。因爲，根據 HIPAA 的規定，醫療人員在揭露 PHI 之前必須要先得到病患的同意，所以，醫療人員也因而有機會與病患更充分地討論其病症性質，以及可能的治療方式[66]。

然而，更值得注意也更值得我們省思的，可能是批評者對 HIPAA 規定內容的檢討意見和其所持的理由，以及這些意見和理由對個人健康醫療資訊隱私保護將造成何等影響：

（一）HIPAA 所引發的成本將大幅超過其所獲致的利益

首先，批評者認爲 HIPAA 的執行將牽涉相當高的成本，將導致弱化醫療照護的品質與持續一貫性的結果[67]，而此一結果和降低醫療照護成本相較之下，並不值得。其次，HIPAA 關於 PHI 的管制太過於複

---

[66] *But see* Peter D. Jacobson & C. John Rosenquist, *The Use of Low-Osmolar Contrast Agents: Technological Change and Defensive Medicine*, 21 J. HEALTH POL. POL'Y & L. 243, 259-60 (1996).

[67] Am. Health Law. Ass'n, *Privacy Rule Will Force Major Changes in Handling of Patient Information*, HEALTH LAW. NEWS, Feb. 2001, at 5-6.

雜瑣碎，而且難以持續實行；這些 HIPAA 的管制一則和其他同樣強調細節的管制之間可能產生衝突，例如對詐欺與濫用醫療的管制，即可能和 HIPAA 產生衝突。再則批評者也認爲 HIPAA 的管制太過於複雜，難以遵循；更重要的是，HIPAA 所規定的經病患同意的要求，原意是在保障隱私權，但是由於 HIPAA 內的管制規定太過於瑣碎，因此，在此種規範架構下，病患同意很可能淪爲僅僅是種達到 HIPAA 所規定標準的方法，導致病患同意遭到濫用的結果，而且在此一規範架構下，未來也可能必須準備各種不同類型的同意書[68]。大家雖然預期 HIPAA 能夠達到提高效率的目的，然而，批評者中不乏認爲目前看來 HIPAA 可能會製造出更多更嚴重的官僚（bureaucracy）問題。例如，如前所述，會多出一些文書工作，尤其是與病患同意書有關的文書工作。 從這個觀點看來，很難想像如何能夠以具有實質意義的方式執行 HIPAA 的規定[69]。

其次，更爲重要的是，HIPAA 此一保護資訊隱私權的規定，被批評爲反而可能侵害隱私權。雖然 PHI 在 HIPAA 之下是受到保護的，然而在 HIPAA 當中仍然允許在某些情形下可以未經授權揭露 PHI，而在批評者眼中，這些例外情形的相關規定實在太多。而且，一旦某一機構獲得病患的同意，PHI 就可能會被輕易地向許多不同的機構揭露，這對病患個人健康醫療資訊隱私的保護反而不利。如前所述，可以想見的是，病患會輕易地在那些並未清楚說明所有該同意書所牽涉者爲何和所影響者爲何的表格上簽名。而且，HIPAA 並未禁止受規範的機構販售 PHI 給其他機構或組織，使用在廣告或行銷用途上，因而會使病患資訊自主權是否受到保護的問題，變得格外嚴重[70]。

---

[68] Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L.REV. 1497, 1503-04 (2002).

[69] *Id.* at 1504.

[70] Lawrence O. Gostin, *National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act*, 285 JAMA 3015,3019-20 (2001).

2001 年 7 月 HHS 所發佈一項隱私權標準指南（Guidance on the Privacy Standards），其重點之一便是受規範之機構不必保證 PHI 的機密性，受規範之機構只需要對 PHI 的機密與安全，盡到「合理努力」（reasonable efforts）的義務即可。更該受非議的是，針對涉及治療、支付和保險處理的問題，HHS 還制定了一項不再需要取得病患同意的規則，雖然醫療提供者等受規範機構在此種情況下依然必須告知患者關於其隱私權的事宜，但是卻不需要在揭露前先取得書面同意，這種規範模式，幾乎表示 HIPAA 可能更進一步地弱化對隱私權的保護。

最後，此一隱私權標準指南中的核心觀念之一，便是受規範機構應該盡到合理努力的注意義務，以便使個人健康醫療資訊的使用，能夠在達成預定的使用、揭露和請求等目的之最低必要性（to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request）[71]範圍內，限制受保護的個人健康醫療資訊之使用和揭露。然而，所謂「最低必要性」標準（minimum necessary standards）的定義究竟爲何，此一觀念在執行層次究竟該如何落實，都仍在未定之天[72]。因此，現階段實在仍然無法預知究竟 HIPAA 的影響好與壞比重將是如何，不過，誠如論者所言，目前開始思考一些其他不同於 HIPAA 既有規定的選擇方案，也許可以幫助 HIPAA 的執行，或者甚至是在 HIPAA 執行失敗時，提供備案。

（二）替代方案的考量

到底，就 HIPAA 目前的內容而言，有哪些層面需要考慮替代方案，由於 HIPAA 內容複雜，無法一一詳述，但仍可就目前批評者已經提出的一些重點：

---

[71] 45 C.F.R. 164.502(b)(1).

[72] John R. Christiansen, *A Preliminary Review of the Final HIPAA Privacy Rule: Re-Engineering the Information Relationship Between Individuals and Healthcare Organizations*, HEALTH L. DIG., Feb. 2001, at 3-12.

（1）個人權利和公共利益的權衡基準不清

雖然不乏有人認爲根據 HIPAA 的規範意旨，應該追求的是個人健康醫療資訊隱私和公共利益兩者之間的平衡，然而，究竟如何決定個人的風險與公益的兩者之間的平衡基準，應該如何決定風險和利益兩者之間的比例，以及未來是否來是傾向於允許揭露，都有待進一步地精緻化。

（2）保障資訊安全的方式

HIPAA 規定雖然對資訊安全有所著墨，但是針對資訊安全條款究竟是應該規定何種方式，以便使資訊揭露行爲可能造成的傷害最小化，則未有適當的要求。例如，是否應該規定採用能夠處理 HIPAA 所要求事項的技術，例如使用數位簽章、身份證件（identity cards）、安全無虞的網路和 E-MAIL，並且對醫療紀錄的使用（access）進行控管[73]等等事項，也都有待進一步精緻化。

（3）私人管制的可行性

除了政府直接的管制和監督之外，是否可以委由私部門的機構在某種程度內取代政府控管的功能，也是論者提出可以考慮其可行性的替代方案之一[74]。

（4）病人最佳利益的考量

---

[73] John T. Lynch & Bruno Lassus, *Mega Enterprise Chooses Smart Cards*, 21 HEALTH MGMT. TECH. 50, 50 (2001).

[74] *See generally* Peter D. Jacobson, *Regulating Health Care: From Self-Regulation to Self-Regulation?*, 26 J. HEALTH POL. POL'Y & L. 1165 (2001).

綜合論者見解，HIPAA 的規範宗旨，應以病人的最佳利益爲基礎。換言之揭露 PHI 的必要性，應該著眼於病人臨床上的需求，以及共享資料以維持具有持續一貫性且具有品質的醫療之需要。取得特定資訊的需求以及所請求共享之資料，是否合於上述需求，其舉證責任應由主張取得使用和揭露 PHI 的機構負擔。如前所敘述，在提供 PHI 之前，受規範的機構必須制訂和適用符合或優於最低必要性檢驗基準（minimum necessary test）的保護隱私政策與程序。受規範之機構對於該病患的病症必須由數種醫療專業人員會診，或者該資訊的分享對於避免負面的醫療結果（例如藥物交互作用之不良）具有重要性，必須負擔說明舉證之責任。唯有如此，才能達到符合病人最佳利益的原則。

第四節　德國與法國健保 IC 卡制度之比較經驗

美國的 HIPAA 雖然是最近幾年來電子化健康醫療資訊比較法制方面的里程碑，其中也有不少規定的內容和相關討論，也有值得我們借鏡之處；不過，值得特別注意的是，美國的 HIPAA 雖然強調健康醫療資訊的隱私保護和效率、公共利益等目的之間的平衡關係，但是，由於美國並未如我國般有全民健保制度這種幾乎滲透率達全國性的健康醫療保險制度，同時也可能是對健康醫療資訊電子化工作的複雜程度抱持比較戒慎恐懼的心態，所以並未有類似台灣目前準備實行的健保 IC 卡一般的全國性電子化健保憑證，所以在討論台灣未來和健保 IC 卡計畫

由於健保制度的差異和資訊隱私保護立法體制的不同，我們必須指出，討論有關健康醫療資訊隱私的問題時，美國制度的內容和經驗不見得能夠完全援用，是此處值得注意之處。究諸實際，台灣目前的健保 IC 卡計畫，經常被關心此一計畫者與歐洲大國法國和德國兩國所

實行的健保 IC 卡計畫相提並論，爲了達到澄清和比較的效果，本報告以下便以簡要的方式，針對法國和德國兩國健保 IC 卡制度的主要內容，做一簡要說明：

不可諱言地，歐洲國家在 IC 卡的應用方面的確是居於領先的地位，不過，其在建置內容方面，卻不見得是以極爲大膽的方式處理個人健康醫療資訊存放在卡片中的問題，因此所引發的爭議似乎也就比較少，是值得我們特別注意之處。

德國與法國目前使用健保 IC 卡的目的，大致上都是爲節省行政支出；換言之，德國健保卡爲德國減少健保行政工作所推行之計畫工作，與健保局目的相同，對象亦均爲全體之國民，而且皆須資訊整合廠商之參與。德國使用的是記憶體卡，卡片裡面只包含了醫療行政方面所需要的八項資料，該等資料之內容簡要羅列如下[75]：

1. 保險機構名稱（the name of the insurance group）
2. 保險憑證號碼（insurance ID number）
3. 被保險人姓名與稱呼（the holder' s name and title）
4. 被保險人住址（address）
5. 被保險人出生年月日（date of birth）
6. 保險狀態（insurance status）
7. 身份識別證件號碼（ID number）
8. 卡片有效日期（card expiry date）

至於法國所使用的卡片類型，則是比較複雜的 CPU 卡，但是目前卡片中所儲存的資料，也仍然是限於醫療行政方面的資訊[76]：

1. 卡片持有人身份（the bearer' s identity）

---

[75] *See* <http://www.biac.org/Textes/BIAC_TEXTES/BIAC_SubmissionsPDF/Health/srbg9709.pdf>.

[76] *See*<http://specials.ft.com/ftit/april2001/FT3PVEYVKLC.html>.

2. 社會安全號碼（social security number）
3. 卡片持有人特有權利（the bearer’ s specific rights）
4. 卡片持有人之撫養者和受益人（the identity of possible dependants and/or beneficiaries）

值得注意的是，因爲法國的保險申報方式，和美國的申報方式大致相近，是由被保險人先付款之後，再向保險公司申報退費。因此在使用 IC 卡做爲健保卡之前，無論是個人、醫療院所和保險機構往往爲了處理紙張形式的申報表，需要耗費大量的人力物力，而引進 IC 卡的目的，便是爲了減低這項行政成本。然而，與法國健保制度相較之下，我國目前的申報方式與法國截然不同，因此，我們的醫療院所與個人缺乏像法國制度背景下那樣的誘因。這或許也是爲什麼 IC 健保卡制度著手推行以來，不少醫療院所怨聲載道的原因之一。

其次，就法國和德國兩者針對未來所規劃的計畫來看，凡是牽涉到個人醫療資料，皆是採取個人自願參與加入的模式，並且賦予個人極大的資訊自主控制權。爲了因應資訊科技應用在醫療和健康照護上的趨勢，上述制度的原貌也開始出現了某些修正，不過，即使如此，在法國的第二代健保 IC 卡計畫當中，卡片主要是被用來做爲存取伺服器的鎖匙（key），真正載入卡片當中的資料，根據目前規劃內容來看，將只有進行緊急醫療所需的相關資訊。在德國的規劃中，雖然也有將個人醫療紀錄載入 IC 卡的計畫，但是這也是準備以自願的形式爲之。因此，自願和自主的選擇，是健保 IC 卡納入個人健康和醫療資訊與否的關鍵。而且，此處更值得強調的是，由於我國的健保制度是具有強制納保的性質，民眾實際上少有選擇不加入全民健保制度的自由，因此，健保局在許多作爲上，可能更必須採取非常尊重個人自願和自主選擇權的態度，才足以取得民眾對主管機關和健保局保護人民資訊隱私權的信任。

最後，IC 卡在健康照護上的應用，在歐洲已經有許多的計畫在實施當中[77]，健保局或許應該經常持續地注意這方面的發展，同時也應該深入瞭解各個國家在實施這些健康照護制度時，採取了怎樣的相關配套措施，以及在推動時所有相關的社會、政治與法律的配套架構，同時，或許應該更注意我國健保局具有相當特殊的市場獨佔地位此一事實，方能真正從德國和法國這些同樣施行健保 IC 卡制度的國家，學得正面經驗，並且區辨異同。

爲了方便比較起見，茲就以上所述各國之健保資訊和健保憑證制度內容簡單列表如下：

台灣、美國、法國和德國之健保資訊和健保憑證制度內容簡要比較表

項目＼國家	台灣	美國	德國	法國
健保憑證制度之有無	有	無	有	有
法律規定	全民健康保險憑證管理與使用須知	訂定本報告前述規範健康保險相關機構之之法令規範健康和醫療資訊相關資訊之使用	立法規定自一九九二年一月一日起每一德國公民均需持有健康保險卡	無
健保憑證制	控制行政	X	降低行政	控制因紙

[77] http://www.eeurope-smartcards.org/Download/01-4.pdf

度之主要追求目的	成本和健康保險成本		負擔控制健康保險成本 增進保險人、被保險人和醫事專業人員數者之間的溝通效率	卡和書面申報所引起的巨額行政成本 控制健康保險之成本 增進保險人、被保險人和醫事專業人員數者之間的溝通效率
身份辨識證件之關係	具有國民身分證此一法定之單一身分辨識證件	具有法定之社會安全號碼，但無法定單一之國民身分辨識證件	無法定單一之國民身分辨識證件	無法定單一之國民身分辨識證件
具體發展過程	由紙卡直接改爲 IC 晶片卡， 但有兩卡並用之過渡期間	直接規範健康和醫療資訊本身之使用，不特別區資訊之載	由磁條卡漸進改爲目前之晶片卡	以比較複雜的 CPU 卡取代紙卡

		具		
具體作法	全民健保具有相當高之強制納保特性，個人是否可以選擇不將某些特定資訊載入晶片卡中，目前尚未決定	除法律特別規定外，尊重個人之資訊自主控制權	目前晶片卡中所記載者乃健保行政所需之八項資訊 具有將個人醫療紀錄載入 IC 晶片卡的計畫，但規劃中以自願選擇加入的形式爲之	目前晶片卡中所記載者乃健保行政所需之四項資訊 卡片主要扮演存取伺服器的鎖匙此一角色，真正載入卡片中者，僅有進行緊急醫療所需之相關資訊

資料來源：本研究自行整理

第四章　現行全民健保 IC 卡制度應修正改進之處

本章之主要內容，乃是本於前面各章之說明和論述所得，針對我國目前正在著手推動當中的健保 IC 卡計畫內容中未臻周全之處，進行分析，並且分就健保 IC 卡的法制面補強措施（法律依據和契約相關事宜之分析），資訊安全疑慮的澄清，以及資訊隱私的保護等幾大部分，提出本研究計畫認爲就目前情形而言仍屬可行的調整和修正方向。

第一節　法制面的補強

爲了針對健保 IC 卡計畫的特性說明其在法制面應該採行的補強措施，本節將區分成「現行法律的檢討和修正」以及「健保 IC 卡相關契約之檢視」兩個部分，進行論述和分析。

一、現行法律的檢討和修正

就我國憲法層次的依據而言，雖然並未有明文對「隱私權」加以保護的條文，但憲法第八條所保障的「人身自由」、第十條所保障的「居住自由」、第十二條所保障的「秘密通訊自由」，就其本質而言，都可以說是與人民隱私權的保護有密切關係，也都涉及人民自主控制的權利；大法官會議在釋字第二九三號解釋中，亦已明確承認隱私權是人民的基本權利之一[66]。

---

[66] 參見 293 號解釋解釋文：「銀行法第四十八條第二項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘

由此推論，想要爲以個人資料保護爲主的資訊隱私權，在我國憲法上找到適當的基礎，並非難事。不論是自前述憲法條文加以解釋擴張其適用範圍，或者是自釋字二九三號解釋所承認之「隱私權」概念加以延伸，甚或借用德國基本法的模式，直接上溯憲法和釋憲實務都一致肯認的「人性（格）尊嚴」[78]概念，或者透過我國現行憲法第二十二條的概括人權保障條款的解釋適用，確認資訊隱私權或個人資訊自決權，都是可行的途徑。所以，「資訊隱私權」或「個人資訊自決權」屬於憲法上所保障之基本權利，應無問題。

基於上述憲法依據，具有我國個人資料保護基本法地位的電腦處理個人資料保護法，應該是我們探討健保 IC 卡計畫中的個人資料保護問題之出發點。我國有關個人資料保護之法制，並未採取歐洲國家之模式，亦即制訂一般性之「個人資料保護法」（data protection law），而是以電腦處理個人資料領域爲範疇，於民國八十四年訂定「電腦處理個人資料保護法」（以下簡稱「個資法」），然本研究報告之研究對象即屬個資法所規範之典型。各資法主要將個人資料的保護分爲兩大類，其一爲「公務機關處理個人資料」，另一則爲「非公務機關處理個人資料」的情形，從健保 IC 卡的建置和使用範圍來看，應該同時涉及個資法所規範的公務機關和非公務機關兩種，殆無疑問。

依個資法第一條之規定，該法之立法目的爲「規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用」。至於該法所稱「個人資料」的範圍，則係指所有「足資識別該個人之資料」而言，從此一定義來看，我們認爲健保局在定義何謂涉及個人隱私的資料時，也應該採取比較嚴謹的態度爲之，不應該將許多表面上看來無法和個人直接聯繫起來的資料，便簡化爲不具有隱私意義的資料，而

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』----」。

[78]依我國電腦處理個人資料保護法第一條之規定，保護個人資料之原因，即係爲避免「人格權」受侵害。

是應該以「足資識別該個人」與否，做爲判斷標準。就應該規範的事項而言，個資法的相關規定尚稱完備：

1.個人資料蒐集之要件（第七條）
2.個人資料利用之目的與範圍（第八條）
3.個人資料的國際傳遞的限制（第九條）
4.個人資料檔案保存之公告（第十條、第十一條、第十四條）
5.人民查詢、請求閱覽之權利（第四條、第十二條）
6.個人資料正確性的維持（第十三條）
7.個人資料檔案的安全維護（第十七條）
8.處理當事人各項請求之期限（第十五條）[79]

不過，隨著社會事務之複雜化和電腦科技的迅速進展，個資法的闕漏也一一浮現，例如，不確定法律概念與概括排除條款過多[80]：尤其第八條特定目使用限制之例外規定高達九款，其內容之寬廣，幾乎已經等同於對個人資料的使用沒有任何限制。其次，程序規定的欠缺，也是個資法實際操作上極爲嚴重的致命傷。換言之，我國現行個資法在以下幾個層面出現明顯的闕漏現象：（1）蒐集個人資訊的程序，特別是對「蒐集資訊必要性之有無」的評估程序和資訊蒐集時的「告知」程序規定，都付之闕如；（2）未規定進行目的外利用時所需踐行之程序；（3）當事人各項權利行使之程序，也未加以規定。此等程序規定的欠缺，一則可能影響當事人權利的行使，再則也爲必須遵循個資法規定的機關滋生無窮困擾，長遠之計應該是適度參考國外法制予以彌補。

正因爲例外規定過多，以及程序規定過於簡陋，所以個資法制定至今，所發揮的規範實效可以說是相當有限，另一方面，例外規定過

---

[79] 有關個資法「處理期限」之規定，可謂我國法的特例，在通常情形下，我國法律中就行政機關的作業期限均未設有規定。

[80] 就此而言，目前由法務部研究草擬之「電腦處理個人資料保護法」部分條文修正案，即針對「不確定法律概念、概括條款過多」之問題，做出部分修法建議。

多和程序規定闕漏，也成爲關切資訊隱私者批評個資法無從發揮規範健保 IC 卡所帶來的一連串個人資訊隱私問題功能的主要理由之一，我們認爲，未來在此一過於疏鬆的個資法體制下，健保局和其他相關之機關機構在個人資料保護法律的適用上將出現許多模糊而無所適從的困難，導致資訊隱私不保的疑慮長期無法解套的困局。

從目前的資訊保護法制來看健保 IC 卡計畫的內涵和相關的資訊隱私疑慮，我們認爲在個資法修訂之前，至少應該考慮採取以下的補救措施：

（一）衛生署和健保局應要求相關機構就資訊蒐集和處理事務建立自我審查機制

我們在參照美國政府資訊公開之相關法制和前述 HIPAA 之規定之後，都可以發現，雖然兩者均不乏基於公共衛生（public health）目的、國家安全和緊急狀況等法定例外理由，而准予在未遵守個人資訊自主控制原則揭露個人健康或醫療資訊的規定，但是，爲了紓緩個人和政府機關及醫療衛生機構兩者之間所掌握之資源不均等的現實，確保個人健康醫療資訊受到自主控制原則的規範，兩者均以相當比例之篇幅，規定行政機關和進行資訊蒐集和處理時應該建置之自我審查機制。我們認爲，此一機制配合內部稽核和外部規範之設計，頗能收促使公務和非公務機關遵守相關法令之效。就我國目前之情形而言，我們認爲醫藥衛生事務主管機關衛生署和健保局兩者，做爲全民健保制度運作的監督者和全民健保制度中唯一的給付者，應該善用醫療法和全民健保法中所規定的醫療機構監督權力，在健保 IC 卡制度正式上路之前，全面建立上述機制，例如，爲了避免個人資訊隱私保護相關法律徒然具有宣示性意義或效果，而醫療衛生機構在日常管理運作過程中卻依舊發生各種洩漏個人健康或醫療資訊的情事，與其藉由事後的法律訴訟予以補救，不如考慮利用全民健保制度中比較系統性的經濟懲罰方式，在全民健保總額預算的協商過程中，援用各種透過內部自

我審查和外部審查機制（詳如以下所述）運作所得的調查結果，針對資訊隱私保護工作和病患應有權益宣導教育工作執行不符要求的醫事機構，進行預算之適當調整，一則收警惕之效，再則亦能減輕主管之行政機關和健保局在保護個人資訊隱私權方面的行政負擔和行政成本。同時，爲了落實上述建議，主管機關則應該考慮進一步嚐試在醫療法和全民健保法兩項法律中尋找或儘速建立授權依據，設計出相應的細緻管制手段，要求健保 IC 卡制度下所涉及的醫療衛生機構建立此一資訊蒐集和處理事務的自我審查機制，以便大幅減少未來因健保相關資訊之蒐集和處理所可能引起的反彈。

（二）建立不同機關間資訊流用的標準、限制規定和相關程序要求

根據現行個資法的規定，雖然不同機關間之資訊流用本有限制，但是，同法中之例外規定，又往往使得該等限制規定形同具文，尤其是健保 IC 卡計畫這類追求相當重大的效率提升目的之行政措施，更是明顯。然而，根據目前電腦個人資料保護法的立法精神，無論是公務機關或者非公務機關，即使是在符合所謂不同的機關間可以進行個人資訊互相流用的例外情形下，亦需在受到法令規範的前提下，方得爲之；亦即就個人資訊互相流用時應該遵循的標準，決定是否應該流用之際應該踐履哪些程序據以決定，流用時應該遵守的實質和程序規定爲何，以及不得逾越哪些限制等等，都應該透過更加細密的法令予以進一步規範。

