計畫編號：DOH89-TD-1090

行政院衛生署八十八年下半年及八十九年度

科技研究發展計畫

資訊專業倫理與醫療資料安全之研究

研 究 報 告

執行機構：　元智大學資訊社會學研究所

計畫主持人：曾淑芬教授

研究人員：　呂瓊雯、謝豫立、何錦昌

執行期間：88 年 07 月 01 日至 89 年 08 月 15 日

目錄

目次

表次、附錄

中文摘要

在醫療院所作業資訊化的時代，個人醫療記錄的資訊化與整合已是必然的趨勢。在此趨勢下，涉及高度個人隱私的醫療資訊之安全問題便成為十分重要且必須深思的議題。本研究由「隱私權」出發，探討其與具體的「醫療資訊安全」的關係，並討論醫療資訊安全與「醫療資訊倫理」當中，醫療資訊人員對於資料安全的概念，及遵守專業倫理守則的情況。

本研究以分層比例抽樣方式，並採郵寄問卷調查法，共回收 566 份有效問卷，醫院回覆率為 71.30%、問卷回覆率為 49.65%。結果發現目前國內醫院的電腦化與醫療資料資訊化的程度兩者之間仍有落差，只有醫學中心或部份醫療評鑑甲等的區域醫院已有能力達到電子病歷的要求且擁有預防入侵的資訊技術。其次，無論醫院規模層級，絕大多數受訪者對於病歷資料做不符合醫療用途的行為均有所警覺，但在後續處置措施方面較為模糊不清。再者，受訪者就「人員與病歷資料之關係」及「資料敏感度」有不同程度的隱私認知，「資料用途」則沒有明顯的隱私認知差異。另外，本研究依研究結果綜合建構出一項醫院整體資訊安全指數，醫學中心在資訊安全硬體設施部分明顯高於區域與地區醫院，而在人員專業素養及醫療資訊隱私認知上各級醫院則無明顯地差異。

因此，研究建議目前在醫療組織部分需優先強化的政策事項為 1.有明

確的保護病患資料安全與機密的政策、2.設立保護病患資料安全與機密方面的委員會、3.明訂病患資料洩露所因應的危機處理守則、4.加強一般資訊安全素養之教育與訓練方面的課程、5.明確的處分機制；在資訊技術層面則為 1. 獨立設置個別使用者權限、2.管制網路連結、3.加強病患資料的安全防護與備份復原能力、4.增進整體系統評估能力。另外，研究針對目前在政府部門可優先強化之建議為：1.政府與民間合作研究出醫療資料隱私需求及相符之安全標準、2.建立第三者運作及監督機制、3.延伸應用醫療資訊安全標準於醫療相關產業。

總之，目前國內醫療機構的醫療資訊安全表現均有待提昇，而就安全技術標準與診療資料標準化的問題亦有待政府、醫療院所及學術界三方面共同努力，以追求一個具隱私保障且兼顧資訊需求的醫療資訊應用環境。

關鍵詞：電子化病歷、醫療資訊安全、資訊隱私權、醫療專業倫理、資訊專業倫理。

英文摘要

The security and the privacy concerns become more and more important as health information move from paper to electronic data collection. This paper argues that the issues are not only related to the information security hardwares but also the professional ethics and the medical privacy consensus of the informational workers in hospitals. This paper also argues that the development of guiding privacy, confidentiality and security principles is necessary to help balance of patients' privacy interests against appropriate information access.

A national mail survey to hospitals' staffs in patient record department and information technicians was conducted. A total of 566 valid responses were collected, with a response rate at 49.65%.

The results reported a significant difference of information security and privacy concerns in various levels of hospital, where medical center hospitals have adopted more computerized patient record information systems and have shown a higher score on the total information security index. In general, most respondents show a high score on professional ethics and reported a high sensitivity on exposing patients' medical records. However, respondents did show inconsistency in responding exposure episodes. Our results suggest the importance of establishing organizational guideline of information security as well as developing security information management systems. Several technical recommendations, such as authentication, access control, audit trails, and organizational recommendations, such as formal policy, committee, education and training were suggested for medical information security and medical privacy.

Keywords: Computerized Patient Record; Medical Information Security; Information Privacy; Medical Professional Ethics; Informational Professional Ethics.

第一章　緒　論

第一節　研究背景

早在民國七十五年間，行政院即以核定「籌建醫療網計畫」，衛生署隨後在七十七年正式進行「建立全國醫療資訊網計畫」，至今已經完成四個區域資訊中心、五項公用性系統、十七項個別性醫院管理系統，以及衛生所資訊系統等建置工作，並仍有新系統正在陸續開發中。與醫療資訊網連線的單位中，除了有：衛生署、省衛生處、各縣市衛生局、健保分局以及公立醫院等公務單位外，各級私立醫療院所及社區藥局等也在系統的涵蓋範圍之內。此外，行政院 NII 小組並將推動社會及醫療服務網路化列為當前的工作重點。目前於電子保健推動現況，在網際網路上提供民眾各種醫政、藥政、食品衛生、防疫及保健等醫療保健資訊及服務。而目前工作為規劃醫療健保資料庫，提供民眾基層醫療保健服務、醫療法規全文檢索服務、醫療資訊佈告欄服務（醫療資訊網、熱訊）、緊急醫療管理服務、預防注射語音系統、全球資訊網等資訊。在可預見的未來，個人醫療記錄的資訊化與整合亦是必然的趨勢。在此趨勢下，醫療資訊安全便成為十分重要且必須深思的議題。

就個人隱私的角度而言，醫療資訊是特別難以防守的也是特別有價值的。在醫療資料庫涵蓋範圍越來越大、不同的資料庫也透過網際網路流通

的時候，亦必須花費更大的功夫方能維護醫療資訊的安全性。此外，如製藥、健康食品、復健器材、人壽保險或是其它醫療相關產業若得以運用數量龐大的醫療資料記錄，一則可以藉此研究開發產品，再則可以準確掌握市場需求，兩者相輔相成便創造了無限商機。也因此可能促使部份業者欲透過各種管道，以不正當的方式取得個人醫療紀錄，以獲取個人醫療紀錄背後所隱藏的龐大經濟價值。

Haywood（1998）提到一些有關醫療資訊安全及隱私權的實例：英國醫療協會（BMA, British Medical Association）在 1996 年的年度大會上投票決定，除非個人資料私密性能夠被保證，將反對醫院的資料庫鏈結到國內網路。而在 BMA 的資訊科技委員會中，一位在波士頓的愛滋病診所工作的律師舉出證據說，總有病人先去問她，在電腦臨床病歷可以被保險公司合法取得的情況下，他們要如何安全的告訴醫生他們的病情。馬里蘭州一位身兼健康中心主任的銀行家，使用健康中心的資料庫資訊，調出在那裡治療癌症病人的負債情況，並干涉這些病人的貸款；在英國，人們也了解病人資訊在轉移時是不安全的。然而，這個問題並不是駭客闖入，而是有人想出售這些個人資訊。這些有關個人隱私的資訊，雖然是不能被公開得取的，但竟然可以被如此的容易交易且便宜。然而，Simpson（1996）提出，醫療資訊安全遭受侵犯的案例數是很難有一個明確的統計數字來說

明的，因為當這類事件被察覺的時候，有關單位總是會盡量隱藏事實，以避免可能的尷尬。然而，根據 FBI 的調查，有高達 85%的資訊安全問題是由內部人員所造成的。此外，Woodward（1995）也指出，曾有醫務人員利用職務之便，窺視兒童的病歷紀錄，並且以電話騷擾病人達數月之久。

第二節　研究內容

在病歷記錄、線上資料庫、消費者健康資訊、以及遠距治療及醫囑等均數位化、儲存於電腦設備內甚或更進一步以網路方式相互構連之後，健康照顧（health care）等醫療行為也會令高度私密的個人資訊遭到不當公開、更改以及使用的風險。病人的權益奠基於資訊作業的完善及可靠。尤其當病人的醫療資料已離開紙張作業，安全可靠的電腦化醫療記錄系統將會顯得格外的重要。這個系統除了在電腦軟硬體設備的加強之外，資訊作業人員本身的安全觀念更是保障個人資料的重要因素。

醫療資料乃涉及高度個人隱私的資料，在醫療院所作業資訊化的時代，對個人資料私密性的保障進行通盤的研究，並研擬確實可行的個人資料保護原則，自有其迫切需要。國外研究大多注重在隱私權的探討，因此本研究將由「隱私權」出發，探討其與具體的「醫療資訊安全」的關係，並討論醫療資訊安全與「醫療資訊倫理」當中，醫療資訊人員對於資料安全

的概念，及遵守專業倫理守則的情況。簡言之，本研究之研究目的為：

壹、了解國內外醫療資料資訊化與資訊安全之相關現況；

貳、調查國內之醫療院所資訊從業人員之專業倫理（ethical code）與醫療資訊隱私的認知；

參、建立「整體醫療資訊安全指數」以供評量參考。

第二章　文獻回顧

第一節　隱私權與資訊隱私權

壹、隱私權的定義與內涵（Wang，1997）

隱私權是十九世紀末期開始出現的法律概念，起源於美國，主要的核心思考是「不受干擾的權利」（the right to be left alone）。論者對於隱私權的分析觀點有三：1.基本權利觀點（Fundamental Rights Perspective）；2.經濟分析觀點（Economic Analysis Perspective）以及3.社區導向觀點（The Community-oriented Perspective）。

一、基本權利觀點：

基本權利觀點(Fundamental Rights Perspective)主張隱私是一項相當重要的價值，並且是民主社會當中鼓勵個人達到自主(autonomy)的重要因素之一。所謂自主，依據 Edward Shils(1964)的說法，包括有決定的權力、公佈行動原則的權力、個人或組織依其需要轉讓資源或聘任人員的權力。這個觀點也相信人們應該有權維持一個不受政府干涉的私密生活空間。是故，本派認為政府及商業的資訊電腦化是一種邪惡，因為政府和民眾間有形或無形的界限會被資料庫的建立而摧毀，致使民眾的隱私權遭到破壞。隱私權想要保障的是尊重個人及維護人類尊嚴的社會價值，但

是一但當隱私權遭受侵害時，人們可能因此而失去工作機會，或是有經濟上的損失等。

二、經濟分析觀點：

經濟分析觀點(Economic Analysis Perspective)是基於一個假設：法律最好是被法官認定為是把經濟利益最大化的公式。抱持本觀點的人們都會延續上述的假設，並且相信法律上的任何原則都應基於經濟考量，如成本最小化、利益最大化等。當隱私權的經濟被考量到時，則是強調「私密是法律所保障的，因為它必須保護再獲得社會有價資訊時的投資，但是它不應該是保密一個會降低個人價值的事，如身為一個員工、借貸者、朋友、配偶或是其他的交易對象等」。經濟分析觀點有別於基本權利觀點之處在於它只著重於可以計算的事實部分如經濟上的支出和獲利，即使不必然是財務上的也是一樣。但像是「品味」就是不列入考慮的因素之一。

三、社區導向觀點：

社區導向觀點(The Community-oriented Perspective)著重於個人權利與公眾利益的平衡點。這個觀點在隱私權理論當中是屬於較中立的，尤其是和前兩個理論比較起來更是如此。不同於經濟

分析觀點主要注重於公眾利益，社區導向觀點也重視個人價值，他們相信有部份人希望享有完全的隱私，如同完全孤立於世外一般，但是這樣以社會的觀點來看似乎是沒有法律的世界。因此，本學派會小心地在個人希望的隱私和公眾利益間求取一個平衡。Ruth Gavison 將隱私定義為：限制他人對個人的接近（access）。即是說：個人有秘密資訊的權利，個人有自主權，個人有獨居的權利。

四、資訊隱私權（information privacy）

時至今日，隨著科技的快速發展及不斷的進步，人類的生活也更加便利。隱私權的定義也愈加明確，內涵亦不斷擴充，資訊隱私權的觀念更彰顯出個人隱私權的價值。廖緯民（1999）便指出隱私權的內涵包含有四個面向：1.個人屬性的隱私權（Privacy of a Person's Persona）：如一個人的姓名、身份、肖像、聲音等，由於其直接涉及個人領域之第一層次，應屬隱私權保護之首要對象；2.通訊內容的隱私權（Privacy of a Person's Communications）：個人之思想與感情，原本存於其腦中，不亦為人所識；惟當與外界溝通時，即易於完整發展；匿名之隱私權（Anonymity)：群體生活中，集體之價值未必與個人之想法相符，此種落差常易引

發個人以匿名方式表達其意見之需求。此種匿名權利之適度容許，常能鼓勵個人之參與感，並保護其自由之創造力空間；而就群體而言，亦常能藉之收真知直諫之效，而得進步之動力；以及 4. 個人資料的隱私權（privacy of data about a person）：意即當個人屬性被抽離成文字之描述或記錄時，如果其指涉之客體為獨一且個人化(unique and personal)，則此等資料即含有高度之個人特性而常能辨識該個人之本體，此可謂間接之個人屬性而亦應以隱私權加以保護，這亦為資訊隱私權的基礎。

貳、資訊隱私權的保護

在這高科技的時代裡，由於人們的各項活動越來越依賴科技所發明的工具，個人之私人生活領域的活動也越來越容易被科技所揭露，個人對於私人生活領域範圍的決定權也越來越容易被壓縮。在享受科技帶來的便利同時，卻得要忍受個人隱私權被蠶食的可能，其中又以間接性質的個人資料隱私權最容易受到侵害，而隨電腦等資訊科技的日益發達更助長這樣的發展趨勢。晚近對於個人資料隱私的保護，在歐美各國也都有一定的共識，同時亦訂定許多相關的規定，以下就針對 OECD、歐盟及美國的相關規定分述之。

