行政院國家科學委員會補助專題研究計畫成果報告

（□期中進度報告/■期末報告）

計畫名稱：電子病歷隱私保護政策遵循之探討－整合理性行為理論與保護動機理論觀點

計畫類別：■個別型計畫　□整合型計畫
計畫編號：NSC102－2410－H－214－019－
執行期間：102 年 08 月 01 日至 103 年 07 月 31 日

執行機構及系所：義守大學醫務管理學系

計畫主持人：郭光明
共同主持人：楊晴雯
計畫參與人員：曾溥元、黃韋慈

本計畫除繳交成果報告外，另含下列出國報告，共 一 份：
□執行國際合作與移地研究心得報告
■出席國際學術會議心得報告

期末報告處理方式：

1. 公開方式：
   □非列管計畫亦不具下列情形，立即公開查詢
   ■涉及專利或其他智慧財產權，□一年■二年後可公開查詢
2.「本研究」是否已有嚴重損及公共利益之發現：■否 □是
3.「本報告」是否建議提供政府單位施政參考 ■否 □是，____（請列舉提供之單位；本會不經審議，依勾選逕予轉送）

中　華　民　國 103 年 09 月 15 日

電子病歷隱私保護政策遵循之探討－整合理性行為理論與保護動機理論觀點

摘要

本研究計畫主要有兩個目的，分別為在於電子病歷情境下：1)探討醫院資訊單位員工對於電子病歷資訊隱私保護政策態度之影響因素，以及 2)探討醫院資訊單位員工遵循電子病歷資訊隱私保護政策行為意圖之影響因素。研究對象為國內醫學中心資訊單位員工，採用問卷方式蒐集資料，共回收 275 份問卷，所蒐集資料利用結構方程模式進行分析，結果顯示：「認知脆弱性」與「認知嚴重性」對於資訊單位員工的「恐懼引發」有顯著的影響；而「恐懼引發」、「回應效能」「自我效能」顯著影響其對於電子病歷隱私保護政策的「態度」，而「態度」與「主觀規範」對於其「電子病歷隱私保護政策遵循行為意圖」均有顯著影響。

關鍵字：病歷隱私保護政策、遵循、電子病歷、保護動機理論、理性行為理論

Understanding the Compliance of Privacy Policy for Electronic Medical Records - An Integration of the Theory of Reasoned Action and Protection Motivation Theory Approach

Abstract

The purpose of this project is twofold. The first purpose is to explore the factors that influence the attitudes toward the privacy policy among hospital employees in the context of electronic medical records. The second purpose is to explore the determinants of behavioral intentions to comply with privacy policy of electronic medical records among hospital employees. Survey methodology was used to collect 275 responses from staff of information department in hospitals. The collected data was analyzed using Structural Equation Modeling. The results demonstrated that perceived vulnerability and perceived severity significantly influence employees' fear arousal. Further, fear arousal, response efficacy, and self-efficacy significantly impact employees' attitude toward privacy policy of protecting electronic medical records. Finally, attitude and subjective norm significantly predict employees' intention to comply with privacy policy of protecting electronic medical records.

Keywords: Medical records privacy policy, compliance, electronic medical records, protection motivation theory, theory of reasoned action

目錄

壹、前言

實務界與學術界均認為資訊科技對於組織營運有極大的幫助，因此資訊科技已是目前各產業用以改善作業流程、提高營運效率與效能的主要方法之一(Luo *et al.*, 2012)。儘管醫療產業採用資訊科技的速度較一般產業落後約 10-15 年(Goldschmidt, 2005)，然由於醫療資源有限，加上民眾醫療需求日增，對於醫療品質的要求也日亦提高，使得越來越多醫療機構開始嘗試採用資訊科技，用以協助醫療服務之提供與相關行政業務之管理，期望能透過資訊科技快速處理與分享等特點，達到成本控制、減少醫療錯誤進而提升醫療品質之目標(Laric and Pitta, 2009; Li and Shaw, 2008; Palvia *et al.*, 2012; Rothstein, 2007)。電子病歷(Electronic Medical Records, EMRs)可視為是資訊科技在醫療產業的主要運用之一(Caine and Hanania, 2013; Goldschmidt, 2005; Palvia *et al.*, 2012; Virga *et al.*, 2012)，以往在紙本病歷時代，由於一般民眾生病時間具不確定性，導致就醫地點也不定，民眾就醫病歷資料往往也隨之分散於不同地點(Rothstein, 2007)；此外，這些病歷當中也可能包含許多錯誤，當民眾須轉診時，亦需要透過手工方式書寫，可能造成病人轉診作業流程效率不佳，不僅影響民眾治療契機，嚴重者甚至因轉診病歷內容書寫不清或錯誤因而造成誤診現象，這些都是紙本病歷潛在問題(Rothstein, 2007)。然藉由電子病歷將以往紙本病歷以數位化方式儲存與管理，不僅能提高病歷資料內容正確性，更可透過網路將電子病歷資料快速與其他醫療機構交換，進一步提高民眾病歷資料正確性(Goldschmidt, 2005)，並能及時傳送到正確醫療機構，讓醫護人員能獲得充足且正確的病歷資訊，減少不確定性，進而做出診斷，讓民眾可獲得更適合的醫療服務。

將紙本病歷轉化為電子病歷應能改善醫療照護品質、減少醫療錯誤、降低醫療成本支出並讓整個醫療照護系統作業流程更順暢(Li and Shaw, 2008; Park *et al.*, 2012)，然而，由於病歷當中經常包含許多敏感性個人資料，例如心理疾病、愛滋病、癌症等心理或生理方面疾病資料(Caine and Hanania, 2013; Medlin *et al.*, 2008; Rindfleisch, 1997; Rothstein, 2007)，醫療機構必須保障病歷資料的機密性，並確保只有經過授權之相關人員能存取病歷資料(Li and Shaw, 2008)；在電子病歷時代，由於所有病歷資料均已電子化，電子病歷的存取更加容易，加上網路技術的發達，電子病歷可從醫療機構任何地點進行存取，甚至可和其他醫療機構進行電子病歷交換(Caine and Hanania, 2013; Virga *et al.*, 2012)，不僅使得電子病歷更容易外洩，也導致民眾的病歷隱私遭受到侵犯(Medlin *et al.*, 2008; Rindfleisch, 1997)；然而電子病歷的推展必須先獲得民眾接受與支持，電子病歷唯有符合社會個人隱私認可前提下，方能實施與採用(Caine and Hanania, 2013)。

對於避免民眾資料隱私遭受侵犯，學術界與實務界一般均認為須採取妥善的資訊安全措施，然「資訊安全」與「隱私」是兩個相關但並不相同的概念。「資訊安全」指組織必須有適當的政策、實務(Practices)與技術方能透過網路進行具安全保障的電子化交易(Volonino and Robinson, 2003)，而「隱私」指民眾能夠控制其個人資訊的使用以及是否揭露(Medlin and Cazier, 2007)；此外，「資訊安全」也可視為是一種過程，而隱私則是結果(Herold, 2002)，儘管目前各組織大部分已採用資訊安全措施，並藉由資訊科技來協助落實，然而資訊科技和資訊安全措施並無法完全避免組織內部員工洩漏重要資訊(Medlin and Cazier, 2011)，可見資訊隱私雖可藉由適當資訊安全政策達成，然單純的資訊安全政策仍不足以確保隱私達成，仍需搭配隱私

保護政策(Laric and Pitta, 2009)。就醫療產業而言，所謂「隱私政策」指可以讓醫院員工知道醫院將如何處理病歷資訊以及病人隱私權之管理指引(Management directives)(Li and Shaw, 2008)，更精確來說，隱私政策說明醫院員工必須遵循的隱私保護規範，達到讓民眾可控管個人資訊之目的(Volonino and Robinson, 2003)。一般而言，醫院都必須有隱私保護政策，如果醫院沒有正式隱私保護政策，則民眾病歷隱私可能受到嚴重威脅(Li and Shaw, 2008)。此外，隱私政策必須讓民眾易於閱讀與瞭解，且必須是最即時的，更重要是須讓組織內部員工瞭解並督促其嚴格遵守(Volonino and Robinson, 2003)。

以往各產業所發生資料破壞(Data breach)事件中，醫療產業佔了相當高的比例，而內部員工更是這些資料破壞事件發生的主因之一，例如 Ayyagari (2012)針對全世界 2005-2010 年所發生的資料破壞事件進行分析，結果發現共有 2,633 件經報導事件，進一步分析，發現醫療產業發生次數高達 532 次，占整體比例約 20.2%，較其他產業高；此外，在這些資料破壞事件當中，屬內部員工所造成事件次數約 278 件，占整體比例約 10.59%，亦為不低數據。對醫療產業而言，任職於醫療機構員工有更多機會接觸到病人病歷資料(Medlin *et al.*, 2008; Medlin and Adriana, 2007)；此外，依據 Medlin and Cazier (2011)的統計資料顯示，美國在 2008-2009 年間，有許多醫院病人資訊外洩事件，被洩漏病歷資訊所屬病人人數最高更達 50,000 人，造成這種病人資訊外洩主要原因正是醫院內部員工。儘管國內外均有相關法律(U.S. Department of Health and Human Services, 2002；Volonino and Robinson, 2003; 行政院法務部, 2011)規範民眾個人資訊隱私，甚至明確針對醫療產業病歷資訊的隱私(行政院衛生署, 2004)，並訂有相關罰則，避免病人資訊被任意被外洩，然個人或病歷資訊隱私被侵犯的案例在國內外仍時常發生(Laric and Pitta, 2009; Medlin and Cazier, 2011; 楊漢湶, 2012)。

醫療屬於高度專業的服務，醫療服務往往需由不同專業人員來共同完成(Laric and Pitta, 2009)，因此不同醫療專業人員都有可能接觸到病人的病歷資訊。醫療機構所有工作人員對於病人均負有保密義務，在雙方互誠互信基礎上，醫療人員對於病人的病歷資訊不得加以洩漏(楊漢湶, 2012)。在以往，能接觸到病人病歷資訊主要為醫護相關人員，因此上述和醫療相關的法律規範主要也是針對醫護相關人員，然而隨著電子病歷實施，越來越多病人病歷資料逐漸數位化，並存放於資訊系統當中，而資訊單位員工由於負責維運醫院資訊系統(包含電子病歷系統)，因此有更多機會接觸到病人電子病歷資訊，以往文獻指出組織資訊安全問題最主要的來源在於內部員工(Laric and Pitta, 2009; Medlin and Cazier, 2007; Rindfleisch, 1997)，因此瞭解資訊單位員工對於醫院電子病歷資訊隱私保護態度，對於防範醫院電子病歷隱私破壞事件(例如病歷資料外洩)有其重要性；此外，近年來國內正積極推動電子病歷，期望提高醫療照護品質的同時，深入探討此議題更有其迫切性與必需性。

貳、研究目的

儘管目前已有多項法律規範保護民眾個人隱私資料，醫院對病人病歷資料亦制訂相關隱私保護政策，然病人病歷外洩狀況在國內外仍時有所聞(Laric and Pitta, 2009; Medlin and Cazier, 2011；楊漢湶, 2012)，儘管病歷資訊可能受到醫院外部人員之入侵而外洩，但醫院內部員工也可能在經意或不經意狀況下洩漏，顯示病歷資訊保護仍有有極大改善的空間；此外，由於電子病歷實施，使得電子化的病歷資訊流通與取得更容易，醫院中有更多人可能接觸到電子

病歷，也讓電子病歷資訊外洩機率增加，儘管電子病歷的存取可透過資訊科技予以嚴格管控，然單從技術層面可能無法完全有效避免病歷資訊外洩狀況發生，仍需考量其他組織及社會層面的影響因素，因此，本計畫主要目的在於電子病歷情境下：1)探討醫院資訊單位員工對於病歷資訊隱私保護政策態度之影響因素，以及 2)探討醫院資訊單位員工遵循病歷資訊隱私保護政策行為意圖之影響因素。

一、醫院資訊單位員工對於病歷資訊隱私保護政策態度之影響因素

依據理性行為理論(Theory of Reasoned Action)(Fishbein and Ajzen, 1975)，態度指個人對於某項行為所抱持的正面或負面感覺，也就是個人對於某行為經過評價後所形成的感覺。由於醫院資訊單位員工有更多機會接觸到病人的電子病歷資訊，以往調查報告指出組織內部資料外洩原因中，內部員工所造成此類事件往往佔極大比例，因此有必要瞭解醫院中資訊單位員工對於病人資訊隱私保護政策態度之影響因素，以訂出能導正資訊單位員工態度之規範，提高其遵從度，本計畫以保護動機理論(Protection Motivation Theory)為理論基礎，提出包括：認知脆弱、認知嚴重、恐懼引發、回應效能、自我效能、回應成本等變數，可能直接或間接影響醫院資訊單位員工對於電子病歷隱私保護政策態度。

二、醫院資訊單位員工遵循病歷資訊隱私保護政策行為意圖之影響因素

依據理性行為理論，個人是否會採取某一行為受到其行為意圖影響，換言之，醫院資訊單位員工是否能實際遵守醫院所制定病人隱私保護政策，並保護病人電子病歷資訊，受到其是否願意遵循醫院病人隱私保護政策行為意圖影響。為深入了解影響醫院資訊單位員工是否願意遵循電子病歷隱私保護政策之行為意圖，本計畫以理性行為理論為基礎，提出包括：態度以及主觀規範等變數，可能會影響資訊單位員工遵循隱私保護政策之行為意圖。

為完成本計畫上述兩個目的，本計畫每一個階段均需進行完整且深入文獻探討，以及多次專家會議，提出符合前述目的之研究模式，並發展具有高信度與效度的資料蒐集工具，作為問卷調查的基礎。期望本計畫結果能夠提供學術界、政府衛生主管單位及醫院參考，能以最有效的方式，規劃並擬定符合醫院作業需求以及民眾可充分信任的病人隱私保護政策，並確保醫院員工能確實遵循病人資訊隱私保護政策。本計畫各項研究目的，可細分如下：

- 蒐集與彙整近五年與資訊隱私顧慮與資訊隱私保護政策相關文獻
- 蒐集與彙整近五年與組織員工遵循資訊隱私保護政策之相關研究結果
- 提出威脅評價(認知脆弱、認知嚴重、恐懼引發)、回應評價(回應效能、自我效能、回應成本)、規範、態度、資訊單位員工遵循病歷隱私保護政策等構面變數與衡量問卷
- 提出並驗證威脅評價(認知脆弱、認知嚴重、恐懼引發)、回應評價(回應效能、自我效能、回應成本)、規範、態度對於醫院資訊單位員工遵循病歷隱私保護政策行為意圖研究架構

參、文獻探討

一、隱私與資訊隱私顧慮

Westin (1967)認為「隱私」是一種個人或團體之權利，每個人可自行決定其何時、如何、以及傳達哪些個人資訊讓其他人知道，而所謂「隱私被侵犯」即指個人無法控制他人存取其個人資訊。其他文獻(Warren and Brandeis, 1890)則認為隱私指個人不受干擾之權利；Culnan (1993)則認為隱私指個人能控制他人存取個人資訊的能力，然由於隱私並不易衡量，因此大多透過隱私顧慮(Privacy concern)之方式予以衡量(Culnan and Armstrong, 1999; Smith *et al.*, 1996; Smith *et al.*, 2011)，因此，「隱私顧慮」指民眾預期未來在隱私上可能之損失(Dinev *et al.*, 2006)，在資訊科技快速發展的時代，民眾的資訊隱私更容易遭受侵犯(Mason, 1986)，進而造成民眾產生資訊隱私顧慮(Smith *et al.*, 1996)。更精確來說，資訊隱私指個人能控制他人存取其個人資訊的能力(Culnan and Armstrong, 1999; Stone *et al.*, 1983)；Clarke (1999)則將「資訊隱私顧慮」定義為個人對於控制、影響關於其個人資料處理方式的關心程度。Bélanger and Crossler (2011)認為溝通隱私和資料隱私可以併入資訊隱私當中，因為目前的溝通和資料都已邁入電子化的方式來進行；Clarke (1999)將隱私區分為四個方面：1)民眾的隱私(Privacy of a person)；2)行為隱私(Behavior privacy)；3)溝通隱私(Communication privacy)；4)資料隱私(Data Privacy)。Hoffman (1980)將資訊隱私區分為三種獨特的權益(Rights)：1)民眾有權決定分享哪些個人的資訊給其他人，2)民眾有權知道自己有哪些資訊被蒐集；及 3)民眾亦有權存取個人資料以維持社會運作並規範政府運作。Phelps *et al.* (2000)認為以下原因造成民眾的隱私顧慮：1)民眾被要求提供的資訊類型(Information type)；2)組織提供民眾對於其個人資訊控制程度；3)在民眾與組織資訊交換過程中可能產生之結果與效益；4)民眾的特性。對資訊隱私而言，一般民眾的反應是可能不想讓其他人取得個人的資訊，或者可能認為對於個人與其他人交換資訊之控制程度不如預期，因而讓個人經歷較負面之經驗，導致個人後來無意願提供其資訊，或因為民眾認為組織未告知將如何蒐集個人資料，以及蒐集後的個人資料將如何使用等資訊，導致民眾產生資訊隱私顧慮(Nowak and Phelps, 1995; Stone *et al.*, 1983)。

二、醫療資訊隱私保護相關法律

經濟合作與發展組織(Organization for Economic Co-operation and Development, OECD)在 1980 年針對民眾隱私保護提出八點原則：1)有限資料蒐集原則(Collection Limitation Principle)；2)資料品質原則(Data quality principle)；3)用途明確原則(Purpose specification principle)；4)使用限制原則(Use limitation principle)；5)安全保存原則(Security safeguards principle)；6)開放原則(Openness principle)；7)民眾個人權益(Individual's right)；8)當則原則(Accountability principle)。歐洲與美國亦分別依據 OECD 所制定之個人隱私保護原則陸續定出許多隱私相關保護法規，例如歐洲在 1995 年由歐盟通過 Directive 95/46/EC: The Directive on Protection of Personal Data，該法案主要針對個人資訊處理、取得及揭露進行規範(Volonino and Robinson, 2003)。而美國亦依據 OECD 所提出個人資訊隱私保護原則訂定多項法律，針對醫療資訊方面隱私保護，美國國會在 1996 年公布 Health Insurance Portability and Accountability Act (HIPAA)要求

Department of Health and Human Services 針對民眾照護電子資訊制定全國通用標準，主要包括三個部分：1)交易和代碼組(Transactions and code sets)；2)隱私；3)安全；HIPAA 制訂這三種標準主要目的在簡化保險申報管理作業以及所花費成本，同時也考量民眾在能控制並取得個人醫療資訊狀況下，降低民眾醫療資訊外洩時可能遭遇威脅與風險(Medlin and Cazier, 2007)。

國內目前與醫療資訊隱私保護相關法律可區分為：1)個人資料保護法；2)醫療相關法規；3)電子病歷相關法規三方面。在個人資料保護法方面，政府於民國 84 年制定「電腦處理個人資料保護法」保障民眾個人資料在電腦時代不被誤用，並於民國 101 年 10 月 1 日正式實施，對於資訊時代下民眾個人資料提供更進一步保障，醫院也屬於電腦處理個人資料保護法所規範單位之一。其次，目前國內有相當多與醫療相關法律清楚規定醫護相關人員對於病歷資訊保護與處罰條文，例如醫療法第 72 條規定：醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩漏等，顯示國內對於病人資訊保護相關法律相當重視。此外，前述法律亦訂相關罰則，醫院如違反病歷隱私保護相關規定，當事人或醫院可能須接受相關處罰，對於醫院收入或聲譽都有不良影響。至於電子病歷相關法規方面，在電子病歷時代，因病人病歷資訊均數位化，這些病歷資訊的流通與存取也更容易，造成電子病歷更容易外洩，引發民眾擔心病歷資訊隱私被侵犯狀況，針對病歷隱私問題，衛生署提出包括：「醫療資訊安全與隱私保護指導綱領草案」(行政院衛生署, 2004)與「醫療機構電子病歷製作及管理辦法」(行政院衛生署, 2009)等辦法。「醫療資訊安全與隱私保護指導綱領草案」針對病人隱私問題提出九項指導原則，包含：1)最小需求原則；2)直接取得原則；3)尊重及告知原則；4)公平正義原則；5)符合現行法規原則；6)合理範圍內之最大安全原則；7)病人權利保障原則；8)不可揭露原則；9)生命權及公共利益保障原則。而「醫療機構電子病歷製作及管理辦法」(行政院衛生署, 2009)則針對電子病歷資訊系統提出相關規定，例如：1)人員操作與維護有完善之作業程序；2)電子病歷存取與查閱等使用權限及管控機制有明確規範；3)電子病歷存取與增刪動作之執行人員、時間及內容，應有紀錄併同電子病歷保存等，這些規範之主要目的均期望能達成保護病歷資訊隱私目的。

三、醫療資訊隱私保護政策

美國聯邦貿易委員會(Federal Trade Commission, FTC)已規範組織必須遵循合理資訊實務(Fair information practices)以確保民眾資訊隱私(Choy *et al.*, 2001)，所謂合理資訊實務指能夠提供民眾控制其個人所揭露資訊和這些資訊未來用途之程序(Storey *et al.*, 2009)，主要包括五項指導原則(Choy *et al.*, 2001; Storey *et al.*, 2009)：1)提醒(Notice)：須告知民眾組織將蒐集個人資料；2)選擇(Choice)：組織需提供民眾有權決定其個人資料將如何被處理；3)存取(Access)：組織必須提供民眾能存取其個人資料並驗證其正確性；4)安全性(Security)：組織需確保民眾資料能安全的傳輸及儲存；5)補救(Redress)：組織必須具備處理民眾抱怨的處理流程，對於未遵循網站政策者亦具有罰則。

所謂「醫療資訊隱私保護政策」指可讓醫院員工知道醫院將如何處理病人病歷資訊及病人隱私權的管理指引(Li and Shaw, 2008)。國內大多數醫院均制定有病人隱私保護政策或病人隱私保護相關措施，規範院內員工對於病人醫療資訊的保護，例如衛生署推動國內醫院參與 ISO27001:2005 資訊安全認證，確保醫院能遵循資訊安全管理系統(Information Systems