具體而論，在健保 IC 卡計畫的實施必須同時強調個人隱私保障與行政效率的前提下，我們認爲必須正視即將到來之不同機關和機構之間資訊互相流用所衍生的資訊隱私保護問題。從保護資訊隱私權的角度來看，原則上各個機關依其特定之法律授權，針對特定目的所蒐集之資訊，不得再提供給其他機關，或者基於其他目的使用，不過，爲了減輕人民提供資訊負擔，以及增進效率，不同機關間資訊的流用也不應全面加以禁絕。這也是將來健保 IC 卡計畫正式實施時，必須儘速

全面檢視各個資訊蒐集處理和流通環節，訂定配套措施的根本理由所在；而且，除了短期內必須處理哪些個人資料可以被蒐集和寫入物理形式上爲個人所持有，但是個人並不見得有十分便捷之方式，可以得知其內部所記載之資訊正確度如何的健保 IC 卡之外，尙須處理健保 IC 卡整理網路建置之後所衍生的公務機關和非公務機關之間的病患醫療資訊互相流用的複雜問題。我們認爲，目前暫時可行的作法，固然是依據個資法內已有規定和機制，制定上述進一步規範資訊流用的標準、限制和相關程序的規定，然而，由於目前個資法修正草案有意將個人健康醫療資訊此種特殊敏感之資訊類型，歸爲特種資料，另做比較嚴格的規範處理，而就健保 IC 卡計畫將來的建置遠景來看，個人健康醫療資訊在我國的地位也勢將與其他類型的個人資訊之間，在性質和重要性兩者上均出現相當重大的不同，的確有另予做比較嚴格之規範的必要，因此，我們認爲，長久之計，應該是針對個人健康醫療資料蒐集處理和流用的標準和限制，透過個資法以外的特別法令，予以規範，例如於醫療法或者全民健保法等相關法規中，另立專章，加以明訂。

簡言之，我們認爲，在未來的健保 IC 卡計畫執行方面，究竟「取得該資料之法律依據」、「需要該資訊之目的」、「該資訊的使用方式」和「可能使用期限」，均必須透過立法方式特別加以明定，不應該沿習舊規，任由需用資料的機關概括地以「診療所需」或「業務需要」等模糊的理由，即可取得和處理相關之健康醫療資訊。嚴格來說，即使是放在既有的個資法架構下來看，此等失之模糊的理由，也相當地不合理，因爲，蒐集和處理個人健康醫療資料的機關，在此等情況下是否具備符合電腦處理個人資料保護法第八條特定目的外使用之例外理由，實在無從判斷。

同樣重要的是，由於依照現行實務上之慣常處理方式，個人資料之流用並不盡然會十分詳實地將提供或流用資料的記錄附註於個人資料檔案內，所以相關個人即使依據個資法之規定申請閱覽，也無從得知究竟有哪些機關曾經取得其個人資料，因此個資法所賦予個人之各

項權利，包括查詢、閱覽、補充、更正、停止利用或刪除等等權利，亦將無法落實。這類問題在健保 IC 卡計畫全面上線之後，出現機會將更形頻繁，同時也會更趨於複雜，我們建議應該及早規劃和建立以上所述的相關規範和制度，以便徹底因應。

（三）機關組織架構和機關組織文化的調整與適應

就資訊隱私的保護而言，究竟既有的機關組織架構是否足以擔負這樣的任務，以及機關組織文化是否習慣於保護資訊隱私的程序和作爲，都是值得我們檢視省思之處。首先，就機關內部而言，無論是公務機關或者醫療機構，目前我國幾乎都並未設置負責個人資料保護業務的專責人員或單位，此一現象，不但導致無從建立機關和機構內部自我審查機制，以便確切地落實控管資訊近用和資訊流用行爲的結果，也使得我國各種機關和機構的組織文化中，長期以來均無從培養起尊重資訊隱私的習慣。未來健保 IC 卡正式上線之後，相關機關和機構有無充分資源，可以分別就通案原則和具體個案兩方面，判斷人民健康醫療資訊隱私應該如何受到保護，以及處理資訊安全和資訊隱私有無受到侵害的問題，都格外令人擔憂。所以，未來如何自組織架構的調整和組織文化的適應著手，強化資訊隱私保護所需的基本土壤，應該是值得努力的方向。

再者，我國並未設置如資料保護委員會或隱私保護委員會之類的專責機構，僅由法務部（法律事務司）統籌負責個資法的執行事宜。在此種情形下，當個人資料保護事項發生爭議時，唯一解決途徑幾乎就是直接訴諸司法機關，似乎並不是有效率的解決資訊隱私爭議的方式。因此，我們認爲，在嘗試釐清和解決諸如健保 IC 卡這種現代社會越來越趨複雜的資訊隱私保護問題時，不妨可以考慮針對和資訊相關的事務建立正式的外部審核機制，例如仿照美國根據一九八〇年代制定的 The Paper Reduction Act，在行政權內所設的 OMB（Office of Management and Budget, The Executive Office of the President）轄下之

OIRA（Office of Information and Regulatory Affairs）的設計，建立機關外部審查機制，一方面對資訊蒐集行爲加以明確充分的控管，另一方面也減少不必要之資訊蒐集活動，以便能夠真正地減少浪費和提昇行政效率。我們認爲，此一健保 IC 卡計畫外部審核機制的設立，應該考慮在行政部門內成爲常設性的組織，不應以臨時性或機動性之編組爲之，雖然不見得有另外設立單一部會或局處的必要性，但是卻應該賦予其相當程度的考核權能和審查獨立性，並且可以考慮和電子化政府相關計畫中任何需要外部審核機制者，儘可能進行統一周全的規劃和整合，以收整體一致地規範數位化時代中個人資訊蒐集和利用行爲的功能和綜效。

（四）健保法制中相關規定闕漏問題亟待解決

究諸實際，健保 IC 卡之本質僅屬健保憑證，目前我國對健保憑證之規範，僅有健保局所訂定之「全民健康保險憑證管理與使用須知」，並未有正式之法律授權依據。我們認爲，以健保憑證之本質來說，僅應被賦予確認健保身份的功能，不應該轉而成爲身份證之外的另一身份辨識文件，進而衍生出身份辨識文件可能衍生的僞造變造或濫用等困擾，也不該以健保憑證之持有與否爲依據，越俎代庖地決定病患有無就診的權利。同時，既屬健保憑證性質，其中所記載之事項和內容，即不應逾越憑證功能之所需，以免滋生資訊隱私不保的流弊。

更重要的是，我們認爲，當健保憑證 IC 卡化和健保 IC 卡全面上線之後，健保憑證已經不再只是單純的健保憑證，而是在憑證功能之外，透過卡片儲存和網路傳輸等作用，開拓了增添不少憑證以外功能的無限空間；其所涉及者，是人民資訊隱私權是否能夠受到合法適當保護的問題，同時也涉及人民的資訊隱私權在何等情況下應該妥協，受某種程度之拘束或限制的問題；既然是涉及人民權利義務的事項，依據法治國家的法律保留原則，便應該透過立法的模式，透過全民健康保險法相關規定的修訂，或是訂定仿照美國特別法的方式，明訂健

保 IC 卡的法律定位，徹底解決法源依據的問題；甚且，我們也認爲應該針對健保 IC 卡涉及醫療資訊的部分，修訂醫療法中和醫療資訊有關的規定，不應該繼續因陋就簡，以法規層級甚低的「全民健康保險憑證管理與使用須知」，做爲健保 IC 卡之法律依據。而是應該轉而思考以完整的法制架構和內涵，落實保護人民健康醫療資訊隱私的工作。

二、健保 IC 卡相關契約之檢視

健保局和健保 IC 卡計畫承包廠商東元電機股份有限公司(簡稱東元公司）兩者之間訂有「中華民國國民健保卡建置計畫採購契約」(簡稱採購契約)，契約內容不乏涉及資訊安全和資訊隱私相關事項者；直接涉及資訊安全和隱私保護的規定，無論是比例上或是品質上，對於廠商和實際參與操作者的控管強度，似乎仍嫌不足；由於健保卡計畫相關契約篇幅龐大，然就本研究計畫之目的而言，並無必要一一分析，本報告以下茲就幾個和人民資訊隱私保護相關且經過系統歸納的重點，逐一加以分析：

（一）契約保證事項

整體看來，健保卡採購契約中之建議書內容及備註條款多未明言「保證事項」，唯一例外的卡片品質保證[81]；惟就契約法理觀察，整體契約內容都是廠商應該保證履行的內容；不過，當我們進一步檢視契約內容時，便可以發現絕大多數的契約內容是多涉及硬體相關事項，和資訊隱私相關之事項十分有限。換言之，雖然晶片功能維持保持十年[82]之類的硬體保證事項，以及規訂有契約條款 9.9 之內所列的違反保固與維護事項的情形時，健保局得終止合約，並得沒收保固金作爲懲

[81]備註條款議定事項 1.1，採購契約第一冊。

[82]採購契約第六冊 1.3-19；1.3-27。

罰性違約金及依民法規定定請求損害賠償[83]，但是整體契約內容對於資訊隱私保護相關的權利義務事項，卻少見類似規範。

（二）保險對象對卡片使用情形的控制

基於資訊自主控制原則，持卡者如何簡易獲知卡片使用情形，應屬資訊隱私保障中相當重要的一環，而健保局和承做廠商之間亦應該針對此等事項界定權利義務關係，才足以保護民眾資訊隱私。根據我們檢視的結果，相關契約條款中雖然針對卡片之使用賦予健保 IC 卡持卡人某程度之控制權，訂有具體輔助辦法，但是卻也同時可能因而衍生某些爭議。例如，除在民眾使用 IC 卡場所設置卡片更新查詢設施，更規劃若干地點更新查詢及開卡機設備，以便達到一卡到底免換卡的目的[84]，但是這類規劃畢竟無法做到持卡者可以隨時檢視健保卡相關資訊的結果，是否即足以滿足民眾的資訊自主控制權利，不無疑問。此一疑慮雖然可以透過契約中進一步規劃的廠商將與金融單位、便利商店合作，將健保開卡更新功能植入金融單位的 ATM 或大型資訊站，提供開卡更新查詢服務[85]，並且在金融機構郵匯局[86]提供相同服務，並且嘗試結合 ATM 提供之[87]。然而，這類規劃同時也會衍生出更多人爲或網路上的資訊安全問題，從整體內容看來，我們似乎看不到契約中就如何徹底對健保 IC 卡持卡人做好相應的資訊安全和資訊隱私保全宣導教育工作，似乎並無具體方案，值得擔憂。

---

[83]採購契約第二冊契約條款十六。

[84]參見採購契約第六冊 1.1-2 和第七冊 3-2。

[85]採購契約第十一冊 4.4.5.1-4。

[86]採購契約第十一冊 4.4.7-10。

[87]採購契約第十三冊 4.7-1。

（三）承做廠商作業流程的資訊安全控管

承做廠商在作業流程上是否做好資訊安全控管工作，對於健保相關資訊的保全將會發生相當深遠的影響。綜觀契約內容，雖然列舉了從卡片製造到發卡過程中的控管措施，但是卻偏廢對實際參與作業流程的人員施以正確資訊安全和資訊隱私保護教育訓練的部分，似乎有改進空間。

（四）承做廠商本身之商業發展策略

健保 IC 卡建置計畫承做廠商東元公司和屬同一團隊之廠商，最近數年來曾經在不同時點和不同場合，根據其承做之健保 IC 卡建置計畫，提及其進一步的商業發展策略和加值應用構想，這些內容不乏涉及可能對資訊安全和人民資訊隱私保護造成負面影響者。然而，綜觀整體契約內容，我們似乎無法找到契約針對此類行爲或揭露事項做相應的權利義務規範，因而導致健保局對承做廠商類似行爲無從進行適當的有效約束，而民眾之隱私疑慮也不斷增高的結果。此一部分的問題，或許是可以考慮補救之處。

（五）IC 晶片卡目前和未來規定之存放內容和存取控制

根據「宣導手冊內容及樣稿」[88]和「健保卡使用說明內容及樣稿」[89]之規劃內容，健保 IC 卡系統所存放者，可以整理歸納如下：

（1）健保 IC 卡內之存放資料

1. 基本資料段：辨識身分：姓名、性別、身分證字號、出生日

---

[88] 頁 4-5.

[89] 頁 8-17.

期、照片等。

2. 健保資料段：紀錄就醫相關資料：就醫日期、就醫時間、就醫院所代碼、預防保健紀錄、孕婦產前檢查、卡片有效期限、就醫可用次數、最近一次就醫序號等。

3. 醫療專區：門診處方箋、重要檢查、過敏藥物等。

4. 衛生行政專區：預防接種資料、器官捐贈資料等。

（2）各欄位預定上線時程

A. 第一階段輔導期（91 年 7 月至 92 年 12 月）：
   1. 基本資料段：全部
   2. 健保資料段：如上
   3. 醫療專區：不實施
   4. 衛生行政專區：不實施

B. 第二階段適應期（93 年 1 月至 93 年 12 月）：
   1. 基本資料段：全部
   2. 健保資料段：全部（較第一階段增列：重大傷病代碼、主次診斷、醫師身分證字號、就醫費用、部分負擔）
   3. 醫療專區：部分，包括門診用藥、重要醫令項目 CT、MRI
   4. 衛生行政專區：全部

C. 第三階段穩定發展期（94 年 1 月以後）：
   1. 基本資料段：全部
   2. 健保資料段：全部（增列個人保險費）
   3. 醫療專區：全部（增列門診檢查、治療及手術、住院重要檢查治療或手術、過敏藥物成分名稱）
   4. 衛生行政專區：全部

綜觀以上規劃內容和時程，我們可以發現目前乃是規劃以漸進方式，依照健康醫療資訊的敏感程度高低，逐漸納入健保 IC 卡中，使其最終能夠成爲一張電子病歷卡。我們認爲電子病歷透過此一健保 IC 卡建置起來是否適當，是否符合人民的資訊隱私權期待，仍有討論空

間；再者，上述各個區段欄位內所規劃放入的資料，是否有其必要性，是否對個人隱私期待和資訊自主權造成衝擊，我們建議似乎可以重新評估。

其次，在目前計畫內容中設有醫事人員卡。原則上醫事人員卡是由特約醫療機構醫師所持有，具有防偽設計，在民眾就診時醫師人員藉由此與健保 IC 卡配合，以利讀卡。健保 IC 卡搭配醫事人員卡的使用，可以限制資料的讀取範圍（例如只有搭配醫事人員卡才能寫入病人的處方籤），以保障個人隱私。另本卡的權責單位爲衛生署，將由該單位制訂醫事人員卡的所有相關細節。此外，本卡預定在健保 IC 專案的第二階段（即 93 年 1 月）才上線實施。目前規劃內容中也顯示，醫事人員卡的認證要求必須高於民眾健保卡，而最適宜的認證方式爲要求使用「個人識別碼」（PIN），以辨別持卡人身份。然而，健保局和承做廠商究竟對醫療院所和醫事人員施以何等資訊安全和資訊隱私保護相關的教育訓練，從規劃內容和契約中都無法充分得知，衛生署應該負責制定之醫事人員卡相關規範細節，似乎也尚未出爐，這些現象對於健保 IC 卡正式啓用之後的人民資訊隱私保護均將造成不利的影響，我們認爲應該儘速改善。

第二節　資訊安全如何確保的疑慮澄清

我們認爲，自健保 IC 卡計畫實行至今，其所引發的隱私權爭議，其實多少和健保 IC 卡計畫內所規劃的資訊安全管理措施未臻透明，難以被外界充分了解有關，因此，倘若要試圖消弭民眾對於健保 IC 卡對資訊安全管理和資訊隱私的疑慮，可以從此處著手嘗試尋求雙方的共識。

一般而言，資訊安全管理主要是以文件審查以及訪談爲主。主要的文件爲整體計畫安全書（NHIC-DS-T07），整體安全機制設計文件（NHIC-DS-RT08）以及安全政策管理使用手冊（NHIC-DS-T09）。本計畫並不認爲我們應該對技術的細節進行審視與評論，因爲，在有限的時間與資源下，粗率地做這類評估，進而做出評論，不但危險，而且也不是負責的作法。因此，我們著重於文件的內容呈現，以及健保卡計畫是否依照文件所呈現的內容確實執行，做爲研究的重點。本研究計畫這種作法，與相關的資安管理標準例如 ISO-17799 以及 HIPAA 的 security rule 的精神，也是相符合的。此外，在訪談的過程中，我們也發現，與整體資訊安全息息相關，並且爲大眾所注意的相關網路建置和網路建置安全機制問題，並不在此一健保 IC 卡計畫之範疇內，由於時間和資源的限制，本計畫也不針對和健保 IC 卡相關但卻非屬此次健保 IC 卡計畫內容的網路建置安全問題進行探討。經過文件閱覽及訪談，我們有如下的發現和建議：

一 、文件不足

在健保 IC 卡計畫的整體資訊安全計畫書中，我們發現有些部分需要參照原廠之資訊安全相關文件，但是這些原廠資訊安全相關文件，健保 IC 卡的整體資訊安全計畫書並沒有將其要意呈現出來，此一現象頗爲讓人擔心這些文件是否並不在健保局的有效掌控下。我們建議，做爲承包廠商在我國的唯一買主，健保局應該本著契約的平等和誠信精神，爭取所有理論上應該交付的文件。

二、文件品質不佳

閱讀上述三份有關資訊安全的文件之後，我們常常發現相同的文字不斷的重複，而且有許多地方閱讀起來比較像徵求建議書（RFP），而不是安全計畫的規劃。尤有甚者，實質內容屬於整體『安全政策管

理使用手冊』者，在該文件的封面卻是標明爲『整體安全管理使用者手冊』。而且，在這份文件裡，我們也發現其間每一章節的品質也明顯不同，例如與製卡相關的部分，內容描述就比較仔細，但是，有些明顯涉及資訊安全管理的章節，卻僅僅將該達到的資訊安全目標羅列出來，卻不見使用文字描述究竟應該如何達成該項目標。就相關資訊安全文件所呈現出來的品質而言，此種計畫所能達成的資訊安全任務，令人擔憂。

三、資訊安全相關資訊不夠公開

如前所述，由於網路建置部分並不在目前的健保卡 IC 計劃內，但是我們在此處所主張的資訊安全相關資訊應該儘量公開的原則，也應該適用於將來著手進行的網路建置工作。究其實際，外界對健保 IC 卡的資訊安全了解不足，其主要原因應該是相關資訊不夠公開的必然後果。經過本研究計畫查詢健保局網站的結果，發現在健保 IC 卡的資訊安全方面，一般民眾可以獲得的相關資訊，大約是兩千字左右的說明，但是，這些說明和坊間任何一套資訊系統的安全說明相較之下，並沒有什麼差別。這樣的資訊質量和品質，實在很難建立起民眾的信任。不過，相對地，健保局的確在資訊安全學會的刊物上，介紹了健保 IC 卡相關的資訊安全措施[90]，這樣的作法值得肯定，而我們也希望同樣或類似資訊能夠更加公開，並且能夠在健保局的網站上公告。

四、資訊安全管理相關活動之實質成果和透明度明顯不足

根據我們的調查結果，整體安全計畫書審議會議，總計舉行了七次。但是根據我們訪談的結果，在這七次會議舉行之後，整體安全計

---

[90]李菱菱，健保 IC 卡安全管理機制之管理與設計，資通安全通訊第八卷第三期，2002 年 6 月。

畫書的內容並沒有經過該審議會議的通過。同時，在相關的文件中，提到了數個委員會例如『安全稽核委員會』和『卡廠安全管理小組』等等，但是卻缺乏任何文件，說明各委員會與小組的作爲。

根據以上的觀察和發現，我們提出如下的建議：

一、資訊安全文件公開化原則

儘量公開資訊安全技術文件，針對認爲不該公開的文件，並應公開說明部分文件無法公開的理由；其次，亦應公開資訊安全相關委員會之成員執掌和相關活動之紀錄。

我們之所以主張應該公開這些資訊，理由如下：

（一）符合政府資訊公開法草案之立法精神

目前正待立法院審議通過的政府資訊公開法草案總說明，已經明白宣示『在國家邁向民主化與現代化之今日，施政公開化與透明化，正是政府當前之施政目標，而政府資訊公開制度之建立，更爲達成此目標極重要且不可或缺之一環。隨著社會急速變遷與資訊時代之來臨，人民無論參與公共政策、監督政府施政，抑或投資商業行爲及個人消費等，均有賴大量且正確之資訊，而政府正是資訊之最大擁有者，爲便利人民共享及公平合理利用政府資訊，增進人民對公共事務之瞭解、信賴及監督，政府資訊公開乃成爲當前重要且迫切之施政目標，有必要建立一完整之政府資訊公開制度，此即爲政府資訊公開法立法之主要目的』，我們認爲，針對健保 IC 卡相關之資訊安全文件予以公開，乃符合政府資訊公開法制的立法原則。

（二）符合資訊安全原則

對於不了解資通安全的人來說，或許會認爲將資訊安全相關訊息儘量維持在不爲人所知的狀態，會增進資通安全程度，例如認爲不公開系統內部的密碼模組與使用的協定，應該是屬於比較安全的作法；但是，究諸實際，在資通安全密碼學領域裡有一個大多數專家都認同[91]的原則——Kerckhoffs principle[92]——此一原則的大意是說，就一個好的密碼系統而言，其安全性是植基於密碼金鑰是秘密的，而非植基於其他系統設計的方式是秘密的。這個原則應用到資安系統上，也是相同的道理。如果將系統所有的設計細節都當做是秘密，那麼，爲了保障安全性，所有的資訊都要加強管理，而所有知道這些細節的人也都要受到特別的安全檢查。這在目前的軟體產業中幾乎是不可能的，因爲，系統的發展常需要數個團隊以上方能完成，要對複雜龐大的團對做這樣的管理，其困難度可見一般。

更進一步而言，如果許許多多的資訊都必須保密，那麼資訊安全管理的工作將無法聚焦，以有限的人力物力來保持散佈各地的資訊的私密性，必定會產生許多原先無法意想或預測的疏漏。

當然，以上所述的公開原則，並不是主張所有的資訊都應該公開，但是，在密碼學的研究上，我們的確發現公開最大的好處，便是在於所有資訊安全領域的人都有機會來參與審視與檢驗；我們認爲，目前台灣在資訊安全方面的研究能量已具有相當規模，像健保局這樣規模的大型計畫，可以預料的是足以吸引很多研究者的關心和興趣，如此一來將可收集思廣益之效，也可以讓健保 IC 卡相關系統的資訊安全獲得更多不同角度的檢視機會，獲得更高的保障，進而讓大眾能夠建立

---

[91] *See* <http://www.counterpane.com/crypto-gram-0205.html> & <http://www.securityfocus.com/columnists/80>.

[92] Auguste Kerckhoffs 法國密碼系統專家，於 1883 年提出。參考 <http://www.cl.cam.ac.uk/~fapp2/kerckhoffs>.

