科技部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：如何防止醫院員工違反電子病歷隱私保護政策：一個整合行為模式

計畫類別：■個別型計畫　□整合型計畫
計畫編號：MOST 103－2410－H－214－007－
執行期間：103 年 08 月 01 日至 104 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：
計畫參與人員：林信源、張芷菱

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 104 年 10 月 12 日

如何防止醫院員工違反電子病歷隱私保護政策：一個整合行為模式

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)從威攝角度探討對醫院員工遵循電子病歷隱私保護政策之影響因素，以及 2)探討強化醫院員工遵循病歷資訊隱私保護政策因素之前置因素。研究對象為國內醫學中心員工，採用問卷方式蒐集資料，共回收 289 份問卷，所蒐集資料利用結構方程模式進行分析，結果顯示：「偵測確定性」、「主觀規範」與「敘述性規範」對於醫院員工「遵循電子病歷隱私保護政策行為意圖」有正向顯著的影響；而「電子病歷隱私保護教育訓練」對於「處罰嚴重性」、「處罰確定性」、「偵測確定性」、「認知脆弱性」、「認知嚴重性」、「主觀規範」與「敘述性規範」均有顯著影響。

關鍵字：電子病歷、病歷隱私保護政策、威攝理論、保護動機理論

How to Prevent Hospital Staff from Violating EMR Privacy Policy: A Composite Behavioral Model

Abstract

The purpose of this project is twofold. The first purpose is to explore the factors that can motivate hospital employees to comply with privacy policy from deterrence perspective under the context of electronic medical records. The second purpose is to explore the antecedents of behavioral intentions to comply with privacy policy of electronic medical records among hospital employees. Survey methodology was used to collect 289 responses from hospital staff in hospitals. The collected data was analyzed using Structural Equation Modeling. The results demonstrated that detection certainty, subjective norm, and descriptive norm significantly influence hospital staff's intention to comply with privacy policy in a positive direction. Further, ethics training on electronic medical records also exercise positive and significant influences on punishment severity, punishment certainty, detection certainty, perceived vulnerability, perceived severity, subjective norm, descriptive norm respectively.

Keywords: Electronic medical records, deterrence theory, medical records privacy policy, protection motivation theory

目錄

表目錄

圖目錄

壹、前言

由於醫療資源有限，隨著醫療成本日益升高，然醫療保險給付卻受到限制，加上民眾對醫療品質的要求日趨嚴苛，使得醫療機構必須同時兼顧醫療成本的控制與醫療品質的維持甚至提升。為有效因應這些問題，醫療機構陸續提出各種不同解決方案，期望能有效控制醫療成本支出，同時亦能確保醫療服務品質，而資訊科技便是一個經常被提出的解決方案(Laric & Pitta, 2009; Li & Shaw, 2008; Palvia *et al.*, 2012; Rothstein, 2007)。儘管學術界與實務界均認為資訊科技可有效降低醫療機構營運成本及提高醫療品質，然醫療產業卻是最後一個運用資訊科技的產業(Palvia *et al.*, 2012)，醫療產業採用資訊科技速度較一般產業落後約 10-15 年(Goldschmidt, 2005)。在這種共識下，醫療機構開始採用各種資訊科技，期望透過資訊科技的協助改善其營運，而政府單位有效運有有限醫療資源，亦透過各種激勵措施，鼓勵醫療機構能廣泛採用資訊科技改善醫療服務品質，在這些鼓勵措施當中，以電子病歷的推動最為積極(行政院衛生福利部, 2013)。所謂電子病歷指電子集中式的病患資料，可於醫療機構間或醫療系統間相關利害人，如醫師、保險公司及員工間分享(Angst *et al.*, 2010)，藉由電子病歷，醫療機構可有效控制醫療成本及提高醫療服務品質(Palvia *et al.*, 2012)；此外，電子病歷更可改善病患安全、提高醫療機構營運效率、提供醫學教學與研究等用途(Bates *et al.*, 2003)；採用電子病歷之議題更是目前醫療機構資訊單位主管認為最重要議題之一(Palvia *et al.*, 2012)。

儘管電子病歷可為醫院帶來許多管理與臨床醫療的優點，由於病歷採電子化方式儲存，也造成電子病歷資料更容易遭到破壞與竊取，引發病歷隱私疑慮(Angst *et al.*, 2010)。病歷隱私一直是一爭議許久的議題：包括電子病歷更易於遭到不當揭露、電子病歷的保護較紙本病歷不足、以及隨著資訊科技進步，可能有越來越多針對電子病歷入侵事件發生(Baumer *et al.*, 2000)；換言之，電子病歷對於醫療產業而言是一雙面刃，病歷電子化雖然可讓醫護人員更容易存取，卻也造成電子病歷更易遭受破壞(Angst & Agarwal, 2009; Kapoor & Nazareth, 2012)，亦即造成電子病歷隱私遭侵犯議題，醫療機構也針對病歷隱私保護議題採相關保護措施。

儘管目前可用於避免資訊外洩的資訊科技進步之速度與幅度均較以往高，然而「人」卻是組織在保護其資訊資源最弱的一環(Hu *et al.*, 2011)。以往各產業所發生資料破壞(Data breach)事件中，醫療產業佔相當高比例，內部員工更是資料破壞事件發生主因之一，例如 Verizon (2013)統計報告顯示 2012 年發生超過 47,000 次資料破獲事件(經通報)，總計約有超過 4,400,000 筆資料受影響，在這些破壞事件當中，內部員工所造成比例約 14%；此外，Ayyagari (2012)針對全世界 2005-2010 年所發生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%，顯示員工所造成資料破壞事件持續發生。

對醫療產業而言，醫療機構員工有更多機會接觸病歷資料(Medlin *et al.*, 2008; Medlin & Adriana, 2007)，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，被影響病人人數最高更達 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。儘管各醫院採取包括技術、行政管理以及實體控制等不同措施；例如國內外均有相關法律(U.S. Department of Health and Human Services, 2002；Volonino &

Robinson, 2003; 行政院法務部, 2012)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 & Pitta, 2009; Medlin & Cazier, 2011; 楊漢淶, 2012)。

民眾提供組織的個人資訊如遭受未經授權存取，或因缺乏內部控制機制，甚至個人所提供資料原本使用目的與提供目的不同，且未經授權時，便可稱為對於民眾的隱私侵犯(Culnan & Armstrong, 1999)。對於醫療機構而言，由於資訊科技越來越進步，造成對於資訊科技依賴程度也越來越高，加上電子病歷的採用日益普及，因此如何確保電子病歷資訊不受到內部與外部惡意人士的破壞，造成外洩進而影響病患隱私，便是醫療機構不得不面對的問題，因此病歷隱私保護政策的遵循對於醫療機構而言是維持營運所必須的事項(Appari & Johnson, 2010; Pumphrey *et al.*, 2007)。就醫療產業而言，所謂「隱私政策」指可讓醫院員工知道醫院將如何處理病歷資訊及病人隱私權之管理指引(Management directives)(Li & 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 & Robinson, 2003)。美國 HIPAA 的隱私規則(Privacy Rule)明確規定須確保個人可辨識資訊的隱私(Pumphrey *et al.*, 2007)，對於醫療機構主要的要求包括：1)確保醫療機構所產生、收到、維護或傳輸之受保護民眾電子健康資訊的機密性(Confidentiality)、完整性(Integrity)與可取得性(Availability)；2)保護任何合理可能發生對於受保護的民眾電子健康資訊，避免遭攻擊或危險；3)保護任何合理可能發生對於受保護的民眾電子健康資訊，避免遭未經法律許可使用或揭露；4)確保隱私規則能在工作確實被遵循。換言之，隱私規範除了透過技術與管理程序確保病歷資訊安全外，亦須確保醫療機構的員工能確實遵循隱私保護政策。

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概念。「資訊安全」指組織必須有適當政策、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 & Robinson, 2003)，而「隱私」指民眾能夠控制其個人資訊的使用及是否揭露(Medlin & Cazier, 2011)；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 & 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 & Pitta, 2009)。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 & Pitta, 2009; Medlin & Cazier, 2011; Rindfleisch, 1997)，因此瞭解醫院員工對於醫院電子病歷資訊隱私的態度，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 & Pitta, 2009; Medlin & Cazier, 2011；楊漢淶, 2012)，病歷資訊除可能受到醫院外部人員之入侵而外洩，醫院內部員工也可能蓄意

或不經意洩漏，顯示病歷資訊保護仍有有極大改善空間；此外，由於電子病歷實施，使得電子化病歷資訊流通與取得更容易，醫院中有更多人員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影響因素，因此，本計畫主要目的在於電子病歷情境下：1)從威攝角度探討能讓醫院員工遵循電子病歷資訊隱私保護政策之影響因素，以及 2)探討前述因素是否受到其他前置因素(Antecedents)之強化或減弱。

一、從威攝角度探討能讓醫院員工遵循電子病歷資訊隱私保護政策之影響因素

依據威攝理論(Deterrence Theory)，藉由相關罰則預期可降低民眾從事不法行為(Gibbs, 1968; Tittle, 1969)，對於醫院電子病歷研究情境而言，醫院員工由於任務之故可接觸到電子病歷，因此違反電子病歷隱私保護政策之機率亦相對增加，調查報告(Medlin & Cazier, 2011)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，以往研究(Straub & Welke, 1998)建議組織資訊安全防護第一步在於威攝(Deterrence)，亦即避免資訊安全事件發生為首要任務，因此本計畫特別採取威攝理論作為研究理論基礎，探討可讓員工遵循電子病歷隱私規範影響因素；此外，依據保護動機理論(Rogers, 1975)，當民眾面臨威脅時，民眾亦可能採取自我保護措施，以電子病歷情境而言，員工如感受到電子病歷隱私遭破壞威脅，員工便可能採取自我保護措施(例如不違反電子病歷隱私保護政策)，因此本計畫提出包括：處罰嚴重性、處罰確定性、偵測確定性、認知嚴重性、認知脆弱性、主觀規範、敘述性規範、電子病歷隱私保護教育訓練等變數，可能直接或間接對醫院員工產生嚇阻作用，進而讓員工願意遵循電子病歷隱私保護政策行為意圖之影響因素。

二、激勵醫院員工遵循電子病歷資訊隱私保護政策因素之前置因素

依據威攝理論(Gibbs, 1968; Tittle, 1969)，實施對策(Countermeasures)亦可避免民眾犯行不法行為，以往資訊安全相關研究(Straub, 1990; Hovav & D'Arcy, 2012)亦建議可採取相關對策強化對於處罰認知，進而避免資訊安全事件發生；此外，依據保護動機理論(Rogers, 1975)，民眾面對威脅時所採取自我保護措施亦會受到外部訊息(例如教育訓練)影響而強化自我保護動機。因此，本計畫除找出激勵醫院員工遵循電子病歷隱私保護規範相關因素，更進一步探討這些因素之前置影響因素，以便能深入提出完整讓醫院員工願意遵循電子病歷隱私保護政策的對策。因此，本計畫提出電子病歷隱私保護教育訓練變數，藉以了解該變數是否會強化遏止醫院員工違反電子病歷隱私保護規範之因素。

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，找出如何鼓勵醫院員工遵循電子病歷隱私保護政策，藉以規劃並擬定符合醫院作業需求及民眾可充分信任的病人隱私保護政策。本計畫各項研究目的，可細分如下：

- 蒐集與彙整近五年與違反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/違反資訊隱私保護政策相關研究結果
- 提出正式處罰(處罰嚴重性、處罰確定性、偵測確定性)、非正式處罰(認知嚴重性、認知脆弱性、主觀規範、敘述性規範)、電子病歷隱私保護教育訓練、醫院員工遵循電子病歷隱私保護政策行為意圖等構面變數與衡量問卷
- 提出並驗證正式處罰(處罰嚴重性、處罰確定性、偵測確定性)、非正式處罰(認知嚴重性、認知脆弱性、主觀規範、敘述性規範)、電子病歷隱私保護教育訓練、醫院員工遵循電子病歷隱私保護政策行為意圖研究架構

參、文獻探討

一、醫療資訊隱私保護相關法律與醫療資訊隱私保護政策

針對醫療資訊的隱私保護，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 & 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」(行政院衛生福利部, 2004)與「醫療機構電子病歷製作及管理辦法」(行政院衛生福利部, 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」(行政院衛生福利部, 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。

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 & 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」(行政院衛生福利部, 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。

二、資訊安全行動週期

以往針對組織資訊安全濫用(Abuse)，Straub and Welke (1998)利用威攝理論的觀點提出如圖 3-1 資訊安全行動週期(The security action cycle)，認為資訊安全濫用可透過 4 個步驟處理：1)威攝(Deterrence)；2)預防(Prevention)；3)偵測(Detection)；4)補救(Remedies)。在威攝階段，員工潛在的犯行可透過包括資訊安全政策、指引以及知曉方案等措施予以避免；如果威攝階段的措施無效，則可透過預防的方法，例如資訊安全實體上或程序上的控制機制防止員工犯行；偵測階段主要目的在於強調揭發資訊安全濫用，讓此濫用狀況能被發現；而最後一個補救階段則是當濫用已經發生且被偵測出來時，需處理濫用所帶來的後果，而對於濫用的員工也必須依據組織資訊安政策採取必要措施(例如處罰)。資訊安全週期強調須強化威攝以及預防階段，並盡量減少偵測與補救階段(Straub & Welke, 1998)，Willison and Warkentin (2013)更認為必須在資訊安全週期的威攝階段前便妥善因應資訊安全事件；此外，資訊安全週期亦強調回饋機制，例如威攝階段可收到預防、偵測及補救三個階段的訊息，藉以讓潛在犯行者了解濫用時的可能後果，進而遏止惡意之犯行。因此對於防範組織中資訊安全的風險，理想狀況為採取預防措施，就電子病歷情境而言，要避免電子病歷隱私遭破壞，最佳的因應策略應當能事先防範電子病歷破壞事件發生，否則等到事後才進行補救時，可能因損害過大而不易處理。

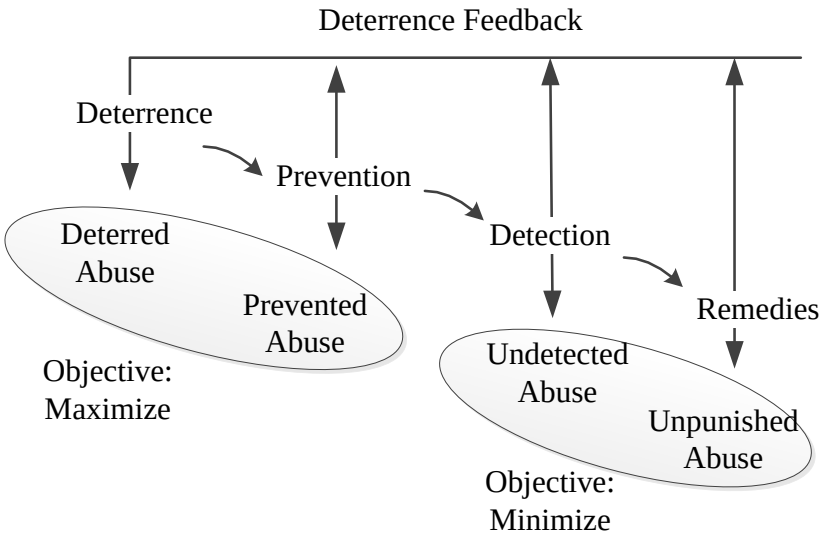

圖 3-1 資訊安全行動週期 (Straub & Welke, 1998, p. 446)

三、資訊系統安全相關行為

Guo (2013)彙整以往資訊安全研究所探討相關行為,發現有相當多的資訊安全行為種類，包括：電腦濫用/違反資訊安全(Computer abuse/Security contravention)、不道德使用(Unethical use)、忽略性資訊安全行為(Omissive security behavior)、資訊系統誤用(IS misuse)、違反資訊系統安全政策(Violation of policy)、非惡毒性違反資訊安全(Non-malicious security violation)、資訊安全政策濫用(Information security policy abuse)、資訊安全政策遵循(Security policy compliance)等。

就本計畫之研究情境而言，醫院中的電子病歷可能遭受的威脅種類相當多，為確保電子病歷隱私，對於不同的威脅均需要深入了解，然本計畫認為必須由最基本且最主要的關鍵，亦即從電子病歷隱私保護政策著手，如同資訊安全政策清楚規範整個組織可接受與不可接受的資訊系統相關行為(Straub, 1990)，如違反組織資訊安全政策，則員工將依組織規定接受處罰，對於醫院而言，如果能確保員工不違反電子病歷隱私保護政策，預期將可降低電子病歷外洩情事發生狀況。然以往文獻(Guo, 2013)指出，針對資訊系統的相關行為研究結果卻仍有不太一致的現象，而造成此現象之原因可能在於所探討的資訊安全行為屬於正向行為(例如遵循資訊安全政策)或負面的行為(例如違反資訊安全政策)，為針對此現象進一步深入了解，本計畫特別針對員工違反醫院電子病歷隱私保護政策的行為意圖進行探討，期望透過不同情境(醫療產業)所獲得結果，進一步累積資訊安全行為意圖的知識。本計畫將違反電子病歷行為意圖定義為醫院員工忽略(Ignorance)或未注意(Negligence)醫院電子病歷隱私保護政策之行為意圖(Siponen & Vance, 2010)。

四、電子病歷系統安全

Loch *et al.* (1992)曾將組織所面臨到資訊系統安全之威脅進行分類，主要可區分為內部與外部兩種威脅，而在內部與外部威脅中又可進一步區分為人為(Human)與非人為(Non-human)