Management Systems, ISMS)之運作機制，對於電子病歷管理能有標準的作業程序，截至目前，共計有 93 家醫院已通過此項安全認證。此外，醫院亦會擬定病歷資訊隱私保護政策與措施，讓醫院員工在處理病歷資訊時能有所依據，例如對於院內較敏感的病歷(如愛滋病人)，須經嚴格審查程序才能調閱該病歷；而依據「醫療機構電子病歷製作及管理辦法」(行政院衛生署, 2009)，醫院的電子病歷系統對於電子病歷使用，不管增、刪、修改、或是審閱電子病歷，系統均會留下紀錄與修改前之原始版本，用以事後追蹤。此外，部分醫院亦針對電子病歷異常使用狀況進行偵測，例如一次下載過多病歷資料，或是含有病人病歷號碼、電話與地址的資料就無法列印或儲存等方式(廖珮君, 2011)；此外，醫院對於所有醫事人員使用電子病歷的權限亦應明確規範(楊漢淙, 2012)，避免病歷資訊的不當存取。

四、理性行為理論(Theory of Reasoned Action, TRA)

依據信念-態度-行為模式(Belief-Attitude-Behavior)，Fishbein 與 Ajzen 在 1975 年發展出「理性行為理論(Theory of Reasoned Action, TRA)」，如圖 3-4-1 所示，用以解釋與預測人類行為決策的過程，該理論主要目的為了解與預測個人行為，其基本假設為個人在採取某行動之前，會「理性」考慮其行為，亦即個人可自主控制其行為(Fishbein and Ajzen, 1975)。TRA 主張一個人對一項行為由「行為信念」與對此行為結果的「評價」，形成他對此行為正反面的評價，亦即內在「態度」；此外，社會大眾與重要他人亦會對此行為有所看法(規範信念)與他順從這些規範意願強弱(依從動機)，這些形成個人認為社會上對此行為看法，可稱為外在「主觀規範」。內在的態度與外在的主觀規範便形成個人行為的「意圖」，這便是個人是否想去從事這項行為的動力，最後當個人有高度意向時，便會從事這項「行為」(Fishbein and Ajzen, 1975)。

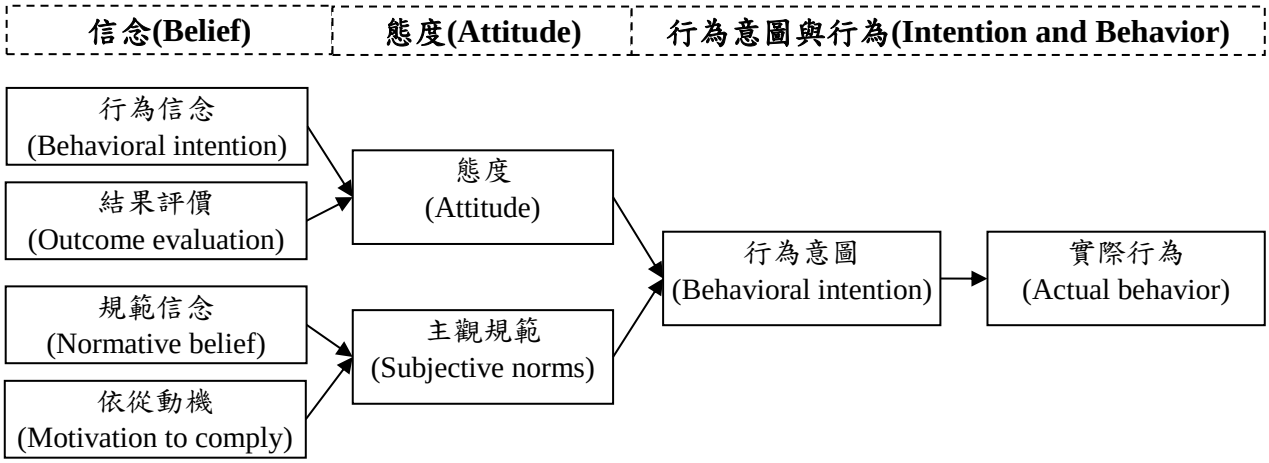


圖 3-4-1 理性行為理論架構(Fishbein and Ajzen, 1975)

理性行為理論已廣泛用於各領域預測民眾的各種行為，且均有一定程度之解釋能力(Sheppard *et al.*, 1988)，例如資管領域當中：如資訊工作選擇傾向(Joshi and Kuhn, 2011)、線上購物(Hansen *et al.*, 2004)等；醫療照護領域當中：如民眾是否願意採用愛滋病防治行為(Fisher *et al.*, 1995)、護理人員是否針對老年病人採取約束(Physical restraint)行為(Werner and

Mendelsson, 2001)、護理人員是否願意採用創新資訊科技(Hebert and Benbasat, 1994)等，Sheppard *et al.* (1988)並建議可採修訂方式進一步驗證理性行為理論。

五、保護動機理論(Protection Motivation Theory, PMT)

保護動機理論(Protection Motivation Theory, PMT)最早由 Rogers (1975)提出，主要目的在釐清「恐懼訴求(Fear appeal)」意涵，恐懼訴求指一種關於對民眾福祉相關威脅的溝通(Milne *et al.*, 2000)。之後 Rogers (1983)再度提出修正版本保護動機理論，使保護動機理論能更廣泛適用於說服性溝通(Pervasive communication)過程，並強調民眾認知過程(Cognitive processes)能中介(Mediate)其行為改變(Boer and Seydel, 1996)。

(一)1975 年版本保護動機理論

Rogers (1975)首先在 1975 年提出第一次的保護動機理論，保護動機理論將民眾面對資訊的處理與因應方式區分為三個階段：1)資訊來源(Sources of information)階段；2)認知中介過程(Cognitive mediating process)階段；以及 3)對應模式(Coping mode)階段(如圖 3-5-1 所示)，亦即民眾首先接收到外來資訊(資訊來源階段)，接著評估所收到的資訊(認知中介過程)，最後則針對所收到的資訊採取因應行動(對應模式)。

Rogers (1975)提出保護動機理論主要目的在於更深入瞭解「恐懼訴求(Fear appeal)」的意涵，Rogers 認為恐懼訴求主要受到三個因素影響：1)某一事件有害的嚴重程度(Magnitude of noxiousness)；2)假使沒有適應性行為或調整現有行為來因應的狀況下，該事件會發生的機率(Probability of occurrence)；3)能夠減少或消除有害事件的建議/因應措施是否存在或其有效性(Efficacy of recommended response)。而恐懼訴求所包含的這三個因素當中任一個因素接著都可能會引發民眾的認知中介過程 (Rogers, 1975)，民眾會依據每個恐懼訴求因素所得到的資訊分別進行評估，包括：評估該事件之嚴重程度(Appraised severity)、預期面臨該事件的機率(Expectancy of exposure)和對於回應措施有效性的信心(Belief in efficacy of coping response)；之後，恐懼訴求經由認知過程的中介讓民眾產生「保護動機(Protection motivation)」，最後藉由保護動機促使民眾採納建議/因應的行為(Rogers, 1975)。

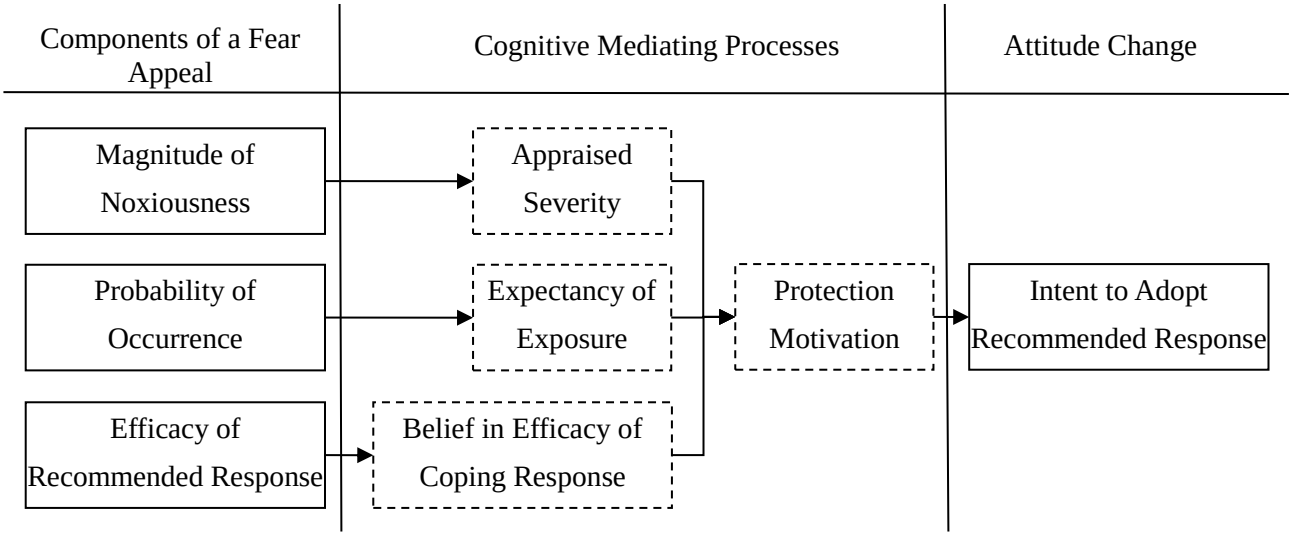


圖 3-5-1 保護動機理論架構圖(Rogers, 1975, p. 99)

(二)1983 年版本保護動機理論

在 1975 年提出保護動機理論之後，為了讓保護動機理論能更完整，Rogers (1983)認為原始的保護動機理論需進行修訂，包括(Maddux and Rogers, 1983; Rogers, 1983)：1)針對引發因應過程的「資訊來源」進行更廣泛的說明；2)提出額外的認知中介過程；以及 3)更充分說明因應模式，修訂後保護動機理論模式如圖 3-5-2 所示。

依據修訂後保護動機理論(Rogers, 1983)，當民眾面臨威脅時，共有四個認知評估過程會中介民眾對於回應威脅行為抉擇：1)根據現有資訊評估該威脅嚴重性(Perceived severity)；2)該威脅發生機率(Perceived vulnerability)；3)民眾認為因應行為能夠移除該威脅的機率(即回應行為的有效性)(Response efficacy)；及 4)民眾認為自己能執行因應行為的能力(即民眾執行因應行為的自我效能)(Self-efficacy)，而這四個評估過程最後產生「保護動機」的心理狀態(Rogers, 1983; Tanner et al., 1991)。此外，Rogers (1983)認為恐懼在保護動機中可能會產生，但不至於直接影響民眾行為，而是透過間接方式影響。

針對 Rogers (1983)所修訂保護動機理論，Floyd *et al.* (2000)認為「資訊來源」可視為保護動機理論輸入因素，包括外部環境及自我內省兩類資訊來源，外部環境資訊來源則包含口語說服(Verbal persuasion)及觀察式學習(Observational learning)，而自我內省資訊來源則包含人格特質變數(Personality variables)和以往經驗，這些資訊來源會引發民眾「認知中介過程」，然 Rogers (1983)亦提及保護動機理論之重點在於認知中介過程，資訊來源非該理論之重點。資訊來源則引發民眾認知中介兩個過程：威脅評價過程與因應評價過程，之後民眾便會針對威脅產生相對回應以嘗試降低威脅，包括：適應不良回應(Maladaptive response)與適應良好回應(Adaptive response)(Floyd *et al.*, 2000)，所謂適應不良回應指民眾所採取的措施僅能降低民眾的恐懼但未能有效降低威脅，反之則稱為適應良好回應。而民眾會先針對威脅進行評價，之後才能針對回應進行評價(Floyd *et al.*, 2000).

威脅評價過程中會評估增加或降低適應不良回應因素，適應不良回應可能是被激發的行為(Rogers, 1983)，例如開始抽菸或開車未繫安全帶。而增加適應不良回應機率因素包括內在激勵(例如身體所感受到壓力)，以及外在激勵(例如社會認同)(Floyd *et al.*, 2000)；至於降低適應不良回應機率因素則包括針對威脅事項評估威脅的嚴重程度及受傷害程度。而激發恐懼會影響威脅事項的認知嚴重程度，且間接影響最後的回應行為。因此威脅評價是所有影響適應不良回應的變數之加總結果，這些變數有的會增加適應不良回應的機率，但有的變數則會降低適應不良回應的機率(Floyd *et al.*, 2000)。

除威脅評價外，民眾也會進行因應評價，包含民眾會判斷預防回應是否能有效避免威脅事項(即回應效能)，及民眾亦會自行評估本身是否具備足夠能力啟動並完成回應行為(即自我效能)，因民眾除具備回應威脅方案外，亦須對自己具足夠信心來執行該方案，而回應效能和自我效能兩個因素會增加採取適應良好回應機率，回應成本則會降低適應良好回應機率，適應良好回應則是兩個效能因素和回應成本總合結果。認知中介過程輸出則為民眾決定要發起、繼續或抑制可行的調適良好回應，換言之，民眾最後經威脅評價和對應評價過程最後形成保護動機，因此一般保護動機理論相關研究依變數主要衡量民眾行為意圖(Floyd *et al.*, 2000)。

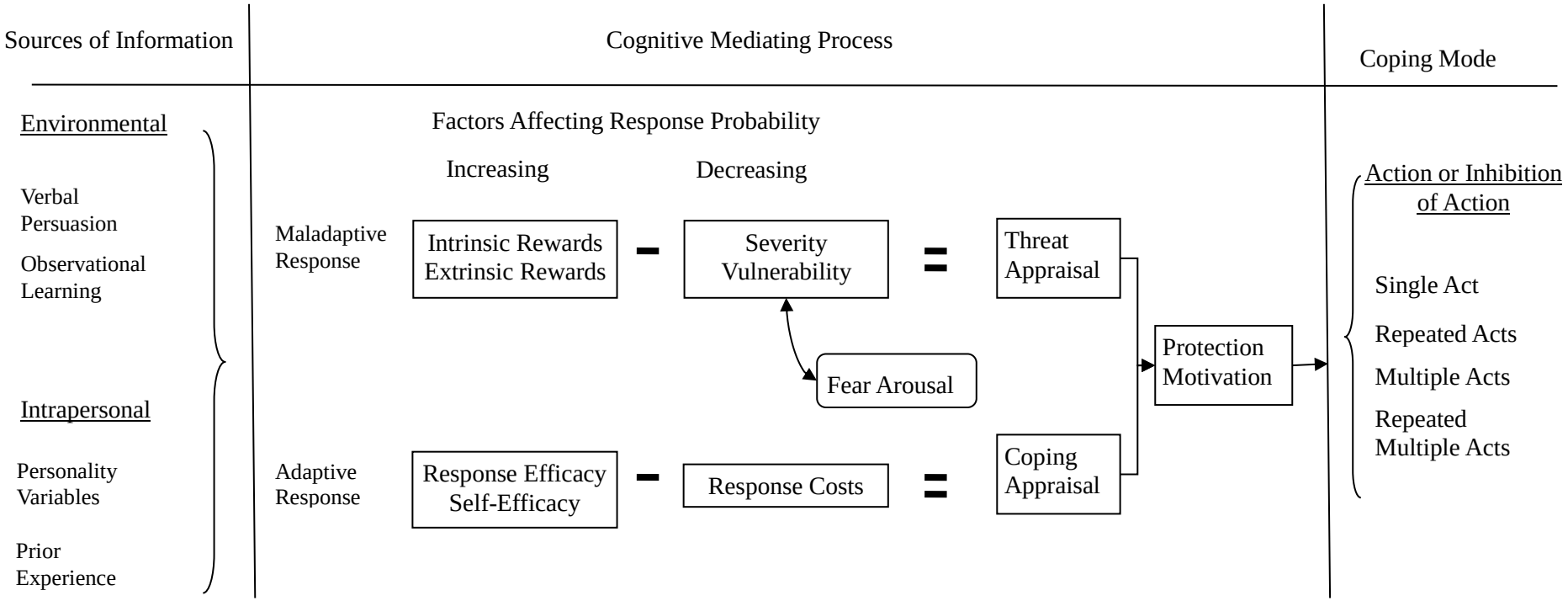


圖 3-5-2 修訂後保護動機理論架構(Rogers, 1983, p. 168)

六、保護動機理論相關研究模式

保護動機理論以往主要運用於健康相關行為之預測(Rogers, 1983)，但後來保護動機理論也逐漸應用於不同領域，包含資管領域，目前資管相關文獻中採用保護動機理論之研究可概略區分為不同研究主題，例如資訊安全政策遵循(Compliance)研究與隱私保護模式等研究。

(一)資訊安全政策遵循研究模式

1.Ifinedo (2012)模式

Ifinedo (2012)針對 124 位經理人及資訊專業人員進行資訊系統安全政策(Information systems security policy, ISSP)遵循影響因素研究，Ifinedo 整合保護動機理論與計畫行為理論提出包括：認知脆弱程度、認知嚴重程度、反應效能、反應成本、自我效能、遵循 ISSP 態度及主觀規範等七個構面可能影響員工對 ISSP 遵循行為意圖(研究架構如圖 3-6-1 所示)，結果發現認知脆弱程度、反應效能、自我效能、遵循 ISSP 態度與主觀規範等五個構面對於遵循 ISSP 行為意圖有正向影響，認知嚴重程度則對於遵循 ISSP 行為意圖呈負向影響。

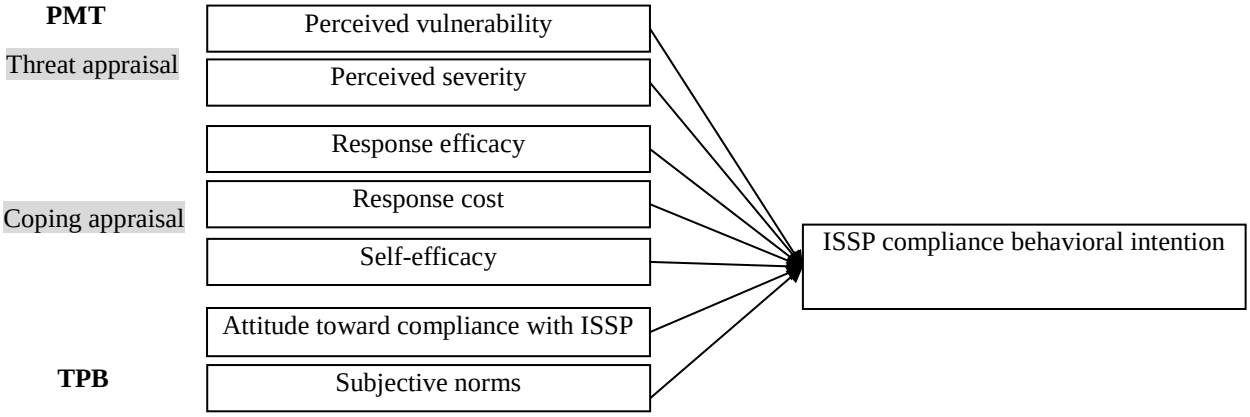


圖 3-6-1 Ifinedo 研究模式

2.Vance *et al.* (2012)模式

Vance *et al.* (2012)認為員工是否能遵守資訊安全政策是目前組織主要顧慮之一，以往研究並未深入探討經驗對員工遵循訊安全政策影響，Vance *et al.*整合保護動機理論與以往經驗，提出圖 3-6-2 研究模式，該模式認為員工以往經驗會影響其對資訊安全政策認知過程中威脅評價與回應評價的因素，包含：認知嚴重程度、認知脆弱程度、獎勵及反應效能、自我效能、反應成本三個變數，而員工威脅評價與回應評價則影響員工是否遵循組織安全政策意願；此外，亦有三個控制變數：情境、真實狀況、與性別，亦可能影響員工是否遵循組織安全政策意願。研究結果顯示僅威脅評價與性別對於員工是否遵循組織安全政策意願無顯著影響。

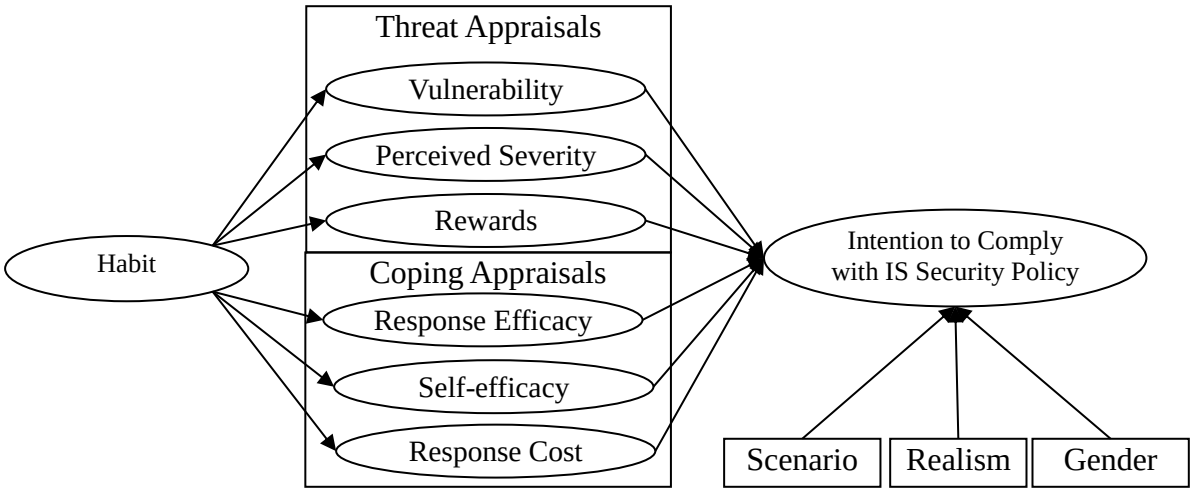


圖 3-6-2 Vance *et al.* (2012)資訊安全遵循研究模式

3.Siponen *et al.* (2010)模式

Siponen *et al.* (2010)依據理性行為理論、保護動機理論、創新擴散理論、遏止理論(Deterrence theory)等不同理論，提出整合式研究架構(如圖 3-6-3 所示)，探討員工對於資訊安全政策遵循的行為意圖以及實際遵循行為，共發出 3,130 份問卷，回收 917 份有效問卷，結果發現規範信念、威脅評價、自我效能、反應效能與可見度等五個變數對遵循資訊安全政策行為意圖有顯著影響；而遏止(Deterrences)和遵循資訊安全政策行為意圖對於實際遵循資訊安全政策行為亦具顯著影響。