起比較強的信心。

（三）避免因爲對事實認知的不同造成的歧見與誤解

我們建議，健保局應以公開誠信的精神，儘量主動公開相關的資訊，以便形成理性討論的基礎。在研究計畫的訪談過程中，我們一再地發現許多的歧見和誤解，是因爲對於事實不瞭解而造成的。我們認爲，儘量在最早的時間，讓資訊以最清楚的方式呈現出來，將有助於提昇各方就不同的議題討論之品質，同時亦可增加健保局在社會大眾心目中的可信賴度。

（四）公開資訊是該項資訊品質的保證

我們認爲，公開資訊等於是宣示特定資訊之品質保證；以資訊安全相關文件爲例，倘若維持目前我們在研究過程中所看到的健保資訊安全文件的水準，我想任何一個人都不願意將其公開，換言之，會被公開的資訊安全文件，在某種意義上便代表了公開者不擔心文件公開之後，其品質可能受到批評。倘若健保局將大量的資訊安全相關文件公開，當做政策，那麼所有與資訊安全管理相關的人員，都會有壓力將資訊安全文件盡量整理好，提高品質。或許有人會認爲即使公開了這些文件，也不會有多少人認真地去看，這麼做可能浪費時間與資源，但是，我們認爲資訊公開本身便代表了負責任的態度，況且大多數的資訊安全文件資料，本來就應該是完備的，因此公開資訊並不應該導致造成太多額外負擔的結果。

（五）資訊安全維護的長期性質

資訊安全維護需要的是長期不斷的努力，除了要有明確的政策與程序文件外，另外一件非常重要的事情，就是各項資訊安全控管事項的實踐，以及資訊安全控管程序的遵循。這方面的活動，必須經由各

種相關事件的紀錄以及會議資料，才能檢驗得出來。爲了避免外界產生健保局和承做廠商是否說一套做一套的疑慮，健保局應該投入必要的資源，將上述各項活動與會議之記錄做詳實的整理及公告，以昭公信。

二、儘量邀請代表不同民眾的社會團體參與資訊安全相關委員會議

在民主社會裡，政策的溝通與辯論，是凝聚共識以及尋求完備作法的不二法門。在此次的健保 IC 卡爭議中，健保局在政策形成之初期，並未積極地找尋政策溝通之機會，也沒有積極的尋找與思考可能的困難。一直到政策形成，計畫開始實施了之後，才開始做宣導工作，而且其宣導多以醫療院所爲對象，少有針對與人權團體與其他社會團體所進行的互動。例如在早期中研院資訊所即提出了替代方案，並質疑當時規劃的第二第三期的資料，將對個人隱私造成衝擊，很可惜的這樣的意見並沒有被重視，而目前的發展，卻正驗證了當初中研院資訊所人員的擔憂。又如我們經常聽到的 IC 健保卡例子，是法國的例子，可是卻從來沒有認真地去思考法國的申報程序與我國不同，在法國是由被保險人先付錢然後檢附單據向保險公司申請給付。這與我國目前的現況有極大的不同，所以也不應該自陷引喻失義的境地。這樣的資訊是健保界的學者早已知悉之事情，但政策形成之時卻沒有考慮到其間差異可能造成的影響，實有值得檢討改進的空間。雖然，在民主多元社會裡，大家都深知「流汗比流血好，遊行比暴動好」的道理，但是我們應該追求的是在會議桌前理性地解決歧見，達到不需流汗也不需要遊行的目的。要達到這樣的目的，健保局應該敞開心胸，儘量在早期即讓可能有相左意見的社團代表的聲音能夠表達出來，並且提出切中問題要點的回應。而其具體的作法除了儘量的公開資訊外，也應該儘量的讓各方意見的代表來參與會議，或是在網路上提供訂閱電子郵件的功能以及電子郵件討論論壇，讓所有關心 IC 健保卡相關事宜的人都可以在最快的時間內，接獲最新的資訊。

三、針對攸關健保 IC 卡的建置計畫所涉之資安事宜做整體規劃考量

如前所述，本研究發現，與資訊安全及資訊隱私息息相關的系統整合事項，以及上傳網路之規劃，並不在這次健保 IC 卡計畫當中。但是由於系統各部門整合時，很可能造成資訊安全漏洞，而且各相關計畫很可能專注於各自的計畫包含範圍內之安全問題，而忽略了整合時所需要注意的資訊安全問題，導致當初未預期的問題出現。因此，我們建議應該將整體系統建置與運作相關之資訊安全規劃與實施，以獨立之標案爲之，以確保系統整合不會成爲安全之漏洞。

四、尋求與承包廠商無任何關係之個人或資安顧問公司之協助

資訊安全即使是在資訊科學領域中，都是相當專業的領域，健保局沒有也不需要在內部設置這方面的專家。但是，爲了確保系統的安全性和未來資訊安全之持續維持，我們認爲有必要找尋獨立的個人或資安顧問公司協助監督健保 IC 卡計畫的資訊安全事宜。依據我們的研究發現，此一工作目前是由承包廠商來建置與完成資安相關之作爲，而由健保局內部組成的資訊安全小組來監督，小組內或有邀請國內相關的研究專家來參與者。但依據訪談的結果，我們這樣的作法可能不夠完備。例如專家的參與絕大多數僅止於開會而已，但是和資訊安全相關的監督工作，卻需要長期持續的投入，這樣的工作比較適合願意專心投入的個人或者業界的顧問公司來擔任。這與營建業有業主，建築師與包商的角色分工，是相同的道理。當然很可能在計畫規劃之時，健保局並未編列這方面的獨立預算，我們認爲這也是這項重大計劃實施的一大疏漏——畢竟，任何有經驗的人，都應該知道資安與隱私將會是健保 IC 卡這個計畫當中十分重要的一環，當時不願意編列相當的預算來尋求專業顧問的監督協助，使得健保局人員需要努力學習資訊安全方面的知識，卻又無法達到預期的專業水準，如此的經費配置方式，或許有重新討論的空間。

第三節　資訊隱私如何確保的疑慮澄清

除了資訊安全的問題備受質疑之外，健保 IC 卡所提供的空間，對許多人來說確實可能有救命的作用，例如藥物過敏資料。同時，我們也相信健保 IC 卡確實可以提昇醫療品質與減低醫療浪費，例如記錄上次檢驗和上次用藥。然而，從本研究報告以上的論述中，可以發現健保 IC 卡可能引發的資訊安全疑慮，以及對個人的隱私造成傷害，也是不必多加以爭執的事。

首先，我們可以用目前的紙本保險憑證爲基礎，來分析健保 IC 卡使用後可能對個人的資訊自主控制造成的影響，並提出未來可能的解決方向。現行的紙卡系統裡，被保險人其實可以選擇是否要告知醫師過去的診斷檢驗與治療，也可以選擇是否要出示重大傷病卡。然而，在健保 IC 卡系統根據目前的規劃上線後，尤其是在第二階段實施之後，被保險人將會失去這項控制的權力。不過，從另一方面來看，以健保局的立場而言，其最需要的是健保 IC 卡內所儲存的醫療行爲相關資料之上傳，該項資料之上傳，可以做爲醫院申報稽核之用，也是健保局在 IC 卡計畫中宣示之 IC 卡效益當中，最爲重要的一個部份。就這一部份而言，爲了平衡個人權利和公共利益，也爲了杜絕目前難以平息的爭議，健保局似乎可以研究是否可以提供被保險人選擇各項醫療資訊是否要讓醫療機構讀取的處理模式。但是，因爲健保局本就可以從醫療院所的申報資料當中，取得儲存在卡片上的資料，因此，在『資料從 IC 卡內被竊取出來以及在傳送時被擷取的風險很低』的假設下，經由個人之健保 IC 卡將就醫相關資料上傳，似乎並未對個人的隱私做出進一步的明顯傷害，或許還在可以理解和接受的範圍內。然而，在我們的建議下，因爲個人可以選擇是否要將該部分的醫療資料允許醫療人員讀取，如此一來，在不影響健保局行政需求的情況下，個人的自願性和自主選擇權利，也受到了保障。

至於重大檢驗項目，在未來的健保 IC 卡計畫設計內容當中，很可

能醫療院所必須在確定沒有重複執行昂貴重大檢驗之時，才可以進行該項檢驗，因此醫療院所在實施重大檢驗之前，必須能夠知道被保險人是否曾在近期已進行該項檢驗。如此看來，似乎結論會是在健保 IC 卡內必須儲存重大檢驗的資訊，而且必須讓醫療人員可以讀取。但是，我們認爲，既然健保 IC 卡計畫同時也實際上醫療院所也可以直接向健保局查詢該項資料，也就是說健保局可以要求類似現在信用卡所用的授信確認制度，如此一來就可以避免這樣的紛爭了。以務實的角度來看大多數的人將會允許醫療人員讀取他們在 IC 卡上的相關醫療資訊。所以需要直接向健保局查詢的件數也不會太多。但這樣的設計將可以尊重每一個人之自由選擇權。

總結以上的論述和分析，我們建議健保局應該仔細思考下列幾個重點，以平衡健保 IC 卡計畫所追求的效益，以及人民自願選擇和資訊自主控制的權利：

一、慎重且徹底地評估將可能引發爭議的資料之讀取權限讓被保險人自行決定的可能性和可行性。根據我們的瞭解，目前所採行的健保 IC 卡應該有這樣的彈性可資運用。同時，在進行評估之際，也儘量不要預先假設某些類型的個人醫療健康資訊本質上不牽涉到個人隱私保護的問題，而是應該儘量將所有資訊推定爲牽涉到個人隱私，這種處理模式應該有助於降低爭議。

二、必須讓上述個人自主控制機制盡量地簡單方便，做到大多數人都可以簡單的學會如何行使這項選擇權利的地步，以徹底落實個人自願性和自主選擇的意旨。

三、研究最適當的資料分割方式，來滿足個人資訊自主控制的要求；當然最有彈性的作法是讓被保險人對每一項資料都可以決定是否要讓醫療人員讀取，但這樣的作法可能會增加卡片應用程式的負擔，需要研究適當的平衡點爲何。

四、以資訊公開，建立監控權責單位來讓大眾相信上述『資料從IC卡內被竊取出來以及在傳送時被擷取的風險很低的假設』爲真。

五、健保IC卡過去至今的決策分析品質過份粗糙，在分析利弊得失的時候並沒有仔細的評估可能遭到的困難，今後似有修正改進的空間。例如，IC健保卡減少醫療浪費的功能，必須在第二第三階段階段實施後才可能發揮，但是在計畫初期，就可以預見這些敏感資料的存放必定引起大眾的疑慮與人權和社會團體的反彈。我們認爲，未來若能追求更加公開透明的決策過程，或者以設立隱私委員會的方式來處理資訊隱私相關問題，而不是將這類問題直接交由衛生署的醫療倫理委員會，做成可否的決策，可能是比較完備而且能夠服人的修正方向。

六、未來個人資訊自主控制的規劃：健保局應該仔細分析評估如何在尊重個人意願與隱私的條件下將IC健保卡的功能發揮到最大。例如，首要任務之一，便是研究如何在充分尊重個人意願的情形下，在個人有完全控制的條件下，將醫療相關資訊載入卡中。

就卡片資料讀取的具體規劃方向而言，在IC卡內的資料，可以有下列的操作方式：(一) 載入(輸入)；(二) 讀取 (輸出)：在此所謂的讀取，是指醫療院所與健保局以及個人所做的讀取動作；(三) 上傳 ：將資料上傳到健保局(上傳當然可以視爲是讀取的一種，但是因其操作特殊，所以分別列之)。

其次，對每一樣操作方式，可將個人的控制權力區分爲：(a) 強制： 個人沒有拒絕這項操作的權力；(b) 自願(預設允許)：這項操作可以由個人控制，但是預設值爲允許該項操作，個人需在表達不願加入後才可阻斷這項操作；(c) 自願(預設不允許)：同二但預設個人不允許該項操作，必須在個人同意後才可操作；(d) 不允許操作(某項資料如果控制強度爲d則代表不允許載入IC卡)。根據以上的敘述，顯然可知，對個人控制能力的尊重程度 或稱爲控制強度 d > c > b > a。

我們可以將某一資料的控制向量定義爲 （x, y, z)，其中 x,y,z 都是 {a,b,c,d}這個集合的元素。例如 （a, c, a) 代表這項資料必須強制載入 IC 卡內，但是否允許讀取由個人決定，不過必須上傳到健保局。如果某一項量 A 其每一分量
強度皆大於等於另一向量 B 之對應的分量稱該向量 A 強於 B，例如（a, c, b) 強於 （a, b, a)。

目前健保 IC 卡第一階段之資料皆爲（a, a, a) 形式。而爭議最大的是第二階段以後的資料其第二項操作控制是否可以是 a。對於每一項操作之控制強度是否適當，我們提出如下的一般性建議：

（一）選擇的控制強度必須與提供該項控制所需的成本，對個人隱私的侵害以及因此得到的公眾利益 取的平衡。

（二）對於各項利弊之分析，應全部公開，讓任何人都可以做檢驗。同時公開之資料應以讓一般民眾可以瞭解的方式爲之。

（三）應有一特別設置的專責審核委員會，就上述之資料取得平衡點，且應公開最後決定之理由。

爲了節省行政資源我們建議符合下列條件之資料可以免開審核委員會：

（一）該項資料爲法定健保局需蒐集資料，且控制向量爲（a, c, a) 以上者。（此處可以考慮以（a,b,a）取代 （a,c,a） ）

（二）在充分告知的情形下控制向量爲（c, b, b）以上者。

（三）公開資料說明如何讓所保證的控制權力交付與個人。若資料中有不可避免之專業知識，則應公開資料使得客觀的專業人士能做獨立之判斷。例如，如果就醫記錄爲健保局需蒐集之資料，則在允許個人

可控制讀取操作的條件下，應可蒐集。

最後，我們認爲，健保 IC 卡計畫執行至今，陸續引發不少爭議的原因，在於溝通過程未臻理想，導致健保 IC 卡過去至今決策分析品質粗糙的質疑不斷，換言之，無論是就社會溝通層次或者執行技術層次而言，主事機關先前在分析利弊得失時，似乎並沒有仔細評估可能遭到的困難，今後似有修正改進的空間。尤其是在比較敏感的資料存放，引起大眾的疑慮與人權和社會團體的反彈方面，我們認爲，未來若要追求更加公開透明的決策過程，主事者應該考慮就本研究報告附錄中針對民間人權和社會團體所表達的關切重點，以及學者專家所提出的改進重點，建立知識管理資料庫，以便分析彙整重要訊息，做爲進一步的決策參考，在對社會大眾做誠懇有效宣導的同時，追求未來健保 IC 卡計畫正式上線後常設的客戶服務中心的基本要求。

第五章　結論與建議

基於以上研究過程和以上各章的論述，本章將提出以下幾點經過歸納後的主要看法，並且區分立即可行建議和中長期建議兩者，附上本研究所建議之主辦機關及協辦機關，做爲結論。

首先，在立即可行的建議方面，我們的建議如下：

一、加強健保 IC 卡之健保憑證意義和身份辨識證件兩者之間的意義區隔，澄清民眾的混淆所在

以健保憑證之本質來說，僅應被賦予確認健保身份的功能，不應該轉而成爲身份證之外的另一身份辨識文件，進而衍生出身份辨識文件可能衍生的僞造變造或濫用等困擾，也不該以健保憑證之持有與否爲依據，越俎代庖地決定病患有無就診的權利。但是目前由於健保 IC 卡計畫宣傳中所謂照片卡可以免去攜帶身分證就診麻煩的說法，已經導致民眾混淆，有澄清之必要。同時，既屬健保憑證性質，其中所記載之事項和內容，即不應逾越憑證功能之所需，以免滋生資訊隱私不保的流弊。

主辦機關：衛生署；協辦機關：內政部

二、適當汲取比較法制的經驗，並且慎重分辨實行健保 IC 卡制度的國家和我國現狀不同之處

美國 HIPAAH 此一規範體制的擬定和辯論過程中所突顯出的問題，對於目前相關法制極爲欠缺的我國來說，極具價值，我們建議衛生署和健保局在制定配套措施和相應規範時，應該列爲重要參考依據。其次，當我們討論德國和法國的健保卡經驗時，必須區辨社會和

制度脈絡不同之處。例如，因爲法國的保險申報方式，和美國的申報方式大致相近，是由被保險人先付款之後，再向保險公司申報退費。因此在使用 IC 卡做爲健保卡之前，無論是個人、醫療院所和保險機構往往爲了處理紙張形式的申報表，需要耗費大量的人力物力，而引進 IC 卡的目的，便是爲了減低這項行政成本。然而，與法國健保制度相較之下，我國目前的申報方式與法國截然不同，因此，我們的醫療院所與個人缺乏像法國制度背景下那樣的誘因。這或許也是爲什麼 IC 健保卡制度著手推行以來，不少醫療院所怨聲載道的原因之一。

主辦機關：衛生署

三、強化個資法等相關法令之規範密度和規範強度，儘速確立健保 IC 卡計畫的相關法律基礎

綜合前章所論，我們認爲目前我國規範個人電腦資料處理相關事宜的個資法以及相關的典章制度和組織文化，對於健保 IC 卡可能引發的個人資料保護問題，規範密度強度皆有不足之處，應儘速加強之。

其次，我們認爲，當健保憑證 IC 卡化和健保 IC 卡全面上線之後，健保憑證已經不再只是單純的健保憑證，而是在憑證功能之外，透過卡片儲存和網路傳輸等作用，開拓了增添不少憑證以外功能的無限空間；其所涉及者，是人民資訊隱私權是否能夠受到合法適當保護的問題，同時也涉及人民的資訊隱私權在何等情況下應該妥協，受某種程度之拘束或限制的問題；既然是涉及人民權利義務的事項，依據法治國家的法律保留原則，便應該透過立法的模式，透過全民健康保險法相關規定的修訂，或是訂定仿照美國特別法的方式，明訂健保 IC 卡的法律定位，徹底解決法源依據的問題；甚且，我們也認爲應該針對健保 IC 卡涉及醫療資訊的部分，修訂醫療法中和醫療資訊有關的規定，不應該繼續因陋就簡，以法規層級甚低的「全民健康保險憑證管理與使用須知」，做爲健保 IC 卡之法律依據。而是應該轉而思考以完整的

法制架構和內涵，落實保護人民健康醫療資訊隱私的工作。

主辦機關：衛生署；協辦機關：法務部、研考會

四、健保 IC 卡建置計畫契約中相關權利義務事項規定的修正和加強

如同前章所述，檢視健保 IC 卡建置計畫契約之後，我們發現契約中對於資訊安全事項和資訊隱私保護相關之權利義務事項規定，不是模糊不清，便是付諸闕如。因此，我們建議，契約雙方應在可行之範圍內，儘速予以修正和加強，以落實健保 IC 卡計畫在保護人民資訊隱私方面的正當性。

主辦機關：衛生署；協辦機關：公共工程委員會

其次，在**中長期建議**方面，則可以區分成以下幾點：

一、以資訊安全透明度強化資訊安全

根據我們的觀察結果，我們認爲健保 IC 卡計畫應該追求以資訊安全透明度強化資訊安全的目標。首先，儘量公開資訊安全技術文件，針對認爲不該公開的文件，並應公開說明部分文件無法公開的理由；其次，亦應公開資訊安全相關委員會之成員執掌和相關活動之紀錄。我們之所以主張應該公開這些資訊，主要事基於符合政府資訊公開法制之立法精神、符合資訊安全原則、避免因爲對事實認知的不同造成的歧見與誤解、以公開資訊證明該項資訊之品質保證、以及有利於資訊安全的長期維護等幾個主要理由。同時，我們也建議在資訊安全方面，應該廣邀和廣納社會各界的參與和意見，避免過度的專業獨裁導致不必要的猜測。再者，和健保卡有關的所有建置計畫，其資訊安全規劃事項應該一併處理，不應過度切割，以免造成難以預測和彌補的

漏洞。

主辦機關：衛生署；協辦機關：研考會

二、以強化資訊自主控制落實資訊隱私之保護

我們認爲，秉持資訊自主控制原則，是保護個人資訊隱私的不二法門，因此，就健保 IC 卡計畫而言，應該排除成見和既有規劃，研究最適當的資料分割方式，來滿足個人資訊自主控制的要求；當然最有彈性的作法是讓被保險人對每一項資料都可以決定是否要讓醫療人員讀取，但這樣的作法可能會造成卡片應用程式很大的負擔，需要研究適當的平衡點爲何。其次，健保 IC 卡過去至今的決策分析品質過份粗糙，在分析利弊得失的時候並沒有仔細的評估可能遭到的困難，今後似有修正改進的空間。例如，IC 健保卡減少醫療浪費的功能，必須在第二第三階段階段實施後才可能發揮，但是在計畫初期，就可以預見這些敏感資料的存放必定引起大眾的疑慮與人權和社會團體的反彈。我們認爲，未來若能追求更加公開透明的決策過程，或者以設立隱私委員會的方式來處理資訊隱私相關問題，而不是將這類問題直接交由衛生署的醫療倫理委員會，做成可否的決策，可能是比較完備而且能夠服人的修正方向。至於有關未來個人資訊自主控制的規劃方面，健保局應仔細分析評估如何在尊重個人意願與隱私的條件下將 IC 健保卡的功能發揮到最大。例如在充分尊重個人意願的情形下，在個人具有完全控制的條件下，將醫療相關資訊載入卡中。

主辦機關：衛生署；協辦機關：研考會

三、健全資訊稽核制度的建立和加強資訊倫理教育訓練

我們發現，在健保 IC 卡整體計畫中，無論是機關或機構之內部或外部，對於相關之資訊稽核審查制度，均未有充分的考量，我們建議

應該仿照美國相關法制和措施，做完整之規劃，方足以確保健保 IC 卡計畫安全而順暢的運作，例如，醫藥衛生事務主管機關衛生署和健保局兩者，做爲全民健保制度運作的監督者和全民健保制度中唯一的給付者，應該善用醫療法和全民健保法中所規定的醫療機構監督權，在健保 IC 卡制度正式上路之前，全面建立上述機制，至少應該嚐試在醫療法和全民健保法兩項法律中尋找或儘速建立授權依據，設計出相應的細緻管制手段，要求健保 IC 卡制度下所涉及的醫療衛生機構建立此一資訊蒐集和處理事務的自我審查機制，以便大幅減少未來因健保相關資訊之蒐集和處理可能引起的反彈。同時，在健保卡計畫參與人員和醫療院所人員的資訊倫理教育訓練方面，目前之規劃也嚴重不足，就確保資訊安全和保護資訊隱私來說，也還有相當大的改進空間。

主辦機關：衛生署；協辦機關：研考會

四、非常之緊急狀況下不應亂求藥方，誤將健保 IC 卡當做醫療衛生政策之萬靈丹

政府行政和立法兩個部門，在檢討此次 SARS 疫情蔓延原因的過程中，數度提及健保 IC 卡可以有效預防疫情擴散，我們認爲此種主張有混淆之虞，充其量只展現出國人習於在非常緊急狀況下亂求藥方的陋規，才會誤將健保 IC 卡當做醫療衛生政策之萬靈丹，甚至可能將使各界更輕忽防疫真正關鍵問題。我們只要稍微回頭檢視感染擴大的原因，便可了解目前 95%的 SARS 感染都發生在醫院中，釐清導致各家醫院院內感染的根源。而經過歸納，SARS 疫情擴大原因可能包括：一、病人不知已遭感染，仍到急診室求診；二、醫師因爲各種原因對病情判斷有誤；三、病人疑似感染仍四處看病；四、醫療人員防護不足；五、醫院管理階層擔心收容 SARS 病患影響生意或導致封院，隱匿可能病例或將其轉院；六、疑似感染者隱身社區不願就醫；七、居家隔離執行令鬆散等。

想要解決前述第一與第二項癥結，必須從民眾公衛教育與醫療人員再教育著手。第三至五項則牽涉全國標準化的可疑病例後送與照護程序，避免病患成爲「人球」，同時得改善醫療院所過度商業化問題，否則，醫院將以考慮營運成本和效益爲優先，不願通報病例或未告知轉診醫院病患可能罹患 SARS，也可能爲了節省成本，要求前線醫護人員繼續使用可能已污染的防護設備，問題或病患刻意隱匿病例均非 IC 卡可解之問題。基本上病人就診史本可從紙卡背面戳記得知，並不需以健保 IC 卡達到此目的，病患倘若有意隱匿病史，也恐怕根本不願出示健保卡，甚或以其他特殊的就醫行爲來迴避。更詳細的確認病例亦應由胸腔 X 光、RT-PCR 檢測處理，不應指望記錄各種隱私資料（懷孕、經期、各種篩檢與疾病）的健保 IC 卡在此發揮此功效。