兩類，內部人為威脅主要來自於員工，內部非人為威脅則來自於包括硬體故障、灰塵影響、電流湧浪(Power surge)等因素；外部人為威脅則包含駭客或間諜，外部非人為威脅則包括天然災害、惡意軟體、電力故障等。上述資訊系統威脅中，尤其以來自內部員工對於資訊系統的威脅是目前主要的研究主軸之一(Willison & Warkentin, 2013)，內部員工所造成的威脅也比非員工更嚴重(Straub, 1990)。Appari and Johnson (2010)將組織資訊隱私威脅區分為兩個來源：1)組織型威脅(Organizational threats)；2)系統性威脅(Systemic threats)，所謂組織型威脅主要指內部員工濫用資訊系統存取權限或外部人員攻擊資訊系統弱點；而系統性威脅則指在資訊流過程中，資訊流上的參與者將資訊用於其他目的，與原本的用途並不相同。而此兩類的資訊威脅當中，內部員工均有可能參與其中，造成資訊隱私破壞，儘管大部分醫療機構員工均認同病患的病歷資訊應當維持正確性，且須避免未經授權存取(Baumer *et al.*, 2000)。針對組織中電腦誤用的資訊安全破壞事件，Straub (1990)曾提出預防性控制(Preventive control)和威攝性控制(Deterrent control)兩種方法予以因應，預防性控制指透過資訊安全軟體避免未經授權存取，並設計安全之實體資訊設備；威攝性控制則利用指引(Guideline)或政策規範宣導電腦之合法使用、安全簡報和電腦稽核等事項。

電子病歷屬於醫院中的資訊系統，同樣會面臨許多資訊安全問題，而電子病歷如遭受到破壞，立即可見的影響除了醫師無法即時查詢病人的病歷資訊，更嚴重的問題是病人較隱私不願外流的病歷資訊可能因而洩漏出去，輕則造成當事人感覺顏面無光，嚴重者上只可能影響當事者喪失工作機會(Health Privacy Project, 2007)，因此為確保電子病歷隱私的安全，醫院必須找出如何避免內部員工違反電子病歷隱私保護政策之方法。

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。

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 (1975)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)。

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，修訂後保護動機理論(Rogers, 1983)指出當民眾面臨威脅時，

共有五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)；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)及 5)回應威脅所需成本(Response cost)，而這五個評估過程最後產生「保護動機」的心理狀態(Rogers, 1983; Tanner *et al.*, 1991)。

六、威攝理論

威攝理論(Deterrence Theory)最早的源起可追朔至 Thomas Hobbes (1588-1678)、Cesare Beccaria (1738-1794)和 Jeremy Bentham (1748-1832) (Onwudiwe *et al.*, 2005)。該理論植基於傳統犯罪學觀點所發展之威攝理論(D'Arcy & Herath, 2011; Onwudiwe *et al.*, 2005)，其主要論點在於一般大眾在犯下犯罪行為或是放棄從事犯罪行為之決策主要依據個人利益之最大化以及付出成本最小化，而處罰(Sanction)則可降低大眾犯罪之發生(Straub, 1990)。處罰可進一步區分為正式或非正式兩類(Gibbs, 1968)。傳統威攝理論著重於正式處罰(Gibbs, 1968)，所持論點為當處罰越重，且確定會處罰不法行為，而只要一違法便會立即進行處罰時，民眾從事不法行為的機率便會降低。更精確來說，如果處罰具有下列三種狀況：1)如犯罪處罰的程度越嚴重，從理性角度進行決策的社會大眾便不太可能從事犯罪行為；2)而社會大眾一旦犯罪，則確定會遭到法律制裁；3)如社會大眾犯罪後，也會立即接受到法律制裁，以遏止犯罪發生。就組織資訊安全情境而言，所謂正式處罰指組織訂定規範與程序，藉以確保員工能遵循資訊安全政策(Guo & Yuan, 2012)。

而所謂非正式處罰指的是非法律性成本(Non-legal costs) (Pratt *et al.*, 2006)，可能包含社會不認同(Social disapproval)、自我不認同(Self-disapproval)、道德壓抑等，例如某不法行為未獲得朋友或同儕的認可(Guo & Yuan, 2012; Piquero & Tibbetts, 1996)，然而此不法行為並不須付出法律的代價(Siponen & Vance, 2010)，依據以往威攝理論彙整分析(Meta-analysis)結果，非法律性成本對於遏止非法行為的強度較處罰確定性與不法行為之間關係高(Pratt *et al.*, 2006)。威攝理論認為社會大眾會將正式與非正式處罰所可能帶來的認知風險與成本納入考慮，再決定是否從事非法行為(Pratt *et al.*, 2006)。威攝理論所提出之正式處罰包含三個主要部分(Gibbs, 1968; Tittle, 1969)：1)嚴重性(Severity)、2)確定性(Certainty)與 3)立即性(Celerity, Swiftness)。威攝理論一直到 1968 年代左右才開始有正式的進行假說驗證，然而相關的實證研究卻相當稀少(Onwudiwe *et al.*, 2005)，較受矚目為 1968 年左右才有研究實際驗證威攝理論，結果為透過處罰嚴重性與處罰確定性可能對於防止自殺的行為有遏止作用(Onwudiwe *et al.*, 2005)。

在資訊管理領域研究當中，此理論是目前資訊安全領域最常被引用的理論基礎之一(Straub, 1990; D'Arcy *et al.*, 2009b; D'Arcy & Herath, 2011; Herath & Rao, 2009a; Herath & Rao, 2009b)，然儘管威攝理論在犯罪相關領域有相當強的理論基礎與實證研究支持(Pratt *et al.*, 2006)，但將此理論運用於遏止資訊安全非法行為研究，所得到之結果卻仍有不一致(D'Arcy & Herath, 2011; Guo & Yuan, 2012)，而目前將威攝理論運用於醫療產業，尤其是電子病歷相關研究則尚不多見。

由於以往運用威攝理論的研究主要採用處罰之嚴重程度與處罰之確定性，本計畫針對與資管相關領域之研究進行分析(如表 3-1 所示)。結果顯示威攝理論所包含的正式處罰與非正式

處罰均有研究嘗試予以衡量。在正式處罰變數方面，主要以處罰嚴重程度和處罰確定程度較多研究所採用，而處罰立即性則較少研究採用(Onwudiwe *et al.*, 2005)，然處罰嚴重程度和處罰確定程度的研究結果卻呈現並不一致現象，D'Arcy and Herath (2011)認為造成這種結果不一致的現象主因可能在於未納入其他變數以及和研究方法相關的議題(如抽樣、未回應誤差、不同統計分析方法等)所造成。在研究變數方面，D'Arcy and Herath (2011)也建議可加入例如自我控制、電腦自我效能、道德信念、工作地點以及員工職位等變數，以進一步驗證威攝理論，本計畫亦分析針對道德信念相關的變數於威攝理論的應用，結果發現採用此變數的研究量並不多，研究結果也同樣有不一致的現象，顯示道德信念類的因素對於組織員工遵循資訊安全政策之研究數量仍有所不足(Guo & Yuan, 2012)，仍需進一步的深入探討，此觀點與 Pratt *et al.* (2006)針對威攝理論所進行彙整研究之建議一致。

表 3-1 威攝理論於資訊管理相關研究所使用變數彙整

文獻	正式處罰			非正式處罰
	嚴重程度	確定程度	立即性	道德信念
Hovav and D'Arcy (2012)[a]	X	V	N/A	V
Hovav and D'Arcy (2012)[b]	V	V	N/A	X
Kankanhalli *et al.* (2003)	V	X	N/A	N/A
D'Arcy *et al.* (2009b)	V	X	N/A	N/A
Herath and Rao (2009a)	V	V	N/A	N/A
Herath and Rao (2009b)	V	V	N/A	V
Peace *et al.* (2003)	V	V	N/A	N/A
Hu *et al.* (2011)	X	X	X	N/A
Li *et al.* (2010)	X	V	N/A	X
Zhang *et al.* (2009)	X	V	N/A	N/A
Guo and Yuan (2012)	X	N/A	N/A	V
Siponen and Vance (2010)		X		X
Siponen *et al.* (2010)		V		N/A
Gopal and Sanders (1997)		V		N/A

註 1：V 表與依變數成顯著相關，X 表關係不顯著，N/A 表未採用該變數；a/b 美國/韓國樣本

七、威攝理論相關研究模式

威攝理論以往主要運用於犯罪行為之預測(Gibbs, 1968)，但後來威攝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威攝理論之研究大部分為資訊安全政策遵循(Compliance)或違反(Violation)或資訊系統誤用(Misuse)等研究，相關研究架構說明如下。

(一)資訊安全政策遵循或違反研究模式

1.1 Li *et al.* (2010)模式

Li *et al.* (2010)以理性選擇理論(Rational choice theory)為理論基礎，所使用變數與威攝理論相似，Li *et al.* (2010)調查不同組織員工對於網際網路使用規範遵循的影響因素(研究架構如

圖 3-2)，採線上問卷方式進行資料蒐集，共回收 246 份有效問卷，結果發現偵測機率(Detection probability)、安全風險(Security risks)、認知效益(Perceived benefits)和個人規範(Personal norms)顯著影響員工遵循網際網路使用規範之行為意圖；當中個人規範對於處罰嚴重程度(Sanction severity)和員工遵循網際網路使用規範行為意圖之間的關係具調節作用。而組織規範(Organizational norms)和組織認同(Organizational identification)則顯著影響個人規範。

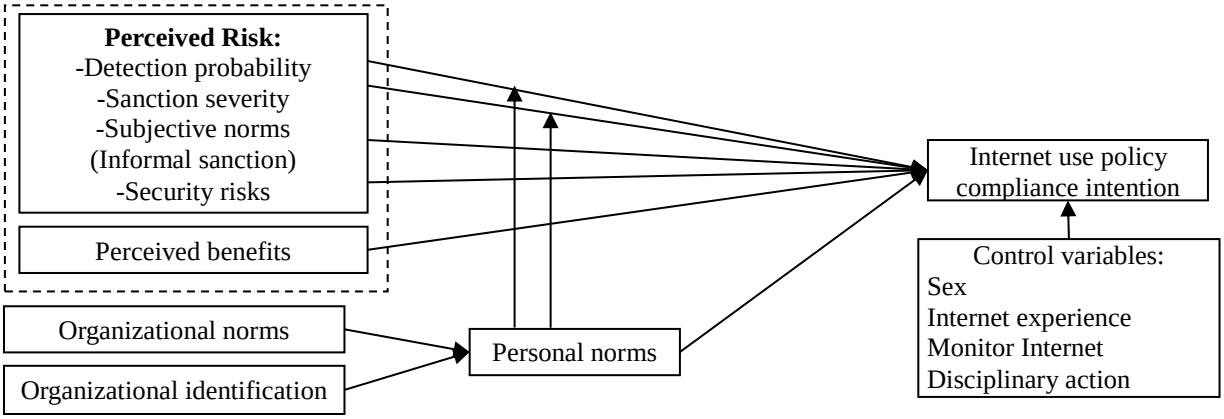

圖 3-2 Li *et al.* (2010)研究模式

1.2 Kankanhalli *et al.* (2003)模式

Kankanhalli *et al.* (2003)依據威攝理論提出如圖 3-3 的研究架構，探討如何讓組織資訊安全發揮效果，亦即能防止組織員工未經授權使用或誤用組織資訊資產。該模式認為組織的威攝努力程度(Deterrent efforts)、威攝嚴重程度(Deterrent severity)和預防努力程度(Preventive efforts)共同影響組織資訊安全效能，而組織威攝努力程度(Deterrent efforts)、威攝嚴重程度(Deterrent severity)和預防努力程度(Preventive efforts)又分別受到組織規模(Organization size)、高階主管支持(Top management support)和產業類別(Industry type)影響；Kankanhalli *et al.* (2003)針對組織資訊單位主管進行調查，共回收 63 份有效樣本，分析結果顯示威攝努力程度和預防努力程度顯著影響組織資訊安全之效能，而組織規模僅對威攝努力程度有顯著影響，高階主管支持僅對預防努力程度有顯著影響，產業類別(金融產業)則顯著影響威攝努力程度與威攝嚴重程度。

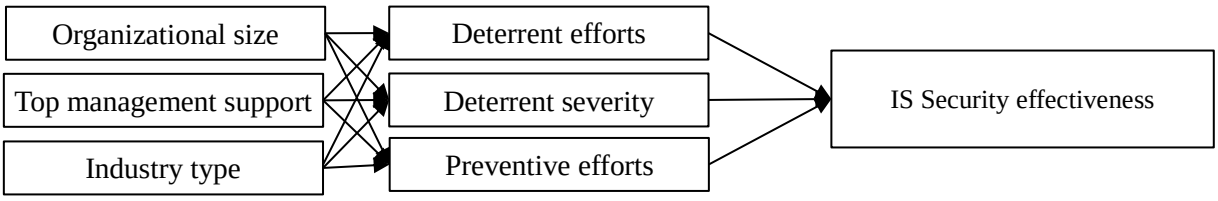

圖 3-3 Kankanhalli *et al.* (2003)資訊安全效能研究模式

1.3 Siponen *et al.* (2010)模式

Siponen *et al.* (2010)依據理性行為理論(Theory of planned behavior)、保護動機理論(Protection motivation theory)、創新擴散理論(Innovation diffusion theory)、威攝理論(Deterrence theory)等不同理論，提出整合式研究架構(如圖 3-4 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；而威攝(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。

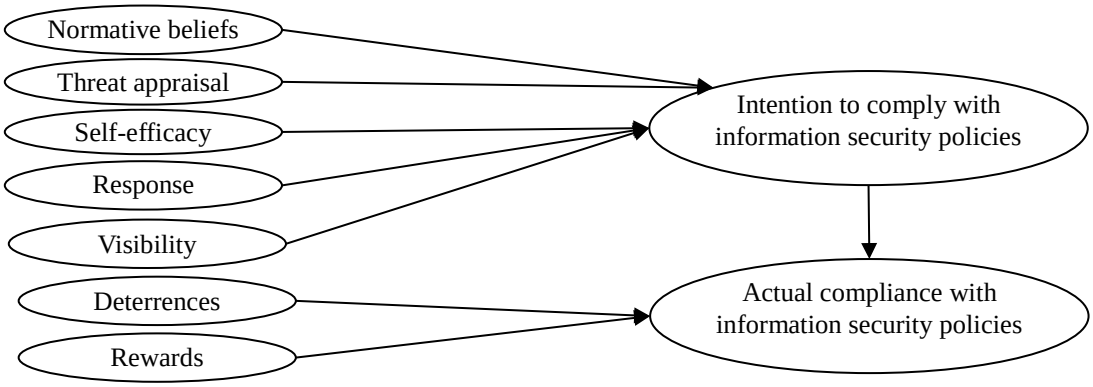

圖 3-4 Siponen *et al.* (2010)研究模式

1.4 Herath and Rao (2009a)模式

Herath and Rao (2009a)以代理人理論(Principal agent theory)與威攝理論為基礎，提出如圖3-5研究架構，以瞭解員工對資訊安全政策遵循意圖之影響因素，結果發現處罰嚴重度(Severity of penalty)、偵測確定性(Certainty of detection)敘述性規範信念(Normative beliefs)、同儕行為(Peer behavior)與認知資訊安全政策效能(Perceived effectiveness)均顯著影響員工遵循資訊安全政策之行為意圖。

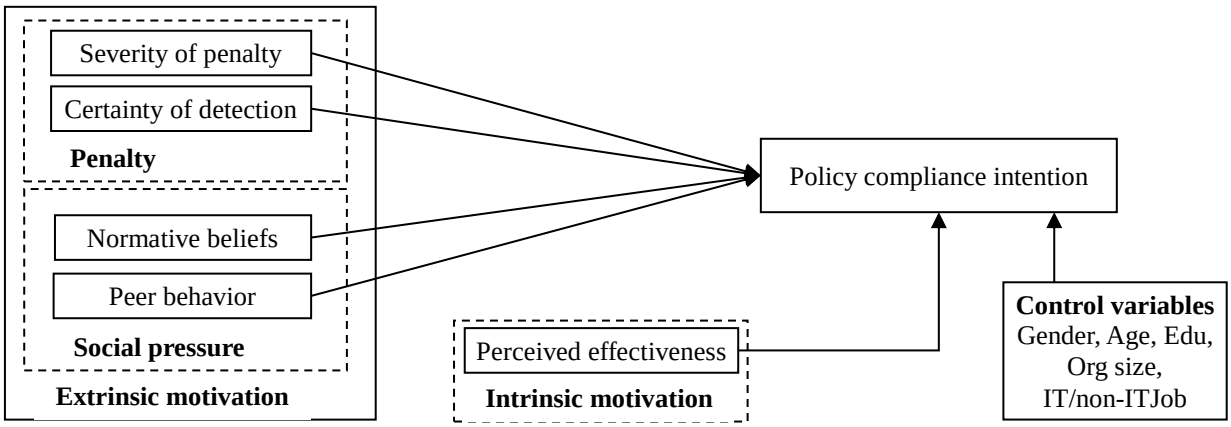

圖 3-5 Herath and Rao (2009a)研究模式

1.5 Herath and Rao (2009b)模式

Herath and Rao (2009b)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 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(Perceived severity of security breach)影響安全漏洞顧慮程度(Security breach concern level)，而安全漏洞顧慮程度影響安全政策態度(Security policy attitude)；2)反應成本(Response cost)、反應效能(Response efficacy)、自我效能影響安全態度政策；3)資源可取得性(Resource availability)影響自我效能；4)組織承諾(Organizational commitment)影響反應效

