《高大法學論叢》

第 13 卷第 2 期（03/2018），頁 63-134

以 HFMEA 檢視我國醫療資訊保護法制

紀振清 * / 陳永鴻 **

摘要

醫療行為之目的係為解決患者病痛及維護健康，而醫療資訊之取得與分析，則為進行醫療行為時不可或缺過程，於該資訊蒐集過程中，均無可避免涉及諸多患者部分隱私，依醫療法相關規定，醫療機構有管理保存該資訊責任，然因其內容之特殊性，病患對己身之醫療資訊應如何主張其管理權？醫療機構是否有權於未經該資料當事人同意即擅自使用該資訊？現行個人資料保護主要法規—個人資料保護法，因僅要求持有者對資料當事人採被動式告知同意，該規定對患者醫療隱私之保障是否充足妥適？且如

* 國立高雄大學法律學系專任副教授兼系主任及公法研究中心主任，國立台灣大學法學博士。

** 高雄市立小港醫院醫療秘書及婦產科主任，國立高雄大學法律學系碩士。

投稿日期：12/23/2016；接受刊登日期：12/29/2017
責任校對：李兆麒、葉蕙禎

欲主張其資訊自主權之範圍究係為何？此皆值得吾人深思探討。

依傳統法律之立法，多採社會發生案例分析歸納方式，進而將此分析結果反應於立法草案擬定中，惟此方式難免忽略潛在問題，而無法全面透視真正問題所在以防範未來；倘能建立一套推演模式，於草案擬定或修法前即加以科學分析，尋找出真正問題焦點進而完整性立法或修法，將可降低日後頻頻修法以因應實際狀況之窘境。基此，本文爰舉題例，自醫療資訊之特性，加以分析該醫療資訊內容之權利歸屬，探討現行法規對醫療資訊保護之密度，並參酌外國法例，以檢視本國對於醫療資訊權之保障是否完備，並嘗試創新運用健康照護失效模式與效應分析（Healthcare Failure Mode and Effect Analysis，HFMEA）以檢視現行法規或管理上之問題，且由 HFMEA 結果得知，安全管理措施、授權同意及健保資料庫使用，乃隱私權侵害可能性最高之三大主因。

針對此三大問題進行強化保護之對策，本文建議採資訊安全標準化管理措施，並參酌美國健康保險可攜性及責任法（Health Insurance Portability and Accountability Act，HIPAA）規定授權同意模式，且將健保資料蒐集目的與使用範圍具體化、明確化，並嚴守研究資料將個人資料去辨識規定，此除可減少民眾疑慮，更兼及隱私保護與資料利用之最大化目的。

Applying the HFMEA Model to the Protection of Medical Information

Chen-Ching Chi[***] / Yung-Hung Chen[****]

Abstract

Medical behaviors focus on reliving pains and maintaining health. The acquisition and analysis of medical information is one indispensable process when conducting medical behaviors. In the process of obtaining such information, patient`s privacy may be unavoidably violated. According to Medical Law, the medical agencies have the responsibilities for managing and preserving the medical information held. Due to the nature of special information, how the patients should advocate the management rights? Whether the medical agencies are entitled to use the information without consents of patients? The adequacy of passive notification to the patients for disclosing their medical records remains questionable under Personal Information Protection Act. What the scope the parties to the information advocate their rights? As such requires in-depth discussion.

[***] Associate Professor and Chief of Department of Law, Chief of Research Center of Public Law in College of Law, National Kaohsiung University; Ph.D. in Law, National Taiwan University.

[****] Secretariat of Medical Affairs and Chief of Department of Obstetrics & Gynecology, Kaohsiung Municipal Siaogang Hospital; LLM, National Kaohsiung University.

This paper has analyzed the ownership of medical information contents, discussed over the protection intensity of the current laws and regulations posing on medical information from the perspective of medical information characteristics, and inspected whether the domestic protective mechanisms for medical information rights are well-established by referring to foreign legislation; as well as probed into the problems of current laws and regulations or management by creatively applying with Healthcare Failure Mode and Effect Analysis (HFMEA). According to the result of HFMEA, safety management measures, granted permits as well as the use of National Health Insurance Database proved to be the potential reasons for privacy violation.

The reinforced and protective measures for these three problems are proposed. Firstly, the legalization of standard provisions is worthy of being adopted for information security requirements. Secondly, domestic regulations may refer to the mode of granted permits of the American HIPAA rules. Finally, public concerns can be reduced, privacy protection and maximum information utility be reached as long as the purposes and scopes for healthcare information collection and use can be specific and explicit, and comply with the rule of personal information identified.