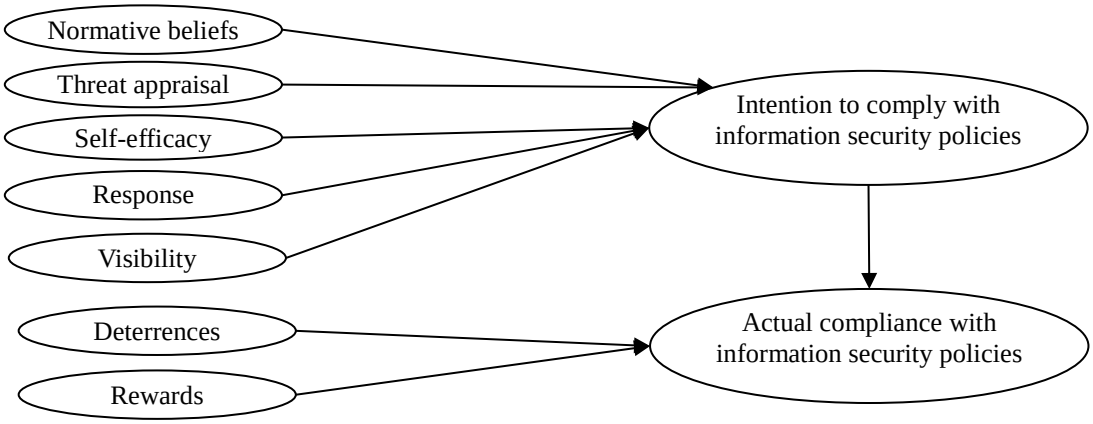


圖 3-6-3 Siponen *et al.* (2010)研究模式

4.Siponen *et al.* (2006)模式

Siponen *et al.* (2006)以保護動機理論三階段：外部環境影響、認知中介過程、保護動機行為改變為主要理論基礎，加上理性行為理論，提出如圖 3-6-4 研究架構，以瞭解員工對資訊安全政策遵循意圖與行為影響因素，結果發現規範信念與可見度對於威脅評價有顯著影響；規範信念與可見度對於反應效能有顯著影響；規範信念與可見度對於自我效能有顯著影響；威脅評價、反應效能和自我效能對於資訊安全政策遵循意圖有顯著影響；而資訊安全政策遵循意圖亦顯著影響諮詢安全實際遵循行為。

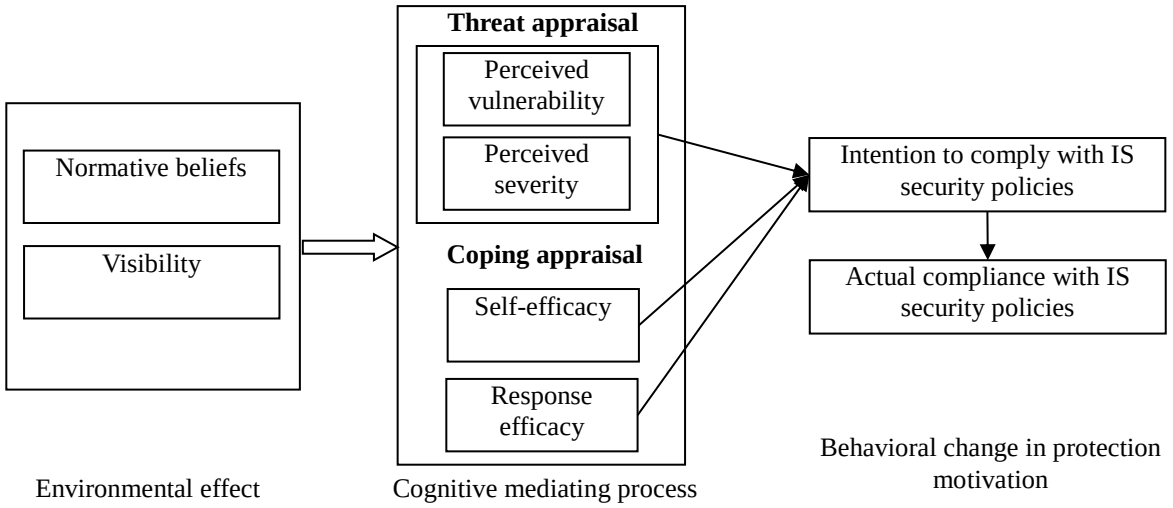


圖 3-6-4 Siponen *et al.* (2006)研究模式

5.Herath and Rao (2009)模式

Herath and Rao (2009)整合保護動機理論、遏止理論(Deterrence theory)、組織行為與解構式計畫行為理論(Decomposed Theory of Planned Behavior)等理論(研究架構如圖 3-6-5 所示)，從 78 不同組織蒐集 312 份資料，以了解組織員工是否願意遵守資訊安全政策，結果發現：1)安全漏洞認知嚴重程度影響安全漏洞顧慮程度，而安全漏洞顧慮程度影響安全政策態度；2)反應成本、反應效能、自我效能影響安全態度政策；3)資源可取得性影響自我效能；4)組織承諾影響反應效能和資訊安全政策遵從意圖；5)偵測確定性、主觀規範和敘述性規範影響資訊安全政策遵從意圖。

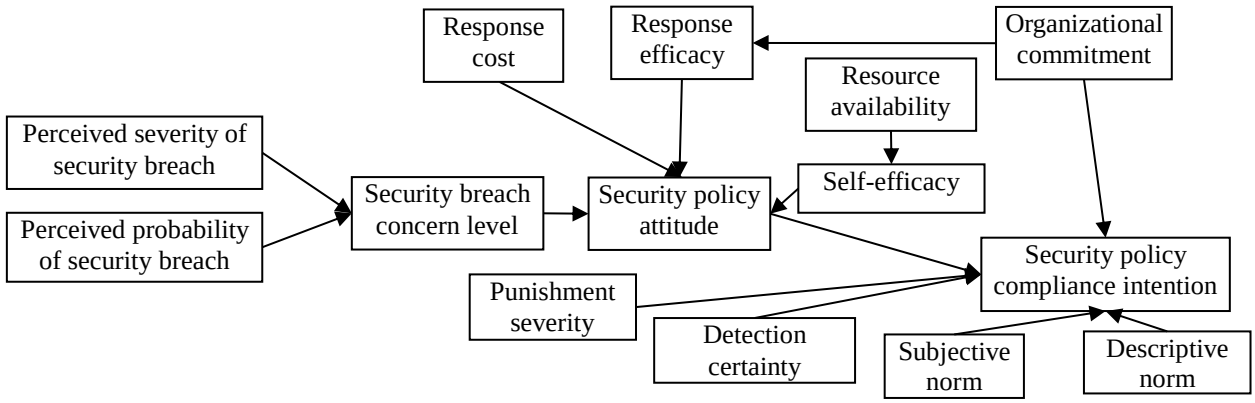


圖 3-6-5 Herath and Rao 研究模式

(二)隱私保護模式

1.Youn (2005)模式

Youn (2005)利用保護動機理論探討青少年對於在網路提供個人資訊給網站現象，Young 認為青少年提供個人資訊給網站前會透過風險利益(Risk-benefit)評估過程，之後引發其降低風險的行為，最後則讓青少年採取保護個人隱私之行為(如圖 3-6-6 所示)。該研究共回收 326 份有效問卷，結果顯示認知風險嚴重程度和認知效益(Perceived benefit)分別顯著負向與正向影響青少年提供個人資訊的意願，而該意願亦顯著負向影響青少年採取保護個人隱私行為。

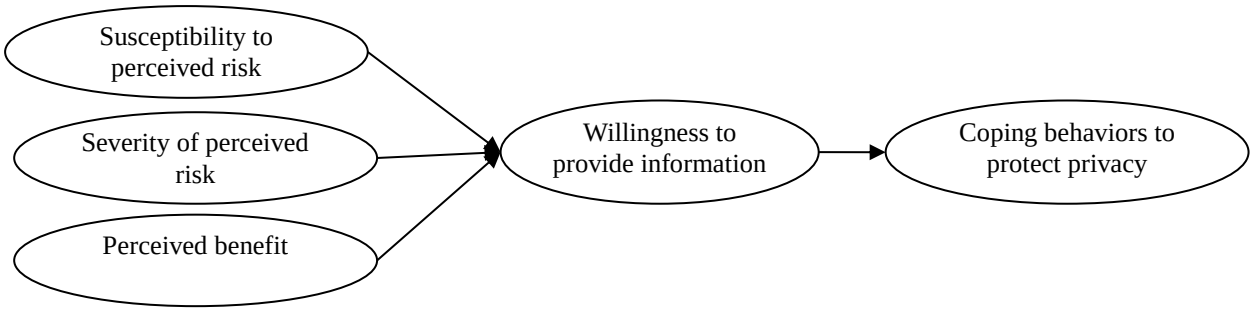


圖 3-6-6 Youn (2005)研究模式

2.Chai *et al.* (2009)模式

Chai *et al.* (2009)整合保護動機理論與社會認知理論(Social Cognitive Theory)提出如圖 3-6-7 研究模式，當中外部資訊隱私顧慮為二階變數，包含家長資訊隱私顧慮、同儕資訊隱私顧慮和老師資訊隱私顧慮三個一階變數。該模式主要探討 9-12 歲青少年網路資訊隱私保護行為，共蒐集 285 份問卷，結果發現青少年認知資訊隱私讀重要性、資訊隱私自我效能、外在資訊隱私顧慮及以往經驗對於資訊隱私保護行為有顯著影響；此外，資訊隱私暴露對於資訊隱私自我效能、資訊隱私自我效能對於認知資訊隱私讀重要性、以往經驗對於資訊隱私自我效能和以往經驗對於資訊隱私顧慮均有顯著影響。

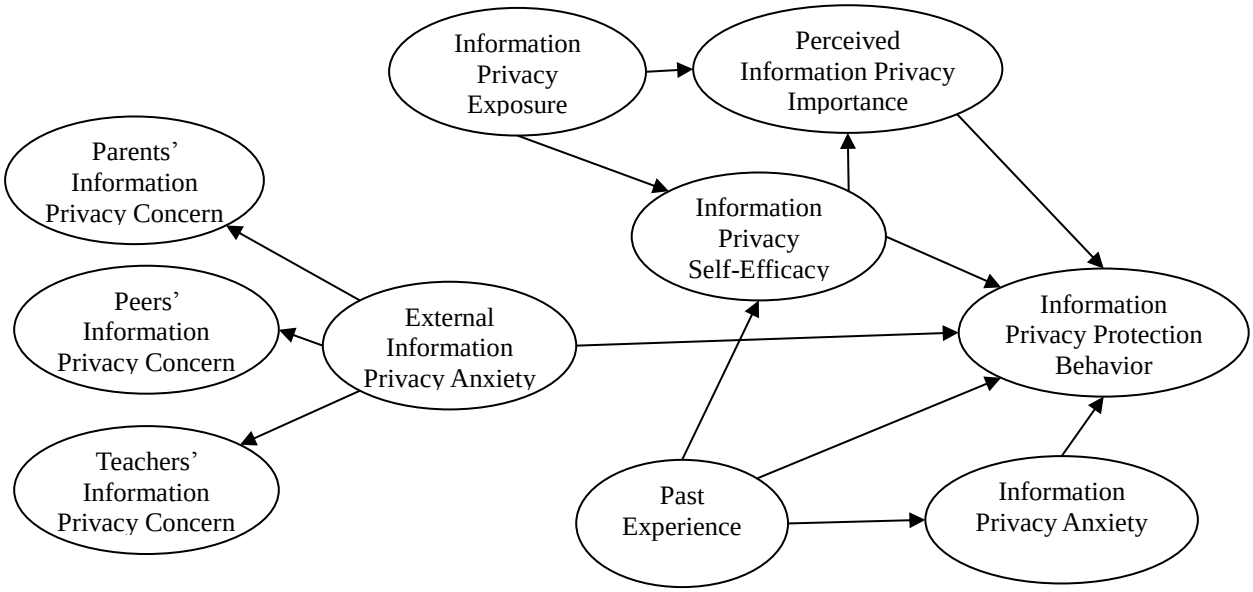


圖 3-6-7 Chai *et al.* (2009)研究模式

3.Junglas *et al.* (2008)模式

雖以往隱私文獻已證明隱私顧慮會影響民眾行為意圖，然對於隱私顧慮影響因素瞭解卻仍有所不足，因此Junglas *et al.* (2008)便探討個人人格特質(Personality traits)對隱私顧慮影響，包括：一致性(Agreeableness)、知覺(Conscientiousness)、情緒穩定性(Emotional stability)、外向性(Extraversion)及開放性(Openness)。Junglas *et al.* (2008)將隱私顧慮視為保護動機理論中的威脅評價過程(如圖 3-6-8)。總共蒐集 550 位大學部和研究所學生，研究結果顯示一致性、知覺與開放性對於隱私顧慮有顯著影響。

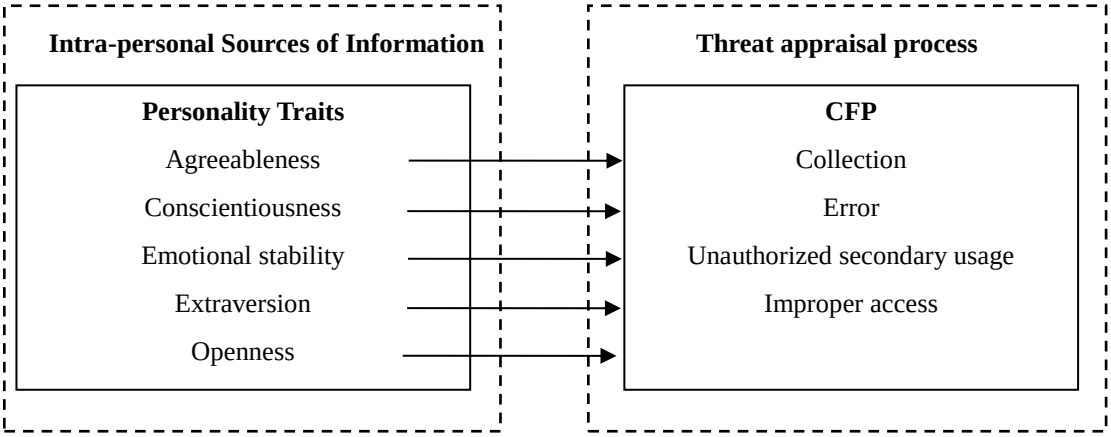


圖 3-6-8 Junglas *et al.* (2008)研究模式

4.Dinev and Hart (2004)模式

Dinev and Hart 驗證所發展衡量個人隱私顧慮量表，並提出兩個隱私顧慮前置影響變數，包含：由保護動機理論借用認知脆弱程度和認知控制能力兩個變數(如圖 3-6-9)。總共回收有效研究樣本 369 份，研究結果顯示所提量表的確具備足夠效度，在研究模式方面，認知脆弱程度對認知隱私顧慮有顯著影響，而認知控制能力對於認之隱私顧慮則不具顯著影響力。

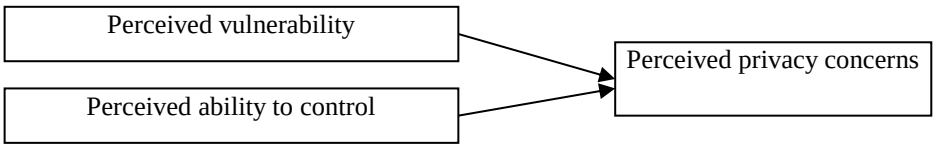


圖 3-6-9 Dinev and Hart (2004)研究模式

5.Youn (2009)模式

Youn (2009)以保護動機理論為研究理論基礎，提出一研究架構(如圖 3-6-10 所示)探討青少年對於網路的隱私顧慮以及其隱私保護行為，影響青少年對於線上隱私顧慮的因素，在人際間資訊來源構面包含：性別、網際網路使用經驗、說服知識；隱私知識等因素；在認知評價構面則包含易受到風險傷害、資訊揭露好處(Info. disclosure benefits)、隱私自我效能；此外，線上隱私顧慮則會影響青少年的隱私保護行為，包含：假造個人資訊、找尋其他資訊與壓抑自我不上網等因素。該研究共蒐集 144 份問卷資料，結果顯示易受到風險傷害對線上隱私顧慮有正向影響；而線上隱私顧慮對於青少年隱私保護行為，如找尋其他資訊有顯著影響。

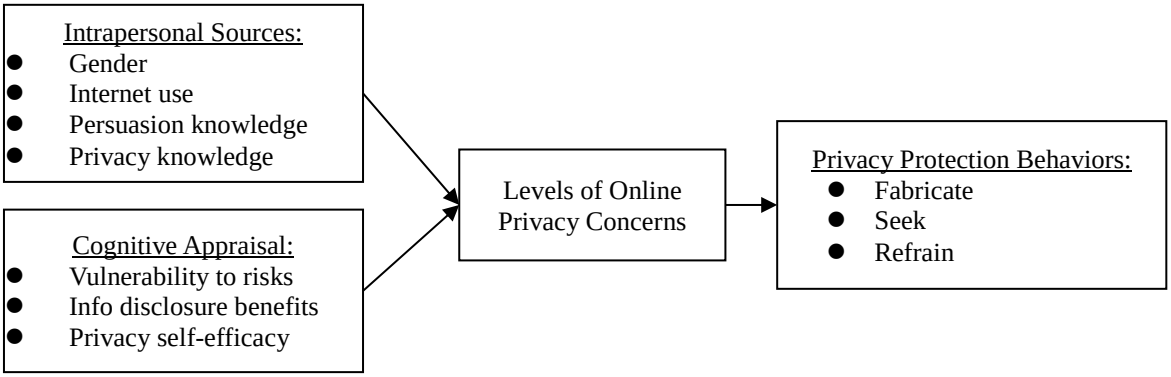


圖 3-6-10 Youn (2009)研究模式

(三)保護動機理論相關模式小結

本計畫進一步依據保護動機理論之變數，彙整前述各研究架構之研究結果(如表 3-6-1 所示)，結果顯示在認知脆弱性變數方面，除少部分研究(Herath and Rao, 2009; Vance *et al.*, 2012)外，大部份的研究結果均呈現顯著；至於認知嚴重性變數同樣少數研究結果(Ifinedo, 2012)不顯著，大部分均支持該變數的影響力；此外，亦有研究將認知脆弱與認知嚴重兩變數合併成認知威脅單一變數來衡量，結果亦呈現顯著現象(Siponen *et al.*, 2006; Siponen *et al.*, 2010)；而恐懼引發變數則較少研究驗證(Herath and Rao, 2009; Youn, 2009)，而結果也都呈顯著；至於回應成本變數的研究結果則較不一致，部分呈現顯著結果(Herath and Rao, 2009; Vance *et al.*, 2012)，其餘則為不顯著(Ifinedo, 2012)；而回應效能變數僅少部分研究結果(Siponen *et al.*, 2010)不顯著，其餘均呈顯著結果；自我效能變數於大部分研究亦同樣呈顯著結果，僅少部分研究不顯著(Youn, 2010)；至於主觀規範於大部分研究均呈現顯著現象(Herath and Rao, 2009; Ifinedo, 2010; Siponen *et al.*, 2006; Siponen *et al.*, 2010)；敘述性規範變數則僅少數研究進行驗證，其結果為顯著(Herath and Rao, 2009)；至於採用保護動機理論為主要研究架構，並且採用態度變數的研究並不多，結果亦呈現不一致現象，如 Ifinedo (2010)的結果為顯著，然 Herath and Rao (2009)的結果則呈現顯著現象。

表 3-6-1 以往保護動機理論研究結果彙整表

文獻	認知脆弱性	認知嚴重性	恐懼引發	回應成本	回應效能	自我效能	主觀規範	敘述性規範	態度
Ifinedo (2012)	V	X	N/A	X	V	V	V	N/A	V
Vance *et al.* (2012)	X	V	N/A	V	V	V	N/A	N/A	N/A
Siponen *et al.* (2010)	V (以認知威脅衡量)		N/A	N/A	X	V	V	N/A	N/A
Siponen *et al.* (2006)	V (以認知威脅衡量)		N/A	N/A	V	V	V	N/A	N/A
Herath and Rao (2009)	X	V	V	V	V	V	V	V	X
Youn (2005)	V	V	N/A	N/A	V	N/A	N/A	N/A	N/A
Dinev and Hart (2004)	V	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Youn (2009)	V	N/A	V (以線上隱私顧慮衡量)	N/A	V	X	N/A	N/A	N/A

註：V 表變數顯著；X 表變數不顯著； N/A 表未採用該變數

肆、研究方法

一、研究架構推導

由於違反電子病歷資訊隱私保護政策可能對於醫院及員工造成嚴重商譽與財務之負面影響，此影響可視為是一威脅，醫院員工便可能採取因應措施而啟動保護動機(例如遵循醫院對於電子病歷之隱私保護政策)，因此本計畫以保護動機理論為主要基礎之一；此外，由於醫院員工應當能自行決定其是否能夠遵循醫院隱私保護政策，因此本計畫再結合理性行為理論(Fishbein and Ajzen, 1975)，依據理性行為理論，個人行為意圖受到態度與主觀規範影響。