能和資訊安全政策遵從意圖；5)偵測確定性(Detection certainty)、主觀規範和敘述性規範影響資訊安全政策遵從意圖。

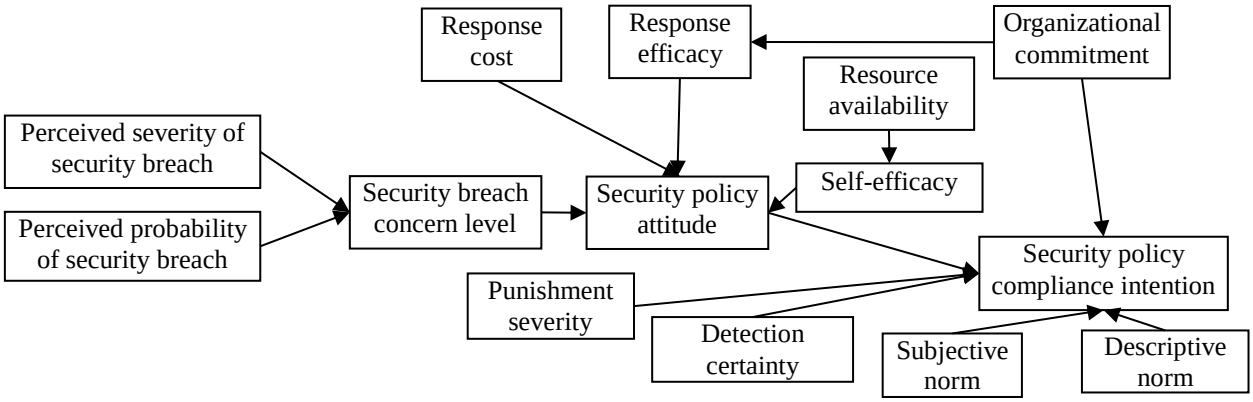

圖 3-6 Herath and Rao (2009b)研究模式

1.6 Siponen and Vance (2010)模式

為了解組織員工為何不遵循資訊安全政策，Siponen and Vance (2010)結合中和理論(Neutralization)和威攝理論提出如圖 3-7 之研究架構，針對三家不同產業的組織員工進行調查以驗證模式，共蒐集 1,449 份樣本。分析結果顯示威攝理論相關構面，包括：正式處罰(Formal sanctions)、非正式處罰(Informal sanctions)和恥辱(Shame)均無法顯著預測員工違反資訊安全政策之行為意圖。

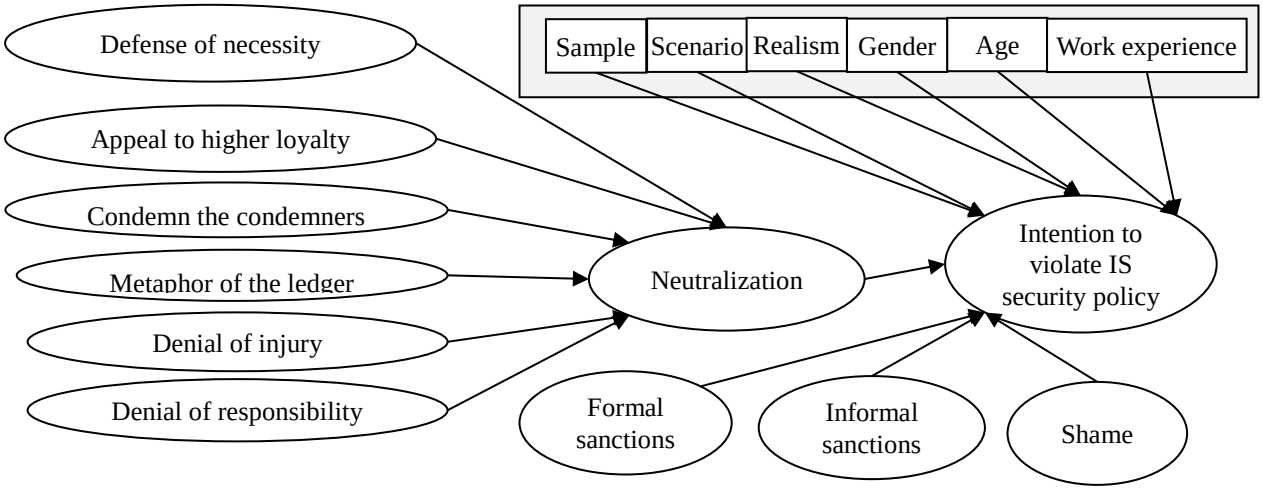

圖 3-7 Siponen and Vance (2010)研究模式

1.7 Hovav and D'Arcy (2012)模式

Hovav and D'Arcy (2012)以威攝理論為基礎提出如圖 3-8 研究模式，探討美國與韓國不同文化環境下影響資訊系統誤用之因素。分別從美國和韓國蒐集 366 和 360 份樣本進行模式驗證，結果發現美國樣本所驗證模式中，僅有認知處罰確定性(Perceived certainty of sanctions)對於資訊系統誤用行為意圖之影響不顯著，而韓國樣本分析結果則包括：技術性反制措施(Technical countermeasures)對於認知處罰嚴重程度(Perceived severity of sanctions)，以及認知處罰嚴重程度和資訊系統誤用行為意圖之影響並不顯著。而文化對於道德認知(Moral beliefs)與資訊系統誤用行為意圖、程序性反制措施(Procedural countermeasures)和認知處罰確定程度、

程序性反制措施(Procedural countermeasures)和認知處罰嚴重程度、技術性反制措施和認知處罰嚴重程度之間的影響並未具調節作用。

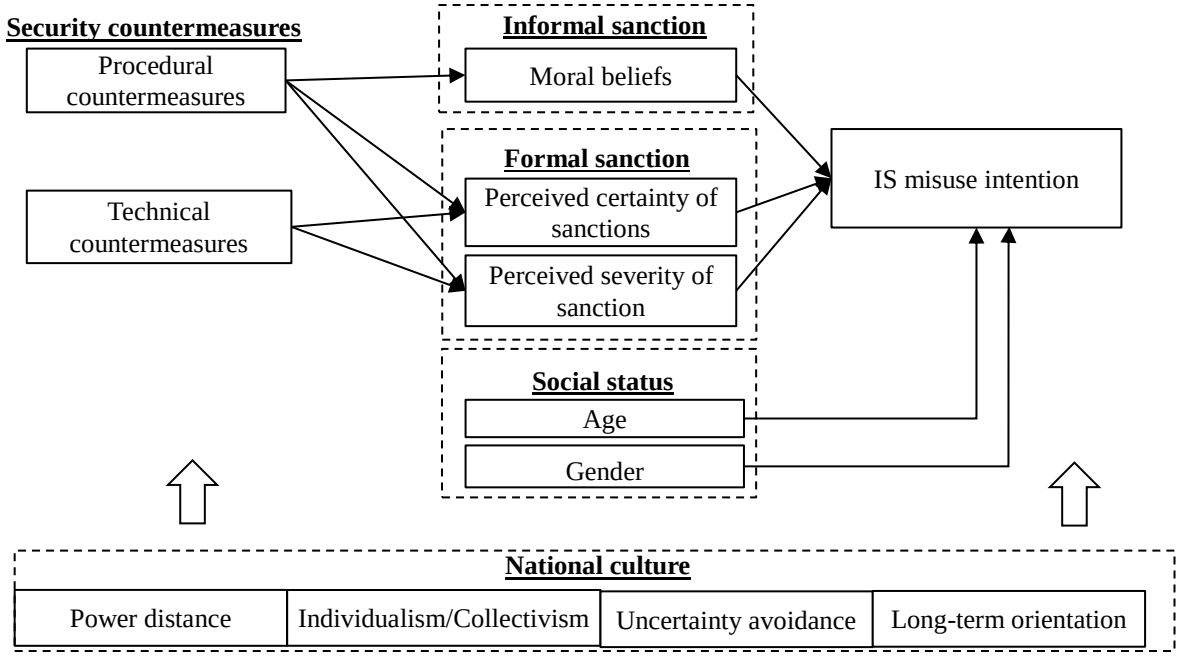

圖 3-8 Hovav and D'Arcy (2012)研究模式

1.8 Hu *et al.* (2011)模式

針對組織資訊安全政策濫用(Abuse)議題，Hu *et al.* (2011)結合威懾理論以及其他行為理論，提出提出如圖 3-9 研究架構，用於探討嚇阻(Deterrences)措施是否能有效防止其違反資訊安全規範行為。該研究架構嚇阻(Deterrence)變數為二階(Second-order)變數，包括認知處罰嚴重程度(Perceived severity of sanctions)、認知處罰確定程度(Perceived certainty of sanctions)與認知處罰立即程度(Perceived celerity of sanctions)，結果嚇阻變數顯著影響認知非正式風險(Perceived informal risks)和認知正式風險(Perceived formal risks)；道德認知(Moral beliefs)顯著影響認知內在效益(Perceived intrinsic benefits)、認知恥辱風險(Perceived risk of shame)、認知非正式風險與認知正式風險；低度自我控制(Low self-control)顯著影響認知外在效益(Perceived extrinsic benefits)與認知內在效益；而認知外在效益和認知外在效益顯著影響員工違反資訊安全政策之行為意圖。Hu *et al.* (2011)進一步分析認知處罰嚴重程度、認知處罰確定程度與認知處罰立即程度對於員工行為意圖之影響，結果發現三個變數均未呈現顯著影響。

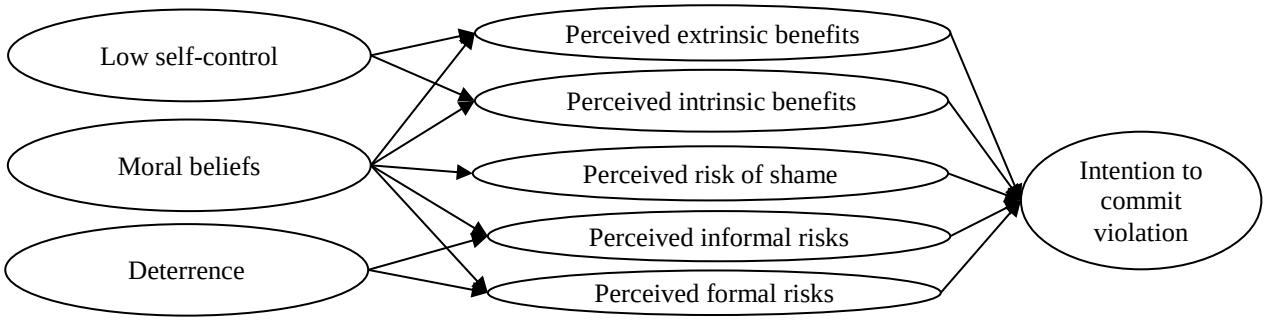

圖 3-9 Hu *et al.* (2011)研究模式

(二)電腦誤用與其他模式

2.1 Peace *et al.* (2003)模式

Peace *et al.* (2003)結合威攝理論、期望效用理論(Expected utility theory)與計畫行為理論，提出如圖 3-10 研究架構，用於探討組織員工對於盜版軟體的認知。該研究共回收 201 份有效問卷用於驗證所提之研究模式，結果顯示員工態度、主觀規範與知覺行為控制顯著影響非法拷貝軟體的行為意圖，而處罰嚴重性(Punishment severity)、處罰確定性(Punishment certainty)與軟體成本顯著影響員工態度，處罰確定顯著影響員工知覺行為控制。

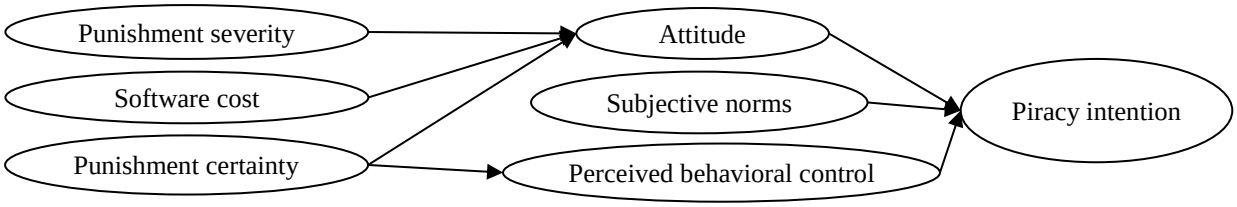

圖 3-10 Peace *et al.* (2003)研究模式

2.2 D'Arcy *et al.* (2009b)模式

D'Arcy *et al.* (2009b)以威攝理論為基礎提出如圖 3-11 研究模式，認為認知處罰確定性(Perceived certainty of sanction)和認知處罰嚴重性(Perceived severity of sanctions)可降低組織員工誤用電腦的行為意圖，而認知處罰確定性和認知處罰嚴重性則可藉由向員工宣導包括：資訊安全政策(Security policies)、教育訓練(SETA program)以及電腦監控(Computer monitoring)等資訊安全措施予以強化。該模式總共蒐集 8 家不同公司 269 位員工，結果發現只有認知處罰嚴重性顯著影響員工誤用電腦的行為意圖，而資訊安全政策、教育訓練以及電腦監控則分別顯著影響認知處罰確定性和認知處罰嚴重性。

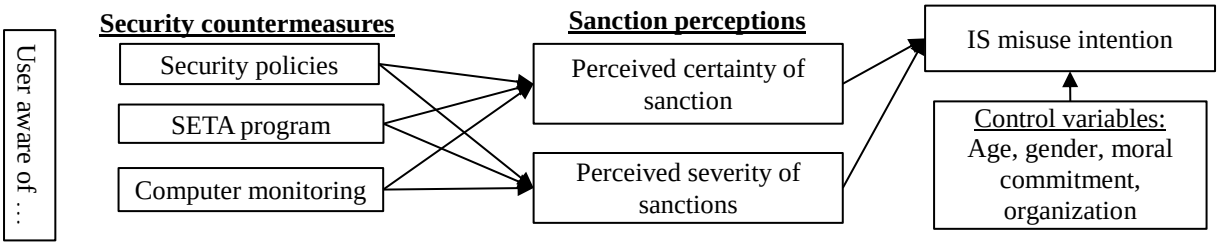

圖 3-11 D'Arcy *et al.* (2009b)研究模式

2.3 Zhang *et al.* (2009)模式

Zhang *et al.* (2009)以威攝理論為基礎提出如圖 3-12 研究模式，探討學生對於數位盜版的認知行為，認為低度自我控制(Low self-control)、處罰確定性(Punishment certainty)和處罰嚴重性(Punishment severity)會影響學生進行數位盜版之行為意圖，而處罰確定性又受到自我效能(Self-efficacy)影響。該模式總共蒐集 207 位學生樣本，結果發現自我效能顯著影響處罰確定性，而處罰嚴重性顯著影響學生進行數位盜版之行為。

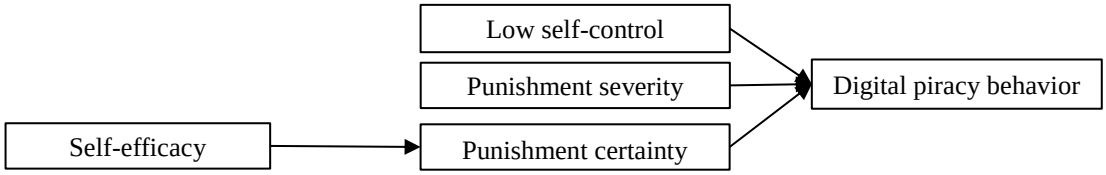

圖 3-12 Zhang *et al.* (2009)研究模式

(三)威攝理論相關模式小結

本計畫更進一步依據威攝理論之主要變數，彙整前述各研究架構之研究結果(如表 3-2 所示)，結果顯示在處罰確定性變數對於依變數的影響並不太一致，較多研究結果為顯著(如 Chen *et al.*, 2012; Herath & Rao, 2009a; Hovav & D'Arcy., 2012; Kankanhalli *et al.*, 2003; Pahnila *et al.*, 2007)，然其他研究則呈現不顯著結果(如 D'Arcy et al., 2009b; Hovav & D'Arcy., 2012; Siponen & Vance, 2010)；此外，在處罰嚴重性與依變數的關係結果亦不太一致，變數呈現顯著(如 Chen *et al.*, 2012; D'Arcy *et al.*, 2009b; Herath & Rao, 2009a; Hovav & D'Arcy, 2012)與不顯著(如 Hovav & D'Arcy, 2012; Kankanhalli *et al.*, 2003)的研究均存在；至於偵測確定性變數與依變數的研究結果則大部分均為顯著(如 Herath & Rao, 2009b; Kankanhalli *et al.*, 2003; Li *et al.*, 2010)；至於在社會規範/主觀規範變數與依變數的關係，大部分的研究結果顯示社會規範/主觀規範均呈現顯著結果(如 D'Arcy & Devaraj, 2012; Guo *et al.*, 2011; Guo & Yuan, 2012; Herath & Rao, 2009b; Hovav & D'Arcy., 2012; Li *et al.*, 2010; Pahnila *et al.*, 2007; Siponen *et al.*, 2010)，僅少部分研究呈現不顯著結果(如 Hu et al., 2011)。

表 3-2 威攝理論相關研究結果彙整表

文獻	主要自變數	主要依變數	方法	樣本	主要發現
Pahnila *et al.* (2007)	Attitude, sanctions, normative beliefs, and habits	Intention to comply	Survey	245 employees from a Finnish company	顯著變數：Attitude (β = .54***)、normative belief (β = .24***)、habits (β = .14*)
D'Arcy *et al.* (2009b)	Perceived certainty of sanctions and perceived severity of sanctions	IS misuse intention	Survey	269 employees	顯著變數：Perceived severity of sanctions (β = -.18**)
Herath and Rao (2009a)	Severity of penalty, certainty of detection, normative beliefs, peer behavior, and perceived effectiveness	Policy compliance intention	Survey	310 employees from 77 organizations	顯著變數：Severity of penalty (β = -.21**)、certainty of detection (β = .26***)、normative beliefs (β = .40***)、peer behavior (β = .16*)、perceived effectiveness (β = .22***)
Herath and Rao (2009b)	Self-efficacy, security policy attitude, punishment severity, detection certainty, subjective norm, and descriptive norm	IS security policy compliance	Survey	312 employees from 78 organizations	顯著變數：Self-efficacy (β = .17**)、detection certainty (β = .16**)、subjective norm (β= .31***)、descriptive norm (β = .10*)
Siponen and Vance (2010)	Neutralization, formal sanctions, informal sanctions, and shame	Intention to violate IS security policy	Survey	395 employees from three organizations	顯著變數：Neutralization (β = .60***)
Li *et al.* (2010)	Detection probability, sanction severity, subjective norms, security risk, perceived benefits, personal norms	Internet use policy compliance intention	Survey	246 employees from various organizations	顯著變數：Detection probability (β = .24***)、security risk (β = .14†)、perceived benefits (β = -.23**)、personal norms (β = .24***)