以 HFMEA 檢視我國醫療資訊保護法制

紀振清 / 陳永鴻

目錄

關鍵字：健康照護失效模式與效應分析（HFMEA）、標準化、資訊自主權、醫療資訊隱私、個人資料保護法

Keywords: Healthcare Failure Mode and Effect Analysis (HFMEA), standardization, informationelles

selbstbestimmungsrecht, medical information privacy, Personal Information Protection Act.

壹、前言

當前世界醫療服務發展潮流，醫療資訊已自傳統人工記載、傳送之處理方式，轉為藉由電子科技設備進行傳輸。而醫療雲之發展，不啻開啟醫療資訊系統一個新的里程碑，且為各國列為醫療產業與經濟科技重點的發展項目之一。因此，行政院與衛生福利部（前衛生署）自 2001 年開始，即著手推動一系列關於醫療健康照護服務計畫，該項計畫即涵蓋整體醫療資訊電子化之軟硬體建置。

醫療電子化具諸多優點與便利性，同時，電子化醫療資訊之便利流通，誠可提升醫療與健康服務品質及效率。然而，因為需要藉由網路傳輸方式，方得以為建構完善，而且，醫療資訊機構之間，可以交互利用，若遇有不當之資訊流通、保存及運用，勢將危害患者醫療隱私甚鉅，故資安問題亦隨之接踵而來，基此，如何兼及提升醫療資訊流通效能與患者醫療隱私，誠屬當前規劃電子化醫療資訊應用管理上，刻不容緩之課題。

無可諱言的，當前我國醫療資訊電子化及雲端化之發展，已遠超越現行相關法規範，保護醫療資訊之法令不足，無以使該醫療資訊當事人受充分之權利保護，此應非吾人所樂見，基此，本文即自此發想，嘗試以健康照護失效模式及效應分析（Healthcare Failure Mode and Effect Analysis，HFMEA），系統性檢視現行主要醫療資訊相關法制對醫療資訊之蒐集、處理及利用，與作業流程模式，是否足以保護醫療資訊免受侵害，及如何於資訊隱私與資訊

利用兩者間取得平衡，並利用分析結果尋求可能解決方案，於發揮醫療資訊流通利用最大效益之餘，尚可防杜醫療資訊當事人權利遭受侵害，且以此法提供迴於當前立法、修法模式，或可另闢一較前衛科學之方法。

貳、醫療資訊之發展與保護

當前的時代正處於不斷的社會重大變遷當中，而且充滿了不確定性。資訊科技之進步發展，固然帶來了諸多方便，但亦潛在著侵害基本權之虞。科技價值固然具有中立性，無關善與不善，端賴利用者如何使用之。惟利用電腦於處理資料時，經常發生大量迅速處理個人資料，以致個人隱私幾近呈現赤裸狀態；被運用之個人資料或有相互矛盾處，或被斷章取義式地部分使用，以致造成對資料主體判斷錯誤。倘若建置錯誤資料，非僅不易發現，亦容易造成利用者對資料主體有構成錯誤認識。因此，隨著電腦網路之發展，終端機端的使用者，極可能藉由電腦操作，使個資處於系統安全陷於不周延的環境下，無端地遭受無正當權限者對資料加以不當利用、修改及加工等危險[1]。

以醫療資訊而言，當患者之醫療資料被資訊化處理後[2]，

[1] 許文義（2000），《個人資料保護法論》，頁 3，台北：三民。

[2] 資料與資訊係二不同概念，資料（Data/ Daten）指一切得以足資識別個人特徵之個別資料言，資訊（Information）則泛指任何現在或未來可任人或其他生物之感官所察覺之事實或想法，因此，有認為資訊係經過處理之資料，而資料則係片段、零星、不盡可靠之消息。實際上，資料與資訊係二個相對之觀念，只有被人認定具有意義時，資料方才成為資訊，故其二者間之認定上，具相當程度使用者之主觀意思。惟其內涵上仍具相當高程度之重疊，如以資料保護立法觀察，其旨在當事人隱私有受侵

因該資訊被集中化及祕密使用，資料主體將隨時生活在資料陰影下，因此，個人醫療資料自蒐集、處理、傳遞與利用，每一過程皆存有風險，甚或對資料主體造成莫大傷害，不可不慎。

一、醫療資訊發展概論

「醫療資訊」係進行醫療行為、預防保健、公共衛生統計，甚或為制定公共衛生政策所不能或缺之依據，至於醫療資訊乃指醫療機構所製作與醫療或保健相關之紀錄，包含疾病就診，健康檢查或預防保健資料，且不以書面為限，舉凡紙本病歷、電子病歷、雲端醫療資料如雲端藥歷、影像資料或遠距照護資料等等均在其範圍之內。