一、OECD 及歐盟的規定：

就 OECD 及歐盟的規定而言，在合理的範圍內蒐集並利用使用者的個人資料是被允許的，但卻強調運用個人資料的目的要明確、且要受到蒐集目的之限制。OECD 於 1980 年公佈了「Guideline on the Protection of Privacy and TransBorder Flows of Personal Data」，其中提出了會員國應予遵守的八項個人資料保護的原則：1.限制蒐集（collection limit）之原則；2.資料內容完整、正確（data quality）之原則；3.資料利用目的明確化（purpose specification）之原則；4.限制利用（use limitation）之原則；5.安全保護（security safeguards）之原則；6.公開（openness）之原則；7.個人參加（individual participation）之原則；8.責任（accountability）之原則。許多國家以此作為資料保護立法的基礎[1]。至於歐盟（European Union）對於個人資料保護的規定，在 1995 年所通過的「資料保

[1]A.限制蒐集之原則：個人資料之收集並非「漫無目的」的，而是必須在有「特定需要及目的」並在「當事人同意」之情形下爲之。
B.資料內容完整、正確之原則：個人資料務求完整、正確，以避免對當事人之權益造成傷害，同時並需依當事人之請求做適時之修正、增刪以達維持個人資料之完整與正確。
C.資料利用目的明確化之原則：搜集個人資料之目的應明確，使用時亦不得與原目的違背。如信用卡公司在未經持卡人的同意之下即將其相關資料轉交行銷公司的情況即違反此一精神。
D.限制利用之原則：個人資料之利用，需與收集時之目的相符，不可任意移作他用。例如爲學術目的所作的調查而收集的個人資料，不可以移作商業用途。
E.安全保護之原則：擁有個人資料之機構企業必須對個人資料妥善保護，以免遭人竊取、竄改、破壞等，損及當事人權益，或遭人窺探資料內容，使當事人之隱私受到侵害。
F.公開之原則：對於個人資料之處理，應予公開，以昭公信。同時也應公開計劃主持人之聯絡方式，以方便當事人更正錯誤資料。
G.個人參加之原則：當事人有參與資料製成之權利，以保障其權益。

護一般指令」中，除了將 OCED 的原則加以落實，明確規定之外，更規定禁止會員國內的個人資料禁止流入缺乏適當資料保護的國家。落實保護隱私的積極性由此可證。

二、美國的相關原則

美國鑒於 NII 發展過程中，人民隱私權的維護將成為一個重大議題，NII 小組成立之後，即在其「資訊政策委員會」(Information Policy Committee）之下設「隱私權工作小組」（Privacy Working Group），於 1995 年 6 月提出「隱私權與 NII」最終報告，該報告針對隱私權保護一般性原則、資訊使用者以及資訊提供者三方面提出意見，其內容精神與 OECD 相去不遠[2]。這一份報告書主要是在確立美國在 NII 建設當中，政府及其他相關單位對於隱私權的保障原則。另外在美國電信傳播法 Telecommunication Act of

---

H.責任之原則：違法者必須負起相關之法律責任。

[2] **A.**在一般性原則方面：
個人資料不應被不適當地改變或銷毀。個人資料應保持正確、即時、完整，並和所提供與使用的目的相符。個人資料的取得、公開及使用必須尊重當事人的隱私。

B.針對資訊使用者的原則：
a.在蒐集、公開或使用個人資料時，應評估其對個人隱私的衝擊；並應只蒐集、使用爲目前或計劃中的活動所需的資料。
b.資訊蒐集者必須對個人提供正確及相關的下列資訊：蒐集目的、使用於何處、保持資料機密、完整及品質的方法、提供或不提供資料的後果及任何更正、補救的權利等。
c.資訊使用者需以適當的方法來保護資料的機密與完整。
d.除有強烈的公益考量，資訊使用者不應對資料做超出個人理解使用範圍以外之使用。
e.資訊使用者應教育自己及大眾關於資訊隱私如何維護。

C.針對資料提供者的原則：
a.個人應有權獲得下列正確而相關的資訊：蒐集目的、使用於何處、保持資料機密、完整及品質的方法、提供或不提供資料的後果及任何更正、補救的權利。
b.個人應有權利以下列方法維護自身隱私：i.取回其個人資料；ii.對缺乏品質的個人資料加以更正，以確保使用的公平性；iii.以適當的技術（如：加密）保護通訊與交易的機密與完整；iv.在適當的時候保持匿名（anonymous）。

D.在個人資料被不適當地公開或使用的情形下，個人應有適當的救濟方法。

1996 中的第 222 條「客戶資料隱私」中則是規定電信服務業者有義務維護客戶資料及與客戶相關的資料（custom proprietary network information）的機密性。該條文亦對這類客戶資料的使用、揭露、近用權設限。（47 U.S.C. § 222）然而，1999 年 8 月美國第十巡迴上訴法庭，於 U.S.West Inc. v. FCC 案中，認定該條文中對於使用 CPNI 須經客戶透過書面、口頭或電子形式的「明確表示同意」（opt in）之規定，違反美國憲法第一增補條款。該判決認為，即便限制 CPNI 的使用是符合政府的主要利益考量，FCC 並未能證明採用 opt in 的顧客同意限制的必要性，相較於「默示同意」（opt-out）的方式，亦即「未明確表示不同意者即視為同意」的方式反而是已損及電信服務業者之商業言論自由。雖然本案雖未由美國聯邦最高法院審理判決定讞，但由此可見美國對於消費者的個人資料保護的態度上是比較偏向於促進商業利用發展且較歐盟消極的。

參、我國的相關法律規定

在我國的法律雖然沒有明文提及「隱私權」一詞，但是在民法、刑法中均有對於個人隱私權利的保護規定、在醫療法、醫師法、建築師等相關法律中，亦有明文規定「保密義務」以維護隱私權。而在我

國對於隱私有比較完整規定的則是於民國八十四年通過的電腦個人資料保護法。電腦處理個人資料保護法的立法原則主要是以經濟合作發展組織（OECD）於 1980 年所提出的個人資料保護八大原則為基礎。該原則在本文前面已經提到。「電腦處理個人資料保護法」分六章，共計四十五條，內容包括有行政規劃、民事責任與刑事責任等有關規定。其適用範圍包括：個人資料之電腦處理。並兼及於供電腦處理所謂個人資料之收集與經電腦處理後之個人資料之利用。本法第一條即明顯的說明了電腦處理個人資料保護法的立法重點在：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。在個資法第三條說明該法之用詞定義，同時也明確的指出醫院之電腦資料很明顯的可以適用於個資法的管轄範圍當中。

第二節　醫療資料的隱私概念與安全維護

壹、醫療資料的隱私概念

就資料屬性而言，事涉個人敏感的健康相關狀況的醫療資料亦屬個人資料隱私。目前資訊科技及網際網路可謂十分明顯的影響力量，影響所及，遍佈社會各個層面及各個行業，Latimer（2000）便指出，當醫療體系亦逐漸網路化、醫療資料記錄從傳統紙本逐漸轉移到電子媒介以期提供更方便的資訊連結與傳送時，對於醫療資訊的保密性（

confidentiality）、安全性（security）是除了隱私權的概念之外的二個重要思考面向。Buckovich 等人（1999）在一項比較文獻的研究中，依據美國 HIPAA（Health Portability and Accountability Act of 1996）法案、DHHS（Department of Health and Human Services）之醫療資訊安全規定與電子簽章標準與前述 1995 年歐盟所制定的「資料保護一般指令」中所列舉的規定，歸納出上述相關規定條例中，對於醫療資訊所共通的隱私、保密、資料安全、系統安全等四項概念，並整理出二十八項原則，以下分述該四項概念。

一、隱私（Privacy）

所指的是個體有不受生理或精神方面上的干擾或是所擁有的事物不被錯誤使用的權力。這也包括能自在地控制屬於自己的個人資料，不受任何外在影響自由行動。如「個人有權利使用、修改及複製其個人醫療資料」、「個人有權利決定自己的醫療資料是否採用資訊化電子格式儲存、管理或傳送」等原則均是屬於隱私的概念。

二、機密（Confidentiality）

主要是指對於醫療資訊敏感度的考量，由於醫療資訊較其它個人屬性資料更為敏感，因此需要被保護，避免被他人偷取、揭

露或是不當使用，亦即以統一的方法來限制資訊的分享與公開等行為。如「醫療服務提供者應具有醫療資料保密義務」、「除醫病關係外，醫療資訊未經同意或授權不得揭露」等原則。

醫療資料敏感度高低的差異，主要來自於資源內容本身，以及資料使用者與資料擁有者的關係而定。

（一）內容敏感度

病歷資料依照其內容的敏感度分成三個等級：1.極度敏感，如：精神疾病、性病等重大疾病、藥物濫用、生活型態方面的資料；2.一般敏感，如：與病患就醫疾病有關的資料；3.較不敏感，如：預防注射，某些健診記錄（National Research Council, 1997）。

（二）關係敏感度

依據病歷資料使用者與病患的關係來決定敏感程度，例如以醫院為界線時，病患就醫之醫師與該醫院之行政人員與病患關係較為接近，若是醫療保險、推銷藥物等就與病患關係較為間接，學術研究、訂定醫療法令等用途就與病患關係最為疏遠。與病患關係越為疏遠時，其安全顧慮亦會隨之提高（Lo, et al, 1993）。

三、資料安全（Data Security）與系統安全（System Security）

安全性大多著重於技術層面的思考，亦即以近用權設限（access control）等管制技術來掌控資料的安全性。資料安全意指資料被保護的程度，如會不會被竊賊盜取、被操作系統錯誤所破壞、電力短缺或短路或是極端溫度等物理性質破壞來決定。系統安全較強調資料以外的包含各種軟硬體與災難預防等措施的整體性保護。如「醫療資訊系統應具備供病患使用的檢查機制」、「醫療資訊必須在安全的環境下之傳輸及維護」等原則。

貳、醫療資訊相關工作人員對於醫療資訊的態度

一、醫學生對於病歷資料的態度

Davis（1999）在 1996 年針對醫學院一年級學生進行一項有關電腦病歷態度的研究，其結果指出，學生們認為自己對電腦化的病歷資料的私密性應該負責，但另一方面對於許多實際上操作時的技巧過於疏忽，而在美加地區，學校內對於醫療道德專業的課程時數也過少。這份報告也同時指出就算是受過專業訓練的醫療人員，也大多疏於注意電腦化病歷的私密性。這份報告中建議應對於醫療人員施予基本的醫療道德專業與醫療資訊課程，以達到電腦化病歷的隱私及私密性。

二、資訊人員的專業守則

電腦機構協會（ACM）專業守則當中提到電腦專業人員盡到的義務與責任部份（ACM，1992）。身為資訊專業人員比一般人更尊重對方隱私與保護系統資料，認為維持其專業能力是重要的、充份了解此專業領域中各項相關法律。

參、醫療資訊的安全維護

首先，「病歷遭不當使用」則是在最常被論及違反醫療資訊隱私的情況，它同時亦是醫療資訊安全的維護重點。

一、病歷遭不當使用的案例

Woodward（1995）舉出了一些有關醫療紀錄遭到濫用的案例，其中有一件是在馬里蘭州有職員利用職務之便竊取州政府醫療資料庫的內容加起販售圖利。對內部人員而言，瀏覽病歷資料是相當容易的一件事，同時也是經常發生的，即使法令已明文禁止這類行為的發生。這些行為背後的原因可能是因為：好奇（看看朋友或是親戚、名人的資料）、變態（窺視他人的性偏好）、報復或是為了其他經濟、政治上的因素等。

在波士頓地區，即發生一例兒童強暴犯在得到一份醫院工作後，以不正當手段取得了瀏覽病歷資料的密碼，在閱覽兒童病歷

資料之後，以電話對兒童及其家人進行長達數月的騷擾。

由此可見，資訊安全除了技術層面之外，更需要的是資訊人員本身對資訊安全的認知與執行，在本文之前提到數個國外的例子，資料的流出都是由於「人」在居間操控，甚少有電腦軟體或是硬體上的問題。好的資訊安全技術若未有良好的制度配合都可能會對個人資料安全及隱私造成威脅，因此，健全的制度、良好的管理及資訊人員對專業倫理的信守對於醫療資訊安全的保障相當的重要。

其次，儘管目前在國際間對於資訊隱私權已有一定程度的認知，也都具備一定程度的安全維護相關規定。但是對於醫療資訊隱私及相關安全維護的規定卻仍嫌不足。Lo & Alpers（2000）針對美國現階段的藥物資訊管理系統（Pharmacy Benefits Management Programs）使用情況進行研究調查後發現，目前有 40%的民眾認為美國已有聯邦層級的法律來保護病患醫療資訊的隱私；然而美國衛生主管機關及立法當局卻坦承，事實上美國目前並沒有任何的聯邦層級甚或是州層級的法律，以提供合理的醫療資訊隱私保護，尤其是醫療資訊使用和揭露之主體（如：醫療機構、藥商、保險公司等）[3]的相關規定更是付之闕如

[3] 醫療資訊使用和揭露之主體原文爲：disclosure and use of information by entities。

。Lo & Alpers 他們同時指出，造成美國藥物資訊管理系統的隱私保護問題的原因主要包括：醫院與病患二者之財務利益衝突、缺乏病患對自身資訊授權機制、未經管制的第三人濫用病患資訊以及病患醫療資訊之保密防護措施不足等。

雖然美國至今仍無明確保護醫療資訊隱私的聯邦法律或規定，即便地方（各州）亦無相關法律規定，但美國國家衛生研究院（NIH）在醫療衛生資料的安全維護上仍有相當多的說明，十分值得我國醫療單位借鏡。

二、美國國家衛生研究院（National Institute of Health）之電腦安全訓練網頁：

美國電腦安全法案（Computer Security Act）要求所有使用電腦的美國政府人員，必須完成了解電腦安全的訓練。所以美國資訊資源管理辦公室（Office of Information Resource, OIRM）的資訊科技中心（Center for Information Technology, CIT）發展了一套以電腦為基礎的訓練課程，用來訓練 NIH 的人員有關電腦安全的議題。