表 3-2 威攝理論相關研究結果彙整表(續)

文獻	主要自變數	主要依變數	方法	樣本	主要發現
Hovav and D'Arcy (2012)	Moral beliefs, Perceived certainty of sanctions, perceived severity of sanctions	IS misuse intention	Survey	269 employees and 97 MBA students from U.S. / 145 employees and 215 MBA students from South Korea	顯著變數：美國樣本-Moral beliefs (β = -.48**)、perceived severity of sanctions (β = -.14**)；韓國樣本-Moral beliefs (β = -.51**)、perceived certainty of sanctions (β = -.20**)
Hu *et al.* (2011)	Perceived extrinsic benefits, perceived intrinsic benefits, perceived risk of shame, perceived informal risks, perceived formal risks	Intention to commit computer misconduct	Survey	207 employees from five organizations in China	顯著變數：Perceived extrinsic benefits (β = .15**)、perceived intrinsic benefits (β = .33***)
Guo and Yuan (2012)	Personal self-sanctions, workgroup sanctions, organizational sanctions	Intentions to violate security policies	Survey	306 employees from various organizations	顯著變數：Personal self-sanctions (β = -.15*)、workgroup sanctions (β = -.41***)
D'Arcy and Hovav (2009a)	Security policy, SETA program, computer monitoring	IS misuse intention (unauthorized access, unauthorized modification)	Survey	507 MBA samples	顯著變數：Security policy (β= -.14**/-.12*/-.14**)、computer monitoring (β = -.17**/-.15**/-.16**)顯著影響 unauthorized modification；SETA program (β = -.16**/-.14**/-.16**)顯著影響 unauthorized access

Note: †p < .1, *p < .05, **p < .01, ***p < .001

表 3-2 威攝理論相關研究結果彙整表(續)

文獻	主要自變數	主要依變數	方法	樣本	主要發現
D'Arcy and Devaraj (2012)	Certainty*severity, social desirability pressure, moral beliefs, virtual status, employment level	Technology misuse intention	Survey	441 MBA samples	顯著變數：Certainty*severity (β = -.17**)、social desirability pressure (β = -.24**)、moral beliefs (β = -.41**)、virtual status (β= -.11*)
Chen *et al.* (2012)	Perceived severity of punishment, perceived significance of reward, perceived enforcement certainty	Information security policy compliance intention	Experiment	200 employees from two organizations	顯著變數：Perceived severity of punishment (F-value = 77.90***)、perceived significance of reward (F-value = 108.72***)、perceived enforcement certainty (F-value = =26.78***)
Kankanhalli *et al.* (2003)	Deterrent efforts, deterrent severity, preventive efforts	IS security effectiveness	Survey	63 IS managers	顯著變數：Deterrent efforts (β = .28**)、preventive efforts (β = .22*)
這篇沒有 Xue *et al.* (2011)	Punishment expectancy, perceived justice of punishment, satisfaction, perceived usefulness	Compliance intention	Survey	118 employees from various organizations	顯著變數：perceived justice of punishment (β = .42**) 、satisfaction (β = .20*)

Note: †$p < .1$, *$p < .05$, **$p < .01$, ***$p < .001$

表 3-2 威攝理論相關研究結果彙整表(續)

文獻	主要自變數	主要依變數	方法	樣本	主要發現
Guo *et al.* (2011)	Attitude toward security policy, relative advantage for job performance, perceived security risk, perceived sanctions, workgroup norm, perceived identity match	Attitude toward non-malicious security violation	Survey	306 employees from various organizations	顯著變數：Relative advantage for job performance (β = .16**)、perceived security risk (β = -.17**)、workgroup norm (β = 0.9***)、perceived identity match (β = -.11**)
	Attitude toward non-malicious security violation, workgroup norm, perceived identity match	non-malicious security violation intention			顯著變數：Attitude toward non-malicious security violation (β = .47***)、workgroup norm (β = .23***)、perceived identity match (β = -.14**)
Siponen *et al.* (2010)	Normative beliefs, threat appraisal, self-efficacy, response efficacy, visibility	Intention to compliance with information security policies	Survey	917 employees from various Finland organizations	顯著變數：Normative beliefs (β = .45***)、threat appraisal (β = .12***)、self-efficacy (β = .17***)、visibility (β = .09***)
	Intention to compliance with information security policies, deterrences, rewards	Actual compliance with information security policies			顯著變數：Intention to compliance with information security policies (β = .40***)、deterrences (β = .09***)

Note: †$p < .1$, *$p < .05$, **$p < .01$, ***$p < .001$

肆、研究方法

本計畫主要研究方法為「調查研究法」。首先，本階段透過文獻探討，找出影響醫院員工遵循醫院隱私保護政策的直接與間接因素，包括：處罰嚴重性、處罰確定性、電子病歷遭破壞嚴重程度、電子病歷遭破壞機率、主觀規範、敘述性規範與電子病歷隱私保護教育訓練等，並提出研究架構雛形、構面、變數及衡量問卷初稿，接著邀請學者及實務界專家，透過專家會議檢視研究架構雛形及問卷內容之表達方式是否適當，以提升內容效度(Straub et al., 2004)。修訂後問卷則進行先導測試，透過填答者角度來檢視問卷問項及語意是否清晰，再依據前測結果進行問卷修訂，之後以南部某醫學中心員工為研究樣本發放問卷，最後則分析所蒐集資料，並完成結案報告。

一、研究架構推導

醫院員工如違反電子病歷隱私保護政策時，嚴重時可能造成醫院商譽與財務損失影響，員工亦必須受到相對之處罰，包括：警告記過、罰款、失去工作甚至須負法律責任。因此為避免員工發生違反電子病歷隱私保護規範狀況發生，本計畫認為可藉由威攝理論的觀點，透過處罰手段達到遏止非法行為的發生(Straub, 1990)，因此威攝理論應當適合做為本計畫主要理論基礎；威攝理論所指的處罰可進一步區分為正式處罰與非正式處罰(Gibbs, 1968)。於本計畫電子病歷情境，所謂正式處罰可指醫院實際的電子病歷規範之罰則，如員工違反相關規定時就須接受相對之罰則，而非正式處罰則指員工所感受到的道德規範的限制(Guo & Yuan, 2012)等非法律性成本(Pratt *et al.*, 2006)，例如洩漏電子病歷是不道德的行為，或感受到醫院營運可能因電子病歷隱私遭破壞而大受影響，甚至可能影響員工的工作機會等威脅。依據威攝理論，這些正式或非正式處罰都可能降低員工違反電子病歷隱私保護政策之行為意圖。此外，威攝理論的主要論點在於潛在犯行者感受到如犯行所可能承擔的風險程度，此風險認知便可能影響其行為意圖(Straub, 1990)，因此，另外依據保護動機理論，如民眾感受到威脅時，將會採取自我保護措施，而組織即使僅有一位員工破壞組織資訊安全，所造成的影響亦可能相當大(Willison & Warkentin, 2013)，因此醫院員工如感受到電子病歷隱私外洩之威脅，例如醫院商譽或營運受損，甚至影響個人工作機會時，醫院員工便可能依據所面臨威脅調整其行為(Workman *et al.*, 2007)，亦即避免違反電子病歷隱私保護規範，進而遵循該隱私保護規範。

依據威攝理論，藉由資訊安全相關教育訓練課程可提高組織員工對於正式與非正式處罰認知(D'Arcy & Hovav, 2009a)，Workman and Gathegi (2007)亦認為道德教育在某些情況下對遏止非法行為有效。本計畫將此推理運用至醫院情境，藉由醫院電子病歷隱私保護相關教育訓練課程，預期可強化員工對違反電子病歷處罰認知，進而降低其違反電子病歷隱私保護政策行為意圖。依據上述理論架構，本計畫提出研究架構雛形包括：電子病歷隱私保護教育訓練、處罰嚴重性、偵測確定性、電子病歷遭破壞認知嚴重程度、電子病歷遭破壞認知脆弱性、主觀規範、敘述性規範及違反醫院電子病歷隱私保護政策行為意圖等九個構面。本計畫研究架構如圖 4-1 所示。

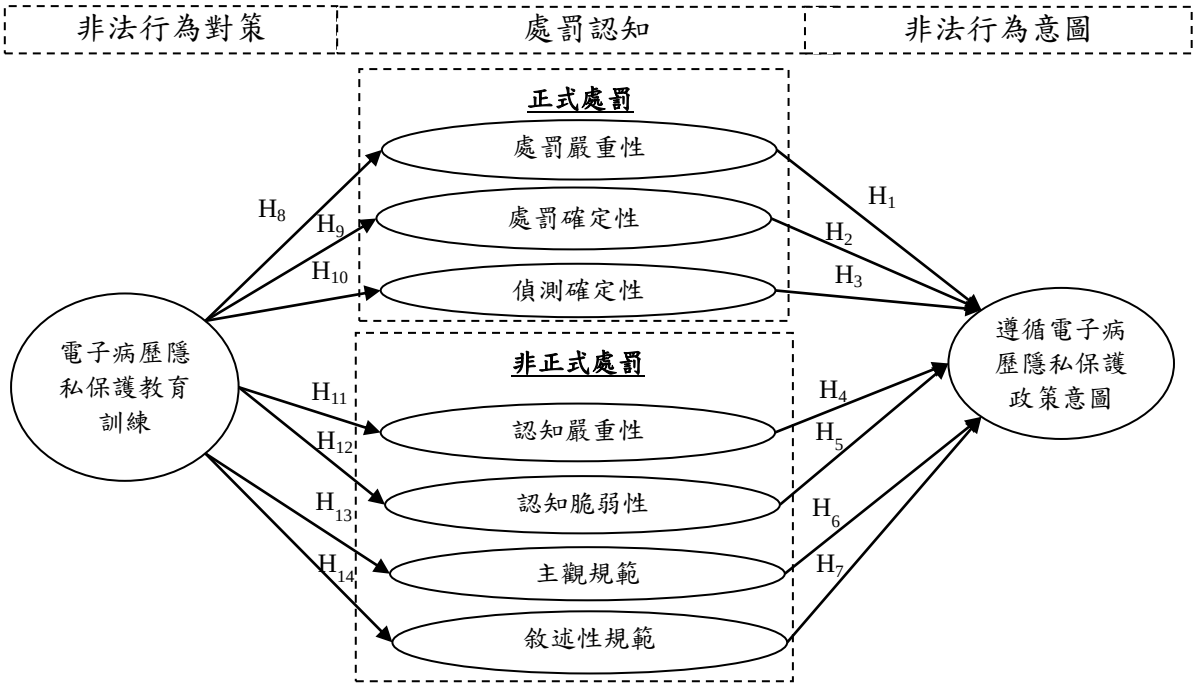

圖 4-1 研究架構雛形

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)正式處罰(Formal sanction)相關變數與員工違反電子病歷隱私保護政策行為意圖之關連

依據威攝理論，如果犯罪行為遭發現，而所須接受的處罰相當嚴重，則民眾權衡得失後便可能不從事違法行為，因此違法行為可因為確定(Certainty)、嚴重(Severity)與迅速(Celerity/Swiftness)的處罰而避免(Gibbs, 1968)，此種方法在民眾犯行的動機不強時更有效(Workman & Gathegi, 2007)。此外，Vroom and von Solms (2004)認為要確保員工能確實遵循組織所擬定資訊安全政策，仍需某種形式評估，以調查員工對於資訊安全的遵循程度，換言之，儘管威攝理論建議透過嚴重且確定的處罰來遏止不法行為，但仍須讓潛在違法者知道組織所採取避免違法行為之預防措施(Straub, 1990)，僅條列式資訊安全政策仍無法落實執行資訊安全政策(Peace *et al.*, 2003)，因此組織需有機制能偵測員工不法行為(Herath & Rao, 2009a; Straub & Nance, 1990)，Park *et al.* (2012)也指出單純的處罰可能不足以避免員工犯行，必須佐以偵測措施。換言之，處罰嚴重性、處罰確定性與偵測確定性可能具備遏止電子病歷隱私遭破壞不法行為的發生。在電子病歷情境下，處罰嚴重性指醫院對於發生電子病歷隱私破壞情況所給予員工處罰的嚴厲程度；處罰確定性指醫院對於發生電子病歷隱私破壞情況所給予員工處罰的確定程度(處罰的機率)；偵測確定性則指醫院對於偵測員工破壞電子病歷隱私等不法行為的確定程度。

以往亦有研究證實處罰嚴重程度、處罰確定程度與偵測確定性會影響民眾/組織員工許多態度或行為意圖，包括： 資訊系統安全效能(Herath & Rao, 2009b; Kankanhalli *et al.*, 2003; Straub, 1990)、軟體盜版(Gopal & Sanders, 1997; Zhang *et al.*, 2009)、資訊安全遵循意圖(Herath

& Rao, 2009b; Li *et al.*, 2010; Siponen & Vance, 2010; Siponen *et al.*, 2010)、資訊系統/政策誤用(D'Arcy *et al.*, 2009a; Guo & Yuan, 2012; Hovav & D'Arcy, 2012; Hu *et al.*, 2011)等。

1.處罰嚴重性與醫院員工遵循電子病歷隱私保護政策行為意圖之關連

在威攝理論中，處罰嚴重性指當民眾採取非法行為被發現時，所接受處罰的嚴重程度。依據威攝理論，如果犯罪行為的處罰相當嚴重，且一旦犯罪行為發生，便須接受處罰，則民眾權衡得失後便可能不從事違法行為，因此違法行為可因為處罰的嚴重(Severity)而避免(Gibbs, 1968)。以往有相當多研究利用處罰嚴重性來避免組織員工利用組織資訊資源或違反資訊安全政策。例如 Straub (1990)利用威攝理論的處罰嚴重程度預測組織員工對於電腦資源的濫用，結果發現組織處罰嚴重性顯著預測員工電腦之誤用；Hovav and D'Arcy (2012)利用威攝理論探討美國與韓國組織員工對於資訊系統誤用之行為意圖影響，結果發現美國樣本所認知處罰嚴重性顯著預測資訊系統誤用之行為意圖；Chen *et al.* (2012)利用威攝理論分析組織員工對於資訊系統資訊安全政策遵循，結果發現組織所制訂違反規定之罰則嚴重性顯著預測員工遵循資訊系統資訊安全政策之行為意圖。

本計畫將處罰嚴重性定義為：醫院員工如破壞電子病歷隱私遭醫院發覺時，所接受處罰的嚴重程度(Herath & Rao, 2009b)。依據國內醫療法第 72 條規範，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，各類醫事人員包括：醫師法第 23 條、護理人員法第 28 條、藥師法第 14 條、醫事檢驗師法第 32 條、醫事放射師法第 32 條、物理治療師法第 31 條及職能治療師法第 31 條等亦均規範不得洩漏病人健康資訊(行政院法務部, 2014)，違反者均有相關之處罰條文，例如刑法第 316 條便規範醫師、藥師、助產士等醫療專業人員，無故洩漏因業務知悉或持有之他人秘密者，處一年以下有期徒刑、拘役或五萬元以下罰金，對於醫事人員而言，如因洩漏病人健康資訊因而遭受法律處罰，對於其工作專業而言將是一相當嚴重之處罰，鑒於洩漏病人電子病歷資訊均有相對嚴重之罰則，醫院員工在處理病人電子病歷資訊應當會更注意。依據上述文獻，本計畫提出以下假說：

H_1：處罰嚴重性與醫院員工遵循電子病歷隱私保護政策行為意圖呈正向顯著相關

2.處罰確定性與醫院員工遵循電子病歷隱私保護政策行為意圖之關連

依據威攝理論，如果犯罪行為的處罰相當確定，一旦犯罪行為發生，便須接受處罰，則民眾權衡得失後便可能不從事違法行為，因此違法行為可因為處罰的確定(Certainty)而避免(Gibbs, 1968)。以往有相當多研究利用處罰確定性來避免組織員工利用組織資訊資源或違反資訊安全政策。例如 Straub (1990)利用威攝理論的處罰嚴重程度預測組織員工對於電腦資源的濫用，結果發現組織確定性顯著預測員工電腦之誤用；Hovav and D'Arcy (2012)利用威攝理論探討美國與韓國組織員工對於資訊系統誤用之行為意圖影響，結果發現韓國樣本所認知處罰確定性顯著預測資訊系統誤用之行為意圖；Chen *et al.* (2012)利用威攝理論分析組織員工對於資訊系統資訊安全政策遵循，結果發現組織所制訂違反規定之罰則嚴重性顯著預測員工遵循資訊系統資訊安全政策之行為意圖。

本計畫將處罰確定性定義為：醫院員工如破壞電子病歷隱私遭醫院發覺時，接受處罰的機率(Siponen & Vance, 2010)。與上述論點相同，依據醫療法第 72 條規範，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，各類醫事人員包括：醫師法第 23 條、護理人員法第 28 條、藥師法第 14 條、醫事檢驗師法第 32 條、醫事放射師法第 32 條、