至於病患不願就醫，根源在於害怕疾病嚴重污名與歧視，這牽涉到官方、大眾與媒體對傳染病的了解與理性程度不足；居家隔離配合度問題，則與民眾教育與公民成熟度和官方配套措施之完備程度有關。上述兩者其實都與 IC 卡均無關聯。試想，既然目前大家都已經知道 SARS 是足以快速致死的傳染病，既然願意上門求診，就代表求診者本來便具有恢復健康以便做長遠人生規劃的誘因，亦即應該有告知醫護人員主要接觸史和病情病史，以便及早獲得妥善治療的誘因，才能增加自己真正的福祉，因此，究竟是何種原因導致求診者決定「損己又損人」地隱瞞病情，就足堪玩味了：是不是錯亂的 SARS 相關資訊和社會不斷製造污名化的結果，造成求診者做出愚蠢的判斷和決策？是不是錯誤的醫療衛生體系設計使得病人有意無意地逛醫院和隱匿病情？甚至，我們是否更該深究到底是個別病人隱匿或是醫院控管粗糙，才是疫情擴散的主因，才更具科學說服力？

甚至，我們可以稍嫌武斷地指出，問題不在於要不要用 IC 卡，而是要有嚴謹的法規和正確的誘因機制，明確規範醫療院所和醫護人員及時回報的義務。

我們只要稍加分析，便可發現政府想透過健保 IC 卡解決的醫院通報問題，可以用更簡單方式解決：醫師診斷出可疑病例，即時以電話、傳真、網路報告衛生署，再由主管機關每天數次彙整通報病患資料給所有醫療院所。這些通報彙整，牽涉行政部門的效率整合，即使有了健保 IC 卡系統，也必須要有相關規劃配合，基本的醫療院所監督工作沒有做好，健保 IC 卡上的就醫紀錄記載得再多也無用。

病毒細菌與人類永遠共存，未來新興疾病只會更多，甚至可能引發更令人感到可怖的緊急狀態，我們認爲政府相關部門應該引此次 SARS 疫情擴散爲殷鑑，徹底檢討傳染病防治策略，而不是以病毒爲藉口，過度誇大健保 IC 卡的效能，反而導致社會各界對資訊隱私和公共利益如何平衡的看法更加偏離焦點分歧的不良結果。

主辦機關：衛生署；協辦機關：研考會

附錄一
健保 IC 卡與隱私權保護座談會會議紀錄〈九十二年三月三日〉

時間：92 年 3 月 3 日上午九時至十二時
地點：中央辦公大樓七樓行政院研考會簡報室
主席：劉靜怡教授

主席致詞

健保局張總經理鴻仁：

關於健保 IC 卡，去年七月開始發卡至今已發行了一千萬卡，雖然此計畫預計要在今年六月完成，但社會大眾對此種措施有廣大的爭議，各方焦點不只在 IC 卡本身，尚有隱私權的問題，故參加此會議要聽取各個專家學者的意見。

健保局江副總經理宏哲：

由於 90-91 年的預算執行，現今已有 1/3 的人口已拿到健保 IC 卡，而本計劃的製發卡及 IC 卡資訊中心資訊系統等作業是由東元這家廠商承包，但會引發外界疑慮，因爲東元未來尚要發展商業業務，尤其是會前進大陸發展，其是否會拿這些人民的資料去做商業上的應用或是賣給對岸，都是引人關切的地方。而東元軟硬體的工作人員是否能受到公司良好的看顧也值得思考。基本上關於此計劃，政府是透過與東元簽訂契約的方式進行，依合約要求東元須提出一份整體安全計畫書，經專家學者審核通過後，據以實施。此外，健保局也成立一個安全防護小組，專門從事過程中安全防護的作業，例如：將照片黏貼資料送往東元整理的過程中須有安全防護，且此後要統一作公開的銷毀儀式。

主席：

開放表達意見。

何建明副所長：

關於健保 IC 卡的機制，提出了一些問題，第一個問題就是隱私權的問題，是否有防禦危險的機制？政府是否有良好的技術與配套措施？第二個問題就是權利與義務的問題，雖然健保 IC 卡的照片是自願性放進去的，但政府機構的公務員會半哄半騙的方式要求人民繳交照片，不然以後看病時會被要求帶身分證明文件以驗證身分，使健保 IC 卡變成了第二張國民卡，政府的全盤政策如何？此外，健保 IC 卡讀卡機設立的花費是由誰來負擔？醫生不可能花錢設置讀卡機，沒有行政程序配合，醫生沒有責任出這筆錢，如果政府需花五十億來設置，則實質上並未節省到什麼錢。（何教授主張政府以抽查的方式來檢驗醫療院所，如果有錯誤要施以重罰，來解決醫療誠信問題）此外，由於健保屬於社會保險機制，容易造成浪費的結果。第三個問題就是政府威信問題，在個資法中，沒有任何負責的主管機關。

李有專教授：

就綜觀上來談，肯定健保 IC 卡的計劃，認爲健保 IC 卡的正面多於負面，現在第一階段發卡已結束，正要展開第二、三階段，到時隱私權的爭議會愈加嚴重，但是當務之急是要培養國人的資訊保護概念。且最有爭議的是病歷史是否要放入健保 IC 卡內，如果放入會產生什麼問題與風險？主要是要讓人民知道其本身資料放與不放的問題及風險所在，了解後，自己選擇並承擔風險。對醫療院所作 auditing trail。舉例來說，在美國可以上網看病歷，全都留下紀錄，經詢問是否會有不當讀取資料問題，據瞭解只曾發生一件案例不當讀取。國內有 IRB 人體試驗委員會，負責控管醫療相關資料。民眾選擇使用 PIN CODE 保護自己的資料，也應了解這種方式的風險所在，如果未來發生緊急醫療救護時，因爲自己無法言語或語言不清，致使無法讓醫療人員使用過往資料，所導致風險，其也必須了解。在美國有 break glass 機制，只要有經過授權，在人命危急的前提下，可以去存取病歷資料，目的就是要讓簽署個人資料保護協定後，不要因此而造成遲延，犧牲了生命。

此外，健保 IC 卡的讀卡機費用基本上已確定由醫療院所自己來出，故應沒有太大的費用分擔問題。但是值得我們去注意的是健保本身對醫界的衝擊，那就是給付的不公平，外科醫師無法領取較高的薪水，但卻可能要負擔較高的風險，而現今我國醫療糾紛的賠償金額起跳是 2000 萬，造成外科醫生乏人問津，都是考上醫科後的最後一名來從事，無怪乎美國哥倫比亞大學教授謂此爲慢性自殺，這市政府要全盤考量的問題之一。

王郁琦教授：

關於隱私權保護與新興科技使用並不必然衝突，隱私權問題在於風險承擔，幾年前預計要推行健保 IC 卡時，還提過要作電子商務，至今終歸取消，雖然健保 IC 卡可使用的範圍相當廣泛，但是基於各種原因仍是要加以限制。可是要以資訊保護爲由來阻礙科技發展及應用終歸將失敗。建議應將資訊分爲三類：(1)無爭議性的資料，現在紙卡就已經有的，(2)較具爭議性但有用的資料，例如病歷，等配套措施做好再放入，(3)絕對不應該放入的資料，就不應該想去放入。所以關於資訊問題應可有安全的配套措施，但是有些資訊，是縱使 IC 卡已廣泛到人手一卡的程度也不能去碰的。

另外一個問題就是程序問題，在醫療資訊的使用上，IC 卡只是冰山一角，如果衛生署第一關都未做好，那法務部就很難接著作些什麼，而個資法成立八年以來，仍未見顯著成效，是值得我們去深入思考的問題。醫療資料庫的使用必須以嚴謹的方式，且絕對要用對方法，那決不是以收費的方式來管理，且如果要將醫療資料庫與其他資料庫（例如財稅資料庫）作交叉運用 CROSS LINK，應該要透過法律層級的程序爲之。

資策會科法中心戴組長豪君：

在此提出了兩個觀念問題，第一就是隱私權的保護必須隨科技發展而進步，第二就是隱私權如果作得好，對於商業模型 business model 也有所保護，可影響商業模型的成敗。許多業者有很多客戶資料與本

身的資料，會將其交由 IBC 與 ASP（資料保護業者）來管理監控。

此外，根據 2 月份的對醫療院所的一項調查結果，在醫療服務中，人民所關心的問題往往與醫療院所所關心的問題不同，容易造成問題及衝突。人民所關心的是資料放在該處的安全與否，會不會遭駭客竊取或被不當利用等外部入侵與內部管理問題，及個人本身對其資料的控制管理權問題，對於資料的審核或授權，是應採每階段同意制或者是全面授權制。而醫院所關心的是相關費用的支出，例如讀卡機成本由誰負責，及如何降低成本。

法務部劉專門委員佐國：

解釋個資法的立法目的，第一是保護個人隱私權，第二是促進個人資料的合理運用。而第二個目的卻也是民眾較缺乏的觀念，因爲即使法律面規範與執行的再完善，都仍是會有隱私權的侵害問題，故不能以保護隱私權爲由，來主張不能蒐集資料。而健保 IC 卡的資料蒐集工作是必須符合特定目的及蒐集要件，並且就算有特定目的也必須符合比例原則，並且須做到安全防護的措施，確保外部人不會未經授權就可以拿到資料。只可惜各個目的主管機關都不甚了解個資法，所以有必要加強宣導，使各主管機關了解個資法的重要性，才能有效確保資料的安全與正確使用。尤其是敏感資料，未來個資法修正案將增列對敏感資料的保護規定，所謂的敏感資料有四種：第一是個人健康資料，第二是個人醫療過程資料，第三是個人基因資料，第四是個人犯罪前科資料，這些資料都是比起一般資料需要更加保護的資料，即使人民同意，政府仍是可基於公益目的而限制其蒐集。

健保局江副總經理宏哲：

第一階段的 IC 卡只紀錄原本紙卡的資料，這是比較沒問題的，而第二、三的階段，可能較具爭議性，包括就醫紀錄、病歷資料等。醫療紀錄並非是由健保局紀錄，而是由醫生在爲病人看病時，直接記錄在 IC 卡內，而健保 IC 卡的記憶容量並不大，只有 32K，所以資料能放的並不多，晶片裡的資料是有加密的，用亂碼存放，並不能被隨便

讀取，只能用由健保局所製作的讀卡機安全模組卡(SAM)及讀卡機(讀卡機由各家廠商生產製造並經工研院認證通過)才能讀出基本資料，另外必須要有醫師卡才能讀出醫療資料。且之所以要在 IC 卡中紀錄一些醫療資料，是爲了保險行政作業需要，如重大傷病代碼，目的就是爲了要替代重大傷病卡，免除病人的部分負擔費用。

健保局張總經理鴻仁：

並不是因爲電腦的出現才造成隱私權問題，而是普遍的電腦化才顯得隱私權愈嚴重，所以要設法分析就醫流程，就各個部分與隱私權的關係做探討，看隱私權保護與健康保護有何衝突？而以電腦化的資料庫與隱私權保護有何衝突？再探討 IC 卡擴大了什麼範圍？增加了什麼功能？第一階段健保局已執行完成，已無什麼彈性，但至於第二、三階段，尚有彈性可以再討論，希望聽取大家的意見再執行，以達到共識。

何建明教授：

我國的健保 IC 卡制度似乎很類似社會保險制度，其中原因可能參雜了政策性問題，其中包含了社會救助與保險的目的，使得不只是醫生分配上出了問題，也使得醫生與病人間產生了不信任問題，在此指的是人民想找信任的醫生，如果 80-90%的病人都信任醫生的話，較不會有信任問題，只有在新增病例的 10%病人，會產生信任問題。而健保 IC 卡的出現會不會更易使病人到處作醫療 shopping？而如果病歷資料可以帶著走，但 B 醫院的醫生又是否能信任前 A 醫院的醫生所記錄的病歷呢？以後出了事，責任應由誰負擔？所以科技仍須符合人性，不然最終仍是會被淘汰。

張顯洋主任：

我們要重視科技，但仍須注重倫理，所以技術不是問題，人性才是最終的問題，就以阿里山的小火車事故而言，直昇機超載的目的是爲了救重傷患者，如果他飛起來了，可能就是我們所謂的英雄，但如果飛不起來呢？

第一階段的運作，IC 卡可以節省許多經費成本，甚至是時間成本(例如換卡)，那些都是社會成本，無法確切用實際金額計算。並且 IC 卡的設計本身已具有許多資料的保密性，尤其比起現在用的紙卡而言，至少他看不出是 A 卡或者是 AA 卡，不用蓋章就看不出哪裡就醫。而第二階段的執行是可以再作衡量取捨 trade off，且許多民眾是較無知的，他們並不關心資料隱私問題，很多民眾拿到健保 IC 卡時是很開心的。

莊庭瑞教授：

我國的健保制度是採強制加保的方式，人民沒有選擇要不要的權利，而不加入是會受到處罰的，那麼要人民如何能信任健保局呢？舉例而言，雖然健保局台北分局經理因不配合警調單位偵查而被控妨害公務的罪名移送，但是中區警調單位不也移送了兩名健保局員工，該員工竊取人民的醫療資料再賣予保險公司，而移送法辦的是兩名員工，處罰的也是兩名員工，健保局的高階經理都未因此而受到處罰，則高階經理又如何會關心要加強保護資料隱密性呢？因爲不處罰全體機關的話，高階人員根本無積極動機去加強保護，而健保 IC 卡計畫也多有延遲，此中根本無信任機制存在，連要信任中央健保局安全維護資料都很難了，更何況要由民間機構東元公司的軟硬體設備來維護，所以要強調之中的信任機制何在、訓練人員素養、安全防護措施等。

健保局張總經理鴻仁：

從行政體系來看，立法院預算到健保局執行，至研考會管考，都應可以確認個人的行政責任與法定責任。而健保 IC 卡的計畫猶如火車已經開始運作，此社會應有能力來將此計畫完好達成，如果隱私權重要到根本不應該有此計畫，則行政院自然會停止這個計畫。所以現在應在已有 IC 卡的情況下，討論如何對民眾作最大保護。

郭明政教授：

我們對 IC 卡的質疑是資訊業的問題，是行政過程的問題(行政公務員的責任)，就像一個很爛的國家是否能做到 High Class 的計畫？這

並不是健保 IC 卡本身的問題，而是資訊保護與專業倫理的問題。所以要不要有第二、三階段可以再作討論，如果質疑的聲音成理，那麼連金融卡、信用卡等也都不該做了，所以我們應該釐清問題所在。健保 IC 卡呈現四個層面：第一是確認被保險人(就像一個保單)。第二是健保資料，主管機關是健保局，第三是醫療資料，主管機關是衛生署，這些機關是資訊保護官，執行資料使用的同意程序。第四是個人資料，資料使用的同意程序要經由本人、健保局、甚至公益團體等。

李有專教授：

第二、三階段的資料建構仍是不可廢的，但可以保留 withhold 一些某程度以上的資料或是敏感性資料。並且談到醫療人員的責任，這些資料可能就具有重要性，如果病人保留某些資料未讓醫療人員得知，而使得醫療人員誤判，則此責任歸誰？所以醫療人員到底能不能詢問病史？能不能建檔儲存？甚至上傳至健保局？或是就儲存在健保 IC 卡內？這些都是值得深思的問題，所以要在資訊一直要求被保留 withhold 的情況下，卻又要求要誤診的機率下降，這是很詭異 tricky 的問題。

主席：

此次的研究計畫並非爲任何人收尾，而是評估健保 IC 卡何處不足，到底是否應廢除健保 IC 卡不在此討論範圍內，此政策的決定是在於行政院與立法院。

許志雄副召集人之代表：

健保局張總經理不能在此表示任何決定是否推動計畫，在上次的人權小組會議中，游院長的意思是要溝通到沒有聲音爲止，所以討論至此，問題是在於強制性問題(病人非主動自願提供自己的健康資訊)、附加問題(相關部分的疑慮，有關修法、個資法、民法、刑法)、合法性問題(法務部須說明立法政策與健保 IC 卡的關係)。

研考會劉專門委員佐國：

由於健保 IC 卡的收益是不能用實際上的金錢來衡量，所以要如何降低成本就是重點所在，例如隱私權的侵害可能就是 IC 卡的成本。而最有異議的就是第二、三階段的資訊是否存入 IC 卡，醫療界認爲第二、三階段的收益很大，附加價值主要就是在第二、三階段的資訊，但就隱私權的疑慮也是在第二、三階段最大，所以要如何取得平衡點是最重要的。

東元公司吳凱源處長：

東元公司是在健保局的嚴格要求下處理資料安全維護，且 IC 卡內的資料只有名字、識別碼、住址，而無其他資訊，如果壞卡則會銷毀，記憶晶片是通過德國公正團體的檢驗。此外，現今的各醫療院所都已建立了病人的病歷資料，反觀人民反而沒有自己本身的病歷資料，如果有健保 IC 卡的話，人民本身就可以有自身的部分病歷資料，是隱私權的進步或是退步？可以做一番調查。

陳耀昌教授：

必須考慮健保 IC 卡計畫是否會改變就醫行爲模式的問題。如果一個 16 歲少女墮胎，她可能可以在紙卡用到第五格後去婦產科墮胎，等六格用完可以丟掉，可是健保 IC 卡使用後，是否會改變其就醫行爲？因爲 IC 卡不能換新的。且健保 IC 卡應屬於保險憑證，但保險憑證是否可以建入病歷資料就是問題？

健保局張總經理鴻仁：

健保 IC 卡內容較紙卡具隱密性，其到哪處就醫外人無法得知，父母更不可能可以從 IC 卡看出來該名少女曾去過婦產科，且 IC 卡內的就醫紀錄每六筆會更新一次，與原紙卡方式無異。

陳耀昌教授：

那如果是該名少女有父母陪同就醫呢？

郭明政教授：

那就與健保 IC 卡沒關係了，紙卡與 IC 卡都相同。

莊庭瑞教授：

保險憑證是由健康保險法而來，而健保 IC 卡所涵蓋的範圍已經超過健康保險法中所授權的範圍了，因此產生了兩個問題：第一就是健保局是否適宜作此 IC 卡的資訊管理與蒐集？第二就是這樣做，對民眾的利益爲何？且第二、三階段的資料以健保局的說法，是可以方便資料流通，以及節省資源浪費，但是之中仍有一些問題，舉例來說：若病人已作了 MRI 的治療，醫療過程上是不能重複再做的，且法律上的配合及醫療行政上是否清楚？最重要的是第二、三階段的資訊揭露有涉及到各個醫療院所的病歷移轉信任關係，如果甲病人曾在 A 醫院看病，病歷儲存在健保 IC 卡中，之後，甲再到 B 醫院看病，B 醫院的醫師是否信任 A 醫院的醫師所載入的病歷資料？出了錯又應該由誰來負責任？如果又因病人本身自己保管 IC 卡不當，致使資料出錯，又該誰來負責任？

健保局張總經理鴻仁：

本次會議主要在於釐清健保 IC 卡與紙卡哪個較具隱密性？本人認爲 IC 卡較具隱密性，而健保 IC 卡是否應註記其爲低收入戶，而造成歧視問題，是一個頗具爭議的問題，這可以用 0 與 1 來做註記，比持一本的低收入戶證明更能保障隱私，而 IC 卡上的病歷資料也是只有醫生可以看的，所以沒有人可以不藉由插入醫師卡就能看到所有資訊。如果是文件洩漏的問題，那就是制度要防範的，而且是例外案件。

健保局江副總經理宏哲：

其實病人要墮胎或看精神科，使用紙卡的話，隱私較不保護，若是文件上的洩漏，則兩者之間已經無差別。而至於保險憑證是否可以儲存健康資訊？本人是認爲可以，因爲保險憑證全世界都有放入被保險人的資料，而醫療院所要提供的醫療費用收據及用藥明細原本是要印出給病患，現在不過是改以放入 IC 卡的方式儲存。

郭明政教授：

有些資料是必要的，不能用某些資料可能會被濫用的理由來反對健保 IC 卡的使用，不然連原本紙卡功能都應被摒棄，而且資料的運用可以用來做正面的追求，例如：收集全世界的病歷資料用來確定病型。如果資料整理能夠有益全民，爲何不可？而且如果以資料隱私爲由，來爭辯健保 IC 卡使用的三階段，第一階段都要吵個三十年了，則第二、三階段就更無法推展了。

白裕彬教授：

對於第二、三階段的執行採保留意見，但原則上贊成可以透過同意制度經由某處下載，而且資料的採集也是浮在檯面上的，可以接受任何人的監控。而檯面下的問題，則是要確切掌握醫生的行爲，所以第二、三階段仍有很大的討論空間。

莊庭瑞教授：

健保 IC 卡的資料是隱性的，但並不代表隱性的資料就比較受到保護，因爲民眾本身可能無法得知其儲存的資料是否有錯誤，更何況去更改錯誤，所以這點仍值得去思考。

附錄二

健保 IC 卡與隱私權保障座談會會議紀錄（九十二年三月四日）

時間：92 年 3 月 4 日上午九時至十二時
地點：中央辦公大樓七樓行政院研考會簡報室
主席：劉靜怡教授

主席：

今天很高興能有這個機會和大家坐下來談，請大家幫研究團隊的忙，讓社會團體的 concern 能反映給主管機關知道。

健保局江副總經理宏哲：

行政院十分關心這個問題，謝謝有這樣的溝通平台，能利用這次的研究計劃，來聽取民間社會團體的意見。

目前健保 IC 卡已發行一千萬張已上，請大家可以去各大醫院試試看。而 IC 卡目前是第一階段，資料內容就相當於現在的紙卡內容(如附表)，沒有任何的病歷資料。其他資料在第二階段(93 年 1 月)才放，但我們是有彈性的，放什麼資料，是要經過對談及討論才決定內容。因爲 IC 卡的容量只有 32K，無法詳細紀錄任何醫療過程，且不如大家所擔心的，此並未放入病歷資料、也沒有個人資料 ，更沒有家族病史、DNA 圖譜等。

第二階段的蒐集仍以健保業務爲主，有助於醫師的診療，可以作跨院的整合。IC 卡的好處在於卡面看不出卡別、醫療院所紀錄，並可節省換卡的時間成本、換卡據點設置等大量的社會成本。

IC 卡的確有其風險，我們的防範措施是用 pin code，並且要以醫師卡，並以讀卡機配合健保局製作發給的讀卡機安全模組卡(SAM)才

讀的出。但有一些疑慮，有關個人資料是否會被盜用、個資法到底有沒有完善保護的問題。

事實上，現在很多醫院都已電子化，醫院資訊也有可能會外洩，不能只說是 IC 卡引起的，而是整個隱私權考量、醫學倫理、科技資訊的問題。

愛之希望協會 丁文：

我們的立場是支持健保制度，但對 IC 卡有意見如下：

(1) 第二、三階段之後會使病患隱私曝露，關於放入何種、多少資料，很少在廣告上看到健保局的宣導。放入的資料用代碼，但也是會被看出；並且放入大量的資料，如 60 筆的用藥紀錄，這幾乎可以是一輩子的用藥量。

(2) 雖然這樣的資料並非完整，但已經是探知人民隱私了。32K 的容量可放 16000 字，容量十分地大，且是由別人寫，寫什麼自己都沒辦法知道，第一階段的資料只用了 8K，還有 24K 可以紀錄，值得擔心。