醫療資訊的內容，具有多元之特性，含有敏感性資料與一般性資料，以及客觀數據與綜合性判斷，分別來自不同來源而取得。而且，於功能上除與自身健康維護息息相關外，更兼具公共利益價值醫療資訊。醫療資訊為資訊主體之識別資訊及敏感性資訊之組合，所涵括之內容均係人格權所保護之範圍，因此，醫療資訊權利為人格權之一部分，兼具私領域權利屬性。

然而，醫學進步有賴於疫學之研究，故須將個人各項醫療資訊蒐集與分析，以了解疾病發生之病理機轉，從而進行疾病之預防與治療。同時，為制定公共衛生良策，進

害之虞時，資料保管者即有保護之義務及責任，亦即係為保護當事人資料免受侵害，而非於當事人隱私權受傷害後之保護或救濟。參閱許文義，同前註 1，頁 18-21。

而為資料之收集、分析、檢討，以提升全體國人之健康，係政府之義務[3]，為達此目的，政府對個人醫療資訊之蒐集與利用乃屬必要行為。基此，屬私領域之個人醫療資訊內容與公益之間，即具緊密的關連性。

（一）醫療資訊權利

1.醫療資訊權利內涵

資訊權乃人格權之一部分，而人格權之維護，則係基於對基本權的核心價值—人性尊嚴的尊重，其內容著重於個人人格健全之形成發展與自主控制。資訊權利尚可進而細分為資訊隱私權[4]與資訊自主權兩個面向；資訊隱私權乃係保護個人內在之人格形成之彈性空間，資訊自主權則為保障個人外在之行動自由[5]。另者，從個人資料保護法之規定內容以觀，實已包含隱私權（第 18 條、第 27 條），與自主權（第 3 條、第 6 條、第 15 條、第 16 條、第 19 條、第 20 條）兩大類型，而且，於大法官釋字第 585 號之理由書及釋字第 603 號解釋[6]，亦將個人資訊隱私類型化為資訊自

[3] 參閱衛生福利部組織法第 2 條，第 5 條。

[4] 資訊與隱私原係兩項憲法保障之基本權利，惟該基本權利所保護之範圍（包括對象與事項）亦可能重疊。參閱李震山（2004），〈法律與生命倫理－以基本權利保障為中心〉，《法官協會雜誌》，6 卷 2 期，頁 65。

[5] 邱文聰（2009），〈從資訊自決與資訊隱私的概念區分－評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，168 期，頁 177。

[6] 關於資訊自主權之論述，參閱：大法官釋字第 585 號解釋文及其理由書、釋字第 603 號解釋理由書；而關於資訊隱私權之論述，參閱釋字第 603 號解釋文及其理由書；李震山（2011），〈論資訊自決權〉，李震山編，《人性尊嚴與人權保障》，四版，頁 222，台北：元照。

主權與資訊隱私權。

（1）資訊隱私權

隱私權概念起源於美國，1890 年 Samuel D. Warren 與 Louis D. Brandeis 發表了「隱私權（The Right to Privacy）」一文 [7]，其中並以隱私權係「神聖不可侵犯之人格權（It is the right inviolate personality.）」，亦即「對其與社會無合法關聯之事項，不得隨意洩漏於公眾之權利」，漸演進至當前具積極性之「資訊隱私權」，具有「免於資料不當公開之自由」或「對自己之資料自蒐集迄使用，有完全決定及控制之權利」。是以，隱私權發展迄今，其內涵至少包括了個人生活安寧之獨處權（Recht auf Einsamkeit）、人格不得被商業化及資訊隱私權（Information Privacy）等權利 [8]；倘以現代權利理論觀察，則實應包含：（一）基於憲法秘密通訊之自由及其他本於此一規定，而由法律加以保護之「隱私」利益；（二）本於安適生活之需要，求為不受干擾之「隱私」利益；（三）基於現代自動化資訊處理之發達與普遍，為控制關於自己資料之「隱私」利益等三種內容。而且，本於基本人權日益擴張之時代趨勢，以及個人於實體法上之權益亦應絕對地受到尊重之觀點，對於隱私權之描述，實應兼含此三種隱私權，方不至於有失偏頗。[9]

隱私權首見於我國官方文件中，係 1992 年大法官釋字

[7] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)；轉引自王勁力（2011），〈新版個資法的衝擊影響：論我國公務機關對特種個資的管控與監督〉，《科技法律評析》，4 期，頁 71。

[8] 許文義（2000），同前註 1，頁 53-54。

[9] 翁岳生等（1987），《資訊立法之研究》，頁 35-36，台北：行政院研究發展考核委員會。轉引自許文義，同前註 1，頁 53-54。

第 293 號解釋，並於爾後釋字第 535 號解釋，以及釋字第 585 號理由書中，確認隱私權為受憲法保障之基本權利；釋字第 603 號解釋則對隱私權由人性尊嚴、人格自由發展、個人資料自主控制，而演繹出隱私權，進而延伸出資訊隱私權概念，對於個人自主控制個人資料之資訊隱私權，定義為「其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」