物理治療師法第 31 條及職能治療師法第 31 條等亦均規範不得洩漏病人健康資訊(行政院法務部, 2014)，違反者均有相關之處罰條文，例如刑法第 316 條便規範醫師、藥師、助產士等醫療專業人員，無故洩漏因業務知悉或持有之他人秘密者，處一年以下有期徒刑、拘役或五萬元以下罰金，對於醫事人員而言，如洩漏病人健康資訊勢必遭到相關法律之處罰，因此醫院員工在處理病人電子病歷資訊應當會更注意。依據上述文獻，本計畫提出以下假說：

H_2：處罰確定性與醫院員工遵循電子病歷隱私保護政策之行為意圖呈正向相關

3.偵測確定性與醫院員工遵循電子病歷隱私保護政策行為意圖之關連

Vroom and von Solms (2004)認為要確保員工能確實遵循組織所擬定資訊安全政策，仍需某種形式評估，以調查員工對於資訊安全的遵循程度，換言之，儘管威攝理論建議透過嚴重且確定的處罰來遏止不法行為，但仍須讓潛在違法者知道組織所採取避免違法行為之預防措施(Straub, 1990)，僅條列式資訊安全政策仍無法落實執行資訊安全政策(Peace *et al.*, 2003)，因此組織需有機制能偵測員工不法行為(Herath & Rao, 2009a; Straub & Nance, 1990)，Park *et al.* (2012)也指出單純的處罰可能不足以避免員工犯行，必須佐以偵測措施；Straub and Nance (1990)更建議組織必須加強不法事件的監測，因這些犯行者往往不易被發現。以往研究亦曾利用偵測確定性的概念探討資訊安全政策遵循或組織資源誤用等議題，例如 D'Arcy and Hovav (2009a)探討電腦監控對於資訊系統誤用之影響，結果發現電腦監控與資訊系統誤用行為意圖兩者間呈負向顯著相關；Kankanhalli *et al.* (2003)亦曾利用威攝理論分析資訊系統安全之效益，結果發現組織針對資訊安全如願意採取預防措施(例如偵測資訊安全遵循)，則資訊安全之效益也越高。

本計畫將偵測確定性定義為：醫院偵測到員工違反電子病歷隱私保護規範的機率程度(Herath & Rao, 2009b; Li *et al.*, 2010)。依據「醫療機構電子病歷製作及管理辦法」第 3 條規定，醫療機構採用電子病歷時，需符合許多規範，例如：訂有操作人員與系統建置、維護、稽核、管制之標準作業程序，並有執行紀錄可供查核、於醫療法第 70 條所定病歷保存期間內，電子病歷之存取、增刪、查閱、複製等事項，及其執行人員、時間及內容保有完整紀錄，可供查核、訂有保障電子病歷資料安全之機制等要求，主要目的均為確保電子病歷之安全，所採取之措施即包含預防以及監控概念，亦即透過偵測與監控方式保障電子病歷資料之安全。依據上述文獻，本計畫提出以下假說：

H_3：偵測確定性與醫院員工遵循電子病歷隱私保護政策之行為意圖呈正向相關

(二)非正式處罰(Informal sanction)相關變數與員工違反電子病歷隱私保護政策行為意圖關連

依據威攝理論，除法律正式處罰外，尚有與法律無關的非正式處罰也可能降低民眾從事非法行為意圖(Pratt *et al.*, 2006)，這兩類處罰均在於增加民眾對於犯罪行為後果的恐懼感(Pratt *et al.*, 2006)，因此本計畫首先採用保護動機理論(Rogers, 1983)，民眾對於外在威脅事件會產生恐懼感，因而採取自我保護行為；此外，違法行為所引發的羞恥心或社會規範等非正式處罰亦可能降低民眾犯行的行為意圖(Pratt *et al.*, 2006)。

1.認知嚴重性/認知脆弱性與醫院員工遵循電子病歷隱私保護政策行為意圖之關連

依據保護動機理論(Rogers, 1983)，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)會引發民眾的保護動機，亦即民眾對

於威脅的保護動機會促使民眾採取防衛措施，或避免採取某一行為(Guo *et al.*, 2011)。Workman *et al.* (2007)研究指出認知嚴重性與認知脆弱性可降低組織員工主觀或客觀上忽略資訊安全政策。以醫院電子病歷情境而言，認知脆弱性指醫院員工認為醫院的電子病歷隱私遭到破壞可能發生的機率，認知嚴重性則指醫院員工評估電子病歷隱私遭到破壞時之嚴重程度(Herath & Rao, 2009b)。依據保護動機理論，醫院員工的認知脆弱性與認知嚴重性越高，則破壞電子病歷隱私的動機也越低(保護動機)。以往亦有研究證實認知脆弱性與認知嚴重性兩個認知過程會影響民眾許多態度或行為意圖，包括：採用防抄襲系統(Lee, 2011)、備份個人資料(Crossler, 2010)、採用防止惡意軟體(Lee & Larsen, 2009)、遵守資訊安全規範(Herath & Rao, 2009b; Ifinedo, 2012; Siponen *et al.*, 2006; Siponen *et al.*, 2010)等。依據上述文獻，本計畫提出以下假說：

H_4：醫院員工的認知脆弱性與其遵循電子病歷隱私保護政策之行為意圖呈正向相關

H_5：醫院員工的認知嚴重性與其遵循電子病歷隱私保護政策之行為意圖呈正向相關

2.主觀規範/敘述性規範與醫院員工遵循電子病歷隱私保護政策行為意圖之關連

依據以往文獻(Fishbein & Ajzen, 1975; Herath & Rao, 2009b)，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 & Ajzen, 1975)，而描述性規範則指個人認為其他人亦應執行該行為的程度(Herath & Rao, 2009b)。Li *et al.* (2010)亦指出以往與員工遵循資訊安全政策之研究經常忽略個人規範之影響，顯示探討員工遵循組織政策應當將規範納入考量。在電子病歷情境下，主觀規範指醫院員工認為對於其重要的其他人認為他是否必須遵守醫院電子病歷使用政策的程度；而描述性規範則指醫院員工認為其他員工也都能遵守電子病歷使用政策的程度。Siponen and Vance (2010)的研究指出威攝理論所提出的正式處罰和非正式處罰對於降低員工違反資訊安全規範的行為意圖為具有顯著影響，原因在於因為中和效應(Neutralization)將罪惡感消彌，但規範類的因素反而可以降低員工不法行為。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；而 Guo and Yuan (2012)針對組織違反資訊安全處罰的研究結果亦顯示違反資訊安全規範所遭受的非正式處罰(個人或群體的規範)顯著降低員工違反資訊安全政策之行為。以往研究(Bulgurcu *et al.*, 2010; Guo *et al.*, 2011; Herath & Rao, 2009a; Herath & Rao, 2009b; Hu *et al.*, 2011; Li *et al.*, 2010; Siponen *et al.*, 2010)針對員工是否願意遵循資訊安全政策的研究亦證實工作群組規範(Workgroup norms)、敘述性規範(Descriptive norms)或規範信念(Normative beliefs)對於其遵循資訊安全政策有顯著正向影響。

H_6：醫院員工所認知的主觀規範與其遵循電子病歷隱私保護政策之行為意圖呈正向相關

H_7：醫院員工所認知敘述性規範與其遵循電子病歷隱私保護政策之行為意圖呈正向相關

(三)電子病歷隱私保護教育訓練對於保護動機理論和威攝理論相關變數之影響

依據保護動機理論(Roger, 1975; 1983)，認知脆弱性和認知嚴重性兩個變數會影響民眾採取保護行為外，不同資訊來源則可強化認知脆弱性和認知嚴重性，此種資訊來源包括外部環境(如口頭說服或觀察式學習)以及個人內部(Intrapersonal)(如人格特性或以往經驗)等，換言之，

外在訊息例如資訊安全教育可能激發民眾的認知脆弱和認知嚴重兩個變數。此外，依據威攝理論(Huston, 2001)，透過資訊安全教育可降低組織員工採行違法行為的意圖；而以往威攝理論相關研究(Peace *et al.*, 2003; Straub, 1990; Straub & Welke, 1998)亦建議組織如能事先偵測員工非法行為，將可更有效落實相對之處罰措施，例如組織可透過資訊安全教育、訓練與知曉方案等方式增加員工對於組織的資訊安全政策與資訊安全防護相關的知識與技能(D'Arcy *et al.*, 2009a; Lee *et al.*, 2004)；Straub and Nance (1990)亦建議組織可透過傳播關於誤用電腦的罰則、指引和政策以宣導合理的使用電腦。依據上述文獻，本計畫認為藉由電子病歷隱私保護教育訓練將可強化處罰嚴重程度、偵測確定性、認知脆弱、認知嚴重和主觀規範與敘述性規範，因此提出下列假說：

H_8：電子病歷隱私保護教育訓練與員工認知處罰嚴重性呈正向相關

H_9：電子病歷隱私保護教育訓練與員工認知處罰確定性呈正向相關

H_{10}：電子病歷隱私保護教育訓練與員工認知偵測確定性呈正向相關

H_{11}：電子病歷隱私保護教育訓練與員工認知嚴重性呈正向相關

H_{12}：電子病歷隱私保護教育訓練與員工認知脆弱性呈正向相關

H_{13}：電子病歷隱私保護教育訓練與員工主觀規範之認知呈正向相關

H_{14}：電子病歷隱私保護教育訓練與員工敘述性規範之認知呈正向相關

三、變數操作型定義與衡量問項

依據威攝理論相關文獻，本計畫研究架構所包含研究構面、研究變數、操作型定義及問項區分為正式處罰(Formal sanction)與非正式處罰(Informal sanction)兩部份說明，底下分別針對各個變數之操作型定義與部分問項進行說明。本計畫所發展初步問卷經由三位專家(2 位醫療實務界人士及 1 位醫療資訊管理專長學者)檢視，本計畫並依專家建議進行修訂；正式問卷發放前並針對 10 位樣本進行小規模前測，用以確認填答者可以瞭解問卷的語句與內容，本計畫完整問卷如附錄一所示。

(一)正式處罰(Formal sanction)相關變數

依據威攝理論(Gibbs, 1968)，處罰可區分為處罰嚴重性(Severity)、處罰確定性(Certainty)與立即性(Celerity, Swiftness)三個部份，其中立即性較少為文獻所探討，因此本計畫研究架構並未納入立即性變數。依據威攝理論，民眾避免非法行為主要原因之一在於處罰之嚴重性(Severity)與確定性(Certainty)；此外，即使組織訂有明確的資訊安全政策，仍需有配套措施確保資訊安全政策能被落實，因此本計畫參考以往文獻(Guo *et al.*, 2011; Herath & Rao, 2009a)，將偵測確定性(Detection certainty)納入研究架構，並分別說明其操作型定義與部分衡量問項。

1.處罰嚴重性(Punishment severity)

處罰嚴重性在威攝理論中指當民眾採取非法行為被發現時，所接受處罰的嚴重程度。在電子病歷情境下，本計畫將處罰嚴重性定義為：醫院員工如破壞電子病歷隱私遭醫院發覺時，所接受處罰的嚴重程度(Herath & Rao, 2009b)，衡量問項(共 3 題)以 Herath and Rao (2009b)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)醫院會懲罰違反電子病歷隱私保

護規範的員工；2)醫院會開除經常違反電子病歷隱私保護規範的員工；3)如果我被發現違反電子病歷隱私保護規範，我可能受到嚴厲懲罰等問項。

2.處罰確定性(Punishment certainty)

處罰確定性在威攝理論中指當民眾採取非法行為被發現時，將接受到處罰的機率。在電子病歷情境下，本計畫將處罰確定性定義為：醫院員工如破壞電子病歷隱私遭醫院發覺時，接受處罰的機率(Siponen & Vance, 2010)，衡量問項(共 3 題)以 Siponen and Vance (2010)和 Siponen *et al.* (2010)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)如果我不遵守電子病歷隱私保護規定，我可能會被處罰；2)如果我違反電子病歷隱私保護規定，我可能會遭到醫院正式的處罰；3)如果我違反電子病歷隱私保護規定，我可能會遭到醫院的訓誡等問項。

3.偵測確定性(Detection certainty)

偵測確定性在威攝理論中指管理單位為避免民眾採取非法行為所進行偵測活動。在電子病歷情境下，本計畫將偵測確定性定義為：醫院偵測到員工違反電子病歷隱私保護規範的機率程度，衡量問項(共 2 題)以 Herath and Rao (2009b)與 Li *et al.* (2010)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)醫院會監控員工是否合法使用電子病歷；2)如果我違反電子病歷隱私保護政策，有可能被醫院發現；3)如果我違反電子病歷隱私保護政策，被醫院發現的機率可能很高等問項。

(二)非正式處罰(Informal sanction)相關變數

除正式處罰外，威攝理論也認為非正式處罰對於民眾非法行為亦具有遏止作用(Gibbs, 1968)，所謂非正式的處罰包括民眾感受到執行非法行為可能帶來的威脅或風險(Hovav & D'Arcy, 2012; Li *et al.*, 2010)，屬於非法律性成本(Pratt *et al.*, 2006)，本計畫另以保護動機理論所提出的威脅概念(Rogers, 1975; 1983)：當民眾面臨威脅時，會根據現有資訊評估該威脅嚴重性(Perceived severity)並估算該威脅發生機率(Perceived vulnerability)；此外，社會或道德規範亦屬於一種非正式的處罰(Hovav & D'Arcy, 2012)，依據以往文獻(Fishbein & Ajzen, 1975; Herath & Rao, 2009a)，社會規範亦會影響民眾是否從是否一種行為，包含：主觀規範(Subjective norms)和敘述性規範(Descriptive norms)兩種規範。

1.認知脆弱性(Perceived vulnerability)

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醫院單位員工，因此在醫院電子病歷情境下，本計畫將認知脆弱性定義為醫院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隱私破壞事件(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；3) 我相信嘗試保護醫院的電子病歷資訊能減少其遭受非法的存取(例如查詢或列印病患的電子病歷)；4)如果連我都不能遵守醫院所擬定的電子病歷資訊隱私保護政策，醫院的電子病歷系統可能遭受損害等問項。

2.認知嚴重性(Perceived severity)

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程度高或低的程度。在醫院電子病歷情境下，本計畫將認知嚴重性定義為：醫院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 & Rao, 2009b)，衡量問項(共 3 題)以 Herath & Rao (2009b)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隱私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；3)我相信醫院的營收可能受到電子病歷隱私破壞的影響等問項。

(三)其他變數

1.主觀規範(Subjective norms)

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 & 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 (2009b)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)醫院高階主管希望員工能遵守電子病歷隱私保護政策；2)我的主管認為我應該遵守醫院電子病歷隱私保護政策；3)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；4)醫院的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等問項。

2.敘述性規範(Descriptive norms)

敘述性規範指民眾認為其他人亦執行該行為的程度(Herath & Rao, 2009b)。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的程度。衡量問項(共 3 題)以 Herath and Rao (2009b)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隱私保護政策；2)我相信醫院其他員工能遵守電子病歷隱私保護政策；3)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等問項。

3.電子病歷隱私保護教育訓練

在電子病歷情境下，本計畫將電子病歷隱私保護教育訓練定義為醫院透過電子病歷安全教育、訓練與知曉方案等方式增加員工對於醫院的電子病歷隱私政策與保護護相關的知識與技能的程度。衡量問項(共 5 題)以 D'Arcy *et al.* (2009a)的量表為基礎，並依據電子病歷情境進行修訂，包括例如：1)醫院會提供相關教育訓練以協助員工了解電子病歷隱私保護之相關議題；2)醫院會提供相關教育訓練以協助員工了解電子病歷隱私保護之相關法律(如人體實驗法、個人資料保護法等)；3)醫院會宣導未經授權而讀取或修改電子病歷的後果；4) 醫院會教育員工對於電子病歷隱私保護的責任；5)醫院會向員工說明未經授權存取電子病歷系統的後果等問項。

4.遵循電子病歷隱私保護規範行為意圖

在電子病歷情境下，本計畫將違反電子病歷隱私保護規範行為意圖定義為醫院員工忽略(Ignorance)或未注意(Negligence)醫院電子病歷隱私保護政策之行為意圖(Siponen & Vance,

2010)，亦即員工未能確實遵循電子病歷隱私保護政策所規範之可接受行為。本計畫主要針對未經授權電子病歷資料之行為，衡量問項(共 5 題)以 Venkatesh *et al.* (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)我傾向遵守醫院電子病歷隱私保護政策；2)我會試著在日常工作中遵循電子病歷隱私保護政策；3)我會持續遵循電子病歷隱私保護政策等問項。

四、研究樣本與抽樣

由於本計畫主要目的在於從威攝觀點探討醫院員工遵循電子病歷隱私保護政策之行為意圖，因此分析單位為個人；此外，調查之醫院也須採用電子病歷，目前國內已宣告實施電子病歷之醫院約有 372 家醫院(行政院衛生福利部, 2015)，包含醫學中心、區域醫院、地區醫院甚至診所，當中醫學中心由於在資源與制度方面均較區域醫院完整，在電子病歷隱私保護制度也較完善，而地區醫院與診所電子病歷之管理制度則較不若區域醫院完整，因此本計畫針對南部某一醫學中心具備電子病歷使用權限之員工進行深入之研究。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(編號：10301-003)。在調查時間方面，本計畫自 2014 年 4 月 1 日開始進行問卷之發放與調查，截至 5 月 31 日止，共計招募 289 位醫院員工參與，由於本計畫委由醫院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五個階段，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，接著進行統計假設的檢定，確保資料分布符合多變量分析要求;之後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 PASW® 18 版分析填答者基本資料與統計假設檢定，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 R 平台(R Core Team, 2013)之 plspm 套件(Sanchez, 2013)進行結構方程模式分析。

伍、結果與討論

一、研究結果

本計畫分三大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，以女性較多，所佔比例約為 58.8%，男性所占比例為 41.2%。