(3) 放上 60 筆用藥紀錄，像用了 RU486 要 60 筆紀錄才會消掉。愛滋病患者一再地被貼標籤，以 AIDS 治而言，只有一半就醫，是因爲原本的醫療制度威脅人民的隱私，如今使用 IC 卡只會使問題加劇。

(4) 健保局提到簡單的註紀可以幫助醫生，其實利用轉診制度就已足夠，無須再疊床架屋。

(5) IC 卡也並非如此方便，因爲每 6 次就要再刷一次，拿藥還要再寫，對病人來說是多一道手續。現在的醫療制度已經有許多的漏洞，使用 IC 卡只是再多複製漏洞。

健保局江副總經理宏哲：

我來解釋一下，所謂的「組」是指存放的空間，因爲一次可能開多種藥，所以需要較大的預留空間。還有更新機就是讀卡機，散佈在各醫院診所，且低於 3 次以下，醫護人員基本上就會自動幫忙更新，

並且系統會直接寫入。關於 32K 其實現在只剩下 8K，因爲還要放其他應用程式，剩下的 8K 目前沒有其他的用途。

健保局 劉經理：

大家一直很關心到底第三階段是什麼，我們說第二、三階段是要等待共識再決定要放入什麼。現在有三種方案，(1)放入資料，用 pin code 保護；(2)有些資料就是完全不放；(3)預留空間，讓人民自己選擇是否放入。這三種方案都有配套措施，要分別討論放與不放的風險。

台權會 莊紀婷：

我要澄清一下，這不是單一的健保 IC 卡個案，是整個國家科技政策的問題，爲什麼國際潮流走向保護隱私，台灣還是採取高風險的作法？問題的重點在於我們要如何來決定自己資料的流何？不應該是政府做了決策再來尋求社會團體配套。

在官方網站上宣導 IC 卡是一卡多用，這根本就是國民卡的翻版。釋字 443 號要求法律規定或明確授權、524 號也要求全民健保應有明確規範，現在沒有電子憑證的明確授權，就算是立法院正在修訂的第 16 條之 1 也沒有考量隱私的問題，行政人員有太寬鬆的解釋空間。如此沒有法律規範之下，怎麼能讓人民相信？

再來是發卡有無必要的問題？民間團體的聲音並未被聽到。我們可以說有人被砍一刀受傷後，就說反正你已經被砍一刀、所以再砍一刀沒關係嗎？(比喻隱私權和 IC 卡的問題) 爲什麼不能設法改善呢？又說這樣做能促進看診品質，但是難道這是唯一的方法嗎？其實健保局有別的目的，就是稽核醫院是否有浪費的情形，但是這難道非要如此嗎？中研院其實有提過改良的卡片計劃，爲什麼不用這個，卻要用花了 38 億又會傷害隱私的方式。

關於民眾的逛醫院(doctor shopping)、重複檢查的問題，這也許是因爲人民不信任醫生診斷，所以才會重複就診。這是醫療倫理有問題，

應由宣導、教育著手，而不是由病患來承擔這樣的風險。

愛之希望協會 丁文：

應該先想一想 doctor shopping、重複用藥、檢查的理由。並且 IC 卡內紀錄並不清楚，仍然需要重複。這可能是轉診制度不完善，應從此改善。

殘障聯盟：

我們從報章雜誌了解，弱勢偏遠山區，因爲沒有病史，常常會延誤診療時機，原本是很樂見 IC 卡能解決病歷傳輸的問題。但是 IC 卡在最初發展時，爲什麼不直接找受影響的民間團體來進行討論，無此已決定方式再來研討問題，最後造成不能實施和延遲的後果，這種是浪費公帑的方式。

並且民間的意見往往未能傳遞，去年衛生署加開醫療改革會議時，沒有一個團體可以與會，但是內政部在開社會福利改革委員會社會團體就可參加，爲什麼內政部可以、而衛生署不行？這是醫療的專業霸權，衛生署會變成醫生署、只聽醫生的意見。

並且 IC 卡的目的是爲了便利人民就醫、節省成本，決不是爲了要稽核醫療院所的浪費，那是不對的，目的就錯了。

主席：

關於衛生署變成醫生署的問題，健保局可以回去反映一下。我們今天在這裡就是希望不要以媒體作爲中介，而是可以用面對面座談的方試討論問題。

健保局江副總經理宏哲：

很抱歉當初計劃發展時未邀請民間團體來參與討論。雖然這是一個不太負責任的說法，但是我在這實在是覺得有點尷尬，因爲當初推行時許多人並不在現在的位置上。93 年要放進什麼東西，邀請大家來

談是一個誠意，絕非趕鴨子上架。原本的概念是把現在收據、藥品明細的資料收錄在 IC 卡中，可以討論什麼樣的項目應該放進去。

性別人權 王蘋：

應該考慮 good intention 是否帶來 good consequence。IC 卡的實施像一個定時炸彈，強烈入侵人民的 privacy，炸彈是本質的問題，最終的結果就是可能會帶來爆炸。

還有關於風險風擔的問題，政府把大家的資料都放在同一個籃子裡，要爛就全部一起爛，沒有分擔的可能，人民也沒有選擇的權利，我實在是想不清楚到底要怎麼來改善。

若說只要放紙卡的內容，那麼這樣 IC 卡的成本是不是太貴了？如果已經討論出來第二階段已經不放，那還有第三階段嗎？我們組織的努力目標是在維持第二階段的內容和第一階段一樣。

想請衛生署評估 IC 卡不做會造成多大的損失、繼續作有多少損失、及改良式的紙卡是否比較合用的問題。

健保局 劉經理：

希望大家快樂一點。健保局對於溝通從未放棄，但是有些力量也有不希望第二、三階段與第一階段一樣。健保局對於放什麼東西沒有定案是可以保證的，一切都可以談，要達成共識才會放進去。分別和不同的代表談，談過以後還要大家再一起談。

主席：

健保局現在是有規劃沒有定案。

張維：

聽下來健保局仍在原點，就是政策就決定了一切，我的焦慮是重

覆的議題一再地被探討。去年想要參加衛生署醫療倫理委員會被拒，人民的聲喝沒有辦法被聽到。如果不發卡，人民的損失是多少？有改良的計劃爲什麼不試？

其實要放什麼資料應該在六月前就要確定，因爲那時大部分的民眾都會拿到新的健保 IC 卡，感染者會擔心隱私受侵害，如果人民因爲不用 IC 卡而自費，這種的制度是可悲的。

有許多民眾因爲發行 IC 卡有疑慮及焦慮，要回頭看看健保 IC 卡的本質是什。基本上是政策決定了什麼，而非人民決定了什麼，IC 卡的病歷是什麼，人民看不懂、也沒辦法讀，只是便利了決策者而已，這樣會強化醫病關係的緊張。如果醫病關係如此緊張，人民會放心將資料放入 IC 卡嗎？我認爲如果不從人性爲出發點，政策並無意義。

健保局江副總經理宏哲：

在討論的過程中，很遺憾不能說服大家，可是健保局不斷被洗腦、被拉向對方，很快樂的部分是大家有說服我們。如果說會讓病人不敢出來就醫，我想在決策上應該沒有官員會做出這樣的決定。重大傷病註記的目的是因爲和其相關的部分可以免除部份負擔。回應剛才的話，應想一想這到底是碰不得或是例外管理的思考。

張維：

是由誰決定放入資料？

健保局 劉經理：

這就回歸到上面說的三種方案，有多樣化的選擇。

台權會 莊紀婷：

重點是健保 IC 卡是強制的，人民沒有選擇的機會，也許對許多種的病患需要，但一般民眾爲何不能選擇使不使用 IC 卡，選擇資訊要不要公開？應將個人跳脫團體來思考，爲什麼我不能自己選擇、自己衡

量風與利益？可否不要用 IC 卡，收據就用紙本？

並且健保 IC 卡都只強調收益而未強調成本，無形的風險也應納入成本(financial loss)來考量。

殘障聯盟：

我要回應莊小姐有關強制性的問題，可不可能設計到由自己來選擇放或不放、使用與否？就像從小老師就決定公開成績，爲什麼我不能自己決定成績要不要公開？爲什麼人民不能自己選擇是否公開？

主席：

討論到了是不是有 100%自主決定的可能，可以就用身分證加上紙卡就有就醫地位嗎？

健保局江副總經理宏哲：

多重選擇、自由意志的問題我們都會納入考量。但是如果我現在沒有評估就回簽，到時候可能變成持紙卡者會反彈被貼標籤。

主席：

自己選擇時就要考慮是否有能力做風險承擔。研究團隊扮演的角色只是建議、告訴健保局有什麼樣的選項，最後的決定權還是在健保局。其實如果現在停止，江副總自己也不會怎麼樣，也許會有行政責任。但是如果永遠用執行者的角色來談也非妥當，應可以諒解。

日日春關懷協會：

其實我很好奇健保局在衡量時利弊時，二千二百萬人的利益怎麼考量？健保局說辦過的 1600 場演講對我們來說好像也不相關，覺得工會朋友們似乎也不怎麼了解。

我舉一個例子，有一個 20 年前是一個性工作者的案例，現在都一直懷疑她被監聽、被瞧不起，以致於沒有工作，很沒有安全感，我也

什麼都不能幫她，只能要她如果再發現有被跟蹤就馬上來跟我講。像是性工作者，拿掉 11 個小孩，紀錄不是都全部留在健保 IC 卡上了？我覺得這樣的暴力無所不在，政府的立意又不說明白，性工作者的隱私很難說出來，只好到時候又發生跳樓事件。我覺得像今天這種場合似乎只能講講苦衷，只是隱約覺得利益很大，現在政府已經以公共安全之名 monitor 性工作者是否感染愛滋病，我想這種情緒，只能等到結果惡化再出來吵了。

我想說的一點是，可不可以請政府把利害講清楚，讓像我這種的白痴小市民能看清楚 A、B、C 是什麼？能知道紙卡、IC 卡到底是可不可以選擇。

主席：

每個人無知之處不同。

王大為教授：

有時不在環境下就不會了解別人是怎麼樣的，參加這樣的座談讓我有很多感受。我想很多是沒有辦法在健保局解的，只能反應意見。昨天莊庭瑞很 upset，因為我們在 2000 年就 predict 健保 IC 卡會變成很貴的紙卡。

因為卡是強制的，健保局的無辜之處在於責任很大，負責所有人的健康，如果是保險公司就可以不必如此。這種集合的價值是 apply 到所有國民，如果讓國民知道問題，是增加政治風險，所以現在的政治風險其實不高。

我的提議是，有沒有可能讓三十幾億的教訓變成十幾億的教訓就好？

我想應該在某種程度上讓個人覺得有 control, 在看病口語交談時是可以的、但是在 IC 卡謂人沒有 control、完全 powerless(不知道寫了

什麼)，只是希望可以減大量的無力感，不過健保局就可能無法達到當初預計的稽核效果。

在公共政策下本來就無法完全符合每個人的意願，這是因爲成本的考量，現在是說，有沒有可在某種控制下，還可發揮原本立意？可否找到共通點(compromise)，讓病患可以 access some control。不過我也懷疑究竟是否有 lesson，好幾百億的都有了，不過我只是想 save20 億。

法務部代表：

本次會議重點在擔心本身隱私權遭受侵害，實際上，我們日常生活的隱私權無時無刻在遭受侵害。像我承擔個人資料保護法的案例，就有遇到懷孕就收到奶粉廣告、早上才住進加護病房下午就有葬儀社廣告、出獄找工作才半年就因被探知而 fire 的案子。IC 卡剛推出，其實我個人也有所存疑；現在我出席這個會議並非爲健保局或衛生署背書，而是爲了了解 IC 卡是否侵犯了隱私權，按照健保局的說法檢視，基本上還算符合個資法。其實各國都在蒐集資料，不能因爲怕會被洩露就不做。

不過希望健保局可尊重個人參加原則，讓人民可以自我選擇紙卡或 IC 卡、或是要記載什麼資料。我個人的看法是，磁卡的隱密性較高，因爲看不出職業、就醫資訊、就診次數。

最近個資法在修正，特別針對敏感資料(特殊資料)的保護，分成四類：(1)健康資料；(2)醫療資料；(3)基因資料；(4)犯罪前科。沒有法律規定不能蒐集，一蒐集就是違法，即使當事人同意，主管機關也可以介入禁止。

愛慈基金會：

我現在聽下來覺得其實紙卡和 IC 卡並行似乎不太可能，因爲健保局一直都沒有針對這個問題回覆，顯然已經是既定政策了，但是希望健保局可以提供幾個配套措施，對全民做調查，將資料分成 ABC 放

入，讓人民可以做選擇。這樣可能會增加健保局的作業程序，但是可否納入考量。

主席：

愛慈相當程度回應了王老師的看法，請多給王老師一些 response。

張維：

希望尊重當事人自主權，確實有一群人不想讓醫生知道他們的資料。可以選擇只要第一階段嗎？並且如果選擇放入是否可以受到有保障的保護，因爲現在似乎只要用行政命令就可以調閱。

主席：

個人選擇階段可以是一種模式。其實充份保護當然是法律應當做的，不管有沒有 IC 卡都應如此，只是現在執行密度可能不足，也可能有些尚未規範。

性別人權 王蘋：

我現在發言只是爲了表非我並不同意，很難同意會議進行到此已經變成增加控制權的結論。台灣並非沒有資源，我覺得與其拿錢去反戰，不如拿來反恐(健保 IC 卡)。我們基本上是關心台灣人權，像是日據時代推行的身分證號碼，現在在日本推動就引起很大的反彈。下一代在成長，我不認爲應該維護既有政策，花奇怪的錢去做奇怪的事。個資法還有很多問題，利用職務之便可以取得很多東西。

我覺得討論到現在，健保 IC 卡已經是既定政策了，我覺得應該去想不做 IC 卡計劃的 financial cost 到底多少，我想台灣是可以承擔的。

主席：

我想基本上沒有在任何既定政策的基礎上來討論這個議題。並且不管 IC 卡是否用，以上討論到如何保護資料的隱私都是法律上必須要去做的。

台權會 莊紀婷：

我覺得台灣有一種 follow 國際的傾向，但是卻很少去聽反面的聲音，也很少去考慮 minimum necessary 的問題。法律部代表說的「全世界都在蒐集資料」，但是什麼國家代表全世界？又必要性何在？是爲了誰？難道沒有其他的 alternative，而必須要全民去 trade-off。在 98 年的菲律賓、99 年的匈牙利都宣佈對民國編碼是違憲的，日本身份證編碼也遭受強烈反彈。

我回應王蘋的話，維持第一階段。或者可以思考爲什麼要做，反面思考如果現在停止可以節省往後的 cost 多少？

法務部代表：

蒐集資料的目的在於建立資料，即使沒有個資法，爲了業務需要都有在蒐集資料。個資法規定是依照 OECD 揭示的原則規定，已達到最低的保護標準，保障合理的使用。我承認現在的個資法的確還有問題，執行上也有窒礙難行之處。我們也十分注重在特定目的外的資料利用問題。

殘障聯盟：

身心障礙手冊是我國獨有的，爲什麼一定要靠鑑定才能確認是否身心障礙，也許是爲了讓政府便於統計預算，但是歐美國家不用殘障手冊也能做好殘障服務，我的確承認資料是有蒐集的必要，但是如何決定、如何管理才是重點。

我認爲隱私並非政府規定的才是隱私，而是個人認爲不能公開的資料就是隱私，每個人想的是不同的。在考量時要住重當事人參與，只有當事人最知道何者有利、何者不利，要有 local 的組織、使用人參與討論才算完整。

主席：

這是有關於福利國家蒐集資料要到何程度、強制力爲何的問題，

人權本來就是少數人的問題。最終的意見可能在於當事人參與，立法保留是民意的展現，團體其實可以 lobby 行政機關要做好到什麼程度，像個資法就是授權過寬。

健保局江副總經理宏哲：

做管理的人都很喜歡去蒐集資料作 data analysis，目的在看 behavior pattern，看怎麼樣能對群體做最大貢獻、而非針對個人，但也衍生了對法律的需求。很謝謝能夠這麼平和友善地討論，健保局會再考量隱私權、自主權和控制權如何平衡的問題。

關於 financial cost/lost 的問題現在我一時無法回覆，因爲還牽涉了價值觀的考量，看拿來跟誰比、還有隱私權的問題。很感謝有這樣一個討論的平台，我們會記下意見回去再討論，要再強調，健保局是有提案但無定案，還有討論的彈性空間。

主席：

執行和不執行都有成本在，也牽涉價值觀的問題，這是決策者要負擔的政治治風險。今天的會議就討論到這個地方，各位如果有具體想法時歡迎反映，還有，這個研究計畫背後是沒有黑手的。

附錄三　期末報告座談會紀錄

「隱私權保障機制 ｜ 以健保 IC 卡計畫爲研究核心」期末報告(初稿)座談會議紀錄

時間：九十二年七月九日（星期三）上午九時三十分
地點：行政院研考會七樓簡報室
主席：紀副主任委員國鐘（宋處長餘俠代）
記錄：顧尙潔

出列席人員：
出席人員：中央研究院資訊科學研究所莊副研究員庭瑞、台北醫學大學醫學資訊研究所李所長有專(請假)、世新大學法律系王教授郁琦、慈濟基金會志業中心資訊處張主任顯洋、長庚大學醫務管理學系白教授裕彬、資訊工業策進會科技法律中心戴組長豪君、行政院人權保障推動小組黃委員文雄（請假）、顧委員立雄、蒙藏委員會汪參事平雲、法務部劉專門委員佐國、行政院衛生署陳專員昶榮、行政院衛生署中央健保局吳專門委員淑惠、張一等專員鈺旋
列席人員：中央大學劉副教授靜怡、中央研究院王副研究員大爲(請假)、何副處長全德(林高級分析師裕權代)、陳副處長悅宜、趙專門委員麗卿、吳科長秀貞、林專員康民

發言重點：

莊副研究員庭瑞：

本報告結論是否將提報行政院人權保障推動小組，將對健保 IC 卡之政策產生何種影響，宜請先加說明。

報告內容充實，尤其在比較法制方面資料的整理殊爲難得。惟第五章所提之結論與建議缺乏系統性，宜就建議的輕重緩急與時間點，將其區分爲立即可行及中長期可行兩大類，俾利政策規劃參考。

報告中仍有許多部分應予補強，如應先就當時之政策制定背景加以探討，列出其可能之政策目的，如降低行政成本、提昇醫療品質、提高整個社會的資訊能力，或者完全是政策的考量，再依個別之政策目的一一檢視是否能夠達成；又整體健保制度的機制是如何運作，是否合理？應該一併加以檢討，以明確責任之歸屬。

本報告第五章之建議三、「強化個資法規範之密度強度，儘速確立健保 IC 卡計畫的相關法律基礎」應就其內容再提出更爲具體可行的建議，例如是否應成立個人資料保護委員會？香港已經設有「個人隱私保護公署」，我國是否應參照辦理等。

王教授郁琦：

首先呼應莊教授之意見，希望看到這樣一個研究計畫對政策造成一定程度之影響，對報告的結論與建議基本上贊同。

健保 IC 卡的定位，應有很清楚的探討及交代，在法律層面上來說，如其定位不包括身分辨識之功能在內，則公務機關就不應該以其取代身分證；至於是否作爲商業用途部分，如果未作此規劃應該明確對外宣示及說明實際用途，以免留下想像空間，造成民間對此有所誤解。

本報告可就個資法，有關隱私權保障部分仍可加強的部分及政府對於醫療資訊處理應有的態度爲何等方向，加以探討，以作爲下次個資法修正或訂定特別法之參考。

有人舉 SARS 爲例，強調健保 IC 卡的迫切性及必要性，其實不應把 SARS 之處理當作常態，更不應把 SARS 那種緊急的狀況，當作未來醫療資料處理的標準，應該建立一個完整的機制，就緊急狀況與非緊急之一般狀況的處理方式，分別加以規範，方能兼顧民眾個人隱私權保障及緊急情況的需要。

張主任顯洋：

本報告在資料及文獻的蒐集都相當豐富完整，尤其是 HIPPA 之說明鉅細靡遺，值得作爲國內推動醫療資訊數位化及網路化之參考，而且分析方法亦相當中肯貼切，對健保 IC 卡推動過程中有關科技與隱私權之平衡，有助日後規劃及溝通之參考。

站在醫院的立場，較偏重技術面的考量。健保 IC 卡作爲醫療憑證，具有多卡合一的功能，惟不含身分辨識的功能，但是民眾仍可能用健保 IC 卡取代身分證，因爲健保 IC 卡較不容易遭僞造。

SARS 僅是實施健保 IC 卡制度的臨門一腳，並非其主要的考量，在宣傳上不應把健保 IC 卡制度未能實施，當作是 SARS 猖獗的主要原因。

在健保 IC 卡推動的第一階段，並無爭議，但進入第二階段以後爭議將隨之而來，雖然已設計相關配套措施如應配合醫事人員 IC 卡方能讀取資料等，但由於醫療資訊事涉敏感，以科技的角度來看，更需要有嚴謹的制度保障個人的隱密性資料。故以科技的角度來看，目前醫院的作法是將病人的資料批次上傳，未來健保 IC 卡制度將有利於醫療資訊的即時傳送及掌握，故應就資訊傳輸的及時性及批次性加以分析，來解讀健保 IC 卡制度的優缺點。整體醫療資訊保障機制規範的對象更不僅只於健保 IC 卡，而是應包含整個制度。

目前健保 IC 卡分三階段推動的方向基本上並沒有錯，但必須有良好的制度來保護民眾的隱私權，例如民眾可以自行決定是否要設置密碼，但亦應有「破窗」機制的設計，以應民眾發生路倒、急病等重大意外之緊急狀況時之需。這是整個醫療制度的問題，個人認爲不應單獨爲健保 IC 卡特別立法，而應將眼光放大放遠，就個人醫療資訊的保障訂定可長可久之特別法律。

有關商機的問題因爲事涉敏感，政府對此均避而不談，但民間對

此的興趣很高，建議本報告應對此一部分多加著墨，並列舉國內外的作法以供參考。

健保 IC 卡關於個人隱私權及個人資料保護，是醫療保障制度的整體性問題，除需依相關法規予規範外，對建置安全機制之技術及行政作業等，也要特別加強保護措施。本研究從不同構面探討，分析比較並提出建議，作爲相關單位針對數位化業務推動時之依據及參考，不但創造多贏，也可達成教育及提升資訊倫理的目的，以尊重個人隱私，確保民眾權益。

白教授裕彬：

對本報告第四十三頁提到以電子化方式管理資料可增進行政效率和降低醫療成本一節表示疑慮，且個人並不認爲由法制面處理是當務之急，法律應是解決問題的最後一道防線，在此之前，可以由體制面處理，以制（修）定行政措施方式可以達到相當或更好的效果，如德國二〇〇一年的國家醫療品質報告，已經將醫療提供者對病人隱私的保障列爲醫療品質評鑑的標準之一，我國也可以考慮仿傚，例如將對個人隱私的保障，列爲次年度公立醫院預算審核的重大參考指標之一，也可能有相當的效果。

顧委員立雄：

報告內容甚具啓發，亦肯定其價值。但錯別字稍多，內容也有重複的部分，可以再調整修正。

應該先確定健保 IC 卡設置的功能與政策目的，而本報告究竟是肯定或否定其目的，以下的討論才能夠繼續。

健保 IC 卡推動的第二階段，應優先納入緊急醫療所需之資訊，初步並應採取自願的方式，由民眾自行決定是否提供資訊，資訊的運用方比較沒有侵犯隱私權的顧慮。在此機制建立之前，不宜貿然推動第二階段。