電腦安全是致力於保護設備、電腦及網路等的機密資訊。健康及人類服務部門（The Department of Health and Human Services,

DHHS）的自動化資訊系統安全計劃（Automated Information Systems Security Program, AISSP）提供了一個指導方向。NIH 將資料的機密分成三個層次，分別為低度、中度及高度。所有的 NIH 資料，就算是公開的資料也都有某個層次的機密。

低度機密（low sensitivity）的資訊需要保護的程度最小，此類資訊是公開的，例如雇員地區分佈的人口比例檔案。在這個層次中，雖然資訊的取得似乎是沒有反面的效應，但是所有資訊還是重要的，否則就不會被收集到資訊系統中。在低度機密的資訊中，要關心的是非故意的更改及破壞資訊。

在中度機密包括了 NIH 重要資料，以保護不被惡意的行動所破壞。在這個層次上，有關給聯邦政府的資訊，以及 NIH 內部的資訊，都應該被適當的控制。這些資訊包括了人員的工作量、職務、部門間連繫、會議記錄以及其他相關文件。雖然這些資料最後仍會以某些形式公佈，但它們仍是受到保護的，在未經受權下不得任意更改。

而高度機密中，需要最高的安全保護措施。高度機密包涵了下面幾點：

（一）對一個組織來說，被視為最機密及重要的電腦化的連繫及

文件，因此要防止被未經授權的更改及揭露。

（二）資訊被擁有時會造成一些資訊是有價的，如藥物處方、貿易機密、以及初步的研究結果。

（三）對個人及組織而言是用來授權或是使其付費的財務資料。

（四）醫學實驗資料。

（五）申請計劃的評估資料。

（六）自動化系統及記錄受到隱私權法案的管制下，未經授權的揭露，將會構成侵犯個人隱私的行為。

（七）這些資料必須受到保護以防止被未經授權的揭露。

根據不同的機密程度，資料處理的能力也被分為三種不同的危機程度（criticality）。低度危機（low criticality）指的是在自動化資訊系統下，使用者使用電腦或網路時只要有最小的保護預防即可。在遇到資料遺失或被更改時，並不太會影響到整個組織，並且能以最低的代價替代這些資訊。

在中度危機（moderate criticality）指的是在自動化資訊系統中，對 NIH 的內部部門管理上，電腦及網路是重要的，但非必要的。如果一個中度危機的電腦系統在一段時間中無法發揮作用，它將不會產生一個壓倒性的衝擊。

高度危機（high criticality）指的是在自動化資訊系統中，電腦及網路對組織而言是必須的。在這個層次上，如果電腦在一段時間內不能發揮作用，它將產生一個劇烈的衝擊。

三、美國國家研究委員會（National Research Council，NRC）對於醫療資訊系統之評估方式

美國國家研究委員會所屬之國家資訊基礎建設維護醫療資訊隱私委員會（Committee On Maintaining Privacy And Security In Health Care Applications of The National Information Infrastructure）（1996）曾經擬訂一項用來評估及衡量醫療資訊系統的標準。其中對於硬體的資訊安全技術提出了八項指標、軟體的組織紀律提出了四項指標，以下分別敘述之。

（一）硬體技術部分

1.確認證明（Authentication）

確認證明是指任何能夠驗證使用者身份的過程，是決定適當連結讀取醫療資訊的首要決定因素。一般而言，利用你所擁有的事物（如：鑰匙、磁卡等）、你所知道的事情（如：密碼，個人辨識碼等），展現你的關係（如：簽名、指紋、聲紋等）與

展現你所在的位置（如：網路 IP，電話號碼）都能夠達到確認證明的功用

2.連結管制（Access Control）

一旦確認身份之後，就需要決定使用者的能夠讀取何種醫療資訊的權限。傳統給予使用者權限的方式僅能在單一系統下擁有單一等級的權限，並不能夠在不同檔案部份給予同一使用者不同等級的權限。

3.追蹤稽查（Audit Trails）

確認使用者身份並給與權限只能算是完成安全防護工作的一部分而已，對於使用者在系統內所進行的各項動作與予記錄，並對於使用者做出惡意破壞系統之動作能夠即時防護採取應變措施，才是讓安全防護工作較為完整。

4.物理性的安全防護與災難復原（Physical Security and Disaster Recovery）

為了預防資訊系統或作業系統突然故障或遭到破壞時，定期與多重備份措施能將傷害降至最低。

5.連結控制（Control of Links）

對於設置防火牆與控制網路 IP 等措施都是為了降低不可預期入侵系統的可能性。

6.加密編碼（Encryption）

加密編碼是保護電腦記錄安全的基本技術，在儲存、傳輸、確認證明等方面都能夠提供更進一步的安全考量。

7.軟體規範（Software Discipline）

在功能方面，電腦軟體是醫療資訊系統的核心。為了提高使用效率或為護安全，對使用者進行在職教育是最有效的方法。

8.系統評估（System assessment）

電腦科技發展逐年變動極為快速，醫療資訊系統每隔固定時間應該評估系統是否還能夠因應醫院的需求等。

（二）軟體組織紀律方面

1.正式的政策宣告（Formal Policies）

醫院組織越是清楚明白自身目的在於維護病患

隱私與安全，對於如何正當使用病歷資料的措施會更為清楚與恰當。對於訓練組織人員，去營造良好的組織文化極有幫助。

2.安全與機密委員會（Security and Confidentiality Committees）

透過委員會的授權來形成責任指派，以達成真正落實保護病患隱私的重要性。

3.教育與訓練（Education and Training）

透過正式的教育訓練課程，將專業倫理及工作守則等傳播予相關工作人員；非正式的教育訓練，能夠幫助工作人員將注重病患隱私部份的價值觀加以內化。

4.處分制度（Sanctions）

對於違反洩露病患機密資料的最有效的處理方式為依據明確政策目標所設置的處分機制來處理。

第三節　國內外醫療資料資訊化之應用現況比較

就國外之醫療資訊系統應用概況而言，從 1991 年 IOM(the institute of Medicine of the National Academy of Sciences）提出了電腦化病歷資料（Computerized Patient Record, CPR）之概念、定義及實施作法之後，醫療資料的資訊化及其應用狀況在全球均有一定程度的發展，而且目前資訊科技的進步，也加速了醫療資料資訊化的趨勢。

但是 Latimer（2000）亦指出，在不同國家地區之間，醫療資料的資訊化及應用其實有相當的差異。

首先總體來說，資訊化醫療資料系統的用途至今仍以行政管理用途最多（administration use）。其次，就不同區域來觀察，如非洲地區，在經濟發展幾乎停滯、醫療資源極度缺乏的情況下，幾乎仍談不上醫療資料的資訊化。若以南非來說，南非政府為增進醫療管理的效率及更合理地分配資源，開始進行 CPR 相關的基礎建設。至 98 年 8 月已有 2 個省份實施 HIS（health information system）。現在南非公私部門均在建立自己的病歷資料庫。目前南非的問題在於醫療資訊系統幾乎均為「進口」購入，而非建置（to buy not build）所以其管理決策灌並不在政府之手。至於如拉丁美洲的巴西及阿根廷則是嚴格說來僅有少數醫療機構具備行政管理及財務管理用途的資訊系統，醫療資料的

資訊化程度亦非常低，並且缺乏軟體技術標準及硬體設施等資源。

至於在澳洲、美國及歐洲等地則可以發現，上述區域之醫療資料資訊化程度較高，應用層面也較高，病患的醫療資料亦有相當程度的整合，如病理檢驗資訊系統；或是特殊病症如癌症、糖尿病、心臟病等之醫療記錄均有類似的整合性醫療資訊系統。在美國另外則是由於醫療照顧體系高度私營化的結果，在相關醫藥、保險產業間具有較整合性的資訊系統；在日本則是有半數以上的醫院具有一個綜合診療、財務及行政的醫療資訊系統。在先進地區固然醫療資料資訊化的發展速度較快，然而卻也遇到一些共通問題，例如安全標準的制訂、疾病症狀、藥品記錄等診療資料的定義與標準化等。這些問題若無法克服，則醫療資料資訊化後亦難在不同的醫療機構間相互流通，如共同醫療照護（shared-care）的推廣也就會受到限制。另外如日本其醫療資訊系統的推廣速度一直非常緩慢，則是受到醫生固有文化及相關醫療法規修訂等結構性因素的影響（Bemmel et al，2000；Tang & Hammond，2000；Latimer，2000）。

至於國內的發展情況，除了在本報告前言所提及的發展之外，因應全民健保之論病例計酬、且申報查驗項目逐年增加的制度，國內的醫學中心亦試圖在不增加多餘的人力及經費之情況下，將論病例計酬

作業融入個別機構原有的資訊系統之中（謝森松等，1999）。亦有個別醫療院所，如台北馬偕、淡水馬偕、台北市立萬芳醫院已安裝測試緊急醫療網重症病患電子病歷轉診系統，透過網際網路以提供醫療人員立即需要的臨床資料（黃柏榮、劉建財、張國頌，1999）。綜上，國內現階段醫療資料的資訊化仍以發展行政系統為主，應用於臨床醫療服務的資訊系統則仍多在實驗或起步階段。

第三章　研究方法

本研究主要在檢視國內之醫療院所之資訊人員之專業倫理，利用問卷調查的形式了解資訊人員對於資訊安全原則重要性之認知、態度、實際操作上的現況等。因此本研究採取問卷調查法，以醫院為抽樣單位，藉此對樣本醫院內之醫療資訊工作人員進行意見調查。

根據衛生署的統計，截至民國 86 年底，台灣地區的公私立醫院共計有 750 家，以上所提及的醫療院所即為本研究之母體。其中醫院又依其歸模大小分為醫學中心，區域醫院，地區教學醫院及地區醫院等四級，以 84 至 86 年度的醫院評鑑合格結果來看，醫學中心(含準醫學中心)共計有 13 家，區域及準區域醫院共有 42 家，地區教學醫院有 63 家，地區醫院有 405 家[4]。此外，據健保局的資料顯示，目前全民健保的特約醫事服務機構之特約率已達到 91.83%左右，因此本研究以健保局所公佈的全民健保特約服務機構名冊作為抽樣框架 (sampling frame)進行抽樣。

第一節　抽樣方法

壹、建立醫院調查名冊

在抽樣方法的部份，本研究採用分層比例抽樣的方式來進行，以醫學中心，區域醫院及地區醫院三級作為分層的依據，預計數量約在

[4] 以上的統計數字不含特殊功能及專科醫院，亦不含中醫醫院，"評鑑合格"是指"合格期效三年"。

100 家醫院左右，再依各院資訊人員比例之不同，決定 1067 份樣本，以達成 95%信心水準與 3%可容忍誤差。首先就抽樣框架（sampling frame）進行整理，依據醫院層級重新分層，將醫學中心與準醫學中心為第一層，區域醫院與區域教學醫院為第二層，地方醫院與地方教學醫院為第三層；其次依照地理區域將醫事機構劃分為北（新竹以北與宜蘭）、中（苗栗以南至雲林以北）、南（嘉義以南至屏東，包含澎湖）、東（花蓮與台東）四區；最後再依據各種規模醫院數量的不同，依比例抽出調查的醫院。第一輪抽出醫學中心 4 家（北區 1 家、中區 1 家、南區 1 家、東區 1 家），區域醫院 11 家（北區 5 家、中區 2 家、南區 3 家、東區 1 家）、地方醫院 85 家（北區 25 家、中區 25 家、南區 33 家、東區 2 家）。另外研究者亦將特殊專科（教學）醫院剔除在名冊之外，以達到研究母群之一致性。

貳、確認人員調查樣本

研究者依據名冊上所登記的連絡電話，與各家醫院內負責病歷資料與資訊電腦業務之相關主管連絡，說明研究目的與意願後，確認該醫院在病歷與資訊部門各有多少位專職的工作人員，研究者寄出符合數量的標準格式說明稿與調查問卷。在確認欲調查之醫院時，研究者以衛生署公文與傳真問卷與說明稿方式增加醫院對此研究之重視與可

信度。連絡過程中，若有無法連絡不到其負責主管或不願 配合研究之情況，研究者持續連絡三次後，確認該醫院無法接受調查。研究者從抽樣框架中依選取下一家醫院以補足第一輪抽樣數量。

利用電話調查決定第一輪抽樣為 100 家醫院，並寄發 985 份問卷後，發現未達到研究預定樣本數。因此，研究者依據各層比例再增加第二輪抽樣名單：區域醫院 2 家（北區 1 家、南區 1 家）、地方醫院 13 家（北區 4 家、中區 4 家、南區 5 家）共 155 份樣本。其確認樣本方式則依照第一輪電話調查；樣本數總計為 1140 份。

第二節　問卷設計與調查

壹、問卷設計

研究者依據研究目的，參考國內外該領域之學術文獻與調查與利用深度訪談了解國內醫療院所對其病歷資料的看法與現況設計問卷。此問卷為不計名自填式問卷，以提高受訪者回答問卷之意願。本問卷包含四部份，第一部份欲調查受訪者的從事部門、職務、年資、學歷等人口特質；第二部份調查醫院病歷資料資訊化程度與資訊安全措施；第三部份調查受訪者對於一般資訊工作守則、專業倫理、醫療專業隱私及資訊專業隱私的認知程度；受訪醫院之資訊工作人員另外增加第四部分－醫院資訊系統與病歷資訊安全現況調查，一般如病歷室工

作人員則無需填答此部分問題。問卷設計完成後，更先在各級醫院中委請 2 家醫療院所之資訊室同仁協助進行前測（pretest）的工作，待前測進行完成，再依據前測受試者的意見對於問卷內容加以修訂，以期完成更準確的調查問卷。

其次，在問卷第三部份對於受訪者之一般資訊工作守則、專業倫理、醫療專業隱私及資訊專業隱私認知程度之計分方式係採李克特式五尺度量表（Likert-scale），5 分表示「非常同意」、4 分表示「同意」、3 分表示「無意見」、2 分表示「不同意」、1 分表示「非常不同意」，以計算受訪者各項認知程度。