（2）資訊自主權

資訊自主權或自決權（informationelles Selbstbestimmungsrecht）則以德國為代表，惟此於德國基本法中並非新生之基本權利，而係聯邦憲法法院判決對一般人格權進一步加以闡述發展出來，且此一名詞早於 1971 年學者 Steinmuller 受德國內政部委託研究中，即提出「關於個人或團體形象之資訊自決權」[10]。惟該用語正式於官方文件中出現，則近至德國聯邦法院於 1983 年「人口普查法判決」始首次正式提出。該判決文中提及「資訊自決權係源自基本人權中之一般人格權與人性尊嚴」、「個人資訊自決權之限制，僅得於有關重大公眾利益時，方得為之」[11]，清楚地傳

[10] 許文義，同前註 1，頁 50。

[11] 李震山，同前註 6，頁 222；判決中譯本，轉引自蕭文生（1990），〈關於「一九八三年人口普查法」之判決〉，《西德聯邦憲法法院裁判選輯（一）》，初版，台北：司法周刊雜誌社，頁 288 以下。

達了資訊自決權之源起與限制理由，且此項限制必須符合明確性原則與比例原則，並以合憲立法方式方得為之。

「資訊自主權」一詞，於我國首見於大法官釋字 585 號解釋[12]，釋字第 603 號解釋理由書則闡釋資訊隱私權亦含有資訊自主權之意涵；所謂「資訊自主權」即係賦予個人對其個人資訊具有自我決定之權利，包含個人可決定是否將資訊揭露之權利、個人存取資訊之權利、知悉資料之使用及同意權、對錯誤資料要求更正權及資料的刪除權等，其與隱私權相異者為，乃於資訊自主權對其人格發展所具有之意義[13]。

資訊自主權，肯認每一人對於涉及自己資料提供、利用之決定過程，皆有積極參與及形成自我決定之可能，且尚得以作為抗拒他人恣意干涉之消極自由權，亦唯有如此，作為主體性之個人，其人性尊嚴方可不受貶損。故依學者見解[14]，資訊自主權至少需有：（一）法律保留；（二）隱私保護；（三）蒐集所獲得資料之使用應受「嚴格目的限制原則」等三個核心，且唯有以此三核心為準據，我國憲法第 23 條限制之解釋方有所依循，亦不違民主法治國精神。

---

[12] 參閱大法官釋字第 585 號解釋理由書之五：「……憲法第十二條保障之秘密通訊之自由、憲法第十五條所保障之營業秘密、隱私權…等等。其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五〇九號、第五三五號解釋參照）……。」。

[13] 邱文聰，同前註 5，頁 174。

[14] Vgl. K. Vogelgesang, Grundrecht auf informationelle Selbstbestimmung?, 1987,S.54ff. 轉引自許文義，同前註 1，頁 53。

2.私權公法化

隱私權概念源自私法，惟已擴及為公法所保障之權利之一[15]，隨著人類社會秩序與需求之改變，公權力對私人活動之控制亦隨之變化，故當今保障私益之法律，亦須兼顧社會之公益，此現象即稱「私法之公法化」或「法律之社會化」。

日本蘆部信喜教授於其所著「憲法」一書中即提及：「隱私的權利屬於私法上的權利。…隨著資訊社會的發達，此權利已被視為『控制有關自己的資訊的權利』(資訊隱私權)；隱私的權利不但在自由權的層面，而且在積極請求公權力保護隱私的層面」[16]，此將隱私權由私法之權利，提升為公法上之保護對象。另者，國際人權宣言[17]中，亦將隱私權納入條款中保護。

（二）我國醫療資訊記錄之發展及利用

病歷紀錄資料自傳統紙本記錄，已發展為雲端化之電子健康紀錄。隨紀錄方式之演進及網際網路普及化，個人健康紀錄於運用上亦趨多樣化。

---

15 李震山，同前註 6，頁 222。惟，值得留意的是，國內學說自外國先進法例引介隱私權之概念的發展，大致上亦是呈現著「由私法至公法」的擴張趨勢，就此請參閱林子儀（2015），〈公共隱私權〉，國立臺灣大學法律學院、財團法人馬氏思上文教基金會編，《第五屆馬漢寶講座論文彙編》，頁 23-30，台北：翰蘆。

16 芦部信喜著，李鴻禧譯（1995），《憲法》，頁 132-135，台北：元照。

17 參閱世界人權宣言第 