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 14.5%。在教育程度方面，以受過大學教育之比例最高，約為 74%，其次為研究所以上，約佔 20.8%，至於專科和高中/職所佔之比例均約為 5.1%。至於填答者身分別方面，最主要的填答者為醫師(約佔 34.6%)，其次為行政人員(約佔 30.86%)，護理人員約佔 11.1%，其他醫事人員則約為 23.5%；至於填答者在醫療產業的總工作年資以 1-5 年者佔大多數(約佔 30.1%)，其次為 16-20 年工作經驗(約佔 22.8%)，超過 21 年的填答者也約佔 10%，填答者詳細基本資料如 5-1 所示。

表 5-1 填答者基本資料

類別	次分類	數量	百分比(%)
性別	男	119	41.2
	女	170	58.8
年齡	20 歲~29 歲	42	14.5
	30 歲~39 歲	128	44.3
	40 歲~49 歲	96	33.2
	50 歲以上	23	8.0
教育程度	高中/職	1	0.3
	專科	14	4.8
	大學	214	74.0
	研究所以上	60	20.8
身份別	護理人員	32	11.1
	醫師	100	34.6
	行政人員	89	30.8
	其他醫事人員	68	23.5
管理階層	是	40	13.8
	否	249	86.1
醫療產業工作年資	1-5 年	87	30.1
	6-10 年	63	21.8
	11-15 年	44	15.2
	16-20 年	66	22.8
	>=21 年	29	10.0

至於填答者對於醫院電子病歷隱私保護政策方面(如表 5-2 所示)，表示「知道，也了解內容」者占大多數(約 54.7%)，表示「知道，但不了解內容」者為其次(約 43.9%)，至於表達「不知道者」最低，約佔 1.4%。

表 5-2 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	158	54.7
	知道，但不了解內容	127	43.9
	不知道	4	1.4

(二)統計假設檢定

為確認資料的分佈狀況，本計畫分別針對常態分配、共線性與離群值進行檢測。

1.常態分配

本計畫依據 Ho (2013, p. 57)建議，分別依據偏態(Skewness)計算其 Z 值，偏態 Z 值公式分別為：$Z_{偏態}$ = 偏態值/√標準誤，分析結果所有 $Z_{偏態}$均介於±1.96，顯示本計畫所蒐集資料符合常態分配(如表 5-3 所示)。

表 5-3 常態檢定

問項變數	個數	最小值	最大值	平均數	標準差	偏態		峰度		$Z_{偏態}$
						統計量	標準誤	統計量	標準誤	
PUS1	289	1	7	5.22	1.054	-0.561	0.143	1.446	0.286	-1.48
PUS2	289	1	7	4.95	1.267	-0.521	0.143	0.482	0.286	-1.37
PUS3	289	1	7	5.11	1.058	-0.612	0.143	1.613	0.286	-1.62
PC1	289	1	7	5.23	.974	-0.434	0.143	1.665	0.286	-1.15
PC2	289	1	7	5.13	1.077	-0.527	0.143	1.124	0.286	-1.39
PC3	289	1	7	5.29	.957	-0.427	0.143	2.184	0.286	-1.13
DC1	289	1	7	5.06	1.121	-0.250	0.143	0.324	0.286	-0.66
DC2	289	3	7	5.42	.829	0.374	0.143	0.139	0.286	0.99
DC3	289	1	7	5.28	.903	-0.192	0.143	1.690	0.286	-0.51
PV1	289	2	7	5.38	1.027	-0.362	0.143	0.705	0.286	-0.96
PV2	289	3	7	5.55	.896	0.158	0.143	-.401	0.286	0.42
PV3	289	2	7	5.58	.879	-0.085	0.143	0.598	0.286	-0.22
PV4	289	1	7	5.53	.932	-0.213	0.143	1.092	0.286	-0.56
PES1	289	1	7	5.15	1.134	-0.628	0.143	1.268	0.286	-1.66
PES2	289	2	7	5.38	.961	-0.291	0.143	1.066	0.286	-0.77
PES3	289	2	7	5.26	.950	-0.257	0.143	0.818	0.286	-0.68
SN1	289	3	7	5.72	.873	0.064	0.143	-.775	0.286	0.17
SN2	289	3	7	5.70	.887	0.089	0.143	-.810	0.286	0.23
SN3	289	3	7	5.57	.899	0.079	0.143	-.541	0.286	0.21
SN4	289	4	7	5.75	.867	0.127	0.143	-1.032	0.286	0.34

表 5-3 常態檢定(續)

問項變數	個數	最小值	最大值	平均數	標準差	偏態		峰度		$Z_{偏態}$
						統計量	標準誤	統計量	標準誤	
DN1	289	3	7	5.42	0.929	-0.102	0.143	-.098	0.286	-0.27
DN2	289	2	7	5.36	0.954	-0.211	0.143	0.206	0.286	-0.56
DN3	289	3	7	5.51	0.882	0.035	0.143	-0.144	0.286	0.09
TR1	289	4	7	5.60	0.864	0.368	0.143	-0.838	0.286	0.97
TR2	289	3	7	5.63	0.872	0.269	0.143	-0.736	0.286	0.71
TR3	289	4	7	5.58	0.866	0.419	0.143	-0.821	0.286	1.11
TR4	289	4	7	5.65	0.845	0.398	0.143	-0.940	0.286	1.05
TR5	289	3	7	5.55	0.856	0.411	0.143	-0.562	0.286	1.09
IVPP1	289	4	7	5.89	0.887	-0.050	0.143	-1.215	0.286	-0.13
IVPP2	289	4	7	5.90	0.876	-0.044	0.143	-1.211	0.286	-0.12
IVPP3	289	4	7	5.90	0.880	-0.040	0.143	-1.231	0.286	-0.11

2.共線性診斷

在共線性檢測方面，本計畫參考 Ho (2013)建議，依據允差值進行判斷，如允差值小於 0.1，則自變數便可能有共線性問題，為避免影響分析結果，須予以移除，本計畫資料分析結果顯示 SN2 值小於 0.1，因此後續分析便將 SN2 予以移除，共線性檢測結果如表 5-4。

表 5-4 共線性檢測

構面	測量變數	允差
處罰嚴重性(PUS)	PUS1	0.333
	PUS2	0.368
	PUS3	0.234
處罰確定性(PC)	PC1	0.147
	PC2	0.192
	PC3	0.207
偵測確定性(DC)	DC1	0.399
	DC2	0.256
	DC3	0.439
認知脆弱性(PV)	PV1	0.345
	PV2	0.277
	PV3	0.357
	PV4	0.290
認知嚴重性(PES)	PES1	0.395
	PES2	0.293
	PES3	0.432

表 5-4 共線性檢測(續)

構面	測量變數	允差
主觀規範(SN)	SN1	0.139
	SN2	0.098
	SN3	0.154
	SN4	0.181
敘述性規範(DN)	DN1	0.185
	DN2	0.169
	DN3	0.211
電子病歷隱私保護教育訓練(TR)	TR1	0.170
	TR2	0.128
	TR3	0.217
	TR4	0.156
	TR5	0.225

3.離群值

本計畫依據 Shiffler (1988)建議，將各問項值予以標準化後，並判斷其絕對值是否大於 4，如大於 4 族可能為離群值，分析結果顯示各問項大部分標準值之絕對值均小於 4，因此本計畫所蒐集資料應無重大離群值問題。

(三)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.7，CFA 分析結果顯示各構面問項最低之交叉負荷量為 0.84 (PES1 問項，屬認知嚴重性)，已符合.7 的建議值(如表 5-5 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 & Larcker, 1981; Wertz *et al.*, 1974) 與 Cronbach's α (Hair *et al.*, 2010)；以往研究(Fornell & 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.7 (Fornell & Larcker, 1981)，本研究 9 個構面中，最低的 CR 值為 0.81(偵測確定性與認知嚴重性)，亦具備足夠的信度；而 Cronbach's α 可接受的值為.7 (Hair *et al.*, 2010)，如果值超過.9 表示信度非常優秀(Excellent)，超過.8 則表非常好(Very good) (Kline, 2005)。在 Cronbach's α 方面，本研究 9 個構面中，最低的 Cronbach's α 值為.85(認知嚴

重性)，顯示具備足夠的信度(如表 5-5 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 5-5 驗證性因素分析結果

構面	問項	平均數	標準差	負荷量	CR[a]	Cronbach's α	AVE[b]
偵測確定性	DC1	5.04	1.15	.86			
	DC2	5.40	0.87	.93	.91	.86	.78
	DC3	5.27	0.94	.86			
敘述性規範	DN1	5.41	0.96	.94			
	DN2	5.34	0.99	.96	.96	.94	.89
	DN3	5.49	0.92	.94			
遵循電子病歷隱私保護規範行為意圖	ICPP1	5.87	0.93	.98			
	ICPP2	5.88	0.92	.99	.99	.99	.97
	ICPP3	5.88	0.92	.99			
處罰確定性	PC1	5.22	1.01	.95			
	PC2	5.11	1.10	.94	.96	.94	.89
	PC3	5.28	0.99	.94			
認知嚴重性	PES1	5.14	1.16	.84			
	PES2	5.37	0.99	.92	.91	.85	.76
	PES3	5.25	0.98	.87			
處罰嚴重性	PUS1	5.21	1.08	.91			
	PUS2	4.93	1.29	.86	.92	.87	.80
	PUS3	5.10	1.09	.90			

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

表 5-5 驗證性因素分析結果(續)

構面	問項	平均數	標準差	負荷量	CR[a]	Cronbach's α	AVE[b]
認知脆弱性	PV1	5.36	1.06	.86	.93	.90	.77
	PV2	5.54	0.94	.90			
	PV3	5.56	0.92	.85			
	PV4	5.52	0.97	.89			
主觀規範	SN1	5.71	0.91	.95	.96	.94	.90
	SN3	5.56	0.94	.94			
	SN4	5.73	0.91	.95			
電子病歷隱私保護教育訓練	TR1	5.58	0.90	.91	.97	.96	.85
	TR2	5.61	0.91	.94			
	TR3	5.56	0.91	.92			
	TR4	5.63	0.89	.93			
	TR5	5.64	0.90	.91			

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

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.5 且顯著(Bagozzi *et al.*, 1991, p. 434; Bagozzi & Yi, 1988, p. 82)；2)CR 值大於.6 (Bagozzi & Yi, 1988, p. 82)；及 3)平均變異萃取量(Average variance extracted, AVE)大於.5 (Bagozzi & Yi, 1988, p. 82; Fornell & Larcker, 1981)。本研究 9 個構面之衡量問項之標準化因素負荷量最低為.84(認知嚴重性 PES1)；其次，本研究構面中最低之 CR 為.91(偵測確定性與認知嚴重性)，高於.6 之建議值(如表 5-5 所示)；第三，本研究構面最低之 AVE 為.76(認知嚴重性構面)，亦高於.5 的建議水準(如表 5-5 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 5-6 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 5-7 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 5-6 構面間相關係數表

變數	A	B	C	D	E	F	G	H	I
偵測確定性(A)	**.88**								
敘述性規範(B)	.55	**.95**							
遵循電子病歷隱私保護規範行為意圖(C)	.60	.63	**.99**						
處罰確定性(D)	.71	.47	.52	**.95**					
認知嚴重性(E)	.55	.44	.45	.55	**.87**				
處罰嚴重性(F)	.65	.45	.50	.84	.52	**.89**			
認知脆弱性(G)	.72	.64	.64	.64	.68	.60	**.88**		
主觀規範(H)	.69	.74	.75	.64	.55	.58	.76	**.95**	
電子病歷隱私保護教育訓練(I)	.63	.66	.74	.58	.51	.50	.67	.77	**.92**

註 1：對角線為 AVE 平方根值

表 5-7 交叉負荷量(Cross Loadings)

	偵測確定性 (DC)	敘述性規範 (DN)	遵循電子病歷隱私保護規範行為意圖(ICPP)	處罰確定性 (PC)	處罰嚴重性 (PES)	認知嚴重性 (PUS)	認知脆弱性 (PV)	主觀規範 (SN)	電子病歷隱私保護教育訓練(TR)
DC1	**.86**	.43	.47	.64	.44	.60	.60	.58	.55
DC2	**.93**	.53	.60	.68	.57	.62	.70	.68	.60
DC3	**.86**	.49	.50	.55	.44	.48	.59	.56	.52
DN1	.55	**.94**	.57	.45	.42	.44	.61	.72	.61
DN2	.47	**.96**	.53	.39	.38	.38	.56	.64	.57
DN3	.53	**.94**	.65	.48	.45	.45	.63	.74	.68
IVPP1	.60	.61	**.98**	.52	.44	.50	.62	.74	.74
IVPP2	.59	.63	**.99**	.51	.44	.48	.63	.74	.73
IVPP3	.58	.61	**.99**	.50	.44	.48	.63	.73	.72
PC1	.68	.46	.52	**.95**	.54	.82	.63	.64	.57
PC2	.64	.42	.45	**.94**	.48	.82	.57	.57	.49
PC3	.68	.45	.50	**.94**	.52	.75	.62	.60	.57
PES1	.36	.26	.23	.36	**.84**	.35	.46	.30	.30
PES2	.50	.41	.41	.49	**.92**	.48	.62	.51	.46
PES3	.56	.46	.48	.55	**.87**	.50	.66	.58	.54
PUS1	.59	.42	.43	.72	.45	**.91**	.54	.53	.45
PUS2	.53	.37	.42	.69	.41	**.86**	.48	.46	.38
PUS3	.60	.41	.47	.82	.53	**.90**	.59	.56	.49

表 5-7 交叉負荷量(Cross Loadings)(續)

	偵測確定性 (DC)	敘述性規範 (DN)	遵循電子病歷隱私保護規範行為意圖(ICPP)	處罰確定性 (PC)	處罰嚴重性 (PES)	認知嚴重性 (PUS)	認知脆弱性 (PV)	主觀規範 (SN)	電子病歷隱私保護教育訓練(TR)
PV1	.68	.46	.50	.58	.57	.53	**.86**	.60	.53
PV2	.65	.53	.55	.61	.61	.57	**.90**	.71	.60
PV3	.62	.64	.62	.57	.57	.52	**.85**	.73	.65
PV4	.58	.61	.55	.48	.63	.49	**.89**	.63	.55
SN1	.66	.67	.70	.64	.54	.58	.72	**.95**	.73
SN3	.64	.74	.69	.58	.49	.55	.71	**.94**	.72
SN4	.66	.69	.73	.58	.52	.52	.74	**.95**	.73
TR1	.59	.60	.69	.54	.44	.47	.62	.72	**.91**
TR2	.61	.58	.71	.54	.46	.51	.62	.72	**.94**
TR3	.58	.61	.68	.54	.49	.45	.61	.70	**.92**
TR4	.61	.63	.71	.56	.50	.48	.62	.74	**.93**
TR5	.53	.61	.62	.47	.46	.39	.62	.65	**.91**

(四)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(處罰嚴重性、處罰確定性、偵測確定性、認知脆弱性、認知嚴重性、主觀規範、敘述性規範、遵循電子病歷隱私保護規範行為意圖)之平均共同性為.84 ((.795 + .895 + .782 + .770 + .763 + .892 + .887 + .973) / 8)，而平均 R^2 為.41 ((.251 + .340 + .400 + .435 + .263 + .584 + .431 + .568) / 8)，因此 GoF 為$\sqrt{}$(.84 * .41) = .59，依據(Wetzels *et al.*, 2009, p. 187)建議：GoF 值為.02 屬於低度適配，.13 屬於中等適配度，.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，電子病歷隱私保護教育訓練對於處罰嚴重性、處罰確定性、偵測確定性、認知脆弱性、認知嚴重性、主觀規範、敘述性規範的解釋變異分別為 24.8%、33.5%、40.0%、45.0%、26.8%、58.9%、43.5%；而處罰嚴重性、處罰確定性、偵測確定性、認知脆弱性、認知嚴重性、主觀規範、敘述性規範共同解釋遵循電子病歷隱私保護規範行為意圖約 58.6%變異。Chin (1998, p.323)認為 R^2 等於.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中等以上解釋能力。

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，結果顯示電子病歷隱私保護教育訓練對於處罰嚴重性具有正向顯著影響(假說 H_1 成立, β = .50, p < .001)；電子病歷隱私保護教育訓練對於處罰確定性具正向顯著影響(假說 H_2 成立, β = .60, p < .001)；電子病歷隱私保護教育訓練對於偵測確定性具有正向顯著影響(假說 H_3 成立, β = .63, p < .001)；電子病歷隱私保護教育訓練對於認知脆弱性具有正向顯著影響(假說 H_4 成立, β = .45, p < .001)；電子病歷隱私保護教育訓練對於認知嚴重性則具有正向顯著影響(假說 H_5 成立, β = .27, p < .001)，電子病歷隱私保護教育訓練對於主觀規範則具有正向顯著影響(假說 H_6 成立, β = .77, p < .001)，電子病歷隱私保護教育訓練對於敘述性規範則具有正向顯著影響(假說 H_7 成立, β = .66, p < .001)，處罰嚴重性對於遵循電子病歷隱私保護規範行為意圖則不具有顯著影響(假說 H_8 不成立)；處罰確定性對於遵循電子病歷隱私保護規範行為意圖則不具有顯著影響(假說 H_9 不成立)；偵測確定性對於遵循電子病歷隱私保護規範行為意圖具正向顯著影響(假

說 H_{10} 成立, β = .11, p < .1)；認知脆弱性對於遵循電子病歷隱私保護規範行為意圖則不具有顯著影響(假說 H_{11} 不成立)；主觀規範對於遵循電子病歷隱私保護規範行為意圖具正向顯著影響(假說 H_{12} 成立, β = .51, p < .001)；敘述性規範對於遵循電子病歷隱私保護規範行為意圖具正向顯著影響(假說 H_{13} 成立, β = .13, p < .1)，結構模式分析結果如圖 5-1 所示，假說檢定結果如表 5-8 所示。