保護動機理論(Rogers, 1983)認為個人保護動機會經威脅評價、恐懼引發及回應評價等認知過程影響而產生，民眾對於威脅事項的評價過程，包含認知脆弱性(Perceived vulnerability)和認知嚴重性(Perceived severity)可能引發民眾對於威脅事項的恐懼，而民眾的恐懼便可能影響其對於威脅因應行為的態度。以醫院電子病歷情境而言，認知脆弱性指員工認為醫院的電子病歷資訊隱私破壞事件可能發生的機率(Herath and Rao, 2009)；認知嚴重性則指員工評估醫院電子病歷資訊隱私破壞事件的嚴重程度(Herath and Rao, 2009)；恐懼引發指員工認為電子病歷資訊隱私破壞事件(威脅)所帶來的恐懼程度(Rogers, 1983)。醫院員工對於電子病歷隱私破壞事件所認知脆弱性與嚴重性便可能讓員工產生恐懼，進而影響其對於電子病歷隱私保護政策之態度。其次，就回應評價過程而言，包含回應效能、自我效能及回應成本可能影像民眾對於威脅回應行為之態度。以醫院電子病歷情境而言，員工如對於電子病歷隱私保護政策是否能因應電子病歷破壞事件的認知越正面，而且也相信本身具備足夠能力遵循電子病歷隱私保護政策，加上不須額外花費大量的心力，則員工便可能對於電子病歷隱私保護政策態度越正向。藉由上述威脅評價與回應評價兩個過程對於員工態度產生影響，而依據理性行為理論，態度亦可能影響民眾的行為意圖，因此醫院員工對於電子病理隱私保護政策的態度便可能進一步影響其遵循電子病歷隱私保護政策的行為意圖。此外，依據理性行為理論，主觀規範可預測民眾的行為意圖，然而規範類變數在資訊科技情境研究中的影響相當複雜(Venkatesh et al., 2003)，因此本計畫再參考 Herath and Rao (2009)的研究將敘述性規範納入研究架構，以深入了解規範類變數對於電子病歷隱私保護政策遵循的影響。

依據上述研究架構推導，醫院資訊單位員工遵守醫院隱私保護政策行為意圖受到其對於醫院隱私保護政策的態度、主觀規範和敘述性規範影響，而員工態度則受到恐懼引發、回應效能、自我效能及回應成本影響；此外，恐懼引發亦受到認知脆弱和認知嚴重影響。依據上述理論架構，本計畫提出研究架構雛形(如圖 4-1-1 所示)包括：認知脆弱、認知嚴重、恐懼引發、回應效能、自我效能、回應成本、主觀規範、敘述性規範、對醫院電子病歷隱私保護政策態度與遵循醫院電子病歷隱私保護政策行為意圖等十個構面。

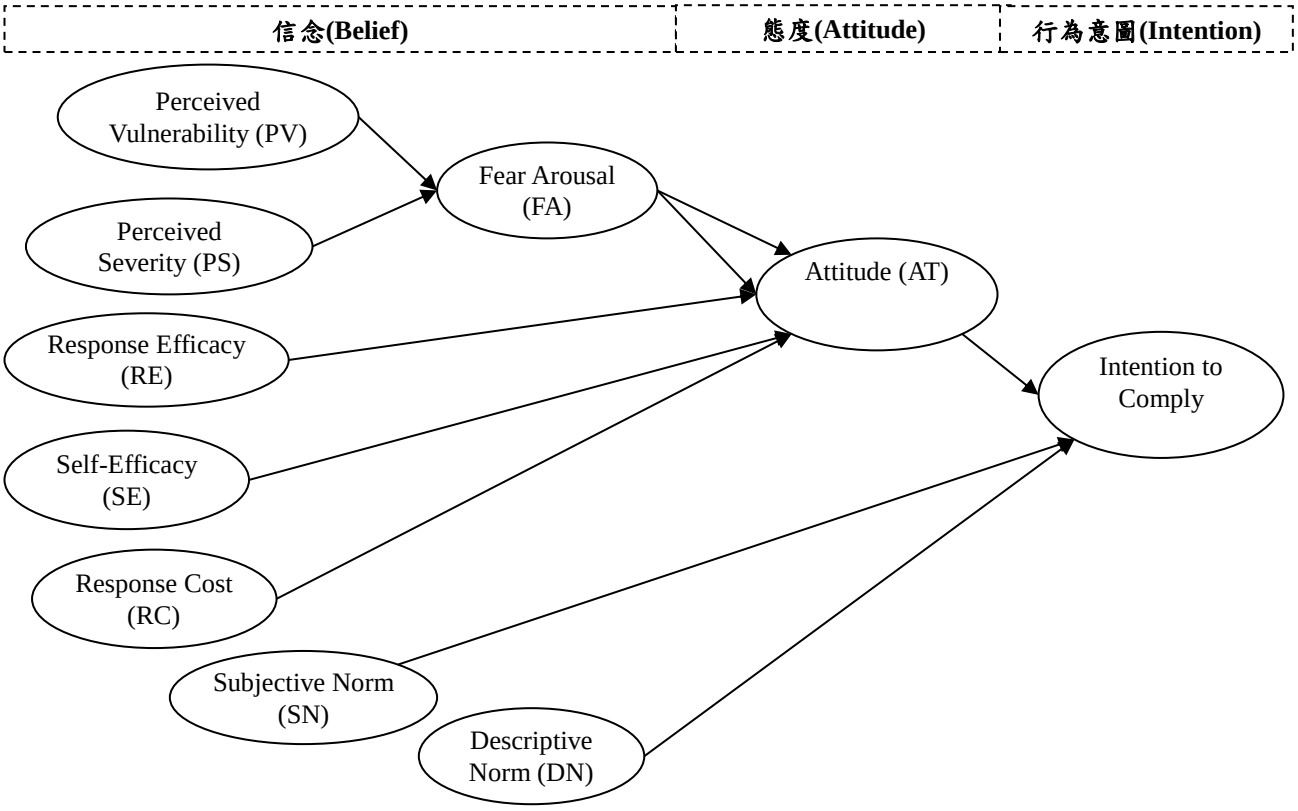


圖 4-1-1 研究架構

二、研究假說

依據本計畫所提出之研究架構，分別說明其假說推導以及支持文獻。

(一)認知脆弱與認知嚴重性對於恐懼引發之影響

「恐懼引發」指民眾對於威脅所感受到的恐懼程度(Milne *et al.*, 2000)，「認知脆弱性」指民眾認為本身會受到威脅影響的程度(Milne *et al.*, 2000)，亦即針對某一個潛在威脅，民眾感覺他/她會受到這個威脅影響的機率大小；而「認知嚴重性」則指民眾認為本身會受到威脅影響嚴重程度(Milne *et al.*, 2000)，亦即當某一個潛在威脅真的發生時，民眾感覺他/她會受到這個威脅傷害的程度大小。依據保護動機理論，當民眾感受到威脅發生機率越高以及威脅的影響越嚴重時，民眾越可能對於該威脅產生恐懼感，當民眾越感到恐懼時，便可能採取自我保護行為；以往保護動機理論主要目的之一即在於透過傳播訊息讓民眾感到恐懼，進而引發其對於可能的威脅產生保護行為(Rogers, 1983)；換言之，民眾對於威脅所認知的發生機率(認知脆弱程度)以及認知嚴重程度可能強化民眾對於威脅的恐懼。就本計畫情境而言，醫院中電子病歷隱私遭受破壞(例如電子病歷資訊外洩)對於醫院和員工均可視為是一種威脅，本計畫將「恐懼引發」定義為資訊單位員工認為醫院電子病歷資訊受到破壞事件威脅的程度(Herath and Rao, 2009)，「認知脆弱性」則定義為資訊單位員工認為醫院電子病歷資訊可能遭受隱私破壞事件(例如外洩)的機率(Crossler, 2010; Ifinedo, 2012)，至於「認知嚴重性」則定義為：資訊單位員工評估醫院電子病歷資訊可能遭受隱私破壞事件(例如電子病歷外洩)影響的嚴重程度

(Crossler, 2010; Herath and Rao, 2009)。當醫院資訊單位員工認為電子病歷系統可能因資訊安全措施不完整、人為蓄意或天災等因素遭到破壞，進而造成醫院財務或醫院聲譽的損失，影響病人的病歷隱私，甚至影響員工工作權時，依據保護動機理論觀點，醫院資訊單位員工便可能越在意該威脅事件的威脅，甚至產生恐懼，擔心發生電子病歷破壞事件極有可能發生，且其後果亦可能相當嚴重；反之，如果醫院資訊單位員工根本不重視電子病歷遭受破壞，甚至是否影響到病人隱私，則其可能根本不會在意電子病歷遭破壞的機率以及嚴重性，亦即資訊單位員工對於電子病歷破壞事件根本毫無畏懼感。以往文獻亦證實「認知脆弱性」和「認知嚴重性」對於「恐懼引發」具顯著影響；例如 Herath and Rao (2009)探討組織資訊安全政策遵循，以「資訊安全顧慮程度」變數衡量保護動機理論的「恐懼引發」變數，結果證實訊安全事件的認知嚴重性(Perceived severity)正向顯著影響「資訊安全顧慮程度」。Youn (2009)利用保護動機理論探討青少年對於網路隱私顧慮所採取的保護行為進行探討，Youn (2009)以網路隱私顧慮程度衡量保護動機理論中的恐懼引發，結果發現認知脆弱性的確對於網路隱私顧慮程度具顯著正向影響。Arthur and Quester (2004)探討菸害廣告對於降低吸菸行為意圖的研究顯示，發生傷害的機率(即認知脆弱性)以及傷害的嚴重性(即認知嚴重性)對於恐懼均具正向顯著影響。本計畫認為醫院資訊單位員工對於電子病歷破壞事件威脅所引發之恐懼，可能會受到員工對於電子病歷破壞事件所感受到的認知脆弱性及認知嚴重性的影響因而強化或減弱。依據上述文獻與討論，本計畫提出以下假說：

H_1：資訊單位員工對於電子病歷隱私破壞事件之認知脆弱性會正向影響其恐懼引發
H_2：資訊單位員工對於電子病歷隱私破壞事件之認知嚴重性會正向影響其恐懼引發

(二)恐懼引發對於態度之影響

「恐懼引發」指民眾對於威脅所感受到的恐懼程度(Milne *et al.*, 2000)，本計畫將「恐懼引發」定義為資訊單位員工認為醫院電子病歷資訊受到破壞事件威脅的程度(Herath and Rao, 2009)，亦即資訊單位員工感受到如電子病歷遭破壞時，可能對於醫院及員工個人產生不良影響的程度；「態度」則指資訊單位員工對於遵守醫院電子病歷隱私保護政策之正向或負向的感覺(Fishbein and Ajzen, 1975)。在電子病歷情境下，醫院電子病歷遭受破壞(例如電子病歷資訊外洩)可視為是一種威脅，依據保護動機理論，當民眾感受到威脅的嚴重或發生機率高時，便可對於威脅產生恐懼，並產生因應威脅保護行為之態度(Roger, 1983)；因此當資訊單位員工感受到電子病歷可能遭受破壞的威脅，且該威脅發生機率越高，便可能越在意該威脅，並採取較正面之態度；反之，如果該威脅並不足以讓員工產生恐懼感，則員工對於該威脅便可能不在意，亦即可能採取較消極之態度。Herath and Rao (2009)探討組織資訊安全政策遵循，以「資訊安全顧慮程度」變數衡量保護動機理論的「恐懼引發」變數，結果證實「資訊安全顧慮程度」正向顯著影響組織員工對於資訊安全政策的態度；Arthur and Quester (2004)探討菸害廣告對於降低吸菸行為意圖的研究顯示，恐懼於降低吸菸行為意圖的確具正向顯著影響。本計畫認為醫院資訊單位員工對於電子病歷破壞事件威脅所引發之恐懼，可能會影響資訊單位員工對於遵循電子病歷隱私保護政策的態度。依據上述文獻與討論，本計畫提出以下假說：

H_3：資訊單位員工對於電子病歷隱私破壞事件之恐懼引發正向影響其對於隱私保護政策態度

(三)回應效能對於態度之影響

「回應效能」指民眾認為回應作為(Coping response)是否能有效減少威脅的程度(Milne *et al.*, 2000)，本計畫將「回應效能」定義為：資訊單位員工認為遵守醫院隱私保護政策能有效防止電子病歷發生隱私破壞事件的程度(Crossler, 2010; Herath and Rao, 2009)，亦即資訊單位員工如果認為醫院所制定電子病歷資訊隱私保護政策對於電子病歷資訊破壞事件的回應效能越高，能有效處理電子病歷隱私破壞事件的發生，則資訊單位員工對於電子病歷隱私破壞事件的因應措施越有信心，則對於遵循電子病歷隱私保護政策之態度也會越正向；反之，如果資訊單位員工不認為電子病歷隱私破壞事件因應措施有實質效果，則其對於電子病歷隱私保護政策之態度也可能越不佳。以往文獻亦證實回應效能對於民眾所採取的保護行為或態度具正向顯著影響;例如 Lee (2011)利用保護動機理論探討大學教職員採用防抄襲系統之影響因素，結果發現回應效能顯著正向影響其採用之行為意圖；Crossler (2010)則利用保護動機理論探討民眾備份個人資料，結果發現回應效能對於備份個人資料具顯著正向影響；Bulgurcu *et al.* (2010)利用理性選擇理論(Rational choice theory)與資訊安全知曉(Awareness)觀點探討組織員工對於資訊安全規範遵循的認知，結果發現員工所認知遵循資訊安全政策(即回應效能)顯著正向影響其遵循資訊安全政策的行為意圖。Chenoweth *et al.* (2009)利用保護動機理論了解民眾使用防護性科技(如電腦防毒軟體)的認知，結果發現民眾的回應效能顯著正向影響其使用保護性科技的行為意圖。Lee and Larsen (2009)採用保護動機理論探討中小企業主管採用防止惡意軟體技術的認知，結果發現主管所認知回應效能顯著正向影響其採用行為意圖。Ifinedo (2012)利用保護動機理論探討組織員工對於資訊安全政策遵循的認知，實證結果發現員工的回應效能對於其遵循資訊安全政策規範的行為意圖具顯著正向影響。Herath and Rao (2009)探討組織資訊安全政策遵循，結果顯示組織員工針對資訊安全問題之回應效能正向顯著影響組織員工對於資訊安全政策的態度。依據上述文獻，本計畫提出以下假說：

H_4：資訊單位員工對於電子病歷隱私破壞事件之回應效能正向影響其對於電子病歷隱私保護政策態度

(四)自我效能對於態度之影響

「自我效能」指民眾認為本身是否具有足夠能力執行回應作為(Coping response)的程度(Milne *et al.*, 2000)，本計畫將自我效能定義為：資訊單位員工認為自己具有足夠能力遵守醫院隱私保護政策以防止電子病歷資訊發生隱私破壞事件(如電子病歷遭到入侵或外洩)的程度(Crossler, 2010; Herath and Rao, 2009)。資訊單位員工如果認為自己具備足夠能力遵循電子病歷隱私保護政策，則對於電子病歷隱私保護政策的態度亦可能越正面；反之，如果資訊單位員工對於遵循電子病歷隱私保護政策缺乏信心，則對於電子病歷隱私保護政策之態度也會越不佳。以往文獻亦證實自我效能對於民眾所採取的保護行為或態度具正向顯著影響;例如 Lee (2011)利用保護動機理論探討大學教職員採用防抄襲系統之影響因素,結果發現自我效能顯著正向影響其採用之行為意圖；Crossler (2010)則利用保護動機理論探討民眾備份個人資料，結果發現回應效能對於備份個人資料具顯著正向影響；Hu *et al.* (2012)探討組織員工遵循資訊安全政策的研究，發現知覺行為控制(Perceived behavioral control)對於員工遵循資訊安全政策之行為意圖呈現顯著正向影響，知覺行為控制指民眾對於執行某一行為的容易或困難程度，概念上與自我效能相近。Bulgurcu *et al.* (2010)利用理性選擇理論(Rational choice theory)與資訊安

全知曉(Awareness)觀點探討組織員工對於資訊安全規範遵循的認知，結果發現員工的自我效能顯著正向影響其遵循資訊安全政策的行為意圖。Lee and Larsen (2009)採用保護動機理論探討中小企業主管採用防止惡意軟體技術的認知，結果發現主管所認知自我效能顯著正向影響其採用行為意圖。Ifinedo (2012)利用保護動機理論探討組織員工對於資訊安全政策遵循的認知，實證結果發現員工的自我效能對於其遵循資訊安全政策規範的行為意圖具顯著正向影響。Herath and Rao (2009)探討組織資訊安全政策遵循，結果顯示組織員工遵循資訊安全政策的自我效能問題正向顯著影響組織員工對於資訊安全政策的態度。依據上述文獻，本計畫提出以下假說：

H_5：資訊單位員工遵循電子病歷隱私保護政策的自我效能正向影響其對於電子病歷隱私保護政策態度

(五)回應成本對於態度之影響

「回應成本」指民眾認為針對威脅所執行回應作為需耗費成本的程度(Milne *et al.*, 2000)，本計畫將回應成本定義為：醫院資訊單位員工認為遵守醫院隱私保護政策所需花費成本(Crossler, 2010; Ifinedo, 2012)。資訊單位員工如果認為遵循電子病歷隱私保護政策不須花費多的心力與時間，則對於電子病歷隱私保護政策的態度亦可能越正面；反之，如果資訊單位員工認為遵循電子病歷隱私保護政策須付出相當多的人力與時間，則對於電子病歷隱私保護政策之態度也會越不佳。以往文獻亦證實回應成本對於民眾所採取的保護行為或態度具顯著負向影響；例如 Lee (2011)利用保護動機理論探討大學教職員採用防抄襲系統之影響因素，結果發現回應成本顯著負向影響其採用之行為意圖；Bulgurcu *et al.* (2010)利用理性選擇理論(Rational choice theory)與資訊安全知曉(Awareness)觀點探討組織員工對於資訊安全規範遵循的認知，結果發現員工所認知遵循資訊安全政策成本(即回應成本) 負向顯著影響其遵循資訊安全政策的行為意圖。Chenoweth *et al.* (2009)利用保護動機理論了解民眾使用防護性科技(如電腦防毒軟體)的認知，結果發現民眾的回應成本顯著負向影響其使用保護性科技的行為意圖。Lee and Larsen (2009)採用保護動機理論探討中小企業主管採用防止惡意軟體技術的認知，結果發現主管所認知回應成本負向顯著影響其採用行為意圖。Herath and Rao (2009)探討組織資訊安全政策遵循，結果顯示組織員工遵循資訊安全政策的回應成本負向顯著影響組織員工對於資訊安全政策的態度。依據上述文獻，本計畫提出以下假說：

H_6：資訊單位員工對於電子病歷隱私政策遵循的回應成本負向影響其對於電子病歷隱私保護政策的態度

(六)態度對於行為意圖之影響

依據理性行為理論(Fishbein and Ajzen, 1975)，「態度」指民眾對於某一種行為所抱持正面或負面的感覺，在電子病歷情境下則指資訊單位員工對於遵守醫院隱私保護政策的正向或負向的感覺；「行為意圖」則指資訊單位員工遵守醫院資訊隱私保護政策的意願。此外，理性行為理論亦指出，民眾對於某一種行為的態度會正向影響其行為意圖，因此本計畫亦假定資訊單位員工對於醫院隱私保護政策的態度會影響其遵守該政策的行為意圖。以往文獻亦證實民眾的態度對於其行為意圖有正向的影響，例如 Herath and Rao (2009)針對員工遵循資訊安全政策的研究發現員工對於遵循資訊安全政策的態度越正面，則員工遵循資訊安全政策的行為意

圖也越高；以往資訊安全相關文獻(Bulgurcu *et al.*, 2010; Guo *et al.*, 2011; Hu *et al.*, 2012; Ifinedo, 2012)均證實組織員工對於組織資訊安全政策之遵循或違反的態度對於其行為意圖有正向顯著影響。依據上述文獻，本計畫提出以下假說：

H_7：資訊單位員工對於隱私保護政策態度正向影響其遵循電子病歷隱私保護政策的行為意圖

(七)主觀規範與敘述性規範對於行為意圖之影響

依據以往文獻(Fishbein and Ajzen, 1975; Herath and Rao, 2009; Taylor and Todd, 1995)，社會規範亦會影響民眾是否採取某一種行為，包含：主觀規範(Subjective norms)和敘述性規範(Descriptive norms)兩種規範，「主觀規範」指對於個人重要的其他人認為其是否應該執行該行為(Fishbein and Ajzen, 1975)，從他人期望的角度來看，而「敘述性規範」指個人認為其他人應執行該行為，個人則會採取相同行為的程度(Herath and Rao, 2009)，亦即個人對於他人行為的模仿。在電子病歷情境下，「主觀規範」指資訊單位員工認為對於其重要的其他人認為他是否必須遵守電子病歷隱私保護政策的程度；而「敘述性規範」則指資訊單位員工認為其他員工也都能遵守電子病歷隱私保護政策，而資訊單位員工也能採取同樣行為的程度。以往文獻證實主觀規範與敘述性規範正向顯著影響民眾之行為意圖，例如 Guo *et al.* (2011)針對組織中員工非惡意性的資訊安全違反行為進行研究，結果發現工作群組規範(Workgroup norm)對於其態度程顯著正向影響；Hu *et al.* (2012)同樣探討組織員工遵循資訊安全政策的研究發現主觀規範對於員工遵循資訊安全政策之行為意圖呈現顯著正向影響；Bulgurcu *et al.* (2010)利用理性選擇理論(Rational choice theory)與資訊安全知曉(Awareness)觀點探討組織員工對於資訊安全規範遵循的認知，結果發現員工的規範性信念(Normative beliefs)顯著正向影響其遵循資訊安全政策的行為意圖，亦即對於員工重要的人(例如主管、同儕等)讓員工所感受之無形社會壓力；Lee and Larsen (2009)採用保護動機理論探討中小企業主管採用防止惡意軟體技術的認知，結果發現主管所認知社會影響(Social influence)顯著正向影響其採用行為意圖；Siponen *et al.* (2010)探討組織員工對於資訊安全政策之遵循，結果發現規範性信念(Normative beliefs)顯著正向影響其遵循資訊安全政策的行為意圖；Ifinedo (2012)針對 124 位經理人及資訊專業人員進行資訊系統安全政策(Information systems security policy)遵循影響因素研究，證實主觀規範(Subjective norms)對於資訊安全政策遵循之行為意圖具顯著正向之影響；Herath and Rao (2009)同時探討主觀規範與敘述性規範對於員工遵循資訊安全政策之影響，結果發現兩者對於員工遵循資訊安全規範均具顯著正向影響。依據上述文獻，本計畫提出以下假說：

H_8：資訊單位員工所認知的主觀規範會正向影響其遵循電子病歷隱私保護政策之行為意圖

H_9：資訊單位員工所認知的敘述性規範會正向影響其遵循電子病歷隱私保護政策之行為意圖

三、變數操作型定義與衡量問項

依據保護動機理論與理性行為理論，本計畫總共採用 10 個變數，包括：認知脆弱性、認知嚴重性、恐懼引發、回應效能、自我效能、回應成本、主觀規範、敘述性規範、態度及行為意圖，底下分別針對 10 個變數之操作型定義與部分問項進行說明，本計畫完整問卷如附錄一所示。