另外就增加問卷回覆正確性的考量而言，資料安全問題對於這些受訪者的確具有其敏感性，因此為了增加回答內容的正確性，問卷題目在設計方面將採用假設法（以假設性情境的題型的設計，一方面可以避免受試者主觀意識所造成的誤差，另一方面又可以瞭解受試者對於此一議題的態度）。本方式在 Davis 等人對於醫學生對電腦病歷態度的研究中曾經使用過。

貳、問卷調查

本研究以「郵寄問卷調查」的方式進行，研究者以電話訪問向欲調查之醫院確認問卷數量後，分別以限時掛號寄給該醫院之資訊與病

歷部門之主管或連絡人。均附上限時掛號之回郵信封以便受訪者方便寄回，以提高回覆率。

研究者郵寄問卷後兩週，依據 Dillman（1978）針對提升郵寄問卷回覆率所運用的 TDM（Total Design Method）問卷調查設計原則進行兩次催覆，以提高問卷回覆率。第一次電話催覆，若有醫院表示未曾收到問卷或短少問卷數量時，研究者予以補寄問卷。第一次電話催覆後兩週，進行第二次電話催覆。

第四章　研究發現

第一節　回覆資料整理與受訪者背景分析

壹、問卷回覆資料整理

本研究自民國八十九年一月開始進行郵寄問卷調查，共計以電話連絡確認願意接受問卷調查之醫院 115 家（醫學中心 4 家、區域醫院 13 家、地區醫院 98 家），寄出 1140 份問卷。有 82 家醫院回覆問卷，總共回收 566 份有效問卷。醫院回覆率為 71.30%（醫學中心回覆率 100%、區域醫院回覆率 84.62%、地區醫院回覆率 68.37%），問卷回覆率為 49.65%（醫學中心問卷回覆率 51.85%、區域醫院問卷回覆率 47.81%、地區醫院問卷回覆率 49.90%）。

另外，研究者根據問卷資料性質加以整埋，以便進行統計分析。首先，所有受訪者共同回答部分計有 1.背景資料；2.醫院病歷資料資訊化及安全保護措施現況；3.專業倫理、一般資訊工作守則；4.醫療資訊隱私與 5.病歷資料外洩之處置等五個部分。其次，資訊人員則增加回答醫院資訊系統與病歷資訊安全現況部分的問題。再者，為了計算醫院整體資訊安全指數以及了解各醫院之病歷資料資訊化程度與資訊安全措施，故研究者以醫院為研究分析單位，自問卷中篩選出各醫院之行政主管或是職務較資深者來反映醫院現況，並獨立做為病歷資

料資訊化程度與資訊安全措施現況分析之用。

貳、受訪者背景資料分析

就醫院所屬地區而言，在 566 位受訪者中以北部地區 207 位最多，佔 36.6%；其次為南部地區，共計回覆 179 位、佔 31.6%；再次為中部地區 163 位、佔 28.8%；而東部地區回覆人數僅佔 3%，共計 17 位。就醫院等級言，來自地區醫院之受訪者最多，共計 257 位，佔 45.4%；醫學中心與區域醫院之受訪者回覆非常接近，分別為 154 及 155 位，樣本比例分別為 27.2%與 27.4%。在職務分類上則以「事務工作人員」最多，幾佔樣本之七成、共計 353 位；其次為「資訊專業人員」，共計 96 位，佔 18.5%；「醫療專業人員」計有 23 位、佔 4.4%；另有 8.9%、亦即 46 位回覆之受訪者職務為「行政主管」。在人員屬性上，依據前述定義，42.9%的受訪者為「資訊人員」，共計 243 位；「非資訊人員」則為 323 位，佔樣本比例為 57.1%。就性別而言，超過四分之三比例之受訪者為女性，共計 434 位；而男性受訪者計 128 位，佔 22.8%。受訪者平均年齡約為 32 歲，依照人數分佈研究者分成四個子群，其中以 31 至 40 歲者最多，共有 182 位，佔 32.9%；其次有 23.9%受訪者年齡為 25 歲以下，共計 132 位；26 至 30 歲之受訪者則佔 23.7%，共 131 位；而 41 歲以上的受訪者亦有 108 位，佔樣本的

19.5%。受訪者學歷以專科為最多，共計 247 位、佔 43.8%；其次為高中職以下，共計 211 位、佔 37.4%；而 18.8%（106 位）受訪者為大學以上學歷。最後，近四成受訪者所畢業科系為醫護相關科系，共計 180 位；商管相關科系畢業者次之，共計 137 位，約佔三成；資訊相關科系畢業者則佔兩成左右，共 95 位；其它文法及理工相關科系畢業者約各佔 6%，均不超過 30 位（詳見表 1）。

第二節　醫院病歷資料資訊化及安全保護措施分析

壹、病歷資料資訊化及安全保護措施現況

就 82 家受訪之醫院來看，超過九成的醫院對於求診病患之「個人背景資料」、「掛號記錄」、「用藥記錄」均已資訊化；「診療記錄」資訊化的醫院比例也超過 85%；具備資訊化的「病歷轉診流向記錄」者則佔 32.9%；而僅有 10 家醫院具有資訊化的「檢驗或其它記錄」，佔樣本比例 12.2%。

就醫院組織對於病歷資料所採取的保護措施來看，在 73 份有效回覆樣本中，有 57.5%的醫院具備「病歷資料安全政策」，亦有 43.8%的醫院具有「病歷安全委員會」；唯具有「資訊安全強化課程」及「病歷糾紛法律顧問」兩項措施者比例偏低，均僅佔 27.4%（詳見表 2）。

貳、病歷資料資訊化及安全保護措施與醫院組織交叉分析

若以醫院層級與病歷資訊化程度進行交叉分析，醫學中心與區域醫院具有「病歷轉診流向記錄」之比例分別為 50%及 63.6%；均遠超過地區醫院之 26.9%，其差異並達顯著水準。其餘五種病歷資料記錄資訊化程度之比較差異則未達顯著水準（詳見表 3）。另外若以醫院層級與病歷資料保護措施進行交叉分析，醫學中心與區域醫院具有「病歷糾紛法律顧問」之比例也較地區醫院來得高，分別為 75%及 54.5%；地區醫院具有「病歷糾紛法律顧問」之比例則僅為 19%。除了「病歷糾紛法律顧問」之交叉分析達顯著水準外，其餘如病歷安全政策等項之比較均未達顯著水準（詳見表 4）。

參、小結

從受訪者回覆結果可以發現，國內醫療機構之醫療資料資訊化以行政相關功能系統之資訊化程度較高。與醫療行為相關的如檢驗報告等系統則資訊化程度較低。值得注意的是超過八成五以上之受訪者表示其所屬醫院已有資訊化之診療記錄系統，這應與配合全民健保相關論病例計酬之申報規定有關。唯診療記錄內容可說範圍十分廣泛，在不同醫療單位內對於診療記錄之記錄方式、用途與內容精細度要求等可能不盡相同，在本研究中並無法再深入細究。

在組織政策方面，「資訊安全課程」及「病歷糾紛法律顧問」是較少實行之作為。其中地區醫院具備「病歷糾紛法律顧問」者更不及二成，此一政策差異，應與組織規模有關。規模較大的醫療院所一則較具財力，二則由於診療人數較多，發生病歷糾紛之機會也為之較高，所以對法律顧問的需求也比較高。

第三節　受訪者專業倫理、一般資訊工作守則與醫療資訊隱私態度分析

壹、受訪者專業倫理、一般資訊工作守則及醫療資訊隱私認知概況

受訪者專業倫理、一般資訊工作守則及醫療資訊隱私認知程度均採李克特式五尺度量表（Likert-scale）計分，同時問卷內反向問題之計分已轉換與其它正向問題一致。換言之，分數最高為五分、最低為一分，受訪者得分越高，表示受訪者對於專業倫理、一般資訊工作守則及醫療資訊隱私認知程度越高，反之則越低。

一、受訪者專業倫理、一般資訊工作守則概況

在專業倫理及一般資訊工作守則分析共分為四個指標：一般資訊工作守則（general usage）、資訊安全威脅認知（security threat awareness）、專業倫理（profession ethics）、不當洩露資訊（improper exposure）等四項。受訪者平均數以「專業倫理」最高，在五尺

度力氏量表平均數中達 4.45、其次「不當洩露資訊」之平均數為 3.83，「一般資訊工作守則」與「資訊安全威脅」認知兩項則較低，平均數都是 3.77（詳見表 5）。

二、受訪者醫療資訊隱私態度概況

在受訪者醫療資訊隱私認知部分，共分為五項指標：「資料敏感度」（sensitivity）；「用途」（purpose）；另外依據人員與病歷資料之關係（relationship）再細分為「院內相關人員」、「直接相關產業」、「其它間接相關行業」等項。

受訪者整體而言，均有相當程度之醫療資訊隱私之認知與了解，但個別指標部分仍有差異。首先在「資料敏感度」部分，受訪者對於高敏感度資料之隱私認知較低敏感度資料高，其平均數為 4.15，而低敏感度資料問題之平均數為 4.07。其次在「用途」部分，受訪者對於「研究用途」得分平均數為 4.43、「商業用途」得分平均數則為 4.46，二者差異不大。在院內相關人員方面，受訪者對行政人員之醫療資訊隱私認知較醫生為高，其得分平均數分別為 4.09 與 3.47。換言之，相較於行政人員而言，受訪者較願意將病歷資料給予醫生。至於在院外之相關產業方面，受訪者對於業務與病歷資料具直接相關的藥廠及保險公司二者之得分平

均數非常接近，藥廠為 4.45、保險公司則為 4.43。然而就其它相關行業來說，受訪者對於大學教授之醫療資訊隱私認知得分平均數為 3.79，但對於電視台人事部門之得分平均數為 4.43。換言之，受訪者較易將病歷資料給予從事學術研究的大學教授，但是對於間接相關的電視台人事部門則和藥商、保險公司二個直接相關產業則是具有較高的隱私認知（詳見表 6）。

貳、受訪者專業倫理、一般資訊工作守則及醫療資訊隱私態度與受訪者人口背景之交叉分析

一、受訪者專業倫理、一般資訊工作守則與人口背景資料交叉分析

就受訪者人口背景與其專業倫理及一般資訊工作守則進行單因子變異數分析比較的結果來看（如表 7），在人員屬性方面，資訊人員在「資訊安全威脅認知」及「不當洩露資訊」二項指標之得分平均數均較非資訊人員來得高，其差異並達顯著水準，資訊人員之得分平均數分別為 4.02 及 3.95，而非資訊人員則為 3.58 與 3.75。

以醫院層級而言，僅「一般資訊工作守則」一項差異達到顯著水準，以醫學中心得分平均數 3.68 為最低，其次為區域醫院 3.72，地區醫院 3.85 最高。而在職務上四項指標之差異皆達顯著水準

，資訊專業人員與行政主管對於「資訊安全威脅認知」及「不當洩露資訊」二項得分平均數較高，均超過 4 分，而另二類工作人員得分平均數則低於 4 分。在「專業倫理」一項之得分平均數都非常高，其中資訊專業人員、事務工作人員、醫療專業人員三者得分在 4.20 至 4.40 之間，行政主管則略高於其它工作人員，得分平均數達 4.68。然而在「一般資訊工作守則」項則是行政主管與事務工作人員得分平均數較高，分別為 3.92 與 3.83，醫療專業人員為 3.78，資訊專業人員 3.56 最低。

在學歷與性別二部分均有三項指標差異達顯著水準。教育程度越高者在「資訊安全威脅認知」及「不當洩露資訊」二項得分平均數越高，大學以上教育程度者得分平均數二項超過 4 分。而「一般資訊工作守則」則是高中以下及專科二者之得分平均數比大學以上程度要高，分別為 3.80 及 3.81 及 3.62；男性在「資訊安全威脅認知」及「不當洩露資訊」二項得分平均數較女性高，男性得分平均數為 4.20、3.98；女性得分平均數為 3.64 及 3.80。而女性在「一般資訊工作守則」部分之得分平均數（3.81）較男性（3.65）為高。

在畢業相關科系與年齡二部分則是僅有二項指標之差異達顯

著水準。資訊相關科系及理工相關科系二者在「資訊安全威脅認知」的得分平均數較高，分別為 4.10 及 4.02，醫護相關科系者 3.77 次之，商管與文法相關科系者 3.66 與 3.67 則最低；至於「一般資訊工作守則」反倒是醫護相關科系得分平均數 3.91 最高，商管與文法相關科系者 3.79 與 3.76 次之，理工與資訊相關科系得分平均數 3.65 及 3.55 最低。在年齡部分則是年齡較低者之得分平均數較年長者為低，25 歲以下者在「一般資訊工作守則」及「資訊安全威脅認知」之得分平均數分別為 3.70 及 3.53，二者均為最低，26 至 30 歲 3.72 及 3.79 次之，31 至 40 歲及 41 歲以上二子群之得分平均數雖然走向不完全一致，總的來說得分平均數仍較年輕者高。

二、受訪者醫療資訊隱私認知與人口背景資料交叉分析

就受訪者醫療資訊隱私認知與人口背景資料進行單因子變異數分析之結果（如表 8）。首先在資料敏感度上，資訊人員與非資訊人員在「低敏感度資料」之隱私認知有差異（4.12 及 4.03）；在資料用途則是資訊人員與非資訊人員在「研究用途」之隱私認知有差異（4.48 及 4.38）；在直接相關產業上，資訊人員與非資訊人員則是在「藥廠」之隱私認知有差異（4.52 及 4.40）；在

間接相關產業上，資訊人員與非資訊人員則是在「大學教授」之隱私認知有差異（3.93 及 3.68），以上差異均以資訊人員得分較高，並均達顯著水準。同時，無論資料敏感度高低，醫學中心、區域醫院與地區醫院對其隱私認知有差異；在院內人員方面，無論是醫生或行政人員，醫學中心、區域醫院與地區醫院對其隱私認知均有差異；在間接相關產業方面，醫學中心、區域醫院與地區醫院對於「大學教授」之隱私認知亦有差異。以上差異均以於醫學中心工作之受訪者具有較高隱私認知，區域醫院者次之，地區醫院者最低，其差異均達到顯著水準。