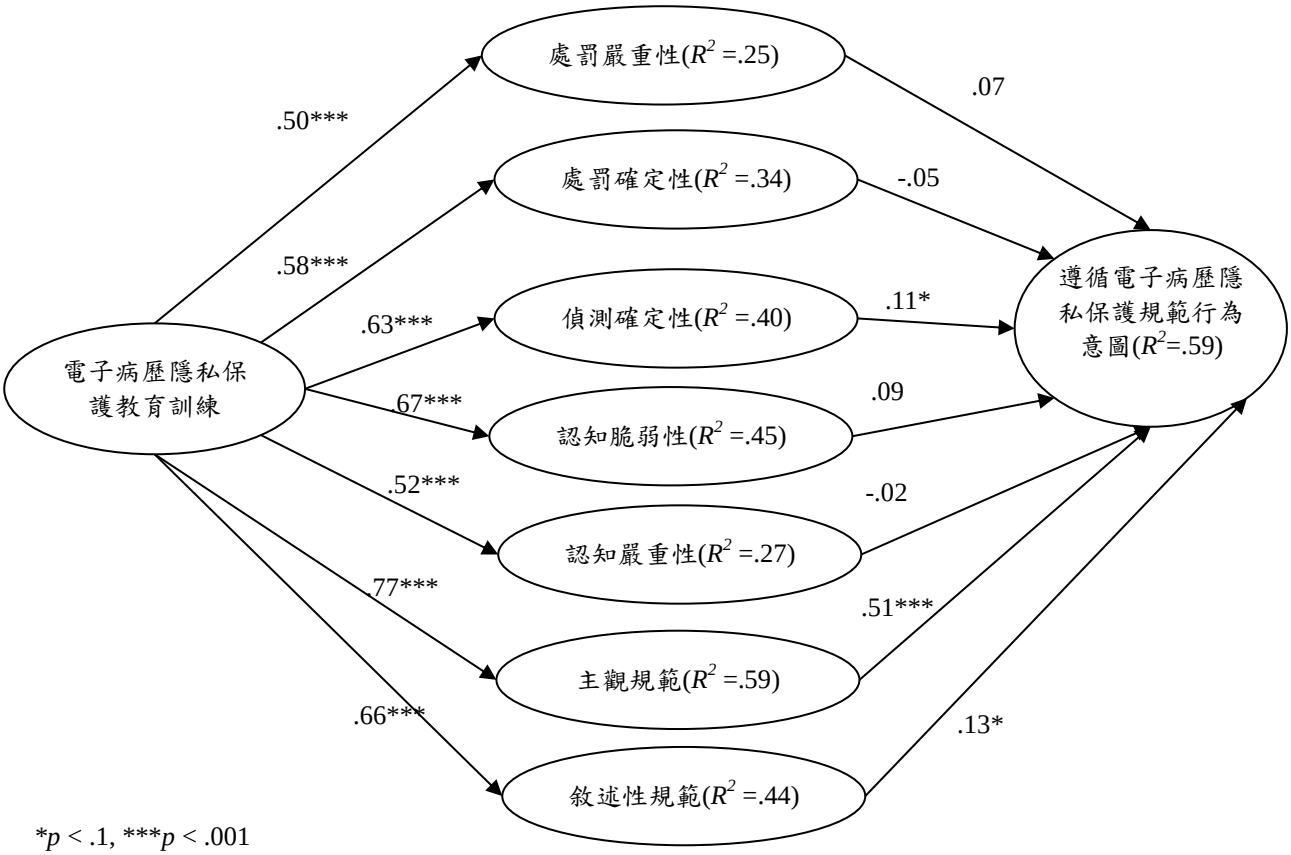

圖 5-1 結構模式結果

表 5-8 假說檢定結果

假說	內容	t 值	成立否？
H_1	處罰嚴重性→遵循電子病歷隱私保護規範行為意圖	0.90	否
H_2	處罰確定性→遵循電子病歷隱私保護規範行為意圖	0.54	否
H_3	偵測確定性→遵循電子病歷隱私保護規範行為意圖	1.75*	是
H_4	認知脆弱性→遵循電子病歷隱私保護規範行為意圖	1.10	否
H_5	認知嚴重性→遵循電子病歷隱私保護規範行為意圖	0.38	否
H_6	主觀規範→遵循電子病歷隱私保護規範行為意圖	6.67***	是
H_7	敘述性規範→遵循電子病歷隱私保護規範行為意圖	1.78*	是
H_8	電子病歷隱私保護教育訓練→處罰嚴重性	7.61***	是
H_9	電子病歷隱私保護教育訓練→處罰確定性	10.59***	是
H_{10}	電子病歷隱私保護教育訓練→偵測確定性	12.47***	是
H_{11}	電子病歷隱私保護教育訓練→認知脆弱性	12.50***	是
H_{12}	電子病歷隱私保護教育訓練→認知嚴重性	8.10***	是
H_{13}	電子病歷隱私保護教育訓練→主觀規範	20.45***	是
H_{14}	電子病歷隱私保護教育訓練→敘述性規範	13.46***	是

*$p < .1$, ***$p < .001$

二、研究結果討論

(一)處罰嚴重性對於遵循電子病歷隱私保護規範行為意圖之影響

本計畫假說 H_1 為「處罰嚴重性與醫院員工遵循電子病歷隱私保護政策行為意圖呈正向顯著相關」，依據結構方程模式分析結果($\beta = .07, t = .90$)，顯示假說 H_1 不成立。「處罰嚴重性」對於「遵循電子病歷隱私保護規範行為意圖」並未具顯著影響；換言之，即使有明文法律規定處罰方式以及清楚規範處罰之嚴重度，當醫院員工違反電子病歷隱私保護政策時，對於醫院員工是否願意遵循電子病歷並未具顯著影響，本計畫於醫療產業進行實證，結果與威攝理論之論點並未相符，然以往文獻亦有採用威攝理論之研究結果與本計畫相同，例如：Hovav and D'Arcy (2012)利用威攝理論探討美國與韓國組織員工對於資訊系統誤用之行為意圖影響，結果發現韓國樣本所認知處罰嚴重性未能顯著預測資訊系統誤用之行為意圖。

就電子病歷情境而言，有相當多醫療法規規範違反電子病歷隱私機密之罰則，對於醫院甚至其員工而言，不僅僅是金錢上的處罰，甚至可能聲譽上受損，更嚴重者或許需入監服刑，因此罰則不可謂不重，然本研究之結果並未與威攝理論相符，可能原因如下：首先，由於醫療法規對於目前國內並未發生電子病歷外洩而造成重大損失的案例，因此填答者可能認為此類事件不太可能發生；其次，以往紙本病歷時代雖發生過病歷外洩的狀況，然而違反規定之當事人或醫院亦未受到嚴重的處罰，因而造成本計畫「處罰嚴重性」對於「遵循電子病歷隱私保護規範行為意圖」並未具顯著影響之結果。儘管處罰嚴重性之影響並不顯著，本計畫仍建議醫院能加強宣導法律所規範的罰則，讓醫院員工能確實瞭解處罰的嚴重性，藉以避免醫院員工以身試法，違反電子病歷隱私保護規定。

(二) 處罰確定性對於遵循電子病歷隱私保護規範行為意圖之影響

本計畫假說 H_2 為「處罰確定性與醫院員工遵循電子病歷隱私保護政策之行為意圖呈正向相關」，依據結構方程模式分析結果(β = -.05, t = .54)，顯示假說 H_2 不成立。「處罰確定性」對於「醫院員工遵循電子病歷隱私保護政策之行為意圖」未具顯著影響；換言之，即使違反電子病歷隱私保護政策時，有明文法律規定處罰方式，對於醫院員工是否願意遵循電子病歷並未具顯著影響，此結果雖與威攝理論之論點以及其他研究不相符(如 Chen *et al.*, 2012; Hovav & D'Arcy, 2012)，然文獻上亦有採用威攝理論之研究結果與本計畫相同，例如：Hovav and D'Arcy (2012)利用威攝理論探討美國與韓國組織員工對於資訊系統誤用之行為意圖影響，結果發現美國樣本所認知處罰確定性未能顯著預測資訊系統誤用之行為意圖。

就電子病歷的情境而言，目前國內有相當多的法律均規範對於電子病歷的保護以及罰則，例如醫療法、醫師法、護理人員法及各類醫事人員法，甚至刑法亦有所規範，因此如果違反電子病歷隱私規範，勢必遭受處罰，然而本計畫研究結果「處罰確定性」對於「醫院員工遵循電子病歷隱私保護政策之行為意圖」未具顯著影響，與威攝理論之觀點並不相符，本計畫推論可能之原因如下：首先，由於病歷隱私從紙本病歷時代便已開始規範，醫院員工均已適應在日常作業中遵循電子病歷隱私的保護規範，即使紙本病歷轉變為電子病歷，保護電子病歷隱私的程序與做法亦大致相近，亦即平時處理病歷時便能遵循相關規定，因此便可能造成「處罰確定性」不顯著影響；其次，與前述「處罰嚴重性」不顯著原因相似，即國內目前未見到代表性的案例，亦可能造成填答者認為「處罰確定性」不顯著。儘管「處罰嚴重性」因素未能顯著影響「醫院員工遵循電子病歷隱私保護政策之行為意圖」，本計畫仍建議醫院能同樣強化宣導電子病歷隱私保護相關規範之罰則，並讓醫院員工能確實了解這些罰則，進而讓醫院員工願意遵循相關規定。

(三) 偵測確定性對於遵循電子病歷隱私保護規範行為意圖之影響

本計畫假說 H_3 為「偵測確定性與醫院員工遵循電子病歷隱私保護政策之行為意圖呈正向相關」，依據結構方程模式分析結果(β = .11, p < .1)，顯示假說 H_4 成立。「偵測確定性」對於「醫院員工遵循電子病歷隱私保護政策之行為意圖」具正向顯著影響；換言之，醫院員工如感受到醫院隨時監測其電子病歷的使用，依據威攝理論，醫院員工便越可能遵循電子病歷隱私保護政策；反之，如果醫院員工認為醫院並未監測其電子病歷的使用狀況，則醫院員工便可能不會落實遵循電子病歷隱私保護政策。本計畫於醫療情境進行，「偵測確定性」對於「醫院員工遵循電子病歷隱私保護政策之行為意圖」影響之研究結果與以往在其他領域(Chen et al., 2012)之研究結果相同。

就目前國內電子病歷應用而言，有許多法律規範各醫院在實施電子病歷時必須確保電子病歷的安全，亦即各醫院須採取不同措施或方法以符合政府機關的要求，例如「醫療機構電子病歷製作及管理辦法」便要求所有電子病歷的使用必須有紀錄可供後續稽核，亦即醫院必須監控電子病歷使用紀錄，本計畫研究結果顯示「偵測確定性」正向顯著影響「醫院員工遵循電子病歷隱私保護政策之行為意圖」，亦即透過監測醫院員工使電子病歷之狀況，醫院員工便越可能遵循電子病歷隱私保護政策，依據本計畫研究結果，建議醫院應當更落實電子病歷監控機制，並須讓醫院員工知道此監控機制，則醫院員工便越能保護電子病歷的隱私。

(四)認知脆弱性對於遵循電子病歷隱私保護規範行為意圖之影響

本計畫假說 H_4 為「醫院員工的認知脆弱性與其遵循電子病歷隱私保護政策之行為意圖呈正向相關」，依據結構方程模式分析結果(β = .09, t = 1.10)，顯示假說 H_5 不成立。「認知脆弱性」對於「遵循電子病歷隱私保護政策之行為意圖」未具顯著影響；換言之，即使醫院員工如果能感受到發生電子病歷外洩事件之機率相當高，對於他們是否願意遵循電子病歷隱私保護政策並未有顯著影響，此結果與保護動機理論之原始觀點或採用保護動機理論相關研究之結果並未相符(如 Ifinedo, 2012; Vance *et al.*, 2012; Youn, 2009)，本研究於醫療情境進行，認知脆弱性未顯著之結果仍與其他文獻(Herath & Rao, 2009b; Vance *et al.*, 2012; Zhang *et al.*, 2009)之研究結果相符。

依據保護動機理論，醫院員工如感受到電子病歷遭受破壞的機率相當大，則醫院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，如果醫院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。然本計畫研究之結果顯示，「認知脆弱性」並無法影響「遵循電子病歷隱私保護政策之行為意圖」，與保護動機理論之觀點並不相同。儘管「認知脆弱性」不顯著，本計畫仍建議醫院應當定時宣導電子病歷的脆弱性，亦即電腦化資料雖方便，但也更容易遭受竊取或破壞，因此須確保醫院員工真的能深切體認電子病歷遭破壞的可能性，進而激發其採取保護電子病歷隱私之認知。

(五)認知嚴重性對於遵循電子病歷隱私保護規範行為意圖之影響

本計畫假說 H_5 為「醫院員工的認知嚴重性與其遵循電子病歷隱私保護政策之行為意圖呈正向相關」，依據結構方程模式分析結果(β = -.02, t = 0.38)，顯示假說 H_6 不成立。亦即「認知嚴重性」對於「遵循電子病歷隱私保護政策之行為意圖」不具影響力；換言之，即使醫院員工認知到電子病歷外洩事件的嚴重性，不論對病人、醫院甚至員工都有不同層面的不良影響，都無法影響醫院員工是否遵循電子病歷保護政策。此結果與原始保護動機理論之觀點以及採用保護動機理論相關研究之結果並不相符(如 Herath & Rao, 2009; Ifinedo, 2012; Vance *et al.*, 2012)，本研究於醫療產業進行，認知嚴重性未顯著之結果仍與其他文獻(Zhang *et al.*, 2009)之研究結果相符。

就電子病歷的使用而言，政府主管機關、醫療實務界與學術界均了解電子病歷所能帶來的效益，然而電子病歷就像兩面刃，也會有其缺點，例如由於病歷均數位化，雖使得電子病歷的搜尋與存取更迅速且方便，然卻也可能容易造成電子病歷外洩的狀況，而電子病歷外洩可能造成的嚴重影響亦可分為不同層面說明。首先，對於病人而言，如果所洩漏之病歷內容非常隱密，則可能造成病人自尊心受損，亦可能造成財物之損失(例如保險因素)；其次，對於醫院而言，由於醫院未善盡保存病人之電子病歷，便可能違反醫療法之規範，醫院除了可能引發法律爭議外，對於醫院的聲譽亦有不良的影響；最後，對於洩漏電子病歷的員工而言，亦違反如醫師法、護理人員法及其他醫事人員等相關法律，可見電子病歷外洩的影響與後果可能相當嚴重。雖然本計畫結果顯示「認知嚴重性」並不顯著，仍建議醫院須宣導電子病歷遭破壞的影響嚴重程度，當醫院員工了解電子病歷隱私如遭受破壞，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。

(六) 主觀規範與敘述性規範對於遵循電子病歷隱私保護規範行為意圖之影響

本計畫假說 H_6 為「醫院員工所認知的主觀規範與其遵循電子病歷隱私保護政策之行為意圖呈正向相關」，依據結構方程模式分析結果($\beta = .51, p < .001$)，顯示假說 H_6 成立。「主觀規範」對於「遵循電子病歷隱私保護政策之行為意圖」具正向顯著影響；換言之，醫院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，依據理性行為理論觀點，醫院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，如果對於醫院員工重要的人並不認為其須遵循電子病歷隱私保護政策，則醫院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 & Rao, 2009b; Ifinedo, 2012; Siponen *et al.*, 2010)之研究結果相同。

本計畫假說 H_7 為「醫院員工所認知敘述性規範與其遵循電子病歷隱私保護政策之行為意圖呈正向相關」，依據結構方程模式分析結果($\beta = .13, p < .1$)，顯示假說 H_8 成立。「敘述性規範」對於「行為意圖」具正向顯著影響；換言之，如醫院其他員工能遵循電子病歷隱私保護政策，對於醫院員工是否遵循電子病歷隱私保護政策具有顯著正向影響；反之，如其他員工未能遵循電子病歷隱私保護政策，則醫院員工亦可能傾向不遵循電子病歷隱私保護政策。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 & Rao, 2009b; Ifinedo, 2012; Siponen *et al.*, 2010)之研究結果相同。

依據本計畫研究結果：醫院員工所認知「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，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」亦具具顯著影響；換言之，當對於醫院員工重要的其他人，包括：主管與病歷管理單位其他同事，如果對於醫院員工能確實保護電子病歷隱私有所期望，則醫院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，以鼓勵醫院員工能確實遵循電子病歷隱私保護政策；此外，針對「敘述性規範」，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。

(七) 電子病歷隱私保護教育訓練對於正式處罰與非正式處罰之影響

本計畫假說 H_8 為「電子病歷隱私保護教育訓練與員工認知處罰嚴重性呈正向相關」，依據結構方程模式分析結果($\beta = .50, p < .001$)，顯示假說 H_8 成立。本計畫假說 H_9 為「電子病歷隱私保護教育訓練與員工認知處罰確定性呈正向相關」，依據結構方程模式分析結果($\beta = .58, p < .001$)，顯示假說 H_9 成立。本計畫假說 H_{10} 為「電子病歷隱私保護教育訓練與員工認知偵測確定性呈正向相關」，依據結構方程模式分析結果($\beta = .63, p < .001$)，顯示假說 H_{10} 成立。本計畫假說 H_{11} 為「電子病歷隱私保護教育訓練與員工認知嚴重性呈正向相關」，依據結構方程模式分析結果($\beta = .67, p < .001$)，顯示假說 H_{11} 成立。本計畫假說 H_{12} 為「電子病歷隱私保護教育訓練與員工認知脆弱性呈正向相關」，依據結構方程模式分析結果($\beta = .52, p < .001$)，顯示假說 H_{12} 成立。本計畫假說 H_{13} 為「電子病歷隱私保護教育訓練與員工主觀規範之認知呈正向相關」，依據結構方程模式分析結果($\beta = .77, p < .001$)，顯示假說 H_{13} 成立。本計畫假說 H_{14} 為