(一)認知脆弱性

認知脆弱性在保護動機理論中指民眾認為本身會受到威脅影響的程度(Milne *et al.*, 2000)，亦即針對某一個潛在威脅，民眾感覺他/她會受到這個威脅影響的機率大小。由於本計畫的研究對象係針對資訊單位員工，因此在醫院電子病歷情境下，本計畫將認知脆弱性定義為資訊單位員工認為醫院電子病歷資訊可能遭受隱私破壞事件(例如外洩)的機率(Crossler, 2010; Ifinedo, 2012)。衡量問項(共 4 題)以 Ifinedo (2012)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)如果我未能遵守醫院所擬定的電子病歷資訊隱私保護政策，醫院可能容易發生電子病歷系統破壞事件(如遭到入侵而發生資訊外洩狀況)；2)如果我沒能遵守醫院的資訊隱私保護政策，我的電子病歷資訊隱私也可能遭受侵犯等問項。

(二)認知嚴重性

認知嚴重性在保護動機理論中指民眾認為本身會受到威脅影響嚴重程度(Milne *et al.*, 2000)；換言之，認知嚴重指民眾認為潛在威脅對於自己的影響高低程度。在醫院電子病歷情境下，本計畫將認知嚴重性定義為：資訊單位員工評估醫院電子病歷資訊可能遭受隱私破壞事件(例如外洩)的嚴重程度(Crossler, 2010; Herath and Rao, 2009)，衡量問項(共 3 題)以 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)我相信醫院的電子病歷資訊可能遭受到破壞事件入侵(例如遭到入侵，造成資訊外洩)；2)我相信醫院的營運和員工都可能受到電子病歷隱私破壞事件(例如遭到入侵，造成資訊外洩)的影響等問項。

(三)恐懼引發

恐懼引發在保護動機理論中指民眾對於威脅所感受到的恐懼程度(Milne *et al.*, 2000)。在醫院電子病歷情境下，本計畫將恐懼引發定義為：資訊單位員工認為醫院電子病歷資訊受到破壞事件威脅的程度(Herath and Rao, 2009)，衡量問項(共 3 題)以 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)電子病歷資訊隱私保護議題會直接影響醫院的形象與營運；2)電子病歷資訊隱私保護議題必須受到高度重視等問項。

(四)回應效能

回應效能在保護動機理論中指民眾認為回應作為(Coping response)是否能有效減少威脅的程度(Milne *et al.*, 2000)。在電子病歷情境下，本計畫將回應效能定義為：回應效能指資訊單位員工認為遵守醫院隱私保護政策能有效防止電子病歷發生隱私破壞事件的程度(Crossler, 2010; Herath and Rao, 2009)，衡量問項(共 3 題)以 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)對於協助醫院保護電子病歷資訊，每位員工都能有所幫助與作為；2)如果我能夠遵守醫院電子病歷隱私保護政策，我就能夠幫助醫院確保電子病歷資訊不至發生隱私破壞事件(如遭到入侵或外洩)等問項。

(五)自我效能

自我效能在保護動機理論中指民眾認為本身是否具有足夠能力執行回應作為(Coping response)的程度(Milne *et al.*, 2000)。在電子病歷情境下，本計畫將自我效能定義為：資訊單位員工認為自己具有足夠能力遵守醫院隱私保護政策以防止電子病歷資訊發生隱私破壞事件

(如遭到入侵或外洩)(Crossler, 2010; Herath and Rao, 2009)，衡量問項(共 3 題)以 Taylor and Todd (1995)與 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)我自信能遵守醫院大部分電子病歷隱私保護政策；2)如果我想要，我能夠很容易遵守醫院電子病歷隱私保護政策等問項。

(六)回應成本

回應成本在保護動機理論中指民眾認為針對威脅所執行回應作為需耗費成本的程度(Milne *et al.*, 2000)。在電子病歷情境下，本計畫將回應成本定義為：資訊單位員工認為遵守醫院隱私保護政策所需花費成本(Crossler, 2010; Ifinedo, 2012)，衡量問項(共 3 題)以 Ifinedo (2012)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)在醫院實施電子病歷資訊隱私保護措施需花費相當多成本(例如需採購相關資訊安全軟體、硬體等成本)；2)醫院要能夠落實電子病歷資訊隱私保護政策將會花費許多時間等問項。

(七)主觀規範

主觀規範指對民眾重要的其他人認為民眾是否應該執行該行為(Fishbein and Ajzen, 1975)，在電子病歷情境下，本計畫將主觀規範定義為資訊單位員工認為對於其重要的其他人認為他是否必須遵守醫院隱私保護政策的程度。衡量問項(共 4 題)以 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：醫院高階主管希望員工能遵守電子病歷資訊隱私保護政策；2)我的主管認為我應該遵守醫院電子病歷資訊隱私保護政策等問項。

(八)敘述性規範

敘述性規範指民眾認為其他人亦執行該行為的程度(Herath and Rao, 2009)。在電子病歷情境下，本計畫將敘述性規範定義為資訊單位員工認為其他員工也都能遵守醫院隱私保護政策，並採取相同行為之程度。衡量問項(共 3 題)以 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)我認為醫院其他員工能遵守電子病歷資訊隱私保護政策；2)我相信醫院其他員工能遵守電子病歷資訊隱私保護政策等問項。

(九)態度

在電子病歷情境下，本計畫將態度定義為資訊單位員工對於遵守醫院隱私保護政策的正向或負向的感覺(Fishbein and Ajzen, 1975)，衡量問項(共 3 題)以 Taylor and Todd (1995)與 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)電子病歷資訊隱私保護(例如不隨意查詢或外洩病人的病歷資訊)是一個好主意；2)電子病歷資訊隱私保護政策是重要的等問項。

(十)行為意圖

在電子病歷情境下，本計畫將行為意圖定義為：資訊單位員工遵守醫院資訊隱私保護政策的意願(Fishbein and Ajzen, 1975)，衡量問項(共 3 題)以 Herath and Rao (2009)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)我很可能遵守醫院的資訊隱私保護政策；2)遵守醫院的資訊隱私保護政策對我而言是可能的等問項。

四、研究樣本與抽樣

由於本計畫之探討主題為醫院員工對於電子病歷隱私政策保護之遵循，因此研究對象須具備電子病歷存取權限，而在醫院當中除醫護人員因照顧病人所需，因此必須具有存取電子病歷之權限外，資訊單位員工則是因維護電子病歷系統所需，亦具有電子病歷存取之權限；此外，就國內不同層級醫院而言，醫學中心往往較區域醫院和地區醫院具有較充足的財務與人力資源,電子病歷的建置與實施亦較完整,相對醫院員工依賴電子病歷的程度亦可能較高，因此本計畫以國內醫學中心資訊單位員工為主要調查對象，依據衛生福利部統計資料(行政院衛生福利部, 2014)，目前國內經評鑑通過之醫學中心共計 20 家，經本計畫聯繫共計有 7 家醫學中心的資訊單位願意協助本計畫之進行，並提供單一聯絡窗口，本計畫在確認具合作醫院之醫學中心資訊單位員工數量後，即依據各醫院資訊單位員工數寄發問卷，由各醫院資訊單位聯絡窗口協助發放與回收問卷。為提高問卷回收率，本計畫採獎勵方式，每完成一份問卷即可領取問卷調查費。此外，為確保本研究符合研究倫理，調查問卷發上前並經奇美醫學中心人體試驗委員會審查通過。在調查時間方面，本計畫自 2014 年 5 月 1 日開始進行問卷之發放與調查，截至 7 月 30 日止，共計招募 275 位資訊單位員工參與，由於本計畫委由各醫院資訊單位聯絡窗口確認問卷之完整性，在問卷填答完畢後，當場由連絡窗口檢查問卷，如發現問卷並未填答完整，當場即由連絡窗口請該院資訊單位員工補齊，所有問卷均完整填答。

五、資料分析方法

本計畫的資料分析過程可區分為四個階段，首先針對填答者基本資料進行分析，以瞭解樣本之人口學基本特性之分佈狀況，接著分析衡量工具之信度與效度，最後則進行研究假說之檢定。本計畫利用 SPSS ® 15 版分析填答者基本資料，而信度/效度分析與假說驗證部分則利用結構方程模式(Structural Equation Model)進行處理，以 SmartPLS® 2.0 M3 軟體(Ringle et al., 2005)進行結構方程模式分析。

伍、結果與討論

一、研究結果

本計畫分三部份進行研究結果之說明，首先是填答者基本資料之分析結果，其次則為本研究之信度與效度分析，最後則為研究假說之檢定結果。

(一)基本資料分析

在填答者基本資料方面，以男性較多，所佔比例約為 62.5%，女性所占比例為 37.5%。在年齡方面，所有填答者年齡均低於 65 歲，主要介於 30-49 歲之間，所佔比例約為 77.5%，其次為 20-29 歲之間，比例約佔 13.1%，50-64 歲之填答者最少，約佔 9.5%比例。在教育程度方面，以受過大學教育之比例最高，約為 50.9%，其次為研究所以上，約佔 42.2%，至於專科和高中/職所佔之比例均約為 6.9%。至於填答者職稱方面，最主要的填答者為程式設計師(約

佔 42.9%)，其次為其他資訊單位之行政人員(約佔 19.6%)；至於填答者在醫療產業的總工作年資超過 10 年者佔大多數(約佔 46.5%)，其次為 1-3 年工作經驗(約佔 26.2%)，填答者詳細基本資料如 5-1-1 所示。

表 5-1-1 填答者基本資料

類別	次分類	數量	百分比(%)
性別	男	172	62.5
	女	103	37.5
年齡	20 歲~29 歲	36	13.1
	30 歲~49 歲	213	77.5
	50 歲~64 歲	26	9.4
教育程度	高中/職	2	0.7
	專科	17	6.2
	大學	140	50.9
	研究所以上	116	42.2
職稱	管理階層(如一/二級主管等)	25	9.1
	系統分析師	28	10.2
	系統設計師	14	5.1
	程式設計師	118	42.9
	硬體/資料庫管理/網管人員	36	13.1
	其他	54	19.6
醫療產業工作年資	1-3 年	72	26.2
	4-6 年	46	16.7
	7-9 年	29	10.5
	>=10 年	128	46.5

至於填答者對於醫院電子病歷隱私保護政策方面(如表 5-1-2 所示)，表示「知道，也了解內容」者占大多數(約 67.6%)，表示「知道，但不了解內容」者為其次(約 30.2%)，至於表達「不知道者」最低，約佔 2.2%。

表 5-1-2 填答者是否了解醫院電子病歷隱私保護政策

類別	次分類	數量	百分比(%)
是否知道醫院電子病歷隱私保護政策	知道，也了解內容	186	67.6
	知道，但不了解內容	83	30.2
	不知道	6	2.2

(二)衡量模式分析

在衡量模式的分析方面，本研究依據以往文獻建議(Henseler *et al.*, 2009, p. 300; Hulland, 1999, p. 198)，分別針對信度與效度進行分析。

1.信度分析

所謂「信度」指所蒐集資料之結果能避免隨機衡量錯誤的狀況發生(Kline, 2005)，在信度分析方面，本研究分別針對(Henseler *et al.*, 2009; Hulland, 1999)：(1)個別問項負荷量(Individual item reliability)；(2)內部一致性(Internal consistency)進行分析。首先針對研究架構所使用之 10 個構面進行驗證性因素分析(Confirmatory Factor Analysis, CFA)，依據以往文獻(Henseler *et al.*, 2009; Hulland, 1999)建議個別問項負荷量之取捨標準 0.707，在第一次 CFA 過程中共有三題問項 FA2 (屬恐懼引發構面)、PS1(屬認知嚴重構面)、RC3(屬回應成本構面)之交叉負荷量低於 0.707 標準(分別為-0.32, 0.63 與 0.46)，因此將此三題移除，並再進行第二次 CFA，結果顯示各構面問項最低之交叉負荷量為 0.83 (DN1 問項，屬敘述性規範構面)，已符合 0.707 的建議值(如表 5-1-3 所示)。

其次在內部一致性評估方面，本研究以文獻中較常用之方式進行評估，包含組合信度(Composite Reliability, CR)(Fornell and Larcker, 1981; Wertz *et al.*, 1974) 與 Cronbach's α (Hair *et al.*, 2010)；以往研究(Fornell and Larcker, 1981)認為 CR 較 Cronbach's α 能更準確衡量信度，就本研究 CR 而言，可接受的 CR 值為 0.7 (Fornell and Larcher, 1981)，本研究 10 個構面中，最低的 CR 值為 0.87(恐懼引發)，亦具備足夠的信度；而 Cronbach's α 可接受的值為 0.7 (Hair *et al.*, 2010)，如果值超過 0.9 表示信度非常優秀(Excellent)，超過 0.8 則表非常好(Very good) (Kline, 2005)。在 Cronbach's α 方面，本研究 10 個構面中，最低的 Cronbach's α 值為 0.70(恐懼引發)，顯示具備足夠的信度(如表 5-1-3 所示)。此外，本研究所使用因此不論從 CR、Cronbach's α 或衡量問項之因素負荷量來判斷，本研究之衡量工具不論在個別問項或構面層級應均具備足夠之信度。

表 5-1-3 驗證性因素分析結果

Dimensions	Items	Mean	S.D.	Std. Loading	T-values	CR[a]	Cronbach's α	AVE[b]
Fear Arousal (FA)	FA1	6.09	0.95	0.86	20.22***	0.87	0.70	0.77
	FA3	6.00	0.95	0.89	21.29***			
Perceived Vulnerability (PV)	PV1	6.08	1.04	0.89	22.40***	0.94	0.92	0.81
	PV2	6.18	0.95	0.91	30.09***			
	PV3	6.19	0.94	0.86	22.03***			
	PV4	6.16	0.90	0.93	22.68***			
Perceived Severity (PS)	PS2	5.34	1.34	0.96	22.24***	0.96	0.91	0.91
	PS3	5.37	1.25	0.96	20.35***			
Response Efficacy (RE)	RE1	6.22	0.89	0.90	29.42***	0.93	0.89	0.82
	RE2	6.04	0.96	0.87	23.45***			
	RE3	6.09	0.89	0.94	30.03***			
Self-Efficacy (SE)	SE1	5.92	0.99	0.90	25.81***	0.93	0.89	0.83
	SE2	5.83	1.03	0.93	23.45***			
	SE3	5.75	1.03	0.90	23.68***			
Response Cost (RC)	RC1	5.69	1.04	0.92	20.37***	0.89	0.76	0.81
	RC2	5.72	0.97	0.87	22.15***			

註：CR 表組合信度(Composite Reliability)，計算方式為標準化係數平方值/(標準化係數平方值+標準化殘差)；AVE 表平均變異萃取量(Average Variance Extracted)，計算方式為標準化係數平方和之平均值，***p<0.001。

表 5-1-3 驗證性因素分析結果(續)

Dimensions	Items	Mean	S.D.	Std. Loading	T-values	CR[a]	Cronbach's α	AVE[b]
Subjective Norm (SN)	SN1	5.97	0.95	0.90	35.48***	0.96	0.94	0.84
	SN2	6.04	0.92	0.95	43.77***			
	SN3	5.84	1.01	0.90	46.36***			
	SN4	6.13	0.90	0.93	38.40***			
Descriptive Norm (DN)	DN1	5.35	1.06	0.83	15.09***	0.91	0.85	0.77
	DN2	5.55	1.05	0.89	24.92***			
	DN3	5.72	0.99	0.90	24.43***			
Attitude (AT)	AT1	6.01	0.94	0.94	58.98***	0.95	0.93	0.87
	AT2	6.16	0.88	0.95	61.81***			
	AT3	5.93	0.99	0.91	54.89***			
Intention to Comply (IC)	IC1	6.08	0.87	0.96	68.24***	0.97	0.96	0.92
	IC2	6.08	0.88	0.97	68.37***			
	IC3	6.06	0.91	0.95	74.34***			

註：CR 表組合信度(Composite Reliability)，計算方式為標準化係數平方值/(標準化係數平方值+標準化殘差)；AVE 表平均變異萃取量(Average Variance Extracted)，計算方式為標準化係數平方和之平均值，***p<0.001。

2.效度分析

所謂的「效度」指衡量工具能準確測量所要衡量的概念(Hair *et al.*, 2010)。一般而言常透過內容效度(Content validity)、收斂效度(Convergent validity)與區別效度(Discriminant validity)來衡量(Hair *et al.*, 2010; Trochim, 2001)。

(1)內容效度

「內容效度」主要評估所用於測量概念的問項是否足以衡量該概念(Hair *et al.*, 2010)，因此此種效度有時被稱為表面效度(Face validity)(Hair *et al.*, 2010; Trochim, 2001)，主要藉由專家來判斷，本研究先由完整的文獻探討，藉以找出和本研究概念相關且經過實際驗證過之衡量問項，之後再經由多次專家會議修訂衡量問項，同時修訂問項語句、問項長度等特性，確保研究衡量問項具備足夠之內容效度。

(2)收斂效度

「收斂效度」指變數衡量問項具有單一構面度，亦即衡量問項均收斂於單一構面(Hair *et al.*, 2010)，判斷衡量問項是否具備足夠收斂效度之準則包括：1)衡量問項之標準化因素負荷量值大於 0.5 且顯著(Bagozzi *et al.*, 1991, p. 434; Bagozzi and Yi, 1988, p. 82)；2)CR 值大於 0.6 (Bagozzi and Yi, 1988, p. 82)；及 3)平均變異萃取量(Average variance extracted, AVE)大於 0.5 (Bagozzi and Yi, 1988, p. 82; Fornell and Larcker, 1981)。本研究 10 個構面之衡量問項之標準化因素負荷量最低為 0.83(敘述性規範 DN1)，其餘均大於 0.5，且所有衡量問項亦呈現顯著性(如表 5-1-3 所示)；其次，本研究構面中最低之 CR 為 0.87(恐懼引發構面)，高於 0.6 之建議值(如表 5-1-3 所示)；第三，本研究構面最低之 AVE 為 0.77(恐懼引發構面)，亦高於 0.5 的建議水準(如表 5-1-3 所示)。由上述結果顯示本研究所採用之衡量工具具備足夠之收斂效度。

(3)區別效度

「區別效度」主要用以確認特定構面與相同研究模式中之其他構面是不相同的(Hulland, 1999)，本研究以 Fornell and Larcker (1981)平均變異萃取量(AVE)法來檢定區別效度。Fornell and Larcker 認為只要構面的 AVE 開平方根植大於與其他構面間的相關係數，則代表研究構面具備足夠區別效度。依據 Fornell and Larcker (1981)的方法進行研究構面區別效度之檢定，結果顯示所有構面之 AVE 平方根值均大於其他構面間之相關係數(如表 5-1-4 所示)，顯示本研究之構面應具備足夠之區別效度。此外，區別效度亦可由因素分析交叉負荷量(Cross loadings)來判斷(Chin, 1998, p.321; Chin, 2010, p.671)，本研究各衡量問項以原本所歸屬變數之交叉負荷量最大(如表 5-1-5 所示)，顯示各構面與衡量問項均應具備足夠區別效度。經上述檢定，本研究之問項與構面應同時具備足夠收斂效度與區別效度，可進行下一階段結構模式檢定。

表 5-1-4 構面間相關係數表

	A	B	C	D	E	F	G	H	I	J
Fear Arousal (A)	**0.88**									
Perceived Vulnerability (B)	0.65	**0.90**								
Perceived Severity (C)	0.43	0.35	**0.96**							
Response Efficacy (D)	0.75	0.70	0.33	**0.91**						
Self-Efficacy (E)	0.64	0.63	0.25	0.75	**0.91**					
Response Cost (F)	0.47	0.47	0.30	0.55	0.57	**0.90**				
Subjective Norm (G)	0.66	0.62	0.29	0.74	0.70	0.53	**0.92**			
Descriptive Norm (H)	0.54	0.45	0.20	0.53	0.62	0.38	0.66	**0.88**		
Attitude (I)	0.71	0.71	0.36	0.75	0.74	0.51	0.75	0.64	**0.93**	
Intention to Comply (J)	0.71	0.68	0.33	0.78	0.77	0.51	0.80	0.64	0.86	**0.96**

註：對角線為 AVE 平方根值

表 5-1-5 交叉負荷量(Cross Loadings)

	Fear Arousal	Perceived Vulnerability	Perceived Severity	Response Efficacy	Self-Efficacy	Response Cost	Subjective Norm	Descriptive Norm	Attitude	Intention to Comply
FA1	**0.86**	0.59	0.41	0.59	0.47	0.42	0.54	0.45	0.56	0.56
FA3	**0.89**	0.55	0.35	0.72	0.64	0.41	0.62	0.50	0.68	0.68
PV1	0.53	**0.89**	0.34	0.60	0.52	0.41	0.52	0.37	0.59	0.56
PV2	0.55	**0.91**	0.31	0.59	0.54	0.43	0.52	0.36	0.60	0.56
PV3	0.60	**0.86**	0.28	0.64	0.56	0.40	0.59	0.42	0.66	0.63
PV4	0.64	**0.93**	0.34	0.70	0.63	0.43	0.61	0.46	0.70	0.67
PS2	0.40	0.33	**0.96**	0.32	0.25	0.26	0.27	0.21	0.35	0.32
PS3	0.42	0.35	**0.96**	0.31	0.23	0.31	0.29	0.18	0.33	0.31
RE1	0.72	0.65	0.30	**0.90**	0.70	0.48	0.68	0.51	0.72	0.72
RE2	0.61	0.58	0.28	**0.87**	0.58	0.48	0.60	0.43	0.58	0.64
RE3	0.71	0.68	0.32	**0.94**	0.74	0.54	0.71	0.50	0.74	0.74
SE1	0.61	0.57	0.24	0.70	**0.90**	0.52	0.65	0.61	0.66	0.72
SE2	0.60	0.59	0.23	0.69	**0.93**	0.52	0.66	0.56	0.71	0.71
SE3	0.53	0.55	0.22	0.66	**0.90**	0.53	0.60	0.53	0.64	0.67
RC1	0.45	0.42	0.27	0.56	0.58	**0.92**	0.53	0.35	0.51	0.51
RC2	0.40	0.42	0.26	0.41	0.44	**0.87**	0.41	0.32	0.39	0.38
SN1	0.58	0.55	0.27	0.65	0.60	0.46	**0.90**	0.60	0.66	0.71
SN2	0.60	0.59	0.26	0.69	0.67	0.50	**0.95**	0.58	0.70	0.76
SN3	0.58	0.52	0.27	0.62	0.64	0.45	**0.90**	0.63	0.64	0.72
SN4	0.67	0.63	0.29	0.75	0.66	0.53	**0.93**	0.63	0.74	0.77