其次，無論資料敏感度、資料用途、院內人員、直接相關產業及間接相關產業等各方面，行政主管與資訊專業人員的隱私認知較高，其差異均達顯著水準。其中除了其它相關產業之「大學教授」一項以資訊專業人員及事務行政人員得分平均數為前二位（4.12 與 3.72）以外，在其餘各項指標上得分平均數均居於前二位；事務行政人員則均次之，醫療專業人員在所有指標之得分平均數都是最低的。另外，無論資料敏感度、資料用途、院內人員、直接相關產業及間接相關產業等各方面，大學以上教育程度之受訪者具有較高之隱私認知，專科教育程度者次之，高中職以下

教育程度者最低，且差異均達顯著水準。亦即教育程度越高，對醫療資訊隱私認知也越高。

再者，在直接相關產業之「保險公司」一項及在間接相關產業的「大學教授」及「電視台」二項指標上，資訊相關科系畢業與理工相關科系畢業者具較高的隱私認知，差異均達到顯著水準；其它醫護、文法、商管相關科系者之得分平均數則均較前二者為低。

最後不論資料敏感度高低，不論院內人員層級，男性受訪者均具較高的隱私認知；另外在間接相關產業的「大學教授」方面，男性亦具較高的隱私認知，其差異均達顯著水準。此外，不論資料敏感度高低，不論院內人員層級，以及在間接相關產業的「大學教授」方面，受訪者年齡越高，在該五項指標的隱私認知也越高，其差異亦均達顯著水準。

參、小結

整體而言，受訪者在「專業倫理」部分的得分表現，是沒有太大差異的，在職務上亦僅看到行政主管是更為重視專業倫理的。而就「資訊安全威脅認知」及「不當洩露資訊」二項則可看到學歷較高、年齡較高、職務為行政主管及資訊專業人員在得分平均數上也較高，尤

其「資訊安全威脅認知」項更可看到男性、資訊或理工相關科系畢業者得分平均數較高，又這些屬性的受訪者在「一般資訊工作守則」上的得分平均數均較低。由此觀之，業務較多，工作規定守則的要求及訓練也較多、較為細緻的醫學中心，其受訪者的「一般資訊工作守則」得分平均數會較低的原因，可能正是由於醫學中心之資訊專業人員的人口背景特性均與上述吻合之故。

另外就醫療資訊隱私認知而言，「用途」及院外的相關產業的差別，對於所有受訪者在醫療資訊隱私認知來說，並沒有太大的差異，均有高度保護隱私的警覺。而「大學教授」可能因身分地位之故，而較為令人接受。其次，醫院層級越高，醫療資訊隱私認知表現也越好；行政主管或因具決策權的關係，在「大學教授」項的得分平均數比其他工作人員來得低，非主管之工作人員亦具高度警覺。教育程度愈高、年齡越高及男性在「資訊敏感度」、「院內工作人員」及「大學教授」三項則較其他屬性的受訪者具有更高的警覺。

第四節　病歷資料外洩處置方式分析

此部分在問卷上係採開放式填答，研究者在譯碼時依其回答內容，歸納為五大類：1.勸阻、2.了解行為原因、3.告知嚴重性（如相關法律規定、侵犯隱私權等）、4.向上級報告、5.取回資料。另外由於從回答中無法完全辨明合併多種行為時，是否一定有其採行先後順序，於是研究者僅以排列組合的方式，窮盡此五類行為所可能出現的組合樣態，若受訪者回答中有提及多類行為處置時，譯碼時均不考慮其因果或先後次序關係，而以「採用該行為與否」為歸納整理之依據。

壹、受訪者病歷資料外洩處置行為概況

就處置行為種類而言（如表 9），有 50%受訪者遇到同事將病歷資料外洩給健康食品公司及 50.8%的受訪者遇到同事將名人病歷資料外洩給雜誌社時會「向上級報告」；其次為「勸阻」，分別為 11.3%及 10.5%之受訪者會採取此類處置行為；再次為「勸阻＋向上級報告」，分別為 9.6%及 9.7%；再次則為「告知嚴重性」，分別為 7.5%及 7.3%；其後依序為「勸阻＋告知嚴重性」、「告知嚴重性＋向上級報告」、「向上級報告＋取回資料」等不同組合方式。而僅一成左右受訪者會採取其它組合、三種以上或是其它種類的處置行為。此外，兩種不同的病歷資料外洩狀況在處置行為上的採用比例趨勢是相同的。

因此以下分析將合併處理。

貳、受訪者病歷資料外洩處置行為與人口背景資料交叉分析

就受訪者病歷資料外洩處置行為與人口背景資料進行單因子變異數分析結果，僅醫院等級的差異達到顯著水準。有 65%以上於醫學中心工作的受訪者在病歷資料外洩處置行為上以「向上級報告」為主，所佔比例高於在地區醫院工作的受訪者（五成左右）以及於區域醫院工作之受訪者（四成左右）；而採取「勸阻」或「告知嚴重性」行為的受訪者，以在地區醫院工作為最多，為 20%以上。而採取「二種以上及其它行為」的受訪者，則是以於區域醫院工作者為最多，比例超過 40%。

參、小結

總體來說，在組織層級較明確的醫學中心裡的受訪者較會循行政管道來處理病歷資料外洩行為，而在組織較為鬆散、分工較為模糊的地區醫院的受訪者則是比較會用個人管道來因應，而界於二者之間的區域醫院的受訪者，其處置行為也比較多樣化。這一點是相當有趣的發現。

第五節　醫院資訊系統與病歷資訊安全現況分析

壹、醫院資訊系統及病歷資訊安全現況

一、病歷資料庫帳號狀態

在 60 家有效回答資訊系統現況的醫院中，有 66.7%的醫院在帳號管理的部分是以個人帳號管理，其次 15.0%以不同等級或類型的醫療人員來區分管理帳號，1.7%的醫院是所有工作人員共用單一帳號。有 3.3%與 13.3%的醫院在管理帳號部份並未設立帳號與無任何措施，詳見表 11。而在因應緊急狀況之優先密碼部份，僅有 8.1%的醫院有設置。在使用各種資訊科技（如：ID 磁卡或密碼等）控制讀取病歷資訊部份，有 72.9%的醫院有使用某一程度資訊科技來控制管制。

二、管制病歷室與資訊室部份

有 19.0%的醫院會使用如 ID 磁卡或密碼等資訊科技管制病歷室的進出；有 62.1%的醫院仍使用傳統方式（如：警衛或特定留守值班人員等）管制病歷室的進出；有 19.0%的醫院並無任何措施。至於在資訊室管制的部分，有 38.2%的醫院會使用資訊科技管制資訊室的進出；有 47.1%的醫院仍使用傳統方式管制資訊室的進出；而有 14.7%的醫院並無任何措施。

三、電腦間網路連線狀態

有 77.8%的醫院採用封閉網路，不與外界相連。有 9.3%的醫院採取開放式網路。有 13.0%的醫院在此方面無任何措施。僅有 6.6%的醫院會架設防火牆。有 19.3%的醫院在儲存病患資料的過程有加密編碼的措施；有 5.3%的醫院在傳輸病患資料的過程有加密編碼的措施。

四、儲存備份病患資料狀態

有 51.8%的醫院在儲存病患資料有多重備份或分散備份的措施，42.9%的醫院只有單一系統備份的措施，有 5.4%的醫院無任何備份措施。

五、檢核資訊系統安全現況

有 33.3%的醫院有預防資訊系統入侵方案，31.6%的醫院會評估資訊系統安全弱點，僅有 7.0%的醫院會模擬演練系統入侵狀況，有 29.8%的醫院會淘汰不合標準的安全技術。

貳、醫院資訊系統及病歷資訊安全與醫院組織交叉分析

若以醫院層級與醫院資訊系統現況進行交叉分析。在電腦間連線狀況中具有開放網路之比例達到顯著水準（詳見表 12），也就是說，地區醫院與區域醫院多屬封閉式網路，醫學中心則是在開放式網路的

比例多於其它醫院。若以醫院層級與檢核資訊系統安全措施進行交叉分析。醫學中心與區域醫院會有「預防資訊系統入侵方案」之比例較地區醫院來得高，分別為 100.0%與 50.0%；地區醫院會有「預防資訊系統入侵方案」僅為 25.5%，達到顯著水準。醫學中心與區域醫院會「評估資訊系統安全弱點」之比例較地區醫院來得高，分別為 75.0%與 50.0%；地區醫院會「評估資訊系統安全弱點」僅為 25.5%，達到顯著水準。另外，在「模擬演練系統入侵狀況」方面，醫學中心之比例為 50.0%，較區域醫院與地區醫院來得高，分別為 0.0%與 4.3%，達到顯著水準。在「淘汰不合標準的安全技術」方面，醫學中心之比例為 100.0%，較區域醫院與地區醫院來得高，分別為 33.3%與 23.4%，達到顯著水準。其餘如備份病患資料等，均未達到顯著水準。

參、小結

從回覆結果發現，國內醫院資訊系統現況，已經使用某一程度的資訊科技在管制醫院資訊系統。但仍以資訊部門為主，其餘如病歷室等傳統部門，則資訊化程度較低。當病患資料逐漸資訊化時，醫院組織會越重視資訊系統，但是反而忽略傳統病歷資料的硬體管理部份，也是需要資訊科技的管理。在電腦連線部份，絕大多數醫院採用封閉式網路，一則可能是無病歷交換的需求，因此無須在增加不必要的風

險之下，採取開放式網路；再則可能是受限於組織規模與財務狀況，無法架設與維持開放網路架構。至於採用開放式網路的醫院則多為醫學中心等級或區域醫院中甲類評鑑的醫院。一方面或為因應衛生署未來政策發展之遠端醫療需求而已經完成架設準備；二來可能由於組織本身規模已達到某一程度，在具有一定之資訊安全維護能力下架設開放式網路。

在檢核資訊系統安全方面，「預防資訊系統入侵方案」與「評估資訊系統安全弱點」是醫學中心與區域醫院已能夠實行的措施。另外，「模擬演練系統入侵狀況」與「淘汰不合標準的安全技術」之措施，僅有醫學中心等級醫院才有此方面之措施，區域醫院與地區醫院均較少實行。此措施差異，應和醫院組織規模有關，需要更先進的技術與經費要求才能進行。

第六節　醫院整體資訊安全指數之建構

由前述之研究文獻回顧可發現，欲評估醫療資訊的安全性，除了從硬體設備層面來衡量之外，相關資訊工作人員的專業素養等層面亦必須加以考量。研究者透過問卷調查之結果，進一步建構出一套醫院整體資訊安全指數，以評估受訪國內醫療院所的資訊安全狀況。

壹、醫院整體資訊安全指數現況及分析

醫院整體資訊安全指數包括四部份：整體醫院資訊隱私認知、整體醫院醫療隱私認知、醫院病歷資料資訊化程度與醫院資訊安全措施。其中整體醫院資訊隱私認知、整體醫院醫療隱私認知係以該醫院全體受訪者之認知平均數為準；醫院病歷資料資訊化程度與醫院資訊安全措施則是以醫院代表問卷之填答狀況為準。在扣除 10 家並沒有任何人員回覆醫院資訊系統與病歷資訊安全問題之醫院後，針對其餘 72 家醫院，利用 Hierarchical Cluster 分析，將醫院整體分數由高至低分成四群，分別代表高度安全、中高度安全、中低度安全、低度安全。分析結果顯示，高度安全醫院共計 15 家，佔 20.8%；有 26.4%（19 家）醫院屬於中高度安全等級；至於中低度安全醫院則有 35 家，佔 48.6%；而低度安全醫院有 3 家，佔 4.2%（詳見表 13）。若以醫院層級與醫院整體資訊安全指數進行交叉分析，發現醫學中心大多屬於中高度安全以上等級，地區醫院則大多屬於中低度安全等級（詳見表 14）。

貳、小結

從分析結果可發現國內醫院的在整體資訊安全表現上，有其待加強的部份。值得注意的地方在於醫學中心與部份的區域醫院均有較高的整體安全分數，而地區醫院可能在「醫院病歷資料資訊化程度」與「醫院資訊安全措施」得分上比醫學中心較低，導致絕大多數的地區醫院均落在中低度安全群中。其原因可能在於地區醫院並無能力架構同醫學中心等級的資訊安全硬體設備，或是在組織編制或醫院規模上無法達到同醫學中心等級的病歷資訊資訊安全措施。相較之下，醫療從業人員的資訊隱私認知及醫療隱私認知等在整體醫療安全指數表現上，便沒有看到顯著的醫療層級上的差異。

第五章　結論與建議

第一節　研究結論

目前國內醫院的電腦化的確已經達到一定程度，但不代表所有醫院均能夠順利地達到醫療資料資訊化（如電子病歷）的程度，兩者之間仍有落差，現階段我國與世界其它各國之醫療資料資訊化程度相仿，亦為提供行政用途為主。只有醫學中心或部份醫療評鑑甲等的區域醫院有能力達到電子化病歷的要求，並且擁有預防入侵的資訊技術。其次，無論醫院規模層級，絕大多數管理病歷資料或資訊系統人員，對於病歷資料做不符合醫療用途的行為均有所警覺，但在後續處置措施方面較為模糊不清。另外，受訪者就「人員與病歷資料之關係」及「資料敏感度」有不同程度的隱私認知，「資料用途」則沒有明顯的隱私認知差異。醫院組織不光只是要擁有保護病歷資訊安全的政策措施，應從病患角度來考量組織在此議題上的責任為何，才能讓組織訂出真正保護病患隱私的政策措施。

壹、就組織層面而論

整體來說，受訪者中資訊專業人員在專業技術上有較高的隱私認知，但在一般資訊工作隱私上則比其他醫療人員不注重，而其學歷越高、年齡越低有更顯著的差異。因此在加強資訊安全在職教育方面，提高專業技術並非是最為優先措施，反而需要強化一般資訊專業素養