未來健保 IC 卡與身分證之區別實益，可加以探討，健保 IC 卡之實施，如涉及個人資料問題，可參照個資法由健保局以訂定行政命令或施行細則方式處理，如涉及醫療資訊問題，可以修正「醫療法」方式處理，毋需訂定特別法。

汪參事平雲：

本報告是依據行政院人權保障小組委員會議結論辦理，首先要對劉教授及研考會表示謝意。

第四章與第五章的內容與架構可以再調整，第四章僅列舉缺失與問題，第五章則爲具體之建議，並依層次分爲健保 IC 卡本身的問題、健保 IC 卡衍生的問題及政府對隱私權保障的問題三層次分別提出建議；另依辦理時程分列，其中刻不容緩的問題如法源不足、採購契約的疏漏之處與補強，商業應用問題以及各機關間對資訊流通的隱私權保障機制等，應列爲最迫切優先的處理項目。

對於報告所提之缺失及具體建議，如資訊安全文件不夠公開透明，及應建立一個完善的醫療資訊保障機制，以解決目前的醫療資訊保護不足問題，而非把健保 IC 卡當作解決問題的萬靈丹等，衛生署及健保局應認真檢討辦理，並具體回應。

對於那些個人資訊應納入資訊保護的範圍，本報告應提出方向性、原則性及程序性之建議。

戴組長豪君：

個人參與國家資通安全會報，依該會報所訂之五級資通安全標準，健保 IC 卡應被列爲第一或第二級。資通會報所訂頒的規範雖非法律，但對於政府機關仍具有約束力，健保局在規劃推動健保 IC 卡制度時應予遵循，並要求廠商配合調整契約。另個資法之修正內容可納入報告第十一頁所提及之集體訴訟及建立健康醫療資訊安全港二種作法。

目前公務機關爲業務需要，常有相互來函要求調閱相關資料的情形，往往造成是否侵犯民眾隱私權的困擾，應有完善的機制加以規範。

報告第五十七頁中提到個資法中有許多不確定的法律概念，但如將這些不確定的部分都刪除，則對民眾隱私的保護往往不是擴大，而是進一步的縮減，建議應作個別的檢視後再作定奪。

報告第十九頁第七行「中研院資訊所同仁」之文字是否適當，請斟酌。

報告第二十二頁至第二十四頁中「此一」文字過多，建議酌作調整。

陳專員昶榮：

社會各界對健保 IC 卡意見很多，本署需調整步伐，廣納各界意見後再行出發。資訊倫理之教育與訓練是最根本的問題，在制度面方面，與東元公司的契約應再補強，在技術面方面，讀卡機的安全機制及民眾可自設密碼的權利，可對隱私權提供充分的保障，應爲對民眾宣傳的重點。

至於健保 IC 卡的法源依據問題，本署已於全民健康保險法修正草案中增訂第十六條之一加入相關法律保留規定，該修正草案目前在立法院審議中。

張一等專員鈺旋：

本研究報告分析透澈，精闢入理，架構完整，所提建議中肯，文中所引國外文獻及經驗，深值本局參考。

有關健保 IC 卡之法律基礎方面，依電腦處理個人資料保護法之規定，公務機關蒐集及利用個人資料必須基於法令職掌及法令規定之目的及範圍內爲之。準此，健保局依健保法及全民健康保險醫療辦法之規定於健保之目的規範內，製發健保 IC 卡，方便民眾就醫，並未逾越

法令之授權，於法尚無不合。依前開規定，健保 IC 卡的定位爲保險憑證，與身分證明不同，民眾如果誤解，健保局會加強宣導。另外，爲提升法律位階，有關保險憑證之法律依據，業已提出全民健康保險法修正草案，目前在立法院審議中。

有關健保 IC 卡建置計畫權利義務之規範方面，「健保 IC 卡建置計畫」契約明訂立約商及其主管、員工、顧問或承攬人應負保密義務；立約商及其供應廠商、協力廠商不得有任何損害健保局權益之行爲，並負連帶賠償責任；立約商若有將卡片非法外流、晶片設計規格公開或洩漏於外，致健保局受損、保險對象基本資料外流等情事之罰則。

有關資訊自主控制及落實隱私權之保護方面，健保 IC 卡之資料必須透過讀卡機才能讀出，且涉及個人隱私之資料可以透過 Pin Code 之方式予以保護，個人隱私資料之讀取已採取必要之防護與尊重當事人之資訊自主權，至於資料到底要放到何種範圍，日後仍有許多可討論之空間。

在資訊稽核制度之建立方面，健保局目前擁有非常龐大之資料庫，健保局內部基於資訊安全之考量，本已建立安全控管機制，限於業務相關人員依授權帳號及密碼始得查閱或處理資料。除此以外，各單位每年度辦理二次自行查核，稽核部門也會針對資訊安全部分辦理專案稽核及年度稽核。另有關資訊安全文件，健保局亦將即刻補強，並適度公開。

資訊安全之防護措施方面，健保局會依循國家資通安全會報相關規範及期程規劃，完成資通安全的防護措施及驗證工作。

其他修正意見：

第六頁「健保 IC 卡系統乃是由承包商負責營運，在營運過程中...」此段文字與事實不符，建請修正爲「健保 IC 卡系統乃是由承包商負責開發建置，在其過程中...」。

第六十一頁有關契約保證事項僅列晶片部分，對於整體之規範並未提及，「健保 IC 卡建置計畫」契約第一・六條明訂立約商及其主管、員工、顧問或承攬人應負保密義務；第一・七條規定立約商及其供應廠商、協力廠商不得有任何損害健保局權益之行爲，並負連帶賠償責任；又第十一條則規範立約商若有將卡片非法外流、晶片設計規格公開或洩漏於外，致健保局受損、保險對象基本資料外流等情事之罰則。建請應予說明。

第八十七頁稱健保 IC 內資料有地址，與事實不符，建請刪除。

劉專門委員佐國：

聯合徵信中心及健保局是目前國內兩大資料中心。個資法對個人資料保護的強度及密度都不足，例如對醫療資料的保護，適用對象僅對有病床之醫療院所，其他診所均不適用，未來修法時將刪除行業別的限制。

據瞭解，現階段健保 IC 卡的相關規定，尚均符合現行個資法之規定。對於強化健保 IC 卡的管理及醫療資訊的保護，法務部贊成訂定法律，由法律明確授權，並提升規範的密度及強度。但個資法爲一般法而非特別法，並非針對醫療資訊的保護而定，醫療資訊屬特種資料個資法修正案已明確規定除有法律授權外，不准進行特種資料的蒐集，建議主管機關衛生署就醫療資料蒐集的要件、程度及標準，訂定子法或行政規劃加以規範，並應納入稽核制度的建立及倫理教育，以及資料外洩之追懲制度，查明資料外洩之源頭、內容及管道。

第五十七頁附註所稱個資法於立法院審議中，請修正爲刻正於法務部修正中，以符實際。

莊副研究員庭瑞：

健保局與東元電機公司間之契約義務將於本（九十二）年八月十一日結束，惟健保局仍應依中央信託局所訂之政府採購合約內容規

範，針對系統細節及完全防護機制之建立，以及個人資料跨國移轉之問題，進行契約內容之補強並要求東元電機公司遵守。

據聯合報載，健保局個人資料外洩事件，迄今仍不知是由何人循何管道流出，顯示個人資料的保護機制有問題；日前亦傳出警政機關去函健保局要求提供嫌犯個人保險資料之事情，亦顯現出機關間資料互相流通缺乏明確規範的問題。

對於健保 IC 卡其他商業用途如是否可作爲大樓門禁管制及俱樂部會員身分識別之用等，亦應有明確之規範。

行政院研考會：

本報告係就推動中的健保 IC 卡制度進行檢視，爲探討建立我國隱私權保障機制之重點案例，惟就研究結論及建議，是否考量將研究報告名稱酌作修正爲「隱私權保障機制 ｜ 以健保 IC 卡計畫爲例」，更爲貼切。

第四章有關現行健保 IC 卡制度應予修正改進之處，建議就其輕重緩急加以區分爲立即可行及中長期之建議，並於第五章中一併歸納整理。下列意見併請參考：

有關建議衛生署及健保局應要求相關機構就資訊蒐集及處理事務建立自我審查機制一節，可進一步探討係何法律授權方可要求相關機構遵照辦理？如考量現行法律未有相關規定，短期內有無立即可行且足資因應之措施？

有關建立不同機關及機構間資訊流用之限制規定及相關程序一節，可進一步探討係依何法律規定辦理，又有何具體措施或制度以爲因應？在制定該措施或制度時，應遵循那些原則。

有關建議建立正式的外部審核機制，以解決目前個人資料保護爭

議事件以訴諸司法機關爲惟一解決途徑一節，請就該審核機制之組織設計、性質、層級及功能型態等提出更具體之建議。

第五章結論與建議中提出八項結論與建議，惟其中包括觀念的澄清與再教育、宣導方向及策略調整、技術層面建議及具體的行動方案等，建議依其性質予以適當之區分，建議事項分爲「立即可行建議」及「中長期建議」兩類，並明列各項建議之主辦及協辦機關，俾利參考遵循。

政策推動的成敗關鍵，往往在社會各界共識的取得。報告中曾多次指出，民間團體及民眾之所以反對健保 IC 卡制度的原因，主要仍在政策制定過程缺乏參與及溝通，以及誤認政府政策已定，僅在事後要求其配合所致。健保局目前所規劃之所謂第一階段「輔導期」、第二階段「適應期」及第三階段「穩定發展期」，亦應配合前述原則酌予調整，以避免給予民眾政策已定不容調整的誤解，造成溝通時的困難。

報告內若干個案之比較，如台灣、法國、德國及美國之健保體制與憑證制度之對照，建議增列比較表，將其制度精神、背景、具體作法及優缺點分析等以表格方式呈現，其他如各國隱私保障相關法律及機制之比較等亦同，俾利一目瞭然。

本案第二、三階段的資料儲存項目及應用，應回歸個人資料保護法及既定政策來探討，個資法精神爲涉及人民隱私者，應先徵得人民的意識表達，獲得同意之下才能進行，健保 IC 卡只是載具，安全機制、隱私權的保障仍是由主管機關規劃設計，因此，建議儘速進行個人意識表達及資料安全機制的相關設計，並落實執行，以根除大眾的疑慮。

與民間團體溝通過程中的相關問題及答復應一一紀錄，發展知識管理，分析彙整重要訊息，作爲下一個類似專案成案前提供主管機關或其他機關參考；或作爲本案對社會大眾宣導、客服中心使用的基礎。

本報告之內容、撰寫方式及印製格式請參照「行政院研究發展考核委員會專案研究作業要點」第十四條規定辦理。

主席結論：

請計畫主持人參酌與會人士意見修正期末報告後送本會。本會將整理報告結論及建議，提報預訂本年八月召開之行政院人權保障推動小組第九次委員會議報告，並請各主管機關預先研擬回應及說明。

散會：中午十二時

附錄四　Health Insurance Portability and Accountability Act of 1996

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.--This Act may be cited as the "Health Insurance Portability and Accountability Act of 1996".

(b) TABLE OF CONTENTS.--The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I--HEALTH CARE ACCESS, PORTABILITY, AND RENEWABILITY

...

TITLE II--PREVENTING HEALTH CARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM

...

Subtitle F--Administrative Simplification

- Sec. 261. Purpose.
- Sec. 262. Administrative simplification.

"Part C--Administrative Simplification

- "Sec. 1171. Definitions.
- "Sec. 1172. General requirements for adoption of standards.
- "Sec. 1173. Standards for information transactions and data elements.
- "Sec. 1174. Timetables for adoption of standards.
- "Sec. 1175. Requirements.
- "Sec. 1176. General penalty for failure to comply with requirements and standards.
- "Sec. 1177. Wrongful disclosure of individually identifiable health information.
- "Sec. 1178. Effect on State law.
- "Sec. 1179. Processing payment transactions.".

Sec. 263. Changes in membership and duties of National Committee on Vital and Health Statistics.

Sec. 264. Recommendations with respect to privacy of certain health information.

...

Subtitle F--Administrative Simplification

SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 262. ADMINISTRATIVE SIMPLIFICATION.

(a) IN GENERAL.--Title XI (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

"PART C--ADMINISTRATIVE SIMPLIFICATION

"DEFINITIONS

"SEC. 1171. For purposes of this part:

"(1) CODE SET.--The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

"(2) HEALTH CARE CLEARINGHOUSE.--The term 'health care clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

"(3) HEALTH CARE PROVIDER.--The term 'health care provider' includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing health care services or supplies.

"(4) HEALTH INFORMATION.--The term 'health information' means any information, whether oral or recorded in any form or medium, that--

"(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

"(5) HEALTH PLAN.--The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

"(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan--

"(i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or

"(ii) is administered by an entity other than the employer who established and maintains the plan.

"(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

"(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

"(D) Part A or part B of the Medicare program under title XVIII.

"(E) The medicaid program under title XIX.

"(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

"(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

"(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

"(I) The health care program for active military personnel under title 10, United States Code.

"(J) The veterans health care program under chapter 17 of title 38, United States Code.

"(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10, United States Code.

"(L) The Indian health service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

"(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5, United States Code.

"(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that--

"(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--

"(i) identifies the individual; or

"(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

"(7) STANDARD.--The term 'standard', when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.

"(8) STANDARD SETTING ORGANIZATION.--The term 'standard setting organization' means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information

transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

"GENERAL REQUIREMENTS FOR ADOPTION OF STANDARDS

"SEC. 1172. (a) APPLICABILITY.--Any standard adopted under this part shall apply, in whole or in part, to the following persons:

"(1) A health plan.

"(2) A health care clearinghouse.

"(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

"(b) REDUCTION OF COSTS.--Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.

"(c) ROLE OF STANDARD SETTING ORGANIZATIONS.--

"(1) IN GENERAL.--Except as provided in paragraph (2), any standard adopted under this part shall be a standard that has been developed, adopted, or modified by a standard setting organization.

"(2) SPECIAL RULES.--

"(A) DIFFERENT STANDARDS.--The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if--

"(i) the different standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives; and

"(ii) the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, United States Code.

"(B) NO STANDARD BY STANDARD SETTING ORGANIZATION.--If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part--

"(i) paragraph (1) shall not apply; and

"(ii) subsection (f) shall apply.

(3) CONSULTATION REQUIREMENT.--

"(A) IN GENERAL.--A standard may not be adopted under this part unless--

"(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and

"(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f), consulted with each of the organizations described in subparagraph (B) before adopting the standard.

"(B) ORGANIZATIONS DESCRIBED.--The organizations referred to in subparagraph (A) are the following:

"(i) The National Uniform Billing Committee.

"(ii) The National Uniform Claim Committee.

"(iii) The Workgroup for Electronic Data Interchange.

"(iv) The American Dental Association.

"(d) IMPLEMENTATION SPECIFICATIONS.--The Secretary shall establish specifications for implementing each of the standards adopted under this part.

"(e) PROTECTION OF TRADE SECRETS.--Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

"(f) ASSISTANCE TO THE SECRETARY.--In complying with the requirements of this part, the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

(g) APPLICATION TO MODIFICATIONS OF STANDARDS.--This section shall apply to a modification to a standard (including an addition to a standard) adopted under section 1174(b) in the same manner as it applies to an initial standard adopted under section 1174(a).

"STANDARDS FOR INFORMATION TRANSACTIONS AND DATA ELEMENTS

"SEC. 1173. (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.--

"(1) IN GENERAL.--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

"(A) the financial and administrative transactions described in paragraph (2); and

"(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

"(2) TRANSACTIONS.--The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

"(A) Health claims or equivalent encounter information.

"(B) Health claims attachments.

"(C) Enrollment and disenrollment in a health plan.

"(D) Eligibility for a health plan.

"(E) Health care payment and remittance advice.

"(F) Health plan premium payments.

"(G) First report of injury.

"(H) Health claim status.

"(I) Referral certification and authorization.

"(3) ACCOMMODATION OF SPECIFIC PROVIDERS.--The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

(b) UNIQUE HEALTH IDENTIFIERS.--

"(1) IN GENERAL.--The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

"(2) USE OF IDENTIFIERS.--The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

(c) CODE SETS.--

"(1) IN GENERAL.--The Secretary shall adopt standards that--

"(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

"(B) establish code sets for such data elements if no code sets for the data elements have been developed.

"(2) DISTRIBUTION.--The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

(d) SECURITY STANDARDS FOR HEALTH INFORMATION.--

"(1) SECURITY STANDARDS.--The Secretary shall adopt security standards that--

"(A) take into account--

"(i) the technical capabilities of record systems used to maintain health information;

"(ii) the costs of security measures;

"(iii) the need for training persons who have access to health information;

"(iv) the value of audit trails in computerized record systems; and

"(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and

"(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

"(2) SAFEGUARDS.--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--

"(A) to ensure the integrity and confidentiality of the information;

"(B) to protect against any reasonably anticipated--

"(i) threats or hazards to the security or integrity of the information; and

"(ii) unauthorized uses or disclosures of the information; and

"(C) otherwise to ensure compliance with this part by the officers and employees of such person.

(e) ELECTRONIC SIGNATURE.--

"(1) STANDARDS.--The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).

"(2) EFFECT OF COMPLIANCE.--Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

(f) TRANSFER OF INFORMATION AMONG HEALTH PLANS.--The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

"TIMETABLES FOR ADOPTION OF STANDARDS

"SEC. 1174. (a) INITIAL STANDARDS.--The Secretary shall carry out section 1173 not later than 18 months after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, except that standards relating to claims attachments shall be adopted not later than 30 months after such date.

"(b) ADDITIONS AND MODIFICATIONS TO STANDARDS.--

"(1) IN GENERAL.--Except as provided in paragraph (2), the Secretary shall review the standards adopted under section 1173, and shall adopt modifications to the standards (including additions to the standards), as determined appropriate, but not more frequently than once every 12 months. Any addition or modification to a standard shall be completed in a manner which minimizes the disruption and cost of compliance.

"(2) SPECIAL RULES.--

"(A) FIRST 12-MONTH PERIOD.--Except with respect to additions and modifications to code sets under subparagraph (B), the Secretary may not adopt any modification to a standard adopted under this part during the 12-month period beginning on the date the standard is initially adopted, unless the Secretary determines that the modification is necessary in order to permit compliance with the standard.

"(B) ADDITIONS AND MODIFICATIONS TO CODE SETS.--

"(i) IN GENERAL.--The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets.

"(ii) Additional rules.--If a code set is modified under this subsection, the modified code set shall include instructions on how data elements of health information that were encoded prior to the modification may be converted or translated so as to preserve the informational value of the data elements that existed before the modification. Any modification to a code set under this subsection shall be implemented in a manner that minimizes the disruption and cost of complying with such modification.

"REQUIREMENTS

"SEC. 1175. (a) CONDUCT OF TRANSACTIONS BY PLANS.--

"(1) IN GENERAL.--If a person desires to conduct a transaction referred to in section 1173(a)(1) with a health plan as a standard transaction--

"(A) the health plan may not refuse to conduct such transaction as a standard transaction;

"(B) the insurance plan may not delay such transaction, or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the ground that the transaction is a standard transaction; and

"(C) the information transmitted and received in connection with the transaction shall be in the form of standard data elements of health information.

"(2) SATISFACTION OF REQUIREMENTS.--A health plan may satisfy the requirements under paragraph (1) by--

"(A) directly transmitting and receiving standard data elements of health information; or

"(B) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse, and receiving standard data elements through the health care clearinghouse.

"(3) TIMETABLE FOR COMPLIANCE.--Paragraph (1) shall not be construed to require a health plan to comply with any standard, implementation specification, or modification to a standard or specification adopted or established by the Secretary under sections 1172 through 1174 at any time prior to the date on which the plan is required to comply with the standard or specification under subsection (b).

"(b) COMPLIANCE WITH STANDARDS.--

"(1) INITIAL COMPLIANCE.--

"(A) IN GENERAL.--Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1172 and 1173, each person to whom the standard or implementation specification applies shall comply with the standard or specification.

"(B) SPECIAL RULE FOR SMALL HEALTH PLANS.--In the case of a small health plan, paragraph (1) shall be applied by substituting '36 months' for '24 months'. For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

"(2) COMPLIANCE WITH MODIFIED STANDARDS.--If the Secretary adopts a modification to a standard or implementation specification under this part, each person to whom the standard or implementation specification applies shall comply with the modified standard or implementation specification at such time as the Secretary determines appropriate, taking into account the time needed to comply due to the nature and extent of the modification. The time determined appropriate under the preceding sentence may not be earlier than the last day of the 180-day period beginning on the date such modification is adopted. The Secretary may extend the time for compliance for small health plans, if the Secretary determines that such extension is appropriate.

"(3) CONSTRUCTION.--Nothing in this subsection shall be construed to prohibit any person from complying with a standard or specification by--

"(A) submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse; or

"(B) receiving standard data elements through a health care clearinghouse.

"GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS

"SEC. 1176. (a) GENERAL PENALTY.--

"(1) IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

"(2) PROCEDURES.--The provisions of section 1128A (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1128A.

"(b) LIMITATIONS.--

"(1) OFFENSES OTHERWISE PUNISHABLE.--A penalty may not be imposed under subsection (a) with respect to an act if the act constitutes an offense punishable under section 1177.

"(2) NONCOMPLIANCE NOT DISCOVERED.--A penalty may not be imposed under subsection (a) with respect to a provision of this part if it is established to the satisfaction of the Secretary that the person liable for the

penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.

"(3) FAILURES DUE TO REASONABLE CAUSE.--

"(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) if--

"(i) the failure to comply was due to reasonable cause and not to willful neglect; and

"(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

"(B) EXTENSION OF PERIOD.--

"(i) NO PENALTY.--The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.

"(ii) ASSISTANCE.--If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the period described in subparagraph (A)(ii). Such assistance shall be provided in any manner determined appropriate by the Secretary.

"(4) REDUCTION.--In the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) that is not entirely waived under paragraph (3) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

"WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

"SEC. 1177. (a) OFFENSE.--A person who knowingly and in violation of this part--

"(1) uses or causes to be used a unique health identifier;

"(2) obtains individually identifiable health information relating to an individual; or

"(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b).

"(b) PENALTIES.--A person described in subsection (a) shall--

"(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

"(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

"(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

"EFFECT ON STATE LAW

"SEC. 1178. (a) GENERAL EFFECT.--

"(1) GENERAL RULE.--Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

"(2) EXCEPTIONS.--A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall not supersede a contrary provision of State law, if the provision of State law--

"(A) is a provision the Secretary determines--

"(i) is necessary--

"(I) to prevent fraud and abuse;

"(II) to ensure appropriate State regulation of insurance and health plans;

"(III) for State reporting on health care delivery or costs; or

"(IV) for other purposes; or

"(ii) addresses controlled substances; or

"(B) subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

"(b) PUBLIC HEALTH.--Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law

providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

"(c) STATE REGULATORY REPORTING.--Nothing in this part shall limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

"PROCESSING PAYMENT TRANSACTIONS BY FINANCIAL INSTITUTIONS

"SEC. 1179. To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing,

transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

"(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

"(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1)--

"(A) for transferring receivables;

"(B) for auditing;

"(C) in connection with--

"(i) a customer dispute; or

"(ii) an inquiry from, or to, a customer;

"(D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer;

"(E) for reporting to consumer reporting agencies; or

"(F) for complying with--

"(i) a civil or criminal subpoena; or

"(ii) a Federal or State law regulating the entity.".