表 5-1-5 交叉負荷量(Cross Loadings)(續)

	Fear Arousal	Perceived Vulnerability	Perceived Severity	Response Efficacy	Self-Efficacy	Response Cost	Subjective Norm	Descriptive Norm	Attitude	Intention to Comply
DN1	0.36	0.29	0.10	0.33	0.45	0.29	0.47	**0.83**	0.40	0.42
DN2	0.49	0.41	0.22	0.52	0.59	0.33	0.62	**0.89**	0.63	0.61
DN3	0.54	0.46	0.19	0.52	0.57	0.36	0.62	**0.90**	0.62	0.61
AT1	0.68	0.67	0.34	0.71	0.72	0.48	0.72	0.64	**0.94**	0.79
AT2	0.67	0.67	0.32	0.71	0.67	0.47	0.71	0.58	**0.95**	0.81
AT3	0.65	0.65	0.34	0.70	0.68	0.46	0.66	0.58	**0.91**	0.80
IC1	0.68	0.64	0.34	0.75	0.73	0.49	0.76	0.60	0.82	**0.96**
IC2	0.69	0.67	0.33	0.75	0.73	0.49	0.77	0.61	0.83	**0.97**
IC3	0.67	0.65	0.27	0.73	0.75	0.48	0.79	0.63	0.82	**0.95**

(三)結構模式分析

當衡量模式具備足夠信度與效度，便可接著進行結構模式檢定，依據 Henseler et al. (2009, p.298)建議，結構模式主要針對內生變數變異解釋程度與路徑係數估計(Estimate)進行檢定；此外，本計畫並針對整體研究架構之適配度進行評估。

1.模式適配度(Goodness-of-Fit, GoF)

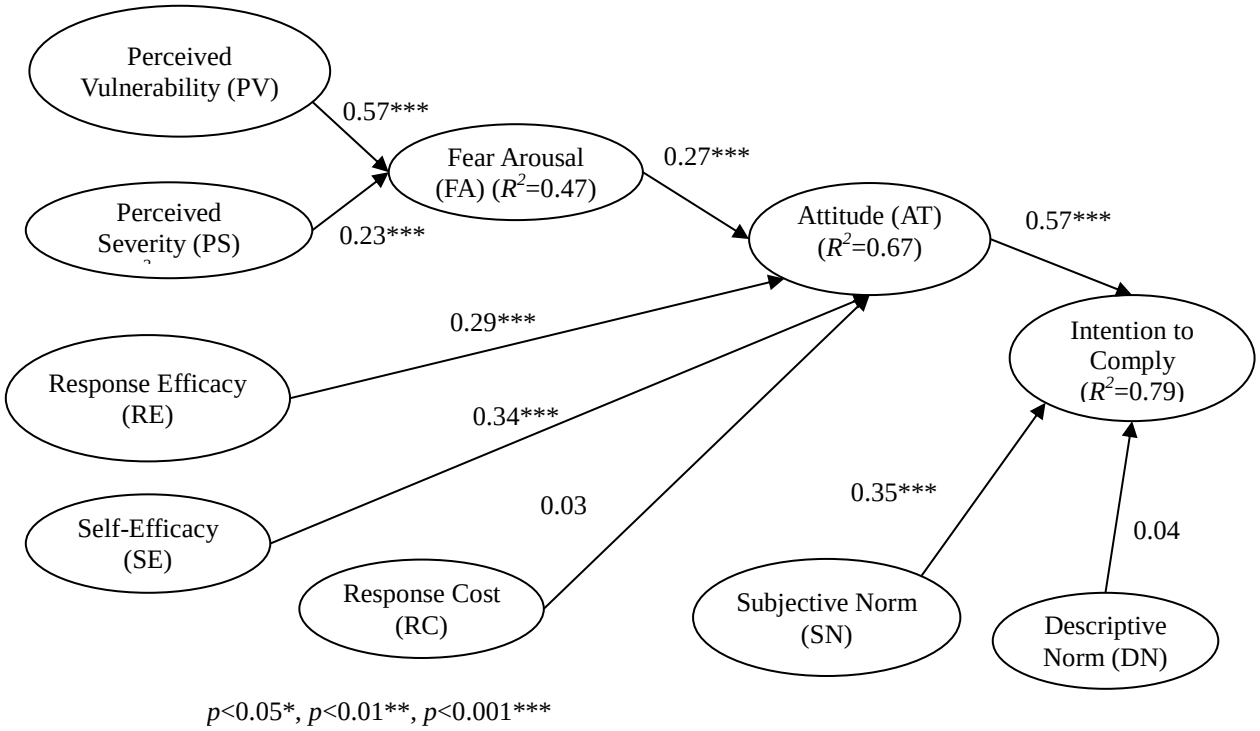
針對整體模式適配度之衡量，Tenenhaus *et al.* (2005)提出 GoF 指標可用於衡量 PLS 模式適配度，其計算公式為內生變數之平均共同性(Average communality)與平均 R^2 之開根號值。而 PLS 之共同性與平均變異萃取量相同(Wetzels et al., 2009, p. 187)，本計畫研究模式之內生變數(恐懼引發、態度與行為意圖)之平均共同性為 0.85 ((0.768+0.872+0.923)/3)，而平均 R^2 為 0.64 ((0.0.470+0.669+0.794)/3)，因此 GoF 為$\sqrt{}$(0.85*0.64) = 0.74，依據(Wetzels et al., 2009, p. 187)建議：GoF 值為 0.02 屬於低度適配，0.13 屬於中等適配度，0.26 則屬於高度適配，顯示本計畫之模式適配度應屬可接受之程度。

2.內生變數變異解釋程度(R^2)

經由 PLS 所計算之 R^2 與複迴歸所得到 R^2 之解讀方式相同，皆可用於說明外生變數對整體變異解釋能力(Henseler *et al.*, 2009)，在內生變數解釋能力程度，認知脆弱性(Perceived Vulnerability)與認知嚴重性(Perceived Severity)共同解釋恐懼引發(Fear Arousal)約 47%變異；而恐懼引發、回應效能(Response Efficacy)、自我效能(Self-Efficacy)和回應成本(Response Cost)共同解釋「態度(Attitude)」約 66.9%的變異；態度、主觀規範(Subjective Norm)和敘述性規範(Descriptive Norm)對於資訊單位員工遵循電子病歷隱私保護政策之行為意圖約 79%的變異(如圖 5-1-1)。Chin (1998, p.323)認為 R^2 等於 0.67 時具有「相當(Substantial)解釋力」，R^2 等於 0.33 時則具「中等程度(Moderate)解釋力」，本計畫之研究模式應具相當解釋能力。

3.路徑係數估計

本階段主要目的為計算外部模式間的路徑係數估計值，並依據路徑係數方向性、強度以及顯著性來評估。本研究路徑係數顯著性利用透過環靴法(Bootstrapping)計算，結果顯示認知脆弱性對於恐懼引發具有正向顯著影響(假說 H_1 成立, $\beta = 0.57$, $p < 0.001$)；認知嚴重性對於恐懼引發具正向顯著影響(假說 H_2 成立, $\beta = 0.23$, $p < 0.001$)；恐懼引發對於態度具有正向顯著影響(假說 H_3 成立, $\beta = 0.27$, $p < 0.001$)；回應效能對於態度具有正向顯著影響(假說 H_4 成立, $\beta = 0.29$, $p < 0.001$)；自我效能對於態度則具有正向顯著影響(假說 H_5 成立, $\beta = 0.34$, $p < 0.001$)，回應成本對於態度則不具有顯著影響(假說 H_6 不成立)；態度對於行為意圖具正向顯著影響(假說 H_7 成立, $\beta = 0.57$, $p < 0.001$)；主觀規範對於行為意圖具正向顯著影響(假說 H_8 成立, $\beta = 0.35$, $p < 0.001$)；敘述性規範對於行為意圖具正向顯著影響(假說 H_9 不成立)，結構模式分析結果如圖 5-1-1 所示，假說檢定結果如表 5-1-6 所示。



p<0.05*, *p*<0.01**, *p*<0.001***

圖 5-1-1 結構模式結果

表 5-1-6 假說檢定結果

假說	內容	t 值	成立否？
H_1	Perceived Vulnerability → Fear Arousal	11.10***	是
H_2	Perceived Severity → Fear Arousal	3.92***	是
H_3	Fear Arousal →Attitude	4.67***	是
H_4	Response Efficacy→Attitude	3.49***	是
H_5	Self-Efficacy→Attitude	4.65***	是
H_6	Response Cost→Attitude	0.58	否
H_7	Attitude→Intention to Comply	7.76***	是
H_8	Subjective Norm→Intention to Comply	5.12***	是
H_9	Descriptive Norm→Intention to Comply	1.06	否

p<0.05*, *p*<0.01**, *p*<0.001***

二、研究結果討論

(一) 認知脆弱與認知嚴重性對於恐懼引發之影響

本計畫假說 H_1 為「資訊單位員工對於電子病歷隱私破壞事件之認知脆弱性會正向影響其恐懼引發」，依據結構方程模式分析結果($\beta = 0.57, t = 11.10, p < 0.001$)，顯示假說 H_1 成立。「認知脆弱性」對於「恐懼引發」具正向顯著影響；換言之，資訊單位員工如感受到電子病歷遭受破壞的機率相當大，依據保護動機理論，則資訊單位員工便越可能感受到此威脅，亦即可

能引發資訊單位員工的恐懼感，擔心電子病歷可能受到破壞所造成的負面影響；反之，如果資訊單位員工認為電子病歷遭受破壞的機率並不高，則其對於電子病歷遭受破壞亦不會產生恐懼感。本計畫於醫療情境進行，「認知脆弱性」對於「恐懼引發」影響之研究結果與以往在其他領域(Arthur and Quester, 2004; Herath and Rao, 2009; Youn, 2009)之研究結果相同。

其次，本計畫假說 H_2 為「資訊單位員工對於電子病歷隱私破壞事件之認知嚴重性會正向影響其恐懼引發」，依據結構方程模式分析結果($\beta = 0.23$, $t = 3.92$, $p < 0.001$)，顯示假說 H_2 成立。「認知嚴重性」對於「恐懼引發」具正向顯著影響；換言之，資訊單位員工如感受到電子病歷遭受破壞時對於醫院甚至個人的影響相當大時，依據保護動機理論，則資訊單位員工便越可能感受到此威脅，亦即可能引發資訊單位員工的恐懼感，擔心電子病歷可能受到破壞所造成的嚴重影響；反之，如果資訊單位員工認為電子病歷遭受破壞所造成影響並不大，則其對於電子病歷遭受破壞亦不會產生恐懼感。

依據本計畫研究結果：資訊單位員工對於電子病歷遭破壞之「認知脆弱性」與「認知嚴重性」對於其「恐懼引發」均具正向顯著影響，換言之，當資訊單位員工了解電子病歷隱私極有可能遭受破壞，而且對於醫院甚至員工本身所產生的影響程度相當大時，則越能引發其對於電子病歷產生憂慮甚至恐懼的認知，進而引發其保護電子病歷隱私的動機。醫院資訊單位員工因職務所需，除了醫護人員外，有較多機會能接觸到電子病歷，因此須確保資訊單位員工真的能深切體認電子病歷遭破壞的可能性以及嚴重性，進而激發其採取保護電子病歷隱私之認知。依據研究結果，本計畫建議醫院應當讓資訊單位員工能夠充分了解：儘管電子病歷雖然有許多保護措施，包括如：醫院須通過 ISO 27001 之安全認證、電子病歷系統檢查以及必須制訂有電子病歷安全防護規範等，然而電子病歷卻仍可能遭受到醫院內部或外部人員的入侵、破壞等潛在威脅，且這些威脅均可能發生，且萬一這些威脅真的發生時，其影響程度也相當的嚴重，進而引發資訊單位員工能產生憂患意識，擔心電子病歷遭受破壞威脅，如此才能激發其保護電子病歷隱私的動機。

(二) 恐懼引發對於態度之影響

本計畫假說 H_3 為「資訊單位員工對於電子病歷隱私破壞事件之恐懼引發正向影響其對於電子病歷隱私保護政策態度」，依據結構方程模式分析結果($\beta = 0.27$, $t = 4.67$, $p < 0.001$)，顯示假說 H_3 成立。「恐懼引發」對於「態度」具正向顯著影響；換言之，資訊單位員工如感受到電子病歷遭受破壞的威脅相當大，依據保護動機理論觀點，資訊單位員工便越可能採取保護自我的態度，亦即越可能產生傾向遵循電子病歷保護政策的態度；反之，如果資訊單位員工認為電子病歷遭受破壞的威脅並不大，則其便可能產生認為不須遵循電子病歷隱私保護政策的態度。本計畫於醫療情境進行，「恐懼引發」對於「態度」影響之研究結果與以往在其他領域(Herath and Rao, 2009)之研究結果相同。

依據本計畫研究結果：資訊單位員工對於電子病歷遭破壞之「恐懼引發」對於其遵循電子病歷隱私保護政策「態度」具正向顯著影響；換言之，當資訊單位員工對於電子病歷遭破壞之威脅感到恐懼時，則其對於電子病歷隱私保護政策之態度也越趨積極，越有可能採取遵循之行為。了解電子病歷隱私極有可能遭受破壞，而且對於醫院甚至員工本身所產生的影響程度相當大時，則越能引發其對於電子病歷產生憂慮甚至恐懼的認知，進而引發其保護電子

病歷隱私的動機。依據研究結果，本計畫建議醫院須激發資訊單位員工對於電子病歷破壞事件的恐懼感，藉由說明此類破壞事件將對於醫院以及員工可能造成的影響，因而引發資訊單位員工的憂患意識，進而激發其採取保護行為因應電子病歷破壞之威脅。

(三) 回應效能對於態度之影響

本計畫假說 H_4 為「資訊單位員工對於遵循電子病歷隱保護政策回應效能正向影響其對於電子病歷隱私保護政策態度」，依據結構方程模式分析結果($\beta = 0.29$, $t = 3.49$, $p < 0.001$)，顯示假說 H_4 成立。「回應效能」對於「態度」具正向顯著影響；換言之，資訊單位員工如感受到電子病歷隱私保護政策對於保護電子病歷具有良好效果，依據保護動機理論觀點，資訊單位員工便越可能對於威脅因應措施的態度越積極，亦即對於遵循電子病歷隱私保護政策的態度越正向；反之，如果資訊單位員工認為電子病歷隱私破壞威脅的因應措施不具效果，則資訊單位員工便可能不認同電子病歷隱私保護政策，對於遵循該政策的態度便可能越不積極。本計畫於醫療情境進行，「回應效能」對於「態度」影響之研究結果與以往在其他領域(Herath and Rao, 2009; Ifinedo, 2012)之研究結果相同，Vance *et al.* (2012)的研究則證實回應效能對於遵循資訊安全政策之行為意圖具顯著正向影響。

依據本計畫研究結果：資訊單位員工所認知電子病歷隱私保護政策之「回應效能」對於其遵循電子病歷隱私保護政策「態度」具正向顯著影響；換言之，當資訊單位員工對於電子病歷隱私保護政策之功效越有信心時，則其對於電子病歷隱私保護政策之態度也將越積極，越有可能採取遵循之行為。依據研究結果，本計畫建議醫院須確保所擬定之電子病歷隱私保護政策確實能有效防範、及因應電子病歷隱私破壞事件，並讓資訊單位以及全院各單位員工能落實遵循，以因應電子病歷隱私破壞事件之威脅。

(四) 自我效能對於態度之影響

本計畫假說 H_5 為「資訊單位員工遵循電子病歷隱私保護政策的自我效能正向影響其對於隱私保護政策態度」，依據結構方程模式分析結果($\beta = 0.34$, $t = 4.65$, $p < 0.001$)，顯示假說 H_5 成立。「自我效能」對於「態度」具正向顯著影響；換言之，資訊單位員工如果自覺有信心執行電子病歷遭受破壞威脅的因應措施，依據保護動機理論觀點，資訊單位員工便越可能對於威脅因應措施的態度越積極，亦即對於遵循電子病歷隱私保護政策的態度越正向；反之，如果資訊單位員工認為電子病歷隱私破壞威脅的因應措施過於複雜，本身並未具備完成能力，則資訊單位員工便可能認為其無法遵循電子病歷隱私保護政策，對於遵循該政策的態度便可能越不積極。本研究於醫療情境進行，「自我效能」對於「態度」影響之研究結果與以往在其他領域(Herath and Rao, 2009; Ifinedo, 2012)之研究結果相同。

依據本計畫研究結果：資訊單位員工所認知遵循電子病歷隱私保護政策之「自我效能」對於其遵循電子病歷隱私保護政策「態度」具正向顯著影響；換言之，當資訊單位員工對於遵循與落實電子病歷隱私保護政策越有信心時，則其對於電子病歷隱私保護政策之態度也將越積極，越有可能採取遵循之行為。依據研究結果，本計畫建議醫院須確保所擬定之電子病歷隱私保護政策所規範之內容應說明清楚，且執行步驟亦需簡單且易於執行，過於複雜的電子病歷隱私保護政策雖然內容可能相當完整，然卻可能導致資訊單位員工感到不易遵循與執行，反而降低其遵循之意願。

(五) 回應成本對於態度之影響

本計畫假說 H_6 為「資訊單位員工對於電子病歷隱私政策遵循的回應成本負向影響其對於電子病歷隱私保護政策的態度」，依據結構方程模式分析結果($\beta = 0.03, t = 0.58$)，顯示假說 H_6 不成立。亦即「回應成本」對於「態度」不具影響力；換言之，不論資訊單位員工評估電子病歷遭受破壞威脅的因應措施所需花費的心力高低，都無法影響其對於遵循電子病歷保護政策的態度。本計畫推論假說 H_6 不顯著的可能原因如下：本計畫用於衡量回應成本之問卷項目分別著重於實施電子病歷隱私保護所需額外花費之軟硬體成本、落實電子病歷隱私保護政策須花費許多時間、以及實施電子病歷保護政策可能造成員工工作不便等主題。首先就推動電子病歷隱私保護政策須額外花費之軟硬體成本而言，一般組織如須強化其資訊系統安全，勢必增加額外的硬體與軟體以達成其目的，就醫院而言也是同樣狀況，然而近幾年衛生主管機關為加速國內電子病歷的推動，陸續提供經費贊助各醫院採購電子病歷所需之軟體與硬體，甚至補助 ISO 27001 資訊安全認證之費用，可能因而導致資訊單位員工認知其醫院並未額外投入成本；其次，病歷資訊隱私的保護在以往紙本病歷時代便開始要求，紙本病歷的隱私保護政策基本上與電子病歷隱私保護政策大致相同，主要差異處在於電子病歷係採用資訊系統加上網路的方式來處理與存放，因此電子病歷隱私保護政策須針對病歷電子化之後可能發生的隱私問題詳加規範，對於資訊單位員工而言，可能認知醫院原本即已實施落實電子病歷保護政策，而不需花費更多時間來落實；此外，許多電子病歷隱私保護政策實際上已融入電子病歷系統中，例如帳號密碼管控、使用權限控管等，更可能造成資訊單位員工認為日常使用電子病歷便已部分遵循電子病歷隱私保護政策，因此不需花費額外時間；最後，實施電子病歷隱私保護政策是否造成員工工作不便，電子病歷實際上解決以往紙本病歷的許多問題，包括：無法長久保存、無法多人同時閱讀、有地點限制等，因此電子病歷對於醫院員工而言反而是一更方便的病歷處理方式，也可能造成回應成本不顯著。Ifinedo (2012)針對資訊系統安全政策(Information systems security policy, ISSP)遵循影響因素研究中亦發現回應成本對於員工遵循資訊系統安全政策並無顯著影響。

依據本計畫研究結果：資訊單位員工所認知遵循電子病歷隱私保護政策之「回應成本」對於其遵循電子病歷隱私保護政策「態度」並未具顯著影響；換言之，不論資訊單位員工認知遵循電子病歷隱私保護政策是否需花費額外成本或時間，對於其電子病歷隱私保護政策之態度並無顯著影響。儘管此變數並不顯著，然本計畫認為醫院實施與落實電子病歷隱私保護政策勢必花費一定之成本，不論是就醫院層級或員工個人角度來看，此部分成本仍需讓醫院員工瞭解，更重要的是讓員工能瞭解電子病歷隱私保護的重要性遠超過所需的成本，員工應儘全力保護電子病歷隱私。

(六) 態度對於行為意圖之影響

本計畫假說 H_7 為「資訊單位員工對於隱私保護政策態度正向影響其遵循電子病歷隱私保護政策的行為意圖」，依據結構方程模式分析結果($\beta = 0.57, t = 7.76, p < 0.001$)，顯示假說 H_7 成立。「態度」對於「行為意圖」具正向顯著影響；換言之，如果資訊單位員工對於遵循電子病歷隱私保護政策之態度相當積極，依據理性行為理論，則其對於遵循電子病歷隱私保護政策的行為意圖亦較積極；反之，如果資訊單位員工對於遵循電子病歷隱私保護政策的態度並不積極，則其對於遵循電子病歷隱私保護政策之行為意圖則同樣不會積極。本計畫於醫療情

境進行,「態度」對於「行為意圖」影響之研究結果與以往在其他領域，包括資訊安全(Ifinedo, 2012)之研究結果相同。

依據本計畫研究結果：資訊單位員工遵循電子病歷隱私保護政策的「態度」對於其遵循電子病歷隱私保護政策的「行為意圖」具正向顯著影響；換言之，當資訊單位員工對於遵循電子病歷隱私保護政策的態度正向時，則其也會越傾向遵循電子病歷隱私保護政策，越有可能採取遵循之行為。依據研究結果，本計畫建議醫院須讓資訊單位員工對於電子病歷隱私保護政策產生正面的態度，惟有越正面的態度，則資訊單位員工越有可能遵循電子病歷隱私保護政策，以達成電子病歷隱私保護之目的。