，強調病歷資訊的洩露不光只是來自於技術層面的入侵，而是更有可能來自於不經意或不當的使用習慣而使病患資料有洩露的危險。另外，學經歷是醫護相關背景出身的醫療人員，在不當曝露病患資訊後行為處置與認知層面有明顯的落差，醫院應該明訂洩露病患資料後所欲採取的危機處理措施。在非正式的教育訓練，醫院或主管應該營造良好的組織文化，對病患隱私權的尊重與給予病患良好的治療是同等重要的。

醫院應該對病患資料安全的保護，提出明確的政策宣示，讓病患了解其對自身資料具有部份的自主權，從此過程中產生責任。讓病患明白那些人可以接觸到他們的資料，以何種目的用途而需要查閱其資料，資料中的那些部份可被何種醫療專業人員所查閱，進而能夠達到約束醫院對病患醫療資料負起應盡之保密責任。

另外，詳細規定院內醫療專業人員或診間調閱病歷的標準程序也有其必要。如此方能提供醫院管理病患資料人員一個客觀依據，避免病歷資料因為不經意的情況而有洩露的危險。同時當侵害病患隱私事件發生後，醫院組織能夠明確、快速的反應機制來界定責任、作出人員處分或是求償等行為處置。

貳、就技術層面而論

在運用醫療資料資訊系統的同時，醫院應當滿足基本的資訊安全技術需求，如獨立使用者權限、加強病患資料的安全防護與備份復原能力與有能力進行評估資訊系統安全，另外為了因應未來的醫療需求環境，資訊系統要具有容易擴充或轉換至新標準的彈性。

醫院除了應將符合基本資訊安全技術標準視為最基本的要求之外，還需考慮該醫院在當地所扮演的醫療角色而做其他部份的增強。區域醫療系統與地區醫院聯盟系統的醫院所欲加強的安全技術需求必定與大型醫學中心有所不同，甚至連設計理念亦會因病患在聯盟之間診療分工模式的差異，而與大型醫學中心迥然不同，如此自然不能以單一制度化標準要求所有醫院遵循，應能因地、因醫院層級制宜，設計出不同模式的安全技術標準。

第二節　未來發展建議

壹、建議醫療組織立即達到的安全事項

在資訊科技逐漸被廣泛運用在醫療組織的情況下，眼前首要課題便是提昇醫療資料的安全性，所有已將病患資料資訊化的醫療組織，無論規模大小均應該接受適當的技術與組織層面保護病患資料安全的措施。

一、組織政策層面

在組織政策部分，目前國內醫療組織需要優先強化的安全事項，可分為下列五個部分：

（一）有明確的保護病患資料安全與機密的政策：明確地指出資料用途、不同人員或產業等之授權使用與資料保護之範圍；

（二）設立保護病患資料安全與機密方面的委員會：具備正式的人員編制在資訊安全的維護上能夠事半功倍；

（三）明訂病患資料洩露所因應的危機處理守則：使得相關工作人員遇到危機時能有統一的處理模範得以依循；

（四）加強一般資訊安全素養之教育與訓練方面的課程：以增進工作人員的相關知識與專業素養；

（五）制訂明確的處分機制：醫療資訊安全是不容輕忽的，確立一處分機制能更加惕厲工作人員注意維護醫療資訊安全；

二、技術方面

在資訊技術部分，目前國內醫療組織需要優先強化的安全事項，可分為下列四個部分：

（一）獨立設置個別使用者權限：方能針對工作人員層級、業務職掌等差異，管制其醫療資料之使用範圍；

（二）加強管制網路連結：以防範非工作人員之侵入與不當使用醫療資訊；

（三）加強病患資料的安全防護與備份復原能力：方能在電腦病毒入侵破壞能力日益強大趨勢下，提供最基本的資料保護防範措施；

（四）增進整體系統之評估能力：醫療組織本身應常測試自身資訊系統之安全性，並模擬演練各類型入侵破壞或資料毀損時之應變措施，方能有效評估組織之整體資訊安全程度。

貳、政府未來政策發展建議

倘若電子化病歷等醫療資料的資訊化，是未來政策發展趨勢的話，從本研究之結果顯示，政府必須要採取建設基本設施之行動以支持電子化醫療資訊的隱私性與安全性。

一、政府與民間合作研究出醫療資料隱私需求及相符之安全標準：

首先，政府應與醫院、學者、業界合作，以促進與鼓勵公開論壇討論的方式來決定病患的隱私與大多數使用者所需要的醫療資訊需求的適當平衡點。進而達到制訂或修改有關法律以因應未來電子病歷的需要。其次政府應該體認自身的政策發展領導地位，持續進行研究，以決定醫療資訊使用者能夠接觸需要病患身份

資料的程度。同時醫療服務機構應與當地的政府、研究人員、業界合作，建立一套提高醫療資訊使用者對於其隱私自覺與對病患醫療、管理、研究的資訊價值的計畫方案。再者，針對目前全球醫療資訊系統發展所共同遭遇到的診療資料記錄標準化的問題，亦應由政府與民間各界共同合作，將診療資訊系統的包含範圍標準化、資料內容（如用藥、症狀描述等）記錄的標準化。而這些有待解決的問題也應當能夠帶領一系列對於提昇消費者對醫療資訊流動的自覺程度的研究。專業的學術與產業團體應該擴展與持續在其研討會與學術出版品中討論有關隱私與安全等議題上的領導地位。

二、建立第三者運作及監督機制：

政府在推動電子病歷交換技術標準的同時，也須一併提出醫療組織在管理事務上的變動提出適當的建議。例如成立建立一個標準化醫療資訊安全標準小組委員會，發展與更新考慮所有醫療使用者的隱私性與安全性的標準。其組織成員應該與現有已參加醫療資訊議題上的有所區隔。

在病患資料隱私領域中討論與研究進行至某一程度時，發展共同病患認證機構是可行的。但是需要去權衡認證機構在隱私利

害關係上所會造成的衝擊與影響。所有醫療環境下被用來辨識病患與連結病患記錄的方法都應該用以下的隱私判斷準則來衡量。

（一）要有明確定義各種違規與合法聯結病患隱私部份的政策架構。這個架構應該從上述一點討論而得來的。

（二）能幫助認證機構容易聚集起來，但在業務上必須約束不適當的壟斷行為。

（三）它在技術層面上保持單向的程度應該是可行的。它應該是幫助有關病患或病患所提供的醫療記錄容易地從適當的連結中取得，但要小心留意病患的身分證明容易地從不同的認證組織間的連結漏洞中被得知。

三、延伸應用醫療資訊安全標準於醫療相關產業：

政府應該鼓勵資訊安全科技方面的交換與轉移技術到醫療產業。衛生署應與產業領域中的重要組織建立正式的聯繫管道，以讓資訊科技能夠運用在至醫療服務，使醫療方面所運用的資訊科技與其他領域所使用的有所落差。衛生署應該嘗試以不同的方法來合併現有的運作方式，在系統存取控制方面達到廉價而便捷的保證，即使是在緊急情況下也能夠允許連結，而不是尋求需要大量經費的更新方案。

總而言之，目前國內醫療資料資訊化及其應用現況與其它先進國家目前的發展相當接近，所面臨的發展困境亦十分相似，從本次研究結果及醫療安全指數亦可看出，目前國內醫療機構的醫療資訊安全表現均有待提昇，而就安全技術標準與診療資料標準化的問題亦有待政府、醫療院所及學術界三方面共同努力，以追求一個具隱私保障且兼顧資訊需求的醫療資訊應用環境。

參考文獻

中文部分

王郁琦：「電腦處理個人資料保護法」與個人資料的商業利用，資訊法務透析，民國 85 年 3 月，第 37 至 41 頁。

王郁琦：NII 與個人資料保護，資訊法務透析，民國 85 年 1 月，第 35 至 41 頁。

王郁琦：網路上的隱私權問題，資訊法務透析，民國 85 年 10 月，第 37 至 45 頁。

行政院衛生署，中華民國公共衛生概況，民國 87 年。

宋餘俠：資訊化社會隱私權維護向前邁進一步，資訊與電腦第 139 期，民國 81 年 02 月，頁 16-18。

李麒麟：資訊安全「管理」與「實施」之深層研議(一)：技術是一回事,然真正實施與管理則又是一回事，自動化科技 152 期頁 46-，自動化科技雜誌社，民國八十七年十二月。

李麒麟：資訊安全「管理」與「實施」之深層研議(二)：資訊安全"止"於落實安全計劃、規範與措施，自動化科技 153 期頁 42-，自動化科技雜誌社，民國八十六年元月。

邱光輝：資訊安全的基本素養，資訊與教育第 40 期， 民國 83 年 4 月，頁 25-30。

柯少齋譯：美國資訊自由及隱私權法案，新聞學研究第 46 期，民國 81 年 09 月，頁 21-34。

徐建業、李彥良、王毓麒、李友專、謝逸中：以 World Wide Web 為基礎之診間醫令系統，國際醫學資訊研討會 1999 年 10 月。

財團法人金融聯合徵信中心編輯委員會：電腦處理個人資料保護法暨相關規定，財團法人金融聯合徵信中心，民國八十五年。

財團法人金融聯合徵信中心編輯委員會：歐洲聯盟網路資料暨隱私保護綱領(草案)，財團法人金融聯合徵信中心，民國八十七年。

張子仁編譯：全球資訊網-安全防護手冊，全華，民國八十七年。

陳同孝：資訊安全中道德教育問題之研究，勤益學報 13 期，民國八十五年二月，頁 337-343。

陳家駿：個人資料在電腦網路上流竄易遭濫用防範未然應及早訂定管理規範，電工資訊雜誌第 72 期，民國八十五年十二月，頁 74-78。

陳家駿：從資訊高速公路--談資訊安全保障及隱私權維護，電工資訊雜誌第 56 期，民國八十四年八月，頁 88-91。

葉賽鶯：「資訊隱私權」之保護--「電腦處理個人資料保護法」-上-，衛生報導，民八十五年六月，頁 29-33。

劉國昌，劉國興編著：資訊安全，儒林，民國八十四年。

樊國楨：網際網路與資訊安全，電腦與通訊 45 期，民國八十四年十二月，頁 39-50。

英文部分：

Appelbaum, Paul S. "Threats to the Confidentiality of Medical Records-No Place to Hide." *Journal of the American Medical Association* 283(6): 795-797, 2000.

Association for Computing Machinery. *ACM Code of thics and professional conduct.* ACM Council, 1992.

Baase, Sara. *A Gift of Fire-- Social, Legal and Ethical Issues in Computing*, NJ: Prentice Hall, 1997.

Bemmel, Jan H., Ginneken, Astrid M. and Lei, J. "A Progress Report on Computer-based Patient Records in Europe." *The Computer-based Patient Record: An Essential Technology for Health Care* , Washington, DC, 1997.

Buckovich, Suzy A. et al. "Driving toward Guiding Principles: A Goal for Privacy, Confidentiality and Security of Health Information." *JAMIA* 6:122-133, 1999.

Castells, Manuel. *The Rise of the Network Society*, Blackwell Publishers,1996 .

Davis, Luke et al. "Attitudes of First-year medical Students Toward the Confidentiality of Computerized Patient Records." *JAMIA* 6(1):53-60, 1999.

Dillman A. D. *Mail and Telephone Survey.* Wiley-interscience Publication 1978.

Dillon, A. "Book Review: Computer and Information Ethics." by J. Weckert and D. Adeney. *Journal of The American Society for Information Science* 49 (9):861-861, 1998.

Gatherer, A. "Book Review: Health Information Ethics." by P.A. Cunniffe. *Journal of Medical Ethics*, 22(6): 365-366, 1996.

Hauptman, R. "Editorial: Information, Technology, and Ethics: Societal Changes." *Journal of Information Ethics*, 7(1): 3, 1998.

Hauptman, R. Book Review: Computer and Information Ethics, by J. Weckert and D. Adeney. *Journal Of Academic Librarianship*, 24(4): 331, 1998..

Haywood, Trevor. "Global Networks and The Myth of Equality: Trickle Down or Trickle Away?" Edited by Loader, Brian D., *Cyberspace Divide-- Equality, Agency and Policy in the Information Society*, 1998.

Information Infrastructure Task Force. *Privacy and The National Information Infrastructure: Principles for Providing and Using Personal Information,*

Final Version, 1995.

Kluge, EHW. "Professional Ethics as Basis for Legal Control of Health Care Information." *International Journal of Bio-Medical Computing* 43(1-2): 33-37, 1996.

Kluge, EHW. "Fostering a Security Culture: A model code of ethics for health information professionals." *International Journal of Medical Informatics*, 49 (1): 105-110,1998.

Laidlaw, Johnson EA. "The Ethics of Information Transfer in The Electronic Age: Scholars Unite!" *Journal of Information Ethics* 5(2): 29-38, 1996.

Latimer, Eleanor W. "The Computerized Patient Record: A Global View." *MD Computing,* http://www.mdcomputing.com/issues/v16n5/cpr.html , 1999.

Lo, Bernard and Alpers, A. "Uses and Abuses of Prescription Drug Information in Pharmcy Benefits Management Programs.", *Journal of the American Medical Association* 283(6):801-806, 2000.

Lo, G., Turek-Brezina, J., Powers, M., Kozloff, R., Faden, R. and Steinauer, D.D. "Privacy and Security of Personal Information in a New Health Care System." *Journal of the American Medical Association*, 270(20):2487-2493, 1993.

National Research Council. *For the Record- Protecting Electronic Health Information.* Institute of Medicine, Washington, DC.: National Academy Press, 1997.

National Research Council. *The Computer-based Patient Record: An Essential Technology for Health Care.* Institute of Medicine, Washington, DC.: National Academy Press, , 1997.

OECD. *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* , 1980.

Saunders, L. "Book Review: The Principles of Information Ethics." by R.J. Severson. *Library Journal* 122 (13):144-144, 1997.