(b) CONFORMING AMENDMENTS.--

(1) REQUIREMENT FOR MEDICARE PROVIDERS.--Section 1866(a)(1) (42 U.S.C. 1395cc(a)(1)) is amended--

(A) by striking ``and" at the end of subparagraph (P);

(B) by striking the period at the end of subparagraph (Q) and inserting "; and"; and

(C) by inserting immediately after subparagraph (Q) the following new subparagraph:

"(R) to contract only with a health care clearinghouse (as defined in section 1171) that meets each standard and implementation specification adopted or

established under part C of title XI on or after the date on which the health care clearinghouse is required to comply with the standard or specification.".

(2) TITLE HEADING.--Title XI (42 U.S.C. 1301 et seq.) is amended by striking the title heading and inserting the following:

"TITLE XI--GENERAL PROVISIONS, PEER REVIEW, AND ADMINISTRATIVE SIMPLIFICATION".

SEC. 263. CHANGES IN MEMBERSHIP AND DUTIES OF NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS.

Section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k))

is amended--

(1) in paragraph (1), by striking "16" and inserting "18";

(2) by amending paragraph (2) to read as follows:

"(2) The members of the Committee shall be appointed from among persons who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Members of the Committee shall be appointed for terms of 4 years.";

(3) by redesignating paragraphs (3) through (5) as paragraphs (4) through (6), respectively, and inserting after paragraph (2) the following:

"(3) Of the members of the Committee--

"(A) 1 shall be appointed, not later than 60 days after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, by the Speaker of the House of Representatives after consultation with the Minority Leader of the House of Representatives;

"(B) 1 shall be appointed, not later than 60 days after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, by the President pro tempore of the Senate after consultation with the Minority Leader of the Senate; and

"(C) 16 shall be appointed by the Secretary.";

(4) by amending paragraph (5) (as so redesignated) to read as follows:

"(5) The Committee--

"(A) shall assist and advise the Secretary--

"(i) to delineate statistical problems bearing on health and health services which are of national or international interest;

"(ii) to stimulate studies of such problems by other organizations and agencies whenever possible or to make investigations of such problems through subcommittees;

"(iii) to determine, approve, and revise the terms, definitions, classifications, and guidelines for assessing health status and health services, their distribution and costs, for use (I) within the Department of Health and Human Services, (II) by all programs administered or funded by the Secretary, including the Federal-State-local cooperative health statistics system referred to in subsection (e), and (III) to the extent possible as determined by the head of the agency involved, by the Department of

Veterans Affairs, the Department of Defense, and other Federal agencies concerned with health and health services;

"(iv) with respect to the design of and approval of health statistical and health information systems concerned with the collection, processing, and tabulation of health statistics within the Department of Health and Human Services, with respect to the Cooperative Health Statistics System established under subsection (e), and with respect to the standardized means for the collection of health information and statistics to be established by the Secretary under subsection (j)(1);

"(v) to review and comment on findings and proposals developed by other organizations and agencies and to make recommendations for their adoption or implementation by local, State, national, or international agencies;

"(vi) to cooperate with national committees of other countries and with the World Health Organization and other national agencies in the studies of problems of mutual interest;

"(vii) to issue an annual report on the state of the Nation's health, its health services, their costs and distributions, and to make proposals for improvement of the Nation's health statistics and health information systems; and

"(viii) in complying with the requirements imposed on the Secretary under part C of title XI of the Social Security Act;

"(B) shall study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information;

"(C) shall report to the Secretary not later than 4 years after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996 recommendations and legislative proposals for such standards and electronic exchange; and

"(D) shall be responsible generally for advising the Secretary and the Congress on the status of the implementation of part C of title XI of the Social Security Act."; and

(5) by adding at the end the following:

"(7) Not later than 1 year after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, and annually thereafter, the Committee shall submit to the Congress, and make public, a report regarding the implementation of part C of title XI of the Social Security Act. Such report shall address the following subjects, to the extent that the Committee determines appropriate:

"(A) The extent to which persons required to comply with part C of title XI of the Social Security Act are cooperating in implementing the standards adopted under such part.

"(B) The extent to which such entities are meeting the security standards adopted under such part and the types of penalties assessed for noncompliance with such standards.

"(C) Whether the Federal and State Governments are receiving information of sufficient quality to meet their responsibilities under such part.

"(D) Any problems that exist with respect to implementation of such part.

"(E) The extent to which timetables under such part are being met.".

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) IN GENERAL.--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) SUBJECTS FOR RECOMMENDATIONS.--The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.--

(1) IN GENERAL.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the

enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

(2) PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

(d) CONSULTATION.--In carrying out this section, the Secretary of Health and Human Services shall consult with--

(1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and

(2) the Attorney General.

附錄五　Standards for Privacy of Individually Identifiable Health Information

Standards for Privacy of Individually Identifiable Health Information

For the reasons set forth in the preamble, 45 CFR Subtitle A, Subchapter C, is amended as follows:

1. Part 160 is revised to read as follows:

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A – General Provisions

160.101 Statutory basis and purpose.

160.102 Applicability.

160.103 Definitions.

160.104 Modifications.

Subpart B – Preemption of State Law

160.201Applicability.

160.202Definitions.

160.203General rule and exceptions.

160.204Process for requesting exception determinations.

160.205Duration of effectiveness of exception determinations.

Subpart C – Compliance and Enforcement

160.300Applicability.

160.302Definitions.

160.304Principles for achieving compliance.

160.306Complaints to the Secretary.

160.308Compliance reviews.

160.310Responsibilities of covered entities.

160.312Secretarial action regarding complaints and compliance reviews.

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d-1329d-8) as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031 and sec. 264 of Pub. L. 104-191 (42 U.S.C. 1320d-2(note)).

Subpart A - General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, and section 264 of Public Law 104-191.

§ 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) To the extent required under section 201(a)(5) of the Health Insurance Portability Act of 1996, (Pub. L. 104-191), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists

in the performance of:
(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
(B) Any other function or activity regulated by this subchapter; or
(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
(3) A covered entity may be a business associate of another covered entity.
Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.
Covered entity means:

(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.
HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.
HHS stands for the Department of Health and Human Services.
Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:
(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management

information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of

health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(vii) An issuer of a long-term care policy, excluding a nursing home fixed- indemnity policy.

(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(ix) The health care program for active military personnel under title 10 of the United States Code.

(x) The veterans health care program under 38 U.S.C. chapter 17.

(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
(2) *Health plan* excludes:
(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
(ii) A government-funded program (other than one listed in paragraph (1)(i)- (xvi)of this definition):
(A) Whose principal purpose is other than providing, or paying the cost of, health care; or
(B) Whose principal activity is:
(*1*) The direct provision of health care to persons; or
(*2*) The making of grants to fund the direct provision of health care to persons.
Implementation specification means specific requirements or instructions for implementing a standard.
Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.
Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Small health plan means a health plan with annual receipts of $5 million

or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:

(i) Classification of components.

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of individually identifiable health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation.
Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
§ 160.104 Modifications.
(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.
(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.
(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.
(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.
(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B - Preemption of State Law_

§160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104-191.

§ 160.202 Definitions.

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity would find it impossible to comply with both the State and federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of

individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting *in loco parentis* of such minor.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the

provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:
(1) The State law for which the exception is requested;
(2) The particular standard, requirement, or implementation specification for which the exception is requested;
(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
(4) How health care providers, health plans, and other entities would be affected by the exception;
(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and
(6) Any other information the Secretary may request in order to make the determination.
(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.
§ 160.205 Duration of effectiveness of exception determinations.
An exception granted under this subpart remains in effect until:
(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or
(b) The Secretary revokes the exception, based on a determination that

the ground supporting the need for the exception no longer exists.

Subpart C - Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.

(a) Cooperation. The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) Assistance. The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.

(a) Right to file a complaint. A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.

(b) Requirements for filing complaints. Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.
(c) Investigation. The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.
§ 160.308 Compliance reviews.
The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
§ 160.310 Responsibilities of covered entities.
(a) Provide records and compliance reports. A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(b) Cooperate with complaint investigations and compliance reviews. A

covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(c) Permit access to information. (1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) Resolution where noncompliance is indicated. (1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308

indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.

(b) Resolution when no violation is found. If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

2. A new Part 164 is added to read as follows:

PART 164 – SECURITY AND PRIVACY

Subpart A – General Provisions

Sec.

164.102 Statutory basis.

164.104 Applicability.

164.106 Relationship to other parts.

Subparts B-D – [Reserved]

Subpart E – Privacy of Individually Identifiable Health Information

164.500 Applicability.

164.501 Definitions.

164.502 Uses and disclosures of protected health information: general rules.

164.504 Uses and disclosures: organizational requirements.

164.506 Consent for uses or disclosures to carry out treatment, payment, and health care operations

164.508 Uses and disclosures for which an authorization is required.

164.510 Uses and disclosures requiring an opportunity for the individual

to agree or to object.
164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.
164.514 Other requirements relating to uses and disclosures of protected health information.
164.520 Notice of privacy practices for protected health information.
164.522 Rights to request privacy protection for protected health information.
164.524 Access of individuals to protected health information.
164.526 Amendment of protected health information.
164.528 Accounting of disclosures of protected health information.
164.530 Administrative requirements.
164.532 Transition requirements.
164.534 Compliance dates for initial implementation of the privacy standards.
Authority: 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. 104-191, 110 Stat. 2033- 2034(42 U.S.C. 1320(d-2(note)).

Subpart A--General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation standards under part C of title XI of the Act and section 264 of Public Law 104-191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are

required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B-D--[Reserved]

Subpart E - Privacy of Individually Identifiable Health Information_

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which consent, individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial

implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non- governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:
(1) A group of records maintained by or for a covered entity that is:
(i) The medical records and billing records about individuals maintained by or for a covered health care provider;
(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.
Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:
(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of health care

professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a

covered entity or, following completion of the sale or transfer, will become a covered entity; and

(v) Consistent with the applicable requirements of § 164.514, creating de- identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

(1) *Marketing* does not include communications that meet the requirements of paragraph (2) of this definition and that are made by a covered entity:

(i) For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or

(ii) That are tailored to the circumstances of a particular individual and the communications are:

(A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the

treatment of that individual; or
(B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.
(2) A communication described in paragraph (1) of this definition is not included in marketing if:
(i) The communication is made orally; or
(ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.
Organized health care arrangement means:
(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the

sharing of financial risk.
(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.
Payment means:
(1) The activities undertaken by:
(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
(ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and

excess of loss insurance), and related health care data processing;
(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider and/or health plan.
Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).
Protected health information means individually identifiable health information:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or
(iii) Transmitted or maintained in any other form or medium.
(2) *Protected health information* excludes individually identifiable health information in:
(i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and
(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).
Psychotherapy notes means notes recorded (in any medium) by a health

care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) Pursuant to and in compliance with a consent that complies with § 164.506, to carry out treatment, payment, or health care operations;

(iii) Without consent, if consent is not required under § 164.506(a) and has not been sought under § 164.506(a)(4), to carry out treatment, payment, or health care operations, except with respect to psychotherapy notes;

(iv) Pursuant to and in compliance with an authorization that complies with § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), and (g).

(2) Required disclosures. A covered entity is required to disclose

protected health information:
(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and
(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.
(b) Standard: minimum necessary. (1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
(2) Minimum necessary does not apply. This requirement does not apply to:
(i) Disclosures to or requests by a health care provider for treatment;
(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section, as required by paragraph (a)(2)(i) of this section, or pursuant to an authorization under § 164.508, except for authorizations requested by the covered entity under § 164.508(d), (e), or (f);
(iii) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
(iv) Uses or disclosures that are required by law, as described by § 164.512(a); and
(v) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.
(c) Standard: uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) Standard: uses and disclosures of de-identified protected health information.

(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) Standard: disclosures to business associates. (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan

sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).

(2) Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) Standard: deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.

(g)(1) Standard: personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions

related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3) Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) Implementation specification: deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) Implementation specification: abuse, neglect, endangerment

situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) Standard: confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) Standard: uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) Standard: disclosures by whistleblowers and workforce member crime victims.

(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care,

services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
(ii) The disclosure is to:
(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.
(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:
(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and
(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).
§ 164.504 Uses and disclosures: organizational requirements.
(a) Definitions. As used in this section:
Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.
Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.
Health care component has the following meaning:
(1) Components of a covered entity that perform covered functions are part of the health care component.

(2) Another component of the covered entity is part of the entity's health care component to the extent that:
(i) It performs, with respect to a component that performs covered functions, activities that would make such other component a business associate of the component that performs covered functions if the two components were separate legal entities; and
(ii) The activities involve the use or disclosure of protected health information that such other component creates or receives from or on behalf of the component that performs covered functions.
Hybrid entity means a single legal entity that is a covered entity and whose covered functions are not its primary functions.
Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.
Summary health information means information, that may be individually identifiable health information, and:
(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and
(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.
(b) Standard: health care component. If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.
(c)(1) Implementation specification: application of other provisions. In applying a provision of this subpart, other than this section, to a hybrid entity:

(i) A reference in such provision to a "covered entity" refers to a health care component of the covered entity;
(ii) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse" refers to a health care component of the covered entity if such health care component performs the functions of a health plan, covered health care provider, or health care clearinghouse, as applicable; and
(iii) A reference in such provision to "protected health information" refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.
(2) Implementation specifications: safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:
(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;
(ii) A component that is described by paragraph (2)(i) of the definition of *health care component* in this section does not use or disclose protected health information that is within paragraph (2)(ii) of such definition for purposes of its activities other than those described by paragraph (2)(i) of such definition in a way prohibited by this subpart; and
(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this

subpart.

(3) Implementation specifications: responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities:

(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.

(ii) The covered entity has the responsibility for complying with § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j).

(d)(1) Standard: affiliated covered entities. Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.

(2) Implementation specifications: requirements for designation of an affiliated covered entity. (i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.

(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).

(3) Implementation specifications: safeguard requirements. An affiliated covered entity must ensure that:

(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and

(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.

(e)(1) Standard: business associate contracts. (i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.
(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
(A) Terminated the contract or arrangement, if feasible; or
(B) If termination is not feasible, reported the problem to the Secretary.
(2) Implementation specifications: business associate contracts. A contract between the covered entity and a business associate must:
(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:
(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and
(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
(ii) Provide that the business associate will:
(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
(B) Use appropriate safeguards to prevent use or disclosure of the

information other than as provided for by its contract;
(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
(E) Make available protected health information in accordance with § 164.524;
(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;
(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;
(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) Implementation specifications: other arrangements. (i) If a covered entity and its business associate are both governmental entities:
(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.
(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.
(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.
(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.
(4) Implementation specifications: other requirements for contracts and other arrangements. (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:
(A) For the proper management and administration of the business

associate; or
(B) To carry out the legal responsibilities of the business associate.
(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:
(A) The disclosure is required by law; or
(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
(f)(1)Standard: requirements for group health plans. (i) Except as provided under paragraph (f)(1)(ii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and discloses of such information by the plan sponsor consistent with the requirements of this subpart.
(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :
(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or
(B) Modifying, amending, or terminating the group health plan.

(2) Implementation specifications: requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health

plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) Implementation specifications: uses and disclosures. A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only

consistent with the provisions of paragraph (f)(2) of this section;
(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;
(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and
(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.
(g) Standard: requirements for a covered entity with multiple covered functions.
(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.
(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.
§ 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations.
(a) Standard: consent requirement. (1) Except as provided in paragraph (a)(2) or (a)(3) of this section, a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.
(2) A covered health care provider may, without consent, use or disclose

protected health information to carry out treatment, payment, or health care operations, if:
(i) The covered health care provider has an indirect treatment relationship with the individual; or
(ii) The covered health care provider created or received the protected health information in the course of providing health care to an individual who is an inmate.
(3)(i) A covered health care provider may, without prior consent, use or disclose protected health information created or received under paragraph (a)(3)(i)(A)-(C) of this section to carry out treatment, payment, or health care operations:
(A) In emergency treatment situations, if the covered health care provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;
(B) If the covered health care provider is required by law to treat the individual, and the covered health care provider attempts to obtain such consent but is unable to obtain such consent; or
(C) If a covered health care provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.
(ii) A covered health care provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.
(4) If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to carry out treatment, payment, or health care operations, provided that such consent meets the requirements of this section.

(5) Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information.
(b) Implementation specifications: general requirements. (1) A covered health care provider may condition treatment on the provision by the individual of a consent under this section.
(2) A health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment.
(3) A consent under this section may not be combined in a single document with the notice required by § 164.520.
(4)(i) A consent for use or disclosure may be combined with other types of written legal permission from the individual (e.g., an informed consent for treatment or a consent to assignment of benefits), if the consent under this section:
(A) Is visually and organizationally separate from such other written legal permission; and
(B) Is separately signed by the individual and dated.
(ii) A consent for use or disclosure may be combined with a research authorization under § 164.508(f).
(5) An individual may revoke a consent under this section at any time, except to the extent that the covered entity has taken action in reliance thereon. Such revocation must be in writing.
(6) A covered entity must document and retain any signed consent under this section as required by § 164.530(j).
(c) Implementation specifications: content requirements. A consent under this section must be in plain language and:
(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment, or health care operations;
(2) Refer the individual to the notice required by § 164.520 for a more complete description of such uses and disclosures and state that the

individual has the right to review the notice prior to signing the consent;
(3) If the covered entity has reserved the right to change its privacy practices that are described in the notice in accordance with § 164.520(b)(1)(v)(C), state that the terms of its notice may change and describe how the individual may obtain a revised notice;
(4) State that:
(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations;
(ii) The covered entity is not required to agree to requested restrictions; and
(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;
(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and
(6) Be signed by the individual and dated.
(d) Implementation specifications: defective consents. There is no consent under this section, if the document submitted has any of the following defects:
(1) The consent lacks an element required by paragraph (c) of this section, as applicable; or
(2) The consent has been revoked in accordance with paragraph (b)(5) of this section.
(e) Standard: resolving conflicting consents and authorizations. (1) If a covered entity has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment, or health care operations, the covered entity may disclose such protected health information only in accordance with the more restrictive consent, authorization, or other written legal permission from the

individual.
(2) A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual described in paragraph (e)(1) of this section by:
(i) Obtaining a new consent from the individual under this section for the disclosure to carry out treatment, payment, or health care operations; or
(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose protected health information in accordance with the individual's preference.
(f)(1) Standard: joint consents. Covered entities that participate in an organized health care arrangement and that have a joint notice under § 164.520(d) may comply with this section by a joint consent.
(2) Implementation specifications: requirements for joint consents. (i) A joint consent must:
(A) Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and
(B) Meet the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the consent covers more than one covered entity.
(ii) If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as practicable.
§164.508 Uses and disclosures for which an authorization is required.
(a) Standard: authorizations for uses and disclosures. (1) Authorization required: general rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use

or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) Authorization required: psychotherapy notes. Notwithstanding any other provision of this subpart, other than transition provisions provided for in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations, consistent with consent requirements in § 164.506:

(A) Use by originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(b) Implementation specifications: general requirements. (1) Valid authorizations.

(i) A valid authorization is a document that contains the elements listed in paragraph (c) and, as applicable, paragraph (d), (e), or (f) of this section.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not be inconsistent with the elements required by this section.

(2) Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c), (d), (e), or (f) of this section, if applicable;
(iii) The authorization is known by the covered entity to have been revoked;
(iv) The authorization lacks an element required by paragraph (c), (d), (e), or (f) of this section, if applicable;
(v) The authorization violates paragraph (b)(3) of this section, if applicable;
(vi) Any material information in the authorization is known by the covered entity to be false.
(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:
(i) An authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined as permitted by § 164.506(b)(4)(ii) or paragraph (f) of this section;
(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;
(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.
(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization under paragraph (f) of this section;
(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:
(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section;
(iii) A health plan may condition payment of a claim for specified benefits on provision of an authorization under paragraph (e) of this section, if:
(A) The disclosure is necessary to determine payment of such claim; and
(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and
(iv) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.
(5) Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:
(i) The covered entity has taken action in reliance thereon; or
(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.
(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).
(c) Implementation specifications: core elements and requirements. (1)

Core elements. A valid authorization under this section must contain at least the following elements:
(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
(iv) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
(v) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
(vi) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;
(vii) Signature of the individual and date; and
(viii) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.
(2) Plain language requirement. The authorization must be written in plain language.
(d) Implementation specifications: authorizations requested by a covered entity for its own uses and disclosures. If an authorization is requested by a covered entity for its own use or disclosure of protected health information that it maintains, the covered entity must comply with the following requirements.
(1) Required elements. The authorization for the uses or disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:

(i) For any authorization to which the prohibition on conditioning in paragraph (b)(4) of this section applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;
(ii) A description of each purpose of the requested use or disclosure;
(iii) A statement that the individual may:
(A) Inspect or copy the protected health information to be used or disclosed as provided in § 164.524; and
(B) Refuse to sign the authorization; and
(iv) If use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result.
(2) Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.
(e) Implementation specifications: authorizations requested by a covered entity for disclosures by others. If an authorization is requested by a covered entity for another covered entity to disclose protected health information to the covered entity requesting the authorization to carry out treatment, payment, or health care operations, the covered entity requesting the authorization must comply with the following requirements.
(1) Required elements. The authorization for the disclosures described in this paragraph must, in addition to meeting the requirements of paragraph (c) of this section, contain the following elements:
(i) A description of each purpose of the requested disclosure;
(ii) Except for an authorization on which payment may be conditioned under paragraph (b)(4)(iii) of this section, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and

(iii) A statement that the individual may refuse to sign the authorization.
(2) Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization.
(f) Implementation specifications: authorizations for uses and disclosures of protected health information created for research that includes treatment of the individual. (1) Required elements. Except as otherwise permitted by § 164.512(i), a covered entity that creates protected health information for the purpose, in whole or in part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must:
(i) For uses and disclosures not otherwise permitted or required under this subpart, meet the requirements of paragraphs (c) and (d) of this section; and
(ii) Contain:
(A) A description of the extent to which such protected health information will be used or disclosed to carry out treatment, payment, or health care operations;
(B) A description of any protected health information that will not be used or disclosed for purposes permitted in accordance with §§ 164.510 and 164.512, provided that the covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i); and
(C) If the covered entity has obtained or intends to obtain the individual's consent under § 164.506, or has provided or intends to provide the individual with a notice under § 164.520, the authorization must refer to that consent or notice, as applicable, and state that the statements made pursuant to this section are binding.
(2) Optional procedure. An authorization under this paragraph may be in the same document as:
(i) A consent to participate in the research;
(ii) A consent to use or disclose protected health information to carry out

treatment, payment, or health care operations under § 164.506; or
(iii) A notice of privacy practices under § 164.520.
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described by §§ 164.506 and 164.508, respectively, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.
(a) Standard: use and disclosure for facility directories.
(1) Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:
(i) Use the following protected health information to maintain a directory of individuals in its facility:
(A) The individual's name;
(B) The individual's location in the covered health care provider's facility;
(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and
(D) The individual's religious affiliation; and
(ii) Disclose for directory purposes such information:
(A) To members of the clergy; or
(B) Except for religious affiliation, to other persons who ask for the individual by name.
(2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information

(including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) Emergency circumstances. (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) Standard: uses and disclosures for involvement in the individual's care and notification purposes.

(1) Permitted uses and disclosures. (i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's

location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.

(2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

(3) Limited uses and disclosures when the individual is not present. If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for

the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written consent or authorization of the individual as described in §§ 164.506 and 164.508, respectively, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) Standard: uses and disclosures required by law. (1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) Standard: uses and disclosures for public health activities.