「電子病歷隱私保護教育訓練與員工敘述性規範之認知呈正向相關」，依據結構方程模式分析結果($\beta = .66, p < .001$)，顯示假說 H_{14} 成立。

依據本計畫研究結果，建議醫院能持續推動電子病歷隱私保護教育訓練，課程內容須包含電子病歷隱私保護規範、罰則，及電子病歷可能的風險與帶來的影響，另外，也必須充分運用醫院員工對於彼此的影響，彼此互相砥礪，確實遵循電子病歷隱私保護規範的要求，於日常病人照護過程，或是處理電子病歷的過程中，均能注意相關細節，以避免電子病歷資料外洩。

陸、研究貢獻

電子病歷已是未來重要發展趨勢，國內衛生福利部自民國 89 年起便開始推動病歷電子化相關作業，分別從法規面、標準面、安全面及推廣面四大構面著手，除了確定電子病歷執行依據外，亦建立電子病歷單張、交換及應用之標準，對於電子病歷資安機制與人員教育訓練亦納入考量，最後並建立電子病歷交換機制與導入院所運作模式，顯示衛生福利部對於電子病歷的運作機制已建立一套模式。截至 2014 年，目前已有 372 家醫院宣告實施電子病歷，其中 342 家醫院提供電子病歷交換服務(行政院衛生福利部，2015)，顯示國內醫院對於電子病歷採用狀況正逐步提高，由於醫療工作特性影響，醫院員工必須透過電子病歷進行臨床照護，因此，如何有效確保醫院員工能確實遵循電子病歷隱私保護政策，將是各醫院在推動電子病歷時必須面對的主要議題之一，本計畫特別從處罰的角度來探討此議題，主要的貢獻分別說明如下：

一、學術貢獻

資訊安全議題為目前組織非常重視的議題之一，組織為確保其資訊安全，往往制定有資訊安全政策，因此有相當多的文獻針對資訊安全政策的遵循進行探討(例如 Hovav & D'Arcy, 2012; Herath & Rao, 2009a, Herath & Rao, 2009b; Hu *et al.*, 2011; Li *et al.*, 2010)，這些研究對於威攝理論已累積相當多的結果，也讓學術界對於威攝理論的應用更為了解，然而這些研究的結果卻不太一致，甚至同一研究採不同樣本亦不不相同(例如 Hovav & D'Arcy, 2012)；此外，以往研究主要的研究對象為一般企業，針對醫療產業的研究較不常見，因此本計畫特別針對目前國內電子病歷情境進行深入的探討，藉由本計畫的執行，對於學術界而言，除了可進一步累積威攝理論的知識外，亦可增加對於員工遵循組織政策議題的瞭解，尤其本計畫特別針對醫療產業進行探討，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，而醫院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. (2014). 全國法規資料庫. 台北市: 行政院法務部. Retrieved from http://law.moj.gov.tw.

行政院衛生福利部. (2004). *確立及推廣醫療資訊安全與隱私保護政策*. 台北市: 行政院衛生福利部. Retrieved from http://www.doh.gov.tw/.

行政院衛生福利部. (2009). 醫療機構電子病歷製作及管理辦法, 台北市: 行政院衛生福利部. Retrieved from http://law.moj.gov.tw/.

行政院衛生福利部. (2015). 行政院衛生署電子病歷金榜. Retrieved from http://emr.mohw.gov.tw/emrlist.aspx.

楊漢湶. (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. *資安人科技網* Retrieved from http://www.informationsecurity.com.tw.

Angst, C.M., Agarwal, R., Sambamurthy, V., & Kelley, K. (2010). Social contagion and information technology diffusion: The adoption of electronic medical records in U.S. hospitals. *Management Science, 56*(8), 1219-1241.

Appari, A., & Johnson, M.E. (2010). Information security and privacy in healthcare: Ccurrent state of research. *International Journal of Internet and Enterprise Management, 6*(4), 279-314.

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.

Bates, D.W., Ebell, M., Gotlieb, E., Zapp, J., & Mullins, H.C. (2003). A proposal for electronic medical records in U.S. primary care. *Journal of the American Medical Informatics Association, 10*(1), 1-10.

Baumer, D., Earp, J.B., & Payton, F.C. (2000). Privacy of medical records: IT implications of HIPAA. *ACM SIGCAS Computers and Society, 30*(4), 40-47.

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.

Chen, Y., Ramamurthy, K., & Wen, K.W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

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.

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

D'Arcy, J., & Hovav, A. (2009a). Does one size fit all? Examining the differential effects of is security countermeasures. *Journal of Business Ethics, 89*(1), 59-71.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091-1124.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009b). User awareness of security countermeasures and Its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*: Addison-Wesley Reading, MA:.

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

Gibbs, J.P. (1968). Crime, punishment, and deterrence. *Southwestern Social Science Quarterly, 48*(2), 515-530.

Goldschmidt, P.G. (2005). HIT and mis: Implications of health information technology and medical information systems. *Communications of the ACM, 48*(10), 68-74.

Gopal, R.D., & Sanders, G.L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13*(4), 29-48.

Guo, K.H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251. doi: 10.1016/j.cose.2012.10.003

Guo, K.H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326. doi: 10.1016/j.im.2012.08.001

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.

Health Privacy Project. (2007). Health privacy stories. Retrieved from http://www.healthprivacy.org

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. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herath, T., & Rao, H.R. (2009b). 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.

Ho, R. (2013). *Handbook of Univariate and Multivariate Data Analysis with IBM SPSS* (Second ed.). Boca Raton: CRC Press.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99-110.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

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

Huston, T. (2001). Security issues for implementation of e-medical records. *Communications of the ACM, 44*(9), 89-94.

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.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y., & Wei, K.K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kapoor, A., & Nazareth, D.L. (2012). Medical data breaches: What the reported data illustrates, and implications for transitioning to electronic medical records. *Journal of Applied Security Research, 8*(1), 61-79.

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, S. M., Lee, S.G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

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, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

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

Loch, K. D., Carr, H.H., & Warkentin, M.E. (1992). Threats to information-systems – Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Medlin, B.D., & Adriana, R. (2007). An investigative study: Health care workers as security threat suppliers. *Journal of Information Privacy & Security, 3*(1), 30-46.

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., & 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.

Onwudiwe, I., Odo, J., & Onyeozili, E. (2005). Deterrence Theory. In M. Bosworth (Ed.), *Encyclopedia of Prisons & Correctional Facilities* (pp. 234-238). Thousand Oaks, CA: Sage Publications, Inc.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, Jan. 2007). *Employees' behavior towards is security policy compliance.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on, Hawaii.

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., Ruighaver, A., Maynard, S., & Ahmad, A. (2012). Towards understanding deterrence: Information security managers' perspective. In K.J. Kim & S.J. Ahn (Eds.), *Proceedings of the International Conference on IT Convergence and Security 2011* (Vol. 120, pp. 21-37): Springer Netherlands.

Peace, A.G., Galletta, A.G., & Thong, J.Y.L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly, 13*(3), 481-510.

Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E., & Madensen, T.D. (2006). The empirical status of deterrence theory: A meta-analysis. In F.T. Cullen, J.P. Wright & K.R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 367-396). New Bronswick, NJ: Transaction Publisher.

Pumphrey, L.D., Trimmer, K., & Beachboard, J. (2007). Enterprise resource planning systems and HIPAA compliance.*Research in Healthcare Financial Management, 11*(1), 57-75.

R Core Team. (2013). R: A language and environment for statistical computing. . Vienna, Austria: R Foundation for Statistical Computing,

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

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.

Sanchez, G. (2013). Pls path modeling with R trowches. Retrieved from http://www.gastonsanchez.com/PLS_Path_Modeling_with_R.pdf

Shiffer, R.E. (1998). Maximum z scores and outliers. *The American Statistician, 42*(1), 79-80.

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.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Straub, D., Boudreau, M.C., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems, 13*, Article 24.

Straub, D.W. (1990). Effective is security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D.W., & Nance, W.D. (1990). Discovering and disciplining computer abuse in organizations - A field-study. *MIS Quarterly, 14*(1), 45-60.

Straub, D.W., & Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

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.

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

Tittle, C.R. (1969). Crime rates and legal sanctions. *Social Problems, 16*(4), 409-423. doi: 10.2307/799950

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., L. Thong, J.Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157-178.

Verizon. (2013). 2013 Data Breach Investigations Report.

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

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

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.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58*(2), 212-222.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory it settings. *Information Systems Research, 22*(2), 400-414.

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.

Zhang, L., Smith, W.W., & McDowell, W.C. (2009). Examining digital piracy: Self-control, punishment, and self-efficacy. *Information Resources Management Journal, 22*(1), 24-44.

研究問卷

「如何防止醫院員工違反電子病歷隱私保護政策」調查問卷

您好：

這是一份學術研究問卷，目的在瞭解醫院員工對於「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，作為未來醫療院所，在保護民眾資訊隱私的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

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、第二頁至第三頁為主要問卷內容。請就您對於醫院電子病歷隱私保護政策之看法填答，依照同意的程度填寫。

醫院電子病歷隱私保護政策：指可讓醫院員工知道醫院將如何處理電子病歷資訊及病人隱私權之管理指引，並說明醫院員工必須遵循的病人隱私保護規範。

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 40 歲 □40 歲(含)以上~未滿 50 歲 □50 歲(含)以上~未滿 65 歲
2. 性別	□男 □女
3. 教育程度	□高中/職(含) □專科 □大學 □研究所(含)以上
4. 身分	□護理人員 □醫師 □其他醫事人員_____ □行政人員
5. 管理職務	□管理階層□一般員工 □其他_____
6. 醫護/行政工作年資	_____年
7. 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

註:『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V』

題項	這部份希望了解您對於**醫院隱私保護政策正式與非正式罰則**看法 請您在適當的格子中打勾	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.	醫院可能會懲罰違反電子病歷隱私保護政策的員工	□	□	□	□	□	□	□
2.	醫院可能會開除經常違反電子病歷隱私保護政策的員工	□	□	□	□	□	□	□
3.	如果我被發現違反電子病歷隱私保護規範，我可能受到嚴厲懲罰	□	□	□	□	□	□	□
4.	如果我不遵守電子病歷隱私保護規定，我可能會被處罰	□	□	□	□	□	□	□
5.	如果我違反電子病歷隱私保護規定，我可能會遭到醫院正式處罰	□	□	□	□	□	□	□
6.	如果我違反電子病歷隱私保護規定，我可能會遭到醫院的訓誡	□	□	□	□	□	□	□
7.	醫院可能會監控員工是否合法使用電子病歷	□	□	□	□	□	□	□
8.	如果我違反電子病歷隱私保護政策，有可能被醫院發現	□	□	□	□	□	□	□
9.	如果我違反電子病歷隱私保護政策，被醫院發現的機率可能很高	□	□	□	□	□	□	□
10.	如果我未能遵守醫院電子病歷資訊隱私保護政策，醫院可能容易發生電子病歷隱私破壞事件(如遭到網路入侵而發生資訊外洩狀況)	□	□	□	□	□	□	□
11.	如果我沒能遵守醫院病歷隱私保護政策，我的電子病歷資訊隱私也可能遭受侵犯	□	□	□	□	□	□	□
12.	我相信好好去保護醫院電子病歷資訊就能減少其遭受非法存取之機會(例如未經授權查詢或列印病患的電子病歷)	□	□	□	□	□	□	□
13.	如果連我都不能遵守醫院電子病歷資訊隱私保護政策，電子病歷系統可能就會遭受損害	□	□	□	□	□	□	□
14.	我相信醫院的電子病歷隱私可能遭受到破壞事件(例如遭到未經授權入侵，造成病歷資訊外洩)	□	□	□	□	□	□	□
15.	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，造成病歷資訊外洩)的影響	□	□	□	□	□	□	□
16.	我相信醫院的營運可能受到電子病歷隱私破壞的影響	□	□	□	□	□	□	□
17.	醫院高階主管希望員工能遵守電子病歷隱私保護政策	□	□	□	□	□	□	□
18.	我的主管認為我應該遵守醫院電子病歷隱私保護政策	□	□	□	□	□	□	□
19.	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	□	□	□	□	□	□	□
20.	醫院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							
21.	我認為醫院其他員工能遵守電子病歷隱私保護政策	□	□	□	□	□	□	□
22.	我相信醫院其他員工能遵守電子病歷隱私保護政策	□	□	□	□	□	□	□
23.	醫院大部分員工應當能遵守電子病歷資訊隱私保護政策	□	□	□	□	□	□	□
題項	這部份希望了解您對於**醫院電子病歷隱私保護教育訓練**看法 請您在適當的格子中打勾	非常不同意	很不同意	不同意	沒意見	同意	很同意	非常同意
24.	醫院會提供相關教育訓練以協助員工了解電子病歷隱私保護相關知識	□	□	□	□	□	□	□
25.	醫院會提供相關教育訓練以協助員工了解電子病歷隱私保護相關法律規範(如人體實驗法、個人資料保護法等)	□	□	□	□	□	□	□
26.	醫院會宣導未經授權而讀取或修改電子病歷的不良後果	□	□	□	□	□	□	□
27.	醫院會教育員工對於電子病歷隱私保護的責任	□	□	□	□	□	□	□
28.	醫院會向員工說明未經授權存取電子病歷系統的不良後果	□	□	□	□	□	□	□
題項	這部份希望了解您對於**病歷隱私政策遵循**的看法 請您在適當的格子中打勾	非常不同意	很不同意	不同意	沒意見	同意	很同意	非常同意
29.	我傾向遵守醫院電子病歷隱私保護政策	□	□	□	□	□	□	□
30.	我會試著在日常工作中遵循電子病歷隱私保護政策	□	□	□	□	□	□	□
31.	我會持續遵循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）
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。 (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,可從處罰之角度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： 104 年 2 月 12 日

計畫編號	MOST－103－2410－H－214－007		
計畫名稱	如何防止醫院員工違反電子病歷隱私保護政策：一個整合行為模式		
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	104 年 2 月 4 日至 104 年 2 月 6 日	會議地點	美國夏威夷
會議名稱	(中文) 2015 年商業與資訊國際研討會-冬季場 (英文) 2015 International Conference on Business and Information – Winter Section (BAI 2015 – Winter Section)		
發表題目	(中文) 醫院資訊單位員工遵循電子病歷隱私保護政策之研究 (英文) Compliance with Electronic Medical Records Privacy Policy by Hospital Information Technology Staff		

一、參加會議經過

本次計畫主持人參加 2015 International Conference on Business and Information – Winter Section (BAI 2015 – Winter Section)會議，由國際商學策進會(International Business Academics Consortium, iBAC)、Academy of Taiwan Information Systems Research (ATISR)及 University of Hawaii at Hilo 所共同舉辦，此次會議場地亦同時舉行 ISTEL 2015 會議。BAI 2015 - Winter 會議於美國夏威夷(Hawaii)舉辦總共為期三天(2015 年 2 月 4-6 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 30 個國家專業人士參與，共計投稿論文 150 篇。

二、與會心得

本次計畫主持人投稿一篇論文，題目為：「Compliance with Electronic Medical Records Privacy Policy by Hospital Information Technology Staff」，透過本次 BAI 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，例如韓國 Hankuk University of Foreign Studies 的 Jun 教授分享其研究，探討韓國中小企業使用社交媒體的績效，結果發現除了強化組織內部溝通及產品促銷外，並無特別之效用，會中亦提及由於韓國人在個性上極度相似，當其他中小企業採用社交媒體時，本身中小企業亦會隨之採用，此論點亦在會議中有許多討論，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,並投稿至 Behaviour & Infomration Technology (SSCI 等級期刊)期刊。最後,感謝科技部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

Compliance with Electronic Medical Records Privacy Policy by Hospital Information Technology Staff

Kuang-Ming Kuo,
Department of Healthcare Administration, I-Shou University,
No.8, Yida Rd., Jiaosu Village Yanchao District, Kaohsiung City, Taiwan (R.O.C.)
kmkuo@isu.edu.tw

Ching-Wen Yang,
Department of Information Systems, Taichung Veterans General Hospitals,
No. 1650 Taiwan Boulevard Sect. 4, Taichung, Taiwan (R.O.C.)
cwhello7@gmail.com

Paul C. Talley,*
Department of International Business Administration, I-Shou University,
No.1, Sec. 1, Syuecheng Rd., Dashu District, Kaohsiung City, Taiwan (R.O.C.)
atlanta.ga@msa.hinet.net

ABSTRACT

The purpose of our study is to explore the factors that motivate hospital employees' compliance with Electronic Medical Records (EMR) privacy policy. More specifically, we draw upon the literature of protection motivation theory (PMT) and theory of reasoned action (TRA) to investigate information technology (IT) staff's perceptions regarding the compliance with EMR privacy policy. The study collects data using survey methodology. A total of 310 IT staff of hospitals was analyzed via Structural Equation Modeling. The results revealed that perceived vulnerability and perceived severity of the threats of EMR breaches predict IT staff's fear arousal levels. Fear arousal, response efficacy, self-efficacy, and subjective norm, in their turn, significantly predict IT staff's behavioral intention to comply with privacy policy of EMR. Response cost was not found to have any relationship with behavioral intention. Our study contributes to the literature of EMR privacy policy by integrating PMT and TRA, which provide a sound theoretical basis, to examine privacy policy adherence intentions. The findings of this study also provide insights for health authorities and hospitals in planning and designing effective strategies for improving IT staff's' adherence to privacy policy in order to diminish the threat of EMR breaches.

Keywords: Electronic medical records, Privacy policy, Compliance, Protection motivation theory, Theory of reasoned action