Schuklenk, U., "BookReview: Ethics, Computing, and Medicine - Information and The Transformation of Health Care." by K.W. Goodman. *Health Care Analysis*, 6(3): 269-270, 1998.

Simpson, Roy L. "Security Threats Are Usually an Inside Job." *Nursing Management* 27(12): 43, 1997.

Smith, MM. "Information Ethics." *Annual Review of Information Science and Technology*, 32: 339-366, 1997.

Tang, Paul C. and Hammond, W Ed. "A Progress Report on Computer-based Patient Records in the United States." *The Computer-based Patient Record: An Essential Technology for Health Care* , Washington, DC, 1997.

Wang, Yu-Chi. *Privacy in the Computer Age: Issues Related to Computer Matching and the Internet,* unpublished S.J.D. dissertation, 1997.

表 1：受訪者背景資料表

		次數	百分比（%）
地區	北區	207	36.6%
N=566	中區	163	28.8%
	南區	179	31.6%
	東區	17	3%
醫院等級	醫學中心	154	27.2%
N=566	區域醫院	155	27.4%
	地區醫院	257	45.4%
職務名稱	事務行政人員	353	68.1%
N=518	資訊專業人員	96	18.5%
	醫療專業人員	23	4.4%
	行政主管	46	8.9%
人員屬性	資訊人員	243	42.9%
N=566	非資訊人員	323	57.1%
性別	男	128	22.8%
N=562	女	434	77.2%
年齡	25 歲以下	132	23.9%
N=553	26-30 歲	131	23.7%
	31-40 歲	182	32.9%
	41 歲以上	108	19.5%
學歷	高中職以下	211	37.4%
N=564	專科	247	43.8%
	大學以上	106	18.8%
畢業科系	資訊相關科系	95	20.3%
N=469	醫護相關科系	180	38.4%
	商管相關科系	137	29.2%
	文法相關科系	29	6.2%
	理工相關科系	28	6.0%

資料來源：本研究資料整理。

表 2：受訪醫院病歷資訊化程度與保護措施表

	具備事項	次數	百分比（%）
病歷資料資訊化程度 N=82	個人背景資料	77	93.9
	掛號記錄	81	98.8
	診療記錄	71	86.6
	用藥記錄	75	91.5
	病歷轉診流向記錄	27	32.9
	檢驗或其他記錄	10	12.2
醫院組織保護病歷資料措施 N=73	病歷安全委員會	32	43.8
	資訊安全強化課程	20	27.4
	病歷資料安全政策	42	57.5
	處理病歷糾紛法律顧問	20	27.4

資料來源：本研究資料整理。

表 3：醫院等級與病歷資訊化程度交叉分析表

N %	背景資料		掛號記錄		診療記錄		用藥記錄		病歷轉診流向記錄		檢驗或其他記錄	
	有	無	有	無	有	無	有	無	有	無	有	無
醫學中心	4	0	4	0	4	0	4	0	2	2*	1	3
	100.0	0.0	100.0	0.0	100.0	0.0	100.0	0.0	50.0	50.0	25.0	75.0
區域醫院	11	0	11	0	10	1	10	1	7	4	2	9
	100.0	0.0	100.0	0.0	90.9	9.1	90.9	9.1	63.6	36.4	18.2	81.8
地方醫院	62	5	66	1	57	10	61	6	18	49	7	60
	92.5	7.5	98.5	1.5	85.1	14.9	91.0	9.0	26.9	73.1	10.4	89.6

*$p<0.01$

資料來源：本研究資料整理。

表 4：醫院等級與病歷資料保護措施交叉分析表

N %	病歷安全委員會		資訊安全課程		病歷安全政策		法律顧問	
	有	無	有	無	有	無	有	無
醫學中心	3	1	1	3	3	1	3	1*
	75.0	25.0	25.0	75.0	75.0	25.0	75.0	25.0
區域醫院	7	4	2	9	7	4	6	5
	63.6	36.4	18.2	81.8	63.6	36.4	54.5	45.5
地方醫院	22	36	17	41	32	26	11	47
	43.8	56.2	29.3	70.7	55.2	44.8	19.0	81.0

資料來源：本研究資料整理。

表 5：受訪者專業倫理及一般資訊工作守則表

	次數	平均數
一般資訊工作守則	544	3.77
資訊安全威脅認知	538	3.77
專業倫理	547	4.45
不當洩露資訊	552	3.83

資料來源：本研究資料整理。

表 6：受訪者醫療資訊隱私認知表

		次數	平均數
資料敏感度	低敏感度（健康檢查）	548	4.07
	高敏感度（HIV）	545	4.15
用途	研究用途	548	4.43
	商業用途	550	4.46
院內相關人員	醫生	546	3.47
	行政人員	549	4.09
直接相關產業	藥廠	551	4.45
	保險公司	550	4.43
其它間接相關行業	大學教授	548	3.79
	電視台人事部門	548	4.43

資料來源：本研究資料整理。

表 7：專業倫理及一般資訊工作守則與受訪者人口背景交叉分析表

平均數		一般資訊工作守則	資訊安全威脅認知	專業倫理	不當洩露資訊
人員屬性	資訊人員	3.76	4.02*	4.48	3.95*
	非資訊人員	3.78	3.58	4.43	3.75
醫院層級	醫學中心	3.68*	3.78	4.47	3.83
	區域醫院	3.72	3.76	4.41	3.85
	地區醫院	3.85	3.79	4.47	3.84
職務	事務行政人員	3.83*	3.63*	4.44*	3.75*
	資訊專業人員	3.56	4.19	4.44	4.05
	醫療專業人員	3.78	3.60	4.42	3.33
	行政主管	3.92	4.08	4.68	4.10
學歷	高中職以下	3.80*	3.65*	4.43	3.79*
	專科	3.81	3.74	4.45	3.78
	大學以上	3.62	4.09	4.50	4.06
畢業相關科系	資訊相關科系	3.55*	4.10*	4.45	3.88
	醫護相關科系	3.91	3.73	4.53	3.81
	商管相關科系	3.79	3.66	4.41	3.93
	文法相關科系	3.76	3.67	4.48	3.55
	理工相關科系	3.65	4.02	4.41	3.88
性別	男	3.65*	4.20*	4.47	3.98*
	女	3.81	3.64	4.45	3.80
年齡	25 歲以下	3.70*	3.53*	4.42	3.73
	26-30 歲	3.72	3.79	4.47	3.79
	31-40 歲	3.80	3.94	4.46	3.90
	41 歲以上	3.90	3.82	4.48	3.91

*p<0.01

資料來源：本研究資料整理。

表 8: 醫療資訊隱私認知與受訪者人口背景資料交叉分析表

平均數		資訊敏感度		用途		院內人員		直接相關產業		間接相關產業	
		低敏感度	高敏感度	研究用途	商業用途	醫生	行政人員	藥廠	保險公司	大學教授	電視台
人員屬性	資訊人員	4.12*	4.19	4.48*	4.51	3.53	4.17	4.52*	4.47	3.93*	4.47
	非資訊人員	4.03	4.12	4.38	4.42	3.43	4.07	4.40	4.40	3.68	4.40
醫院層級	醫學中心	4.17*	4.27*	4.50	4.52	3.69*	4.18*	4.51	4.51	4.01*	4.51
	區域醫院	4.08	4.17	4.41	4.43	3.51	4.13	4.43	4.42	3.77	4.42
	地區醫院	4.00	4.15	4.38	4.44	3.31	3.99	4.45	4.39	3.67	4.39
職務	事務行政人員	4.00*	4.09*	4.38*	4.42*	3.37*	4.02*	4.41*	4.39*	3.72*	4.42*
	資訊專業人員	4.14	4.28	4.49	4.53	3.68	4.15	4.49	4.54	4.12	4.47
	醫療專業人員	3.91	3.88	4.25	4.30	3.20	3.83	4.32	4.23	3.30	4.30
	行政主管	4.41	4.37	4.70	4.73	3.62	4.51	4.76	4.66	3.62	4.67
學歷	高中職以下	3.98*	4.07*	4.34*	4.35*	3.40*	3.99*	3.40*	4.35*	3.69*	4.38*
	專科	4.04	4.13	4.43	4.48	3.42	4.04	3.42	4.44	3.80	4.41
	大學以上	4.32	4.36	4.60	4.64	3.74	4.39	3.74	4.60	3.97	4.58
畢業相關	資訊相關科系	4.13	4.30	4.55	4.56	3.60	4.14	4.52	4.60*	4.05*	4.52*
科系	醫護相關科系	4.07	4.13	4.42	4.49	3.39	4.13	4.47	4.43	3.63	4.47
	商管相關科系	4.10	4.19	4.43	4.47	3.57	4.11	4.45	4.45	3.89	4.44
	文法相關科系	4.08	4.05	4.26	4.22	3.72	4.05	4.26	4.22	3.52	4.10
	理工相關科系	4.07	4.24	4.46	4.50	3.67	4.04	4.48	4.50	4.04	4.50

表 8: 醫療資訊隱私認知與受訪者人口背景資料交叉分析表(續)

平均數		資訊敏感度		用途		院內人員		直接相關產業		間接相關產業	
		低敏感度	高敏感度	研究用途	商業用途	醫生	行政人員	藥廠	保險公司	大學教授	電視台
性別	男	4.20*	4.28*	4.51	4.54	3.69*	4.23*	4.54	4.52	3.98*	4.46
	女	4.03	4.12	4.41	4.44	3.41	4.05	4.43	4.41	3.74	4.43
年齡	25 歲以下	3.95*	4.00*	4.32	4.40	3.29*	3.93*	4.39	4.33	3.57*	4.37
	26-30 歲	4.00	4.10	4.44	4.46	3.29	4.03	4.48	4.43	3.79	4.43
	31-40 歲	4.16	4.23	4.48	4.46	3.64	4.19	4.47	4.47	3.96	4.48
	41 歲以上	4.14	4.23	4.41	4.48	3.66	4.18	4.44	4.45	3.72	4.41

*$p<0.01$

資料來源: 本研究資料整理。

表 9：病歷外洩之處置行為樣態表

	資料外洩至健康食品公司		名人資料外洩至雜誌社	
	次數	百分比	次數	百分比
向上級報告	221	50.0	222	50.8
勸阻	50	11.3	46	10.5
勸阻+向上級報告	43	9.7	42	9.6
告知嚴重性	33	7.5	32	7.3
勸阻+告知嚴重性	20	4.5	22	5.0
告知嚴重性+向上級報告	14	3.2	19	4.3
向上級報告+取回資料	14	3.2	12	2.7
多種及其它處置行為	47	10.6	42	9.6
總和	442	100%	437	100%

資料來源：本研究資料整理。

表 10: 病歷外洩處置與受訪者人口背景資料交叉分析表

百分比		行為模式					
		病患醫療資料交與健康食品公司之處置			名人醫療資料交與雜誌社之處置		
		向上級報告	單一行為(勸阻或告知嚴重性)	二種以上及其它行為	向上級報告	單一行為(勸阻或告知嚴重性)	二種以上及其它行為
人員屬性	資訊人員	55.8	17.3	26.9	55.6	17.3	27.0
	非資訊人員	45.7	20.0	34.3	47.3	18.3	34.4
醫院等級	醫學中心	66.4	16.0	17.6*	65.8	16.2	17.9*
	區域醫院	42.3	14.6	43.1	39.8	14.6	45.5
	地區醫院	45.5	23.0	31.5	49.2	20.8	29.9
職務	事務行政人員	48.4	19.4	32.2	49.6	17.5	32.8
	資訊專業人員	59.0	17.9	23.1	57.7	19.2	23.1
	醫療專業人員	43.8	18.8	37.5	37.5	18.8	43.8
	行政主管	43.9	14.6	41.5	51.2	12.2	36.6
學歷	高中職以下	54.5	15.6	29.9	53.7	14.0	32.3
	專科	47.3	21.2	31.5	48.9	20.9	30.2
	大學以上	48.9	18.9	32.2	51.1	17.8	31.1

*p<0.01

資料來源: 本研究資料整理。

表 10: 病歷外洩處置與受訪者人口背景資料交叉分析表(續)

百分比		行為模式					
		病患醫療資料交與健康食品公司之處置			名人醫療資料交與雜誌社之處置		
		向上級報告	單一行為(勸阻或告知嚴重性)	二種以上及其它行為	向上級報告	單一行為(勸阻或告知嚴重性)	二種以上及其它行為
畢業相關科系	資訊相關科系	57.7	17.9	24.4	55.1	19.2	25.6
	醫護相關科系	49.3	16.9	33.8	50.0	16.2	33.8
	商管相關科系	49.0	20.0	31.0	51.5	17.5	30.9
	文法相關科系	54.2	20.8	25.0	62.5	16.7	20.8
	理工相關科系	45.8	20.8	33.3	45.8	25.0	29.2
性別	男	57.0	16.0	27.0	54.5	18.1	31.8
	女	48.4	19.4	32.3	50.1	16.2	29.3
年齡	25 歲以下	46.7	18.7	34.6	44.8	21.0	34.3
	26-30 歲	51.0	17.6	31.4	51.5	17.8	30.7
	31-40 歲	56.6	20.0	23.4	58.0	16.8	25.2
	41 歲以上	41.0	18.1	41.0	43.9	15.9	40.2

*$p<0.01$

資料來源: 本研究資料整理。

表 11：受訪醫院醫療資訊安全措施現況表

		次數	百分比（%）
帳號狀態	擁有個人帳號	40	66.7
N=60	同種人員共同擁有該種帳號	9	15.0
	所有人員共用同一帳號	1	1.7
	無帳號權限	2	3.3
	無任何措施	8	13.3
緊急優先密碼	有	5	8.1
N=62	無	57	91.9
控制讀取病歷資料	使用資訊科技控制	43	72.9
N=59	無任何措施	16	27.1
管制病歷室	使用資訊科技	11	19.0
N=59	傳統方式	36	62.1
	無任何措施	11	19.0
管制資訊室	使用資訊科技	13	38.2
N=34	傳統方式	16	47.1
	無任何措施	5	14.7
電腦間連線狀況	封閉網路	42	77.8
N=54	開放網路	5	9.3
	無任何措施	7	13.0
架設防火牆	有	4	6.6
N=61	無	57	93.4
限制 IP 與網路卡卡號	有	0	0.0
N=61	無	61	100.0
儲存病歷資料加密編碼	有	11	19.3
N=57	無	46	80.7
傳輸病歷資料加密編碼	有	3	5.3
N=57	無	54	94.7

資料來源：本研究資料整理。

表 11：受訪醫院醫療資訊安全措施現況表（續）

		次數	百分比（%）
儲存病歷資料	多重備份	29	51.8
N=56	單一系統儲存	24	42.9
	無任何備份措施	3	5.4
預防系統入侵方案	有	19	33.3
N=57	無	38	66.7
評估系統安全弱點	有	18	31.6
N=57	無	39	68.4
模擬演練入侵過程	有	4	7.0
N=57	無	53	93.0
淘汰更新不合標準技術	有	17	29.8
N=57	無	40	70.2

資料來源：本研究資料整理。

表 12: 醫院醫療資訊安全措施與醫院等級交叉分析表

		帳號					電腦連線			權限控制	
N %		擁有個人帳號	同種人員共同擁有該種帳號	所有人員共用同一帳號	無帳號權限	無任何措施	封閉網路	開放網路	無任何措施	使用資訊科技控制讀取病患資料	無任何措施
醫院層級	醫學中心	4	0	0	0	0	2	2	0*	4	0
		100.0	0.0	0.0	0.0	0.0	50.0	50.0	0.0	100.0	0.0
	區域醫院	7	1	0	1	0	7	1	0	8	1
		77.8	11.1	0.0	11.1	0.0	87.5	12.5	0.0	89.8	11.1
	地區醫院	29	8	1	8	8	33	2	7	31	15
		61.7	17.0	2.1	2.1	17.0	78.6	4.8	16.7	67.4	32.6

*p<0.01

資料來源：本研究資料整理。

表 12：醫院醫療資訊安全措施與醫院等級交叉分析表（續一）

N %		病歷室管制			資訊室管制			儲存病歷資料		
		資訊科技	傳統方式	無任何措施	資訊科技	傳統方式	無任何措施	多重備份	只儲存在單一系統	無任何措施
醫院層級	醫學中心	0	3	0	2	2	0	3	1	0
		0.0	100.0	0.0	50.0	50.0	0.0	75.0	25.0	0.0
	區域醫院	2	7	0	3	3	2	7	2	0
		22.2	77.8	0.0	37.5	37.5	25.0	77.8	22.2	0.0
	地區醫院	9	26	11	8	11	3	19	21	3
		19.6	56.5	23.9	36.4	50.0	13.6	44.2	48.8	7.0

*$p<0.01$

資料來源：本研究資料整理。

表 12：醫院醫療資訊安全措施與醫院等級交叉分析表（續二）

N %	檢核資訊系統								病歷資料加密編碼			
	預防系統入侵方案		評估系統安全漏洞		模擬演練入侵過程		淘汰不合保護標準技術		儲存病歷資料		傳輸病歷資料	
	是	否	是	否	是	否	是	否	是	否	是	否
醫院層級　醫學中心	4	0*	3	1*	2	2*	4	0*	1	2	0	3
	100.0	0.0	75.0	25.0	50.0	50.0	100.0	0.0	33.3	66.7	0.0	100.0
區域醫院	3	3	3	3	0	6	2	4	1	6	1	6
	50.0	50.0	50.0	50.0	0.0	100.0	33.3	66.7	14.3	85.7	14.3	85.7
地區醫院	12	35	12	11	2	45	11	36	9	37	2	45
	25.5	74.5	25.5	74.5	4.3	95.7	23.4	76.6	19.6	80.4	4.3	95.7

*$p<0.01$

資料來源：本研究資料整理。

表 13：醫療資訊安全指數表

		次數	百分比
病歷安全指數	低度安全	3	4.2
N=72	中低度安全	35	48.6
	中高度安全	19	26.4
	高度安全	15	20.8

資料來源：本研究資料整理。

表 14：醫療資訊安全指數與醫院等級分析表

N %		安全等級			
		低度安全	中低度安全	中高度安全	高度安全
醫院等級	醫學中心	0	0	3	1
		0.0	0.0	75.0	25.0
	區域醫院	0	4	3	4
		0.0	36.4	27.3	36.4
	地區醫院	3	31	13	10
		5.3	54.4	22.8	17.5

資料來源：本研究資料整理。

附錄：調查問卷

您好：

這是一份衛生署研究計畫的不具名問卷調查，本問卷是想要了解貴醫院病患資料資訊化的現況，請病歷室或資訊室等能夠接觸病歷資訊的人員回答這份問卷。本問卷所收集到的各項數據與個人資料僅做研究用途，絕不外洩。本問卷只需花費您十分鐘左右的時間，您的回答對於學術研究極具價值。感謝您的參與！

1.請問貴醫院在醫院評鑑中的等級為？

□醫學中心（含準醫學中心）　□區域醫院（含準區域醫院）

□地區醫院（含地區教學醫院）

2.請問您服務的部門是_____；職務名稱是_____。

3.請問您從事現職工作有多久？

□半年以內　□半年至一年之內　□一年至兩年之內　□兩年至三年之內　□三年以上

4.請問您的學歷是？

□國小以下　□國中及初中　□高中　□專科　□高職　□大學　□研究所以上

5.請問您在學校時就讀的科系為？

□資訊相關科系　□醫護相關科系　□商管相關科系　□其他_____

6.請問您的性別是？

□男性　□女性

7.請問您的年齡是？_____歲

下列問題中所指的病患資料泛指一切能指明病患個人身份的資料，其中包括病患的病歷、個人背景等等。下列的問題選項並無優劣高低之分，請您依照您所明瞭的狀況照實勾選。謝謝！

8.就你所知，請問目前貴醫院的病患資料資訊化（利用電腦系統處理）程度？（可複選）

□個人背景資料

□掛號記錄

□診療記錄

□用藥記錄

□病歷轉診流向記錄

□其他與病患相關的資料，請指出_____

□沒有任何病患資料資訊化

□不清楚這方面的狀況

9.就你所知，請問目前貴醫院對於病歷安全的管理措施包括哪些？（可複選）

□有成立專門處理病歷安全的委員會。
□有專職處理病歷資訊化的工作人員。
□定期開辦加強工作人員對於病歷資訊化安全的課程。
□有對於病歷外洩方面的危機處理方案或制度。
□需要提供病患資料給政府、研究單位、業界時，有一套詳盡的方案。
□為了病歷資訊電子化而重新改進管理流程。
□有處理因為病歷資料所引起的糾紛的法律顧問。
□當病患的病歷記錄被調閱時，院方會通知病患。
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

下列是有關資料管理方面的問題，請您依照其陳述內容，回答您的看法。

	非常同意	同意	不一定	不同意	非常不同意
10.當我工作時需要使用別人的電腦，我會等到徵求對方的同意後才會使用。	□	□	□	□	□
11.當我不在位子上時，我會隨手關上電腦或是用密碼鎖住電腦。	□	□	□	□	□
12.我常留意有關電腦軟體出現安全漏洞的相關報導。	□	□	□	□	□
13.我常注意工作場所中的電腦會被病毒感染的問題。	□	□	□	□	□
14.我認為在工作用的電腦上收發私人的電子郵件是可以接受的。	□	□	□	□	□
15.我認為一個資料管理人員應比他人更尊重隱私權。	□	□	□	□	□
16.我認為一個資料管理人員持續維持專業能力是很重要的。	□	□	□	□	□
17.我認為一個資料管理人員是明瞭在這專業領域中的各項相關法律。	□	□	□	□	□
18.我認為一個資料管理人員應能了解所使用的電腦系統，包括系統中可能存在的危險。	□	□	□	□	□
19.我認為一個資料管理人員有責任保護任何病患的資料。	□	□	□	□	□
20.我的同事會常因好奇去查閱病患資料。	□	□	□	□	□
21.我的同事們常會不經地以病患的狀況當做閒聊話題。	□	□	□	□	□

下列故事與您實際醫院工作經驗無關，請您根據下列故事的情境描述，回答下列的問題。謝謝！

希望醫院，除了紙本記錄之外，同時亦有一套完整的電腦資料庫。阿文任職於希望醫院的病歷室，主要負責維護及管理病患的病歷資料。希望醫院的醫生均會將病患每一次的診療結果詳細地記錄在病歷上。有一天阿文遇到.....

	非常同意	同意	不一定	不同意	非常不同意
22.內科的周醫師向阿文要求在下班時間借閱過去一個月至醫院進行健康檢查的患者健診資料。如果你是阿文，你會把患者資料交給周醫師嗎？	☐	☐	☐	☐	☐
23.掛號室的張小姐向阿文要求在下班時間借閱過去一個月至醫院進行健康檢查的患者健診資料。如果你是阿文，你會把患者資料交給張小姐嗎？	☐	☐	☐	☐	☐
24.某保險業者希望推出一套醫療保險計劃，其業務員向阿文要求借閱所有的健康檢查的患診健診資料，以設計保費制度。如果你是阿文，你會把患者資料交給業務員嗎？	☐	☐	☐	☐	☐
25.某保險業者已推出一套醫療保險計劃，其業務員向阿文要求借閱所有的健康檢查的患者健診資料，以推銷該醫療保險。如果你是阿文，你會把患者資料交給業務員嗎？	☐	☐	☐	☐	☐
26.內科的黃醫師向阿文要求在下班時間借閱過去一個月至醫院求診的 HIV 患者病歷。如果你是阿文，你會把患者資料交給黃醫師嗎？	☐	☐	☐	☐	☐
27.掛號室的謝小姐向阿文要求在下班時間借閱過去一個月至醫院求診的 HIV 患者病歷。如果你是阿文，你會把患者資料交給謝小姐嗎？	☐	☐	☐	☐	☐
28.某藥廠為了研究開發治療 HIV 的新藥，向阿文要求借閱全院的 HIV 病患的病歷。如果你是阿文，你會把患者資料交給藥廠嗎？	☐	☐	☐	☐	☐
29.某藥廠已開發出一種治療 HIV 的新藥，為了推銷新藥，其業務員向阿文要求借閱全院的 HIV 病患的病歷。如果你是阿文，你會把患者資料交給藥廠嗎？	☐	☐	☐	☐	☐
30.賈教授為了進行一項氣喘治療方法的學術研究，向阿文要求借閱全院的氣喘病患的病歷。如果你是阿文，你會把患者資料交給賈教授嗎？	☐	☐	☐	☐	☐
31.某大電視台日前結束人才甄選活動，其人事室根據錄取資料向阿文要求借閱已錄取者的病歷記錄。如果你是阿文，你會把患者資料交給電視台的人事室嗎？	☐	☐	☐	☐	☐

32.阿文發現他的同事將一批病患資料交給健康食品公司。如果你是阿文，你會採取什麼行動？（請說明）

_____

33.阿文發現他的同事將某名人的資料交給雜誌社。如果你是阿文，你會採取什麼行動？（請說明）

_____

若您為資訊室（能接觸到病患資料）相關人員請繼續回答下列問題。若您不是，本問卷到此結束，感謝您的參與。謝謝！

34.請問您知道貴醫院是如何管理使用病患資料的帳號？（可複選）

□每位人員均有屬於個人帳號
□特定的人員才擁有個人帳號
□每一種的人員共同擁有屬於該種類人員的帳號
□所有人共享統一的帳號
□有因應緊急狀態的優先密碼
□不特別設立權限
□其他狀況，請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

35.請問您知道貴醫院有使用何種技術控制讀取病患資料的方式？（可複選）

□利用硬體 IC 卡或 ID 磁卡一類來開啟
□利用軟體密碼來開啟
□利用生物或指紋辨認系統
□其他狀況，請說明_____
□貴醫院在此方面並無採取任何技術
□不清楚這方面的狀況

36.請問您知道貴醫院對於病歷室（存放病患資料場所）的安全管理情況為？（可複選）

□需要硬體 IC 卡或 ID 磁卡一類來開啟
□需要軟體密碼來開啟
□需要生物或指紋辨認系統
□有警衛或看管人員
□當病歷資料超過保留期限時處理有一定的程序
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

37.請問您知道貴醫院能夠察閱病患資料的電腦之間連線情況為？（可複選）

□屬於封閉式網路（不與 Internet 相連）
□屬於開放式網路（能與 Internet 相連）
□使用防火牆防護
□限制特定 IP 或網路卡號才能連線
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

38.請問您知道貴醫院病患資料的加密編碼情況為？（可複選）

□有對於病歷資料庫內容加密編碼
□有對於備份資料進行加密編碼
□有使用數位簽章確認資料
□有對於網路傳輸封包資料進行加密
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

39.請問您知道貴醫院有關儲存、備份病患資料的情況？（可複選）

□病患資料備份在不只一個以上的儲存媒介
□病患資料在儲存時是分成不同部份，存放在不同資料庫上
□病患資料只儲存在單一的系統中
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

40.請問您知道貴醫院資訊室（放置系統主機的場所）的安全管理情況為？（可複選）

□需要硬體 IC 卡或 ID 磁卡一類來開啟
□需要軟體密碼來開啟
□需要生物或指紋辨認系統
□有警衛或看管人員
□當資料超過保留期限或設備報廢時處理有一定的程序
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

41.請問您知道貴醫院對於檢核資訊系統的做法為？（可複選）

□有預防系統被入侵的方案
□會評估系統安全弱點
□模擬演練入侵過程
□會淘汰或更新不合需求的老舊保護技術
□其他狀況請說明_____
□貴醫院在此方面並無採取任何措施
□不清楚這方面的狀況

本問卷到此為止，謝謝您的參與，您的意見對我們的研究極具價值，謝謝！