(七) 主觀規範與敘述性規範對於行為意圖之影響

本計畫假說 H_8 為資訊單位員工所認知的「主觀規範」會正向影響其遵循醫院電子病歷隱私保護政策之行為意圖，依據結構方程模式分析結果($\beta = 0.35$, $t = 5.12$, $p < 0.001$)，顯示假說 H_8 成立。「主觀規範」對於「行為意圖」具正向顯著影響；換言之，資訊單位員工如感受對其重要的人的影響，認為其應當遵循電子病歷隱私保護政策，依據理性行為理論，資訊單位員工便可能採取遵循他人所期待的行為，亦即遵循電子病歷隱私保護政策；反之，如果對於資訊單位員工重要的人並不認為其須遵循電子病歷隱私保護政策，則資訊單位員工遵循電子病歷隱私保護政策之行為意圖便不高。本計畫於醫療情境進行,「主觀規範」對於「行為意圖」影響之研究結果與以往在其他領域(Herath and Rao, 2009; Ifinedo, 2012; Siponen *et al.*, 2010)之研究結果相同。

本計畫假說 H_9 為資訊單位員工所認知的「敘述性規範」會正向影響其遵循醫院電子病歷隱私保護政策之行為意圖」,依據結構方程模式分析結果($\beta = 0.04$, $t = 1.06$)，顯示假說 H_9 不成立。「敘述性規範」對於「行為意圖」不具影響；換言之，不論醫院其他員工是否能遵循電子病歷隱私保護政策，對於資訊單位員工是否遵循電子病歷隱私保護政策均沒有影響。

本計畫推論假說 H_9 不顯著的可能原因如下：本計畫用於衡量「敘述性規範」的問卷項目包括:「我認為醫院其他員工能遵守電子病歷資訊隱私保護政策」、「我能鼓勵醫院其他員工遵守電子病歷資訊隱私保護政策」、以及「醫院大部分員工應當能遵守電子病歷資訊隱私保護政策以確保電子病歷資訊的隱私」。就醫院資訊單位員工而言，由於其工作特性主要從事資訊系統的設計、開發與維護，除了須瞭解使用者資訊需求或則須解決使用者問題時可能須面對面外，大部分的時間都位於資訊單位辦公室進行資訊系統發展與維護作業，因此和外面其他員工(尤其具電子病歷使用權限的醫護人員)接觸時間可能較有限，因而造成對於醫院其他員工是否能遵守電子病歷保護政策可能較不確定，且亦無較多機會管理醫院其他員工遵守電子病歷隱私保護政策，因而造成此變數不顯著之現象。

依據本計畫研究結果：資訊單位員工所認知「主觀性規範」對於其遵循電子病歷隱私保護政策的「行為意圖」具正向顯著影響，然而「敘述性規範」對於其遵循電子病歷隱私保護政策的「行為意圖」並不具顯著影響；換言之，當對於資訊單位員工重要的其他人，包括：主管與資訊單位其他同事，如果對於資訊單位員工能確實保護電子病歷隱私有所期望，則資訊單位員工變越有可能遵循電子病歷隱私保護政策，依據研究結果，本計畫建議醫院能透過各單位主管以及同儕之間的影響力，宣導電子病歷隱私保護的重要性，以鼓勵資訊單位員工

能確實遵循電子病歷隱私保護政策。至於「敘述性規範」雖然不顯著，本計畫亦建議醫院應對員工多多宣導電子病歷隱私保護的重要性，並鼓勵員工能確實遵守電子病歷隱私保護政策。

陸、研究貢獻

電子病歷已是未來重要發展趨勢，國內衛生福利部亦積極推動病歷電子化相關作業，加上各醫院也逐漸體認到病歷電子化所能帶來的效益，因此各醫院亦陸續投入電子病歷規劃與發展。依據衛生署 2005 年針對全國醫療院所進行的病歷電子化調查報告(行政院衛生署, 2005)結果顯示，大部分填答醫院均認為病歷電子化已是未來趨勢，但資訊安全與病人隱私也成為最重要議題之一。截至 2014 年，目前已有 322 家醫院宣告實施電子病歷(行政院衛生福利部，2014)，顯示國內醫院對於電子病歷採用狀況正逐步提高。而衛生署所規劃電子病歷推動方案中，亦包含電子病歷的資訊安全與隱私保護政策(行政院衛生署, 2004)，冀望保障民眾個人健康資訊安全及隱私。

與以往以紙本病歷相比，以電子化方式處理病歷資料，不僅更快速、精確，且能更方便取得，不同醫院間亦能利用網路進行病歷資料的交換，達到節省醫療資源目的。然電子病歷如未能妥善管理，更容易發生電子病歷外洩狀況，所造成病人隱私問題可能較紙本病歷更嚴重，影響層面亦更大；此外，由於病歷均已電子化，醫院中能接觸到電子病歷的員工除原本醫護人員之外，資訊單位員工由於工作性質的關係，亦有更多機會接觸到病人的電子病歷(行政院衛生署, 2004)，衛生署甚至建議應實施監控資訊人員，避免病人醫療資訊外洩。因此，如何有效確保資訊單位人員確實遵循隱私保護政策，將是各醫院在推動電子病歷時必須面對的主要議題之一。

一、學術貢獻

以往文獻較常探討員工遵循資訊安全政策的影響因素，此類資訊安全政策遵循之研究應用於醫療產業並不多見，而進一步探討醫療產業電子病歷隱私保護政策遵循之研究更是少見，藉由本計畫進行，對於學術界而言，將可增加對於員工是否願意遵循病歷資訊隱私保護政策瞭解與認識，未來後續研究更可參考本研究結果，繼續進一步的深入探討此議題。在本計畫的研究變數間的關係方面，本計畫證實認知脆弱性和認知嚴重性可預測恐懼引發，恐懼引發再進而影響其對於某一保護行為之態度，此結果與以往保護動機理論的觀點有所不同(Rogers, 1983)，然以往文獻(如 Arthur and Quester, 2004)亦同樣證實認知脆弱性和認知嚴重性可預測恐懼引發之結果，後續仍須較多研究進行驗證。其次，由於醫療產業具有許多特性與一般產業並不相同，因此本計畫所得到結果將可進一步累積對於電子病歷隱私保護政策遵循的知識，並可與資訊安全政策比較，找出相同與相異結果之處，並釐清造成變數間關係不一致之原因。

二、實務貢獻

對衛生主管機關而言，由於政府單位正積極推動電子病歷及電子病歷交換，如何有效的降低民眾對於電子病歷的資訊隱私顧慮，將是影響能否順利推動電子病歷的一個主要因素之

一，而內部資訊單位員工是否能遵循醫院所制定的病歷資訊隱私保護政策，也會影響民眾對於電子病歷的觀感。而政府單位如何訂定完善的資訊隱私保護政策，亦將會深深影響未來國內醫院對於內部資訊隱私保護政策的擬定，藉由本計畫未來執行結果，將可供政府衛生主管單位政策擬定之參考；對醫院而言，能夠瞭解醫院資訊單位員工對於醫院所制定病歷資訊隱私保護政策的看法及對於是否願意遵循該政策行為意圖影響，醫院更可據以擬出因應之道，確保內部資訊單位員工確實保護民眾電子病歷資訊隱私，消彌民眾隱私顧慮，讓民眾能放心採用電子病歷。

參考文獻

行政院法務部. (2011). 個人資料保護法. from http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021.

行政院衛生署. (2004). *確立及推廣醫療資訊安全與隱私保護政策*. 台北市，台灣: 台灣醫學資訊學會.

行政院衛生署. (2005). 醫療院所病歷電子化現況調查-九十四年度醫療院所病歷電子化現況調查案. 台北市，台灣.

行政院衛生福利部. (2014). 健保特約醫療院所名冊 Retrieved 6th, August, 2014, from http://www.nhi.gov.tw/Resource/webdata/2976_1_hospbsc.zip

行政院衛生福利部. (2014). 電子病歷金榜 Retrieved 15th August, 2014, from http://emr.mohw.gov.tw/emrlist.aspx

楊漢淙. (2012). 電子病歷與病人隱私權保護. *澄清醫護雜誌, 8*(1), 4-8.

廖珮君. (2011). 台北附醫擁抱雲端 不只省錢還要安全. *Information Security 資安人科技網* Retrieved from http://www.informationsecurity.com.tw/

Arthur, D., & Quester, P. (2004). Who's afraid of that ad? Applying segmentation to the protection motivation model. *Psychology and Marketing, 21*(9), 671-696.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security, 8*(2), 33-56.

Bagozzi, R.P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

Bagozzi, R.P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly, 36*(3), 421-458.

Bélanger, F., & Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.

Boer, H., & Seydel, E.R. (1996). Protection motivation theory. In M. Connor & P. Norman (Eds.), *Predicting health behavior: Research and practice with social cognition models* (pp. 95-120). Buckingham, PA: Open University Press.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Caine, K., & Hanania, R. (2013). Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association, 20*(1),

7-15.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H.R., & Upadhyaya, S.J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *Professional Communication, IEEE Transactions on, 52*(2), 167-182.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, 5-8 Jan. 2009). *Application of protection motivation theory to adoption of protective technologies.* Paper presented at the System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on.

Chin, W.W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336): Lawrence Erlbaum Associates, NJ.

Chin, W.W. (2010). How to write up and report pls analyses. In V. Esposito Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds.), *Handbook of Partial Least Squares Concepts, Methods and Applications* (1st ed., pp. 655-690): Springer Berlin Heidelberg.

Choy, A., Hudson, Z., Pritts, J., & Goldman, J. (2001). Exposed online: Why the new federal health privacy regulation doesn't offer much protection to Internet users *Report of the Pew Internet & American Life Project. Health Privacy Project* (pp. 2003). Washington, DC: Institute for Health Care Research and Policy, Georgetown University.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM, 42*(2), 60-67.

Crossler, R.E. (2010, 5-8 Jan. 2010). *Protection motivation theory: Understanding determinants to backing up personal data.* Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

Culnan, M.J. (1993). How did they get my name - An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-361.

Culnan, M.J., & Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management (JGIM), 14*(4), 57-93.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*: Addison-Wesley Reading, MA:.

Fisher, W.A., Fisher, J.D., & Rye, B.J. (1995). Understanding and promoting AIDS-preventive behavior: Insights from the theory of reasoned action. *Health Psychology, 14*(3), 255-264.

Floyd, D.L., Prentice−Dunn, S., & Rogers, R.W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Goldschmidt, P.G. (2005). HIT and MIS: Implications of health information technology and

medical information systems. *Communications of the ACM, 48*(10), 68-74.

Guo, K.H., Yuan, Y., Archer, N.P., & Connelly, C.E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Hair, J.F., Black, W.C., Babin, B.J., & Anderson, R.E. (2010). *Multivariate data analysis - A global perspective* (Seventh ed.). New Jersey: Prentice-Hall, Upper Saddle River.

Hebert, M., & Benbasat, I. (1994). Adopting information technology in hospitals: The relationship between attitudes/expectations and behavior. *Hospital & Health Service Administration, 39*(3), 369-383.

Henseler, J., Ringle, C.M., & Sinkovics, R.R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20*, 277-319.

Herath, T., & Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herold, R. (2002). What is the difference between security and privacy. *CSI Alert newsletter*. Retrieved from http://www.informationshield.com

Hoffman, L.J. (1980). *Computers and privacy in the next decade*. Orlando, FL: Academic Press, Inc.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Hulland, J. (1999). Use of partial seast squares (pls) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195-204.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Joshi, K.D., & Kuhn, K. (2011). What determines interest in an IS career? An application of the theory of reasoned action. *Communications of the Association for Information Systems, 29*(1), 133-158.

Junglas, I.A., Johnson, N.A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

Kline, R.B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York: The Guilford Press.

Laric, M.V., & Pitta, D.A. (2009). Preserving patient privacy in the quest for health care economies. *Journal of Consumer Marketing, 26*(7), 477-486.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*(2), 361-369.

Lee, Y., & Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2),

177-187.

Li, J., & Shaw, M.J. (2008). Electronic medical records, HIPAA, and patient privacy. *International Journal of Information Security and Privacy, 2*(3), 45-54.

Luo, J., Fan, M., & Zhang, H. (2012). Information technology and organizational capabilities: A longitudinal study of the apparel industry. *Decision Support Systems, 53*(1), 186-194.

Maddux, J.E., & Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Mason, R.O. (1986). 4 ethical issues of the information age. *MIS Quarterly, 10*(1), 5-12.

Medlin, B.D., & Cazier, J. (2011). Obtaining Patient's Information from Hospital Employees through Social Engineering Techniques: An Investigative Study. In H. Nemati (Ed.), *Pervasive Information Security and Privacy Developments: Trends and Advancements* (pp. 77-89). Hershey, New York: Information Science Reference.

Medlin, B.D., & Cazier, J.A. (2007). An empirical investigation: Health care employee passwords and their crack times in relationship to HIPAA security standards. *International Journal of Healthcare Information Systems and Informatics (IJHISI), 2*(3), 39-48.

Medlin, B.D., Cazier, J.A., & Foulk, D.P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy (IJISP), 2*(3), 71-83.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Nowak, G.J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing, 9*(3), 46-60.

Organization for Economic Cooperation and Development (OECD). (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Retrieved 4th December, 2012, from http://www.oecd.org.

Palvia, P., Lowe, K., Nemati, H., & Jacks, T. (2012). Information technology issues in healthcare: Hospital CEO and CIO perspectives. *Communications of the Association for Information Systems, 30*, Article 19.

Park, S.Y., Lee, S.Y., & Chen, Y. (2012). The effects of EMR deployment on doctors' work practices: A qualitative study in the emergency department of a teaching hospital. *International Journal of Medical Informatics, 81*(3), 204-217.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Rindfleisch, T.C. (1997). Privacy, information technology, and health care. *Communications of the ACM, 40*(8), 92-100.

Ringle, C.M., Wende, S., & Will, A. (2005). SmartPLS (2M3) (Version 2.0 Beta). Hamburg, Germany. Retrieved from http://www.smartpls.de/

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R.W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. Petty (Eds.), Social psychophysiology (1st ed., pp. 153-176): New York: Guilford.

Rothstein, M.A. (2007). Health privacy in the electronic age. *The Journal of Legal Medicine, 28*(4), 487-501.

Sairosse, T.M., & Mutula, S.M. (2004). Use of cybercafés: study of Gaborone City, Botswana. *Program: electronic library and information systems, 38*(1), 60-66.

Sheppard, B.H., Hartwick, J., & Warshaw, P.R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research, 15*(3), 325.

Siponen, M., Pahnila, S., & Mahmood, A. (2006, Nov. 2006). *Factors influencing protection motivation and IS security policy compliance.* Paper presented at the Innovations in Information Technology, 2006.

Siponen, M., Pahnila, S., & Mahmood, M.A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Smith, H.J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 980-1016.

Smith, H.J., Milburg, S.J., & Burke, S.J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Stone, E.F., Gueutal, H.G., Gardner, D.G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459-468.

Storey, V.C., Kane, G.C., & Schwaig, K.S. (2009). The quality of online privacy policies: A resource-dependency perspective. *Journal of Database Management, 20*(2), 19-37.

Tanner, J.F., Jr., Hunt, J.B., & Eppright, D.R. (1991). The Protection Motivation Model: A Normative Model of Fear Appeals. *Journal of Marketing, 55*(3), 36-45.

Taylor, S., & Todd, P.A. (1995). Understanding information technology usage - A test of competing models. *Information Systems Research, 6*(2), 144-176.

Tenenhaus, M., Vinzi, V.E., Chatelin, Y.M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics and Data Analysis, 48*(1), 159-205.

Trochim, W.M.K. (2001). *Research methods knowledge base* (2nd ed.). Cincinnati: Atomic Dog Publication.

U.S. Department of Health & Human Services. (2002). *Standards for privacy of individually identifiable health information.* Washington, DC.: U.S. Department of Health & Human Services, Retrieved from http://www.hhs.gov.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190-198.

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User acceptance of information

technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Virga, P.H., Jin, B., Thomas, J., & Virodov, S. (2012). Electronic health information technology as a tool for improving quality of care and health outcomes for HIV/AIDS patients. *International Journal of Medical Informatics, 81*(10), e39-e45.

Volonino, L., & Robinson, S.R. (2003). *Principles and practice of information security*: Prentice.

Warren, S.D., & Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Werner, P., & Mendelsson, G. (2001). Nursing staff members' intentions to use physical restraints with older people: Testing the theory of reasoned action. *Journal of Advanced Nursing, 35*(5), 784-791.

Werts, C.E., Linn, R.L., & Jöreskog, K.G. (1974). Intraclass reliability estimates: Testing structural assumptions. *Educational and Psychological Measurement, 34*(1), 25-33.

Westin, A.F. (1967). *Privacy and freedom*. New York: Atheneum Publishers.

Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using pls path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly, 33*(1), 177-195.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs, 43*(3), 389-418.

研究問卷

「電子病歷資訊隱私保護政策遵循影響因素」調查問卷

您好：

這是一份學術研究問卷，目的在瞭解您對於「**電子病歷隱私保護政策**」的觀點，希望藉由本研究所獲得結果，作為未來政府、醫療院所等單位，在擬定保護病人資訊隱私政策與保護措施之參考。

本問卷採不具名方式，所有資料僅供學術研究之用，絕不對外公開。懇請您撥冗回答此份問卷，您的回答對本研究將有莫大的助益與影響。最後，衷心的感謝您熱心的協助與支持，並敬祝您身體健康　萬事如意。

敬祝　　身體健康　萬事如意

計畫主持人

義守大學 醫務管理學系 郭光明 敬上

問卷說明

問卷填寫注意事項：本問卷共 3 頁，第一頁為問卷說明與基本資料、第二至三頁為主要問卷內容。請就您對於電子病歷隱私政策之看法，並依照同意的程度填寫。

電子病歷隱私保護政策：可讓醫院員工知道如何處理與維護電子病歷及病人隱私權的管理指引，該指引除說明保護隱私相關作法外，亦訂有違反相關規定時之罰則。

個人基本資料

1. 年齡	□20 歲(含)以上~未滿 30 歲 □30 歲(含)以上~未滿 50 歲 □50 歲(含)以上~未滿 65 歲 □其他____
2. 性別	□男 □女
3. 教育程度	□高中/職 □專科 □大學 □研究所以上
4. 職稱	□管理階層(如一級/二級主管等) □系統分析師 □系統設計師 □程式設計師 □硬體/資料庫管理/網管人員 □其他____
5. 醫療產業工作年資	□1-3 年 □4-6 年 □7-9 年 □10 年以上
6. 是否知道醫院電子病歷隱私保護政策？	□知道，也了解內容 □知道，但不了解內容 □不知道

題項	『問卷各題目答案無關對錯，只要依照您個人想法回答即可，請依直覺在適合的□打勾∨』	非常不同意	很不同意	不同意	沒意見	同意	很同意	非常同意
1.	如果我不能遵守醫院所制定的電子病歷隱私保護政策，醫院便可能容易發生電子病歷破壞事件(例如遭到入侵而發生病歷資訊外洩狀況)	□	□	□	□	□	□	□
2.	如果我不能遵守醫院的電子病歷資訊隱私保護政策，連我的病歷資訊隱私也可能遭受侵犯	□	□	□	□	□	□	□
3.	我相信嘗試保護醫院電子病歷資訊能減少其遭受非法存取(例如非法查詢或列印病人的電子病歷)	□	□	□	□	□	□	□
4.	如果連我都不能遵守醫院所制定的電子病歷資訊隱私保護政策，民眾電子病歷隱私便可能遭受損害	□	□	□	□	□	□	□
5.	我相信醫院所儲存的電子病歷資訊易於遭到破壞而發生隱私事件(例如遭到入侵，造成病歷資訊外洩)	□	□	□	□	□	□	□
6.	我相信醫院的營運和員工都可能受到電子病歷資訊隱私破壞事件(例如遭到入侵，造成病歷資訊外洩)的影響	□	□	□	□	□	□	□
7.	我相信醫院營運可能受到電子病歷資訊隱私破壞事件(例如遭到入侵，造成病歷資訊外洩)的威脅	□	□	□	□	□	□	□
8.	電子病歷資訊隱私保護議題會直接影響醫院(例如醫院形象)	□	□	□	□	□	□	□
9.	電子病歷資訊隱私保護議題被過度渲染	□	□	□	□	□	□	□
10.	我認為電子病歷資訊隱私保護是嚴重的事情，必須注意	□	□	□	□	□	□	□
11.	對於協助醫院保護電子病歷資訊，每位員工都有義務與責任	□	□	□	□	□	□	□
12.	儘管每位員工對於保護醫院電子病歷資訊隱私所能做的並不多，仍應確實遵循醫院電子病歷隱私保護政策	□	□	□	□	□	□	□
13.	如果我能夠遵守醫院電子病歷隱私保護政策，就能夠幫助醫院確保電子病歷資訊隱私盡一份心力	□	□	□	□	□	□	□
14.	我自信能遵守醫院大部分電子病歷隱私保護政策	□	□	□	□	□	□	□
15.	如果我想要，我能夠很容易遵守醫院電子病歷隱私保護政策	□	□	□	□	□	□	□