(1) Permitted disclosures. A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public

health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration:

(A) To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the Food and Drug Administration;

(B) To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;

(C) To enable product recalls, repairs, or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals, or other problems); or

(D) To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides a health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the

workplace; or
(*2*) To evaluate whether the individual has a work-related illness or injury;
(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;
(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:
(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or
(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.
(2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.
(c) Standard: disclosures about victims of abuse, neglect or domestic violence.
(1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or

protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:
(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
(ii) If the individual agrees to the disclosure; or
(iii) To the extent the disclosure is expressly authorized by statute or regulation and:
(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
(2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:
(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
(d) Standard: uses and disclosures for health oversight activities.
(1) Permitted disclosures. A covered entity may disclose protected health

information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) Exception to health oversight activities. For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) Joint activities or investigations. Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) Permitted uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health

oversight activities as permitted by paragraph (d) of this section.
(e) Standard: disclosures for judicial and administrative proceedings.
(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:
(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or
(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or
(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.
(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative

tribunal; and
(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
(*1*) No objections were filed; or
(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.
(vi) Nothwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section,

if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) Standard: disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) Permitted disclosures: pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;

(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(*3*) De-identified information could not reasonably be used.

(2) Permitted disclosures: limited information for identification and location purposes. Except for disclosures required by law as permitted by

paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) Permitted disclosure: victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(ii) The individual agrees to the disclosure; or

(iii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the

victim has occurred, and such information is not intended to be used against the victim;
(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
(4) Permitted disclosure: decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.
(5) Permitted disclosure: crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.
(6) Permitted disclosure: reporting crime in emergencies. (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
(A) The commission and nature of a crime;
(B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime.
(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any

disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) Standard: uses and disclosures about decedents. (1) Coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) Standard: uses and disclosures for research purposes. (1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16

CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure is sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) Documentation of waiver approval. For a use or disclosure to be

permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than minimal risk to the individuals;

(B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;

(C) The research could not practicably be conducted without the alteration or waiver;

(D) The research could not practicably be conducted without access to and use of the protected health information;

(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;

(F) There is an adequate plan to protect the identifiers from improper use and disclosure;

(G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(H) There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health

information would be permitted by this subpart.
(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(D) of this section;
(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);
(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(*2*) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;
(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use

an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) Standard: uses and disclosures to avert a serious threat to health or safety. (1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) Use or disclosure not permitted.. A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) Limit on information that may be disclosed. A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) Presumption of good faith belief. A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) Standard: uses and disclosures for specialized government functions.

(1) Military and veterans activities. (i) Armed Forces personnel. A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or

entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) Foreign military personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register** pursuant to paragraph (k)(1)(i) of this section.

(2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

(3) Protective services for the President and others. A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) Medical suitability determinations. A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;
(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.
(5) Correctional institutions and other law enforcement custodial situations. (i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:
(A) The provision of health care to such individuals;
(B) The health and safety of such individual or other inmates;
(C) The health and safety of the officers or employees of or others at the correctional institution;
(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
(E) Law enforcement on the premises of the correctional institution; and
(F) The administration and maintenance of the safety, security, and good order of the correctional institution.
(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.
(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.
(6) Covered entities that are government programs providing public

benefits. (i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) Standard: disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(a) Standard: de-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with

generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
(ii) Documents the methods and results of the analysis that justify such determination; or
(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;

(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code; and
(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
(c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:
(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.
(d)(1) Standard: minimum necessary requirements. A covered entity must reasonably ensure that the standards, requirements, and implementation specifications of § 164.502(b) and this section relating to a request for or the use and disclosure of the minimum necessary protected health information are met.
(2) Implementation specifications: minimum necessary uses of protected health information. (i) A covered entity must identify:
(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties;

and
(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.
(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.
(3) Implementation specification: minimum necessary disclosures of protected health information. (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.
(ii) For all other disclosures, a covered entity must:
(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and
(B) Review requests for disclosure on an individual basis in accordance with such criteria.
(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:
(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
(B) The information is requested by another covered entity;
(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum

necessary for the stated purpose(s); or
(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.
(4) Implementation specifications: minimum necessary requests for protected health information. (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.
(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.
(iii) For all other requests, a covered entity must review the request on an individual basis to determine that the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.
(5) Implementation specification: other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, discloses or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.
(e)(1) Standard: uses and disclosures of protected health information for marketing. A covered entity may not use or disclose protected health information for marketing without an authorization that meets the applicable requirements of § 164.508, except as provided for by paragraph (e)(2) of this section.
(2) Implementation specifications: requirements relating to marketing. (i) A covered entity is not required to obtain an authorization under §

164.508 when it uses or discloses protected health information to make a marketing communication to an individual that:
(A) Occurs in a face-to-face encounter with the individual;
(B) Concerns products or services of nominal value; or
(C) Concerns the health-related products and services of the covered entity or of a third party and the communication meets the applicable conditions in paragraph (e)(3) of this section.
(ii) A covered entity may disclose protected health information for purposes of such communications only to a business associate that assists the covered entity with such communications.
(3) Implementation specifications: requirements for certain marketing communications. For a marketing communication to qualify under paragraph (e)(2)(i) of this section, the following conditions must be met:
(i) The communication must:
(A) Identify the covered entity as the party making the communication;
(B) If the covered entity has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and
(C) Except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications.
(ii) If the covered entity uses or discloses protected health information to target the communication to individuals based on their health status or condition:
(A) The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and
(B) The communication must explain why the individual has been targeted and how the product or service relates to the health of the

individual.
(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications, under paragraph (e)(3)(i)(C) of this section, are not sent such communications.
(f)(1) Standard: uses and disclosures for fundraising. A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:
(i) Demographic information relating to an individual; and
(ii) Dates of health care provided to an individual.
(2) Implementation specifications: fundraising requirements. (i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice;
(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.
(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.
(g) Standard: uses and disclosures for underwriting and related purposes. If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

(h)(1) Standard: verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:
(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and
(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.
(2) Implementation specifications: verification. (i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.
(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.
(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).
(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of

government status;
(B) If the request is in writing, the request is on the appropriate government letterhead; or
(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.
(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).
§ 164.520 Notice of privacy practices for protected health information.
(a) Standard: notice of privacy practices. (1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Exception for group health plans. (i) An individual enrolled in a group health plan has a right to notice:
(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or
(B) From the health insurance issuer or HMO with respect to the group health plan though which such individuals receive their health benefits under the group health plan.
(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:
(A) Maintain a notice under this section; and
(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.
(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.
(3) Exception for inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.
(b) Implementation specifications: content of notice.
(1) Required elements. The covered entity must provide a notice that is written in plain language and that contains the elements required by this

paragraph.

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) Uses and disclosures. The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).

(iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:

(A) The covered entity may contact the individual to provide appointment

reminders or information about treatment alternatives or other heath-related benefits and services that may be of interest to the individual;

(B) The covered entity may contact the individual to raise funds for the covered entity; or

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

(iv) Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) Covered entity's duties. The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with

notice of its legal duties and privacy practices with respect to protected health information;
(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and
(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.
(vi) Complaints. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.
(vii) Contact. The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).
(viii) Effective date. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.
(2) Optional elements. (i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).
(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to

issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) Revisions to the notice. The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) Implementation specifications: provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(4) of this section, as applicable.

(1) Specific requirements for health plans. (i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and

(C) Within 60 days of a material revision to the notice, to individuals then
covered by the plan.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant

to the individual or other person requesting the notice.
(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must:
(i) Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider;
(ii) If the covered health care provider maintains a physical service delivery site:
(A) Have the notice available at the service delivery site for individuals to request to take with them; and
(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and
(iii) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(ii) of this section, if applicable.
(3) Specific requirements for electronic notice. (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.
(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.
(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health

care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) Implementation specifications: joint notice by separate covered entities. Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the

joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) Implementation specifications: documentation. A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity as required by § 164.530(j).

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) Standard: right of an individual to request restriction of uses and disclosures. (i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) A covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(i), 164.510(a) or 164.512.

(2) Implementation specifications: terminating a restriction. A covered entity may terminate its agreement to a restriction, if :

(i) The individual agrees to or requests the termination in writing;
(ii) The individual orally agrees to the termination and the oral agreement is documented; or
(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.
(3) Implementation specification: documentation. A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).
(b)(1) Standard: confidential communications requirements. (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,
(2) Implementation specifications: conditions on providing confidential communications.
(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.
(ii) A covered entity may condition the provision of a reasonable accommodation on:
(A) When appropriate, information as to how payment, if any, will be handled; and
(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
§ 164.524 Access of individuals to protected health information.
(a) Standard: access to protected health information. (1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:
(i) Psychotherapy notes;
(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
(iii) Protected health information maintained by a covered entity that is:
(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or
(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
(2) Unreviewable grounds for denial. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.
(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.
(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the

health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause

substantial harm to such other person; or
(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
(4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.
(b) Implementation specifications: requests for access and timely action.
(1) Individual's request for access. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.
(2) Timely action by the covered entity. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.
(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.
(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.
(ii) If the request for access is for protected health information that is not

maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.

(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) Implementation specifications: provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

(ii) The covered entity may provide the individual with a summary of the

protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:
(A) The individual agrees in advance to such a summary or explanation; and
(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
(3) Time and manner of access. The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;
(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.
(d) Implementation specifications: denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.
(1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health

information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) Denial. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) Other responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) Standard: right to amend.

(1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) Implementation specifications: requests for amendment and timely action.

(1) Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) Timely action by the covered entity. (i) The covered entity must act

on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) Implementation specifications: accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with

which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) Implementation specifications: denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) Statement of disagreement. The covered entity must permit the

individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosures. (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as

applicable, to the recipient of the standard transaction.
(e) Implementation specification: actions on notices of amendment. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.
(f) Implementation specification: documentation. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).
§ 164.528 Accounting of disclosures of protected health information.
(a) Standard: right to an accounting of disclosures of protected health information.
(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:
(i) To carry out treatment, payment and health care operations as provided in § 164.502;
(ii) To individuals of protected health information about them as provided in § 164.502;
(iii) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;
(iv) For national security or intelligence purposes as provided in § 164.512(k)(2);
(v) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or
(vi) That occurred prior to the compliance date for the covered entity.
(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or

law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) Implementation specifications: content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) The accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:
(A) A copy of the individual's written authorization pursuant to § 164.508; or
(B) A copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.
(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, or pursuant to a single authorization under § 164.508, the accounting may, with respect to such multiple disclosures, provide:
(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;
(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and
(iii) The date of the last such disclosure during the accounting period.
(c) Implementation specifications: provision of the accounting.
(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.
(i) The covered entity must provide the individual with the accounting requested; or
(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:
(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.
(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
(d) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):
(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;
(2) The written accounting that is provided to the individual under this section; and
(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.
§ 164.530 Administrative requirements.
(a)(1) Standard: personnel designations. (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.
(2) Implementation specification: personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) Standard: training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.
(2) Implementation specifications: training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.
(c)(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
(2) Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
(d)(1) Standard: complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this

subpart.
(2) Implementation specification: documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.
(e)(1) Standard: sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.
(2) Implementation specification: documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.
(f) Standard: mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.
(g) Standard: refraining from intimidating or retaliatory acts. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:
(1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;
(2) Individuals and others. Any individual or other person for:
(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;
(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) Standard: waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) Standard: policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) Standard: changes to policies or procedures. (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and

procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.
(3) Implementation specification: changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.
(4) Implementation specifications: changes to privacy practices stated in the notice. (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:
(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;
(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and
(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.
(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:
(A) Such change meets the implementation the requirements in

paragraphs (i)(4)(i)(A)-(C) of this section; and
(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.
(5) Implementation specification: changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:
(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and
(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.
(j)(1) Standard: documentation. A covered entity must:
(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;
(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and
(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.
(2) Implementation specification: retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.
(k) Standard: group health plans. (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:
(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and
(ii) The group health plan does not create or receive protected health information, except for:
(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.

(a) Standard: effect of prior consents and authorizations. Notwithstanding other sections of this subpart, a covered entity may continue to use or disclose protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information that does not comply with §§ 164.506 or 164.508 of this subpart consistent with paragraph (b) of this section.

(b) Implementation specification: requirements for retaining effectiveness of prior consents and authorizations. Notwithstanding other sections of this subpart, the following provisions apply to use or disclosure by a covered entity of protected health information pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, if the consent, authorization, or other express legal permission was obtained from an individual before the applicable compliance date of this subpart and does not comply with §§ 164.506 or 164.508 of this subpart.

(1) If the consent, authorization, or other express legal permission obtained from an individual permits a use or disclosure for purposes of carrying out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission

obtained from an individual applies, use or disclose such information for purposes of carrying out treatment, payment, or health care operations, provided that:

(i) The covered entity does may not make any use or disclosure that is expressly excluded from the a consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(2) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for a purpose other than to carry out treatment, payment, or health care operations, the covered entity may, with respect to protected health information that it created or received before the applicable compliance date of this subpart and to which the consent, authorization, or other express legal permission obtained from an individual applies, make such use or disclosure, provided that:

(i) The covered entity does not make any use or disclosure that is expressly excluded from the consent, authorization, or other express legal permission obtained from an individual; and

(ii) The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(3) In the case of a consent, authorization, or other express legal permission obtained from an individual that identifies a specific research project that includes treatment of individuals:

(i) If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to protected health information that it created or received either before or after the applicable compliance date of this subpart and to which the consent or

authorization applies, make such use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(ii) If the consent, authorization, or other express legal permission obtained from an individual is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to protected health information that it created or received as part of the project before or after the applicable compliance date of this subpart, make a use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

(4) If, after the applicable compliance date of this subpart, a covered entity agrees to a restriction requested by an individual under § 164.522(a), a subsequent use or disclosure of protected health information that is subject to the restriction based on a consent, authorization, or other express legal permission obtained from an individual as given effect by paragraph (b) of this section, must comply with such restriction.

§ 164.534 Compliance dates for initial implementation of the privacy standards.

(a) Health care providers. A covered health care provider must comply with the applicable requirements of this subpart no later than [OFR - insert date 24 months after the effective date of the final rule in the **Federal Register**].

(b) Health plans. A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:

(1) Health plans other than small health plans – [OFR - insert date 24 months after the effective date of the final rule in the **Federal Register**].

(2) Small health plans – [OFR - insert date 36 months after the effective date of the final rule in the **Federal Register**].

(c) Health care clearinghouses. A health care clearinghouse must comply with the applicable requirements of this subpart no later than [OFR - insert date 24 months after the effective date of the final rule in the **Federal Register**].

參考書目

中華民國國民健保卡建置計畫採購契約

Kristin Baczynski, Do You Know Who Your Physician Is?: Placing Physician Information on the Internet, 87 Iowa Law Review 1303 (2002)

R. Brian Black, Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models From South Africa and the United Kingdom, 34 Cornell International Law Journal 397 (2001)

John d. Blum, The Role of Law in Global E-Health: A Tool for Development and Equality in a Digitally Divided World, 46 Saint Louis University School of Law Journal 85 (2002)

Rene Bowser & Lawrence O. Gostin, Managed Care and the Health of a Nation, 72 Southern California Law Review1209, 1217-18 (1999)

John R. Christiansen, A Preliminary Review of the Final HIPAA Privacy Rule: Re-Engineering the Information Relationship Between Individuals and Healthcare Organizations, Health Law Digest 3-12 (February 2001).

Kevin B. Davis, Privacy Rights in Personal Information: HIPAA And The Privacy Gap Between Fundamental Privacy Rights And Medical Information, 19 The John Marhall Journal of Computer & Information Law 535 (2001).

A. Craig Eddy, A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of The Health Insurance Privacy and Accountability Act of 1996, 9 Loyola University Chicago Institute for Health Law Annuals of Health Law 1 (2000)

Michael Froomkin, Cyberspace And Privacy: A New Legal Paradigm? The Death of
Privacy?, 52 Stanford Law Review, May 1461 (2000)

Catherine Louisa Glenn, Protecting Health Information Privacy: The Case For Self-Regulation of Electronically Held Medical Records, 53 Vanderbilt Law Review 1605 (2000

Susan M. Gordon, Privacy Standards for Health Information: The Misnomer of Administrative Simplification, 5 Delaware Law Review 23 (2002).

Lawrence O. Gostin, Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations, 127 Annals of Internal Medicine 683, 684 (1997).

Lawrence O. Gostin et al., National Conference of State Legislatures, Genetics Policy and Law: A Report for Policymakers (2001).

Lawrence O. Gostin, James G. Hodge, Jr., Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule, 86 Minnesota Law Review 1439, 1455-56 (2002).

Lawrence O. Gostin, James G. Hodge, JR. and Mira S. Burghardt., Symposium: Balancing Communal Goods And Personal Privacy Under A National Health Informational Privacy Rule, 46 Saint Louis University Law Journal5 (2002).

Lawrence O. Gostin, National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act, 285 JAMA 3015,3019-20 (2001).

P. Greg Gulick, E-Health And The Future of Medicine: The Economic, Legal, Regulatory, Cultural, and Organizational Obstacles Facing Telemedicine and Cybermedicine Programs, 12 Albany Law Journal of Science & Technology Albany Law, 351 (2002).

Mark A. Hall et al., Trust in Physicians and Medical Institutions: What Is It, Can It Be Measured, and Does It Matter?, 79 Milbank Quarterly 613, 622 (2001).

Mike Hatch, National Health Information Privacy Regulations Under HIPAA: HIPAA: Commercial Interests Win, 86 Minnesota Law Review 1481 (2002).

Randi Heitzman, The Business Associate Brain Teaser: A Look at Problems Involving The Business Associate Regulations Under The Health Insurance Portability and AccountabilityAct of 1996, 11 Annuals of Health Law 159 (2002).

Jason M. Healy, William M. Altman & Thomas C. Fox, Confidential of Health Care Provider Quality of Care Information, 40 The University of Louisville Brandeis Law Journal 595 (2002)

Edward J. Imwinkelried & D.H. Kaye, DNA Typing: Emerging Or Neglected Issues,76 Washington Law Review 413 (2001).

Peter D. Jacobson, Regulating Health Care: From Self-Regulation to Self-Regulation?, 26 Journal of Health Politics, Policy and Law 1165 (2001)

Peter D. Jacobson, Medical Records and HIPAA: Is It Too Late to Protect Privacy?, 86 Minnesota Law Review 1497 (2002)

Peter D. Jacobson & C. John Rosenquist, The Use of Low-Osmolar Contrast Agents: Technological Change and Defensive Medicine, 21 Journal of Health Politics, Policy and Law 243 (1996)

Marcos D. Jimenez & Dana Foster, The Importance of Compliance Programs for the Health Care Industry, 7 University of Miami Business Law Review 503 (1999).

Mary Beth Johnston & Leighton Roper, HIPAA Becomes Reality: Compliance With New Privacy, Security, And Electronic Transmission Standards, 103 West Virginia Law Review 541 (2001)

Robert John Kane, Information Is The Key to Patient Empowerment, 11 Annuals of Health Law 25 (2002)

Timothy Stoltzfus Jost, Managed Care Regulation: Can We Learn from Others? The Chilean Experience, 32 University of Michigan Law School Journal of Law Reform 863 (1999)

Erika King and John H. Fuson, An Overview of Canadian Privacy Law for Pharmaceutical and Device Manufacturers Operating in Canada, 57 The Food and Drug Law Institute Food and Drug Law Journal 205 (2002)

Shari G. Kleiner, Elizabeth A. Philip & Jennifer Yokoyama, Health Care Fraud,
36 American Criminal Law Review 773 (1999)

Paul T. Kostyack, The Emergence of The Healthcare Information Trust, 12 Health Matrix 393 (Summer 2002)

Jennifer Kulynych & David Korn, The Effect of the New Federal

Medical-Privacy Rule on Research, 346 The New England Journal of Medicine 201, 201 (2002)

Jennifer Kulynych & David Korn, Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule, 28 Boston University School of Law American Journal of Law & Medicine 309 (2002)

John T. Lynch & Bruno Lassus, Mega Enterprise Chooses Smart Cards, 21 Health Management & Technology 50 (2001)

J. Andrew Maniko, Who Should Know?-- The Disclosure Debate Over Genetic Information, 26 Seton Hall Legislative 151 (2001)

Dayna Bowen Matthew, Tainted Prosecution of Tainted Claims: The Law, Economics, and Ethics of Fighting Medical Fraud Under the Civil False Claims Act, 76 Trustees of Indiana University Indiana Law Journal 525 (2001)

David Mechanic, The Functions and Limitations of Trust in the Provision of Medical Care, 23 Journal of Health Politics, Policy and Law 661(1998)

L. Joseph Melton, III, The Threat to Medical-Records Research, 337 The New England Journal of Medicine 1466 (1997)

Betty M. Ng, Universal Health Identifier: Invasion of Privacy or Medical Advancement ?, 26 Rutgers Computer and Technology Law Journal 331 (2000)

Robert E. Nolan Company, Inc., ANALYSIS OF HHS COST ESTIMATES FOR THE FINAL HIPAA PRIVACY REGULATION (March 2001)

Kourtney L. Pickens, Don't Judge Me by My Genes: A Survey of Federal Genetic Discrimination Legislation, 34 Tulsa Law Journal 161 (1998)

Joy L. Pritts, Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule, Yale 2 Journal of Health Policy, Law and Ethics 325 (2002)

James B. Roche, Related Matters: Health Care In America: Why We Need Universal Health Care And Why We Need It Now, 13 St. Thomas Law Review 1013 (2001)

Helena Gail Rubinstein, If I Am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate, 25 Boston University School of Law American Journal of Law &Medicine 203 (1999)

Jack L. Runyan, A Summary of Fed. Laws and Regulations Affecting Agric. Employers: Immigration Reform and Control Act of 1986, Food and Rural Economics Division, Economic Research Service, U.S. Department of Agriculture. Agricultural Handbook No. 719.

Amy Schofield & Linda D. Weaver, Health Care Fraud, 37 American Criminal Law Review 617 (2000)

Gerald S. Schatz, Comment: Health Records Privacy and Confidentiality: Pending Questions, 18 The Catholic University of America Journal of Contemporary Health Law & Policy 685, (2002)

Bonnie Schreiber, Andrea Prasow and Rachel S. Martin, Health Care Fraud, 39 American Criminal Law Review 707 (2002)

Charity Scott, Is Too Much Privacy Bad For Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy, 17 Georgia State University Law Review. 481 (2000)

Shawn C. Helms, Translating Privacy Values with Technology, 7 Boston University Journal of Science and Technology Law, Summer 288 (2001)

Richard Sobel, The Demeaning of Identity and Personhood in National Identification Systems, 15 Harvard Journal of Law & Technology 319 (2002)

Richard Sobel, The Degradation of Political Identity under A National Identification System, 8 Boston University Journal of Science and Technology Law 37 (2002)

Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for InformationPrivacy, 53 Stanford Law Review1393 (2001)

Shaun B. Spencer, Reasonable Expectations and the Erosion of Privacy, 39 San Diego Law Review 843 (2002)

Peter P. Swire & Lauren Steinfeld, Security and Privacy After September 11: The Health Care Example, 86 Minnesota Law Review 1515 (2002)

Sheryl Gaye Stolberg, Health Identifier for all Americans Runs Into Hurdles, The New York Times, July 20, 1998, at A1.

Susan E. Volkert, Telemedicine: RX for The Future of Health Care, 6 University of Michigan Law School Telecommunication and Technology Law Review 147 (2000).

Charles A. Welch, Sacred Secrets - The Privacy of Medical Records, 345 The

New England Journal of Medicine 371 (2001)

Peter A. Winn, confidentiality in Cyberspace: The HIPAA Privacy Rules and The Common Law, 33 Rutgers Law Journal 617, Spring, (2002)

Jonathan Zittrain, What the Publisher can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, 52 Stanford Law Review 1201 (2000)

Brian Zoeller, Health and Human Services' Privacy Proposal: A Failed Attempt at Health Information Privacy Protection, 40 The University of Louisville Brandeis Law Journal 1065 (2002)