16.	即使沒有其他人協助，我還是能夠自行遵守醫院的電子病歷隱私保護政策	□	□	□	□	□	□	□
17.	醫院實施電子病歷資訊隱私保護措施需花費相當多成本（例如需採購相關資訊安全軟體、硬體等成本）	□	□	□	□	□	□	□
題項	『問卷各題目答案無關對錯，只要依照您個人想法回答即可，請依直覺在適合的□打勾∨』	非常不同意	很不同意	不同意	沒意見	同意	很同意	非常同意
18.	醫院要能落實電子病歷資訊隱私保護政策將會花費許多時間	□	□	□	□	□	□	□
19.	醫院實施電子病歷隱私保護政策可能對於員工工作造成不便	□	□	□	□	□	□	□
20.	醫院高階主管希望員工能遵守電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
21.	我的主管認為我應該遵守醫院電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
22.	我的同事認為我應該遵守醫院電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
23.	醫院電子病歷推動委員會(或病歷管理單位)希望員工能遵守電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
24.	我認為醫院其他員工能遵守電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
25.	我能鼓勵醫院其他員工遵守電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
26.	醫院大部分員工應當能遵守電子病歷資訊隱私保護政策以確保電子病歷資訊的隱私	□	□	□	□	□	□	□
27.	電子病歷資訊隱私保護措施(例如不隨意查詢或外洩病人的病歷資訊)是一個好主意	□	□	□	□	□	□	□
28.	電子病歷資訊隱私保護措施是重要的	□	□	□	□	□	□	□
29.	我喜歡電子病歷資訊隱私保護這個想法	□	□	□	□	□	□	□
30.	我很可能遵守醫院的電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
31.	遵守醫院的電子病歷資訊隱私保護政策對我而言是可能的	□	□	□	□	□	□	□

32.	我很確定我會遵守醫院的電子病歷隱私保護政策	□ □ □ □ □ □ □

您的其他意見：

問卷到此結束，請再檢查一次是否有漏填，非常感謝您的協助。

附錄

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標(本計畫成果與原計畫相符，並達成原規劃之目標)

□ 未達成目標（請說明，以 100 字為限）

□ 實驗失敗

□ 因故實驗中斷

□ 其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 ■撰寫中 □無

專利：□已獲得 □申請中 □無

技轉：□已技轉 □洽談中 □無

其他：（以 100 字為限）

郭光明, 馬震中, & 吳鑫瞬. (2014). 醫師與非醫師對於電子病歷隱私保護行為意圖之比較研究. *台灣公共衛生雜誌, 33*(2), 162-173. **(TSSCI)**

致 謝

本研究由國家科學委員會研究計畫(NSC-102-2410-H-214-019)與義守大學研究計畫(ISU102-S-01)補助相關經費，僅此感謝。

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以500 字為限）

(1)學術成就：藉由本計畫之執行，可進一步了解影響醫院資訊單位員工遵循電子病歷隱私保護政策之因素，進一步累積電子病歷隱私保護之研究成果，而藉由本計畫之進行，亦已發表一篇學術論文。

(2)技術創新：本研究非屬技術性研究，並無技術之創新。

(3)社會影響：本計畫之主要應用價值之一在於對於社會之影響，由於政府單位正積極推動電子病歷以及電子病歷的交換，而民眾對於電子病歷的資訊隱私顧慮則可能是影響電子病歷是否能順利推動的重要影響因素之一，如何消彌民眾的資訊隱私顧慮是未來必須面臨之問題。藉由本計畫之進行，了解影響醫院員工遵循電子病歷隱私保護政策之影響因素，所獲得之結果將可分別提供衛生主管機關與醫院之參考，進而擬定更完整且有效的資訊隱私保護政策。

國科會補助專題研究計畫出席國際學術會議心得報告

日期： 103 年 4 月 7 日

計畫編號	NSC－102－2410－H－214－019		
計畫名稱	電子病歷隱私保護政策遵循之探討－整合理性行為理論與保護動機理論觀點		
出國人員姓名	郭光明	服務機構及職稱	義守大學醫務管理學系
會議時間	103 年 4 月 2 日至 103 年 4 月 4 日	會議地點	日本名古屋
會議名稱	(中文) 2014 年商業與管理國際研討會 (英文) 2014 International Symposium on Business and Management (ISBM 2014)		
發表題目	(中文) 醫院網站資訊隱私顧慮之研究 (英文) The Antecedents and Consequences of Information Privacy Concerns: An Empirical Investigation of Hospital Websites (中文) 醫院對於公平資訊處理原則之看法 (英文) How Do Hospitals Regard Fair Information Practices?		

一、參加會議經過

本次計畫主持人參加 2014 International Symposium on Business and Management (ISBM 2013)會議，由 Knowledge Association of Taiwan (KAT)、International Business Academics Consortium (iBAC)及 Nagoya University 所共同舉辦，此次會議場地亦同時舉行 e-CASE & e-Tech 2014、ISEP 2014 等會議。ISBM 2014 會議於日本名古屋(Nagoya)舉辦總共為期三天(2014 年 4 月 2-4 日)，並邀請來自全世界學術界與實務界專業人士參與此次盛會，此次會議共計有 35 個國家專業人士參與，共計投稿論文 686 篇。

二、與會心得

本次計畫主持人投稿二篇論文，題目分別為：「The Antecedents and Consequences of Information Privacy Concerns: An Empirical Investigation of Hospital Websites」與「How Do Hospitals Regard Fair Information Practices?」，透過本次 ISBM 會議的參與，除可吸收較新的研究相關資訊與概念外，並獲得寶貴的機會能和許多學者互相切磋討論，例如泰國 Thammasat University 的 Issarawornrawanich 教授分享其研究，探討組織董事會成員特性和組織績效之間的關聯，當中提及董事會開會次數與公司績效呈負向相關，此論點亦在會議中有許多討論；此外，另外一場由國內學者所發表論文亦得到其他國外學者的建議，此次研討會議中針對各報告論文所提出的見解與建議均對於後學日後的研究與論文投稿均有相當大的助益，對於主持人從事後續研究深具參考價值。投稿論文亦已再度修訂，並分別投稿至 Program: Electronic library and information systems (SSCI 等級期刊，目前正一審修改中)以及 International Journal of Research in Social Sciences (IJRSS) (已接受並刊登)兩本期刊。最後，感謝國科會補助出席國際會議的經費，參與本次會議完成論文發表，並協助本年度研究計畫順利完成。

三、發表論文全文或摘要

The Antecedents and Consequences of Information Privacy Concerns: An Empirical Investigation of Hospital Websites

Kuang-Ming Kuo[a], Wen-Sheng Tzeng[b], Chen-Chung Ma[a*] and Paul C. Talley[c]
[a] Department of Healthcare Administration, I-Shou University,
Yanchao District, Kaohsiung City, 82445, Taiwan (R.O.C.)
[b] Department of Radiology, Chi Mei Foundation Hospital,
Yung-Kang District, Tainan City, Taiwan (R.O.C.),
[c] Department of International Business Administration,
Dashu District, Kaohsiung City, 84001, Taiwan (R.O.C.),

*Corresponding Author: up000238@isu.edu.tw

ABSTRACT

The purpose of this study is to investigate the antecedents (i.e., fair information practices and hospital reputation) and consequences (behavioral intentional towards hospital websites) of individuals' information privacy concerns toward hospital websites. Further, the relationship between fair information practices and hospital reputation was also investigated. Survey methodology was employed to empirically validate the proposed research model. The present study utilized a self-administered questionnaire for data collection, focusing individuals who visited hospitals. Partial Least Square (PLS) technique was utilized to assess the psychometric properties of the instrument and test the proposed research hypotheses. A total of 331 valid questionnaires were collected and analyzed via PLS, the results revealed that fair information practices was found to significantly influence hospital reputation (β=0.61, t=12.57) and information privacy concerns (β=-0.47, t=5.42) respectively. Hospital reputation was found to significantly impact information privacy concerns (β=-0.18, t=2.74) and behavioral intention (β=0.2, t=2.76) respectively. Further, information privacy concerns (β=-0.4, t=6.9) significantly affected behavioral intention. Finally, the proposed research model explains about 27% of the total variance of behavioral intention. This study demonstrates that fair information practices are critical in improving hospital reputation and reducing individuals' information privacy concerns. It is therefore imperative that hospitals should adopt and comply with fair information practices to alleviate individuals' information privacy concerns towards hospital websites.

Keyword: Information Privacy Concerns, Fair Information Practices, Reputation, Hospital Websites

How Do Hospitals Regard Fair Information Practices?: Evidence from a Content Analysis of Their Websites

Kuang-Ming Kuo [a], Pu-Yuan Tzeng [a] and Paul C. Talley [b*]
[a] Department of Healthcare Administration (Master Program), I-Shou University,
No.8, Yida Rd., Jiaosu Village Yanchao District,
Kaohsiung City, 82445, Taiwan (R.O.C.)
[b] Department of International Business Administration, I-Shou University,
No. 1, Sec. 1, Syuecheng Rd., Dashu District,
Kaohsiung City, 84001, Taiwan (R.O.C.)
*Corresponding Author: atlanta.ga@msa.hinet.net

ABSTRACT

The purpose of this study is to investigate whether Taiwanese hospital websites display a defined privacy policy, and if so, do such privacy policy conforms to fair information practices? Content analysis methodology was applied to investigate the privacy policies of the 475 Taiwanese hospital websites. The results reveal that only 19.6% of the hospitals posted defined privacy policies on their websites. Notice was the highest percentage (100%) and access was the lowest percentage (20.4%) of compliance by hospitals. The other percentage for choice, security, and enforcement was 84.9%, 52.7%, and 21.5% respectively. Omissions most often occurred in terms of security, access, and enforcement practices. Further, the privacy policies of hospital websites' should be exceedingly improved to enhance individual's trust of their websites.

Keyword: Privacy Policy, Fair Information Practices, Content Analysis, Hospital Websites

1. Background and objectives

The emergence of the Internet has been considered as an important resource for those seeking personal health information. More and more individuals are making use of the availability of online health information. According to the Pew Internet & American Life Project report from 2013, 35% of U.S. adults have searched for at least one of sixteen major health topics online (Pew Internet and American Life Project, 2013). During the process of online health information seeking, individuals are sometimes asked voluntarily to provide personal information about themselves or their health information (Bansal et al., 2010). Further, the information-seeking behavior may be automatically tracked as well (Rains and Bosch, 2009). Such practices may cause individuals to refrain from disclosing their personal information (Bansal et al., 2010; Schwaig et al., 2013) since online health information seekers care much about their online privacy (Ambrose and Basu, 2012; Pew Internet and American Life Project, 2000). To ensure Internet privacy, the Federal Trade Commission (FTC) recommended that Congress should enact Internet privacy legislation (Culnan, 2000) and proposed fair information practices (FIPs) for guiding the handling of personal information by organizations (FTC, 2000). The FTC (2000) defines FIPs as: *notice*, *choice*, *access*, *security*, and *enforcement*.

On the other hand, individuals are very interested in knowing about a website's information

practices before rendering their personal information online (FTC, 2000; Wu et al., 2012). And there have been a number of strategies proposed to protect Internet privacy, with the most popular being the revealing of online privacy policies (Mundy, 2006; Rains and Bosch, 2009). Online privacy policy refers to comprehensive descriptions of a website's information practices that is located in one place on the website and that can be reached by a hyperlink (FTC, 2000). Currently, FIPs are the most widely-accepted principles for organizational handling of personal information (Culnan, 2000; Liu et al., 2005; Mundy, 2006). The main purpose of this study is to investigate the disclosure of online privacy policies among Taiwanese hospital websites. Concomitantly, it is also necessary to determine whether these online privacy policies conform to established international norms (i.e., the U.S. FTC's FIPs).

2. Methods

2.1 Design

To fulfill the purposes of this study, a content analysis of the online privacy policies of Taiwanese hospitals was carried out during July, 2013. Content analysis is a systematic, replicable data reduction technique that compresses long text into fewer content categories based on explicit rules of coding (Krippendorff, 2003). We first acquired a published hospital list from National Health Insurance Administration of Taiwan. Then we proposed privacy evaluation criteria (Table 1) for the content analysis that are based on the U.S. FTC's FIPs principles and prior studies (O'Connor, 2003; Zhang et al., 2007). The authors of this study visited all the hospital websites to examine whether they contained privacy policy and, if so, the content of the policy based on previously developed evaluation criteria.

Table 1 FIPs evaluation criteria

Practice	Code	Criteria
Notice	N1	Identification of personal information collectors, uses, and potential recipients
	N2	Nature of personal information collected & means of collection
Choice	C1	External use (of personal information)
	C2	Internal use (of personal information)
Access	A1	Access to personal information
	A2	Correction (of personal information)
Security	S1	Managerial procedures (taken to ensure personal information security)
	S2	Technical procedures (taken to ensure personal information security)
Enforcement	E1	Contact information

2.2 Samples and Unit of Analysis

We used the hospital listing (475 hospitals in total) provided by the National Health Insurance Administration to investigate the FIPs found on their websites. The unit of analysis was the hospital's stated online privacy policy. Some hospitals embed their privacy policies in links to other

information such as with legal notices or in terms of usage. To ensure we accurately captured the privacy policies for every hospital, we also examined those related online notices for purposes of discovery.

3. Results

We investigated 475 hospitals that participate in the National Health Insurance Program of the National Health Insurance Administration in Taiwan. These hospitals included 19 medical centers (roughly with > 900 beds), 90 regional hospitals (roughly with 400-600 beds), and 366 district hospitals (roughly with <200 beds). Ninety-three hospitals were found to have a definable online privacy policy. As can be seen from Table 3, the percentage of Taiwanese hospitals with a defined online privacy policy containing at least one kind of the FIPs was 19.6% (93/475). Further, medical centers (52.6%) and regional hospitals (52.2%) had a relative larger incidence (i.e. based on a percentage basis) of revealing online privacy policies than district hospitals had.

Table 3 Hospital distribution of online privacy policies in Taiwan

Accreditation status	Posted (%)	Not posted (%)	Total number
Medical center	10 (52.6%)	9 (47.4%)	19
Regional hospital	47 (52.2%)	43 (47.8%)	90
District hospital	36(9.8%)	330 (90.2%)	366
Total	93 (19.6%)	382 (80.4%)	475

Table 4 depicts a breakdown of the numbers and percentage by FIP categories and by hospital accreditation status. Among the 93 hospitals with stated online privacy policies, each hospital had *notice* practice (100%). Further, the practices of *access* (20.4%) and *enforcement* (21.5%) were found most lacking in the information provided online. As can be seen in Table 4, regarding the five FIPs, none of the three differing status levels of hospitals were found to be statistically significant.

Table 4 FTC Categories frequencies among hospitals with online privacy policy

Accreditation status	Notice	Choice	Security	Access	Enforcement
Medical center level (n=10)	10	9	6	1	3
	100%	90%	60%	10%	30%
Regional hospital level (n=47)	47	38	20	11	12
	100%	80.9%	42.6%	23.4%	25.5%
District hospital level (n=36)	36	32	23	7	5
	100%	88.9%	63.9%	19.4%	13.9%
Total (n=93)	93	79	49	19	20
Percentage	100%	84.9%	52.7%	20.4%	21.5%
Pearson Chi-Square	N/A	1.254	3.972	0.946	2.116
p-value	N/A	0.534	0.137	0.623	0.347

Note: N/A denotes Not Applicable

A closer examination of the contents of privacy policies located in the websites of 93 hospitals revealed that *notice* practice draws the most attention from each hospital: medical centers (100%), regional hospitals (100%), and district hospitals (100%). On the other hand, less than 30% of the hospitals addressed the *access* and *enforcement* practice of the FIPs. Medical centers, regional hospitals, and district hospitals had only 10.00%, 23.4%, and 19.4% of online privacy policies respectively that complied with the *access* component of the FIPs and 30%, 25.5%, and 13.9% for *enforcement* practice. To sum up, the low percentages in the *access* and *enforcement* practices clearly demonstrates that many hospitals' online privacy policies fail to cover the basic FIP categories provided by the exemplary U.S. FTC model. In fact, none of the 93 websites that have posted an online privacy policy fully complied with the entire guidelines for FIPs identified above.

4. Discussion

A part of the findings of this study are somewhat disappointing since more than 80% of the Taiwanese hospitals do not post directed online privacy policies, despite the fact that more that 50% of medical centers and regional hospitals have explicit online privacy policies. Further, a greater majority of online privacy policies failed to adequately meet the basic requirements demonstrated by the U.S. FIPs. The lowered figures of district hospitals might be due to its insufficient human and financial resources which should not be a similar issue for medical centers and regional hospitals. On the other hand, the three differing level of hospitals did not have significant difference regarding the FIPs according to Pearson Chi-square significance test. It might imply that Taiwanese hospitals do not pay enough attention to online privacy protection issues no matter which level of hospitals they are. One plausible explanation is that these hospitals might reason that their websites are just an informational website (i.e. not an open forum), and that privacy protections are automatically covered in their daily transaction practices. However, without the display of defined online privacy policies, individuals have less chance to make an informed choice about the rendering of their personal information (Mundy, 2006). Further, as web technology proliferates and becomes more mature, individuals may also gain more knowledge about the mechanisms, such as with privacy policies and their use, to assess website quality (Mundy, 2006).

5. Conclusions

In this study, we used content analysis methodology to analyze hospitals' online privacy notices in Taiwan. Out of the 475 hospital websites investigated, only 93 (19.6%) hospitals posted online privacy policies. We found that Taiwanese hospitals do have different focuses in preparing their privacy notices among three differing levels of hospital status. Further, none of the 93 online privacy policies posted by Taiwanese hospitals fully conformed to the established U.S. FTC's FTPs. The outcomes of applying the exemplary U.S. FTC FIPs to hospitals' online privacy policies suggest that these online privacy policies of hospitals should be exceedingly improved upon. That is, none of the web sites that were investigated included complete, definable policies conforming to

FIPs. Nevertheless, following the FIPs and revealing the privacy policies online are the minimum requirements for a website to secure individuals' information privacy (Yang and Chiu, 2000). It may take numerous procedures (such as the soundness of legal and enforcement mechanisms, websites' professional ethics standards, or technical / managerial security procedures and best practices) to protect personal information privacy (Milberg et al., 2000; Yang and Chiu, 2000). However, by showing (and adhering to) an extensive privacy policy on the website whenever individual's data is being collected is regarded to be a key stage of development necessary towards building trust with individuals and encouraging them to surrender personal data (Liu et al., 2005; Wu et al., 2012). As per our study results, the following suggestions are provided for governments and hospitals respectively to enhance their online privacy policy disclosure and compliance with international norms.

5.1 Implications for government

Despite the fact that Taiwan has promulgated the Personal Information Protection Act since 2010 (Ministry of Justice, 2010), the government has not paid much real attention to the privacy issues of websites (Yang and Chiu, 2002), not to mention those of hospital websites. Further, not all elements of privacy protection principles, as with those set forth for by the U.S. FTC, are required by law in Taiwan. For example, the technical aspect of security is not even mentioned in the Personal Information Protection Act whatsoever. Thus, the government could reference the laws and experiences of other countries, such as the U.S. and the European Union, about online privacy protection and further integration of other countries' laws and experiences into Taiwan's legislation (Yang and Chiu, 2002).

5.2 Implications for hospitals

It is vital for hospitals not only to develop and post an online privacy policy but also to faithfully execute it in both practice and principle. Hospitals should establish a comprehensive system to protect patients' rights to online privacy. The protection of individuals' information integrity could be regarded as an effective means of improving their confidence regarding the use of hospital websites (Wu et al., 2012) and of the prevention of a negative impact on the vibrancy of hospital websites. Further, since online privacy is in a parallel evolutionary track with technology advances, hospitals should frequently review their online privacy policies to ensure compliance with current laws and general societal expectations (Rains and Bosch, 2009).

Regarding the limitations of this research, this study did not have sufficient data to align privacy statements coincident with individual hospital practices. This is due in large part to the posting of privacy policies, which does not necessarily mean that a site follows any or all FIPs as the policy might address only certain practices, while not addressing others. A further cross-validation of the study findings, such as performing a survey on patient satisfaction with privacy policies and practices by hospitals, may be required.

REFERENCES

1. Ambrose P. & Basu C. Interpreting the Impact of Perceived Privacy and Security Concerns in Patients' Use of Online Health Information Systems. *Journal of Information Privacy & Security* 2012, **8**(1), 38-50.
2. Bansal G., Zahedi F.M. & Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems* 2010, **49**(2), 138-50.
3. Culnan M.J. Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing* 2000, **19**(1), 20-26.
4. Federal Trade Commission. *FTC Report to Congress: Privacy online: fair information practices in the electronic marketplace*. Federal Trade Commission, U.S.A., 2000.
5. Krippendorff K. Content Analysis: An Introduction to Its Methodology. 2nd ed. California, USA: Sage Publications; 2003.
6. Liu C., Marchewka J.T., Lu J. & Yu C.S. Beyond concern - a privacy-trust-behavioral intention model of electronic commerce. *Information & Management* 2005, **42**(2), 289-304.
7. Milberg S.J., Smith H.J. & Burke S.J. Information Privacy: Corporate Management and National Regulation. *Organization Science*, 2000, **11**(1), 35-57.
8. Ministry of Justice. *Personal Information Protection Act*. Taipei: Ministry of Justice, Taiwan, 2010.
9. Mundy D.P. Customer privacy on UK healthcare websites. *Informatics for Health and Social Care* 2006, **31**(3), 175-193.
10. O'Connor P. What happens to my information if I make a hotel booking online: an analysis of on-line privacy policy use, content and compliance by the international hotel companies. *Journal of Services Research* 2004, **3**(3), 5-28.
11. Pew Internet and American Life Project. *The Online Health Care Revolution*. Washington D.C.: California Healthcare Foundation, 2000.
12. Pew Internet and American Life Project. *Health Online 2013*. Washington D.C.: California Healthcare Foundation, 2013.
13. Rains S.A. & Bosch L.A. Privacy and health in the information age: A content analysis of health web site privacy policy statements. *Health Communication* 2009, **24**(5):435-446.
14. Schwaig K.S., Segars A.H., Grover V. & Fiedler K.D. A model of consumers' perceptions of the invasion of information privacy. *Information & Management* 2013, **50**(1), 1-12.
15. Wu K.W., Huang S.Y., Yen D.C. & Popova I. The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior* 2012, **28**(3), 889-897.
16. Yang H.L. & Chiu H.K. Privacy disclosures of Web sites in Taiwan. *Journal of Information Technology Theory and Application (JITTA)* 2002, **4**(3), Article 4.
17. Zhang X., Sakaguchi T. & Kennedy M.A. Cross-Cultural Analysis of Privacy Notices of the Global 2000. *Journal of Information Privacy & Security* 2007, **3**(2):18-36.

四、建議

藉由參與此類型國際會議，對於拓展研究人員之視野以及人脈均有相當大的助益，期望國科會能多補助此類型之活動。

五、攜回資料名稱及內容

此次參加研討會共攜回大會手冊以及研討會論文光碟一片。

六、其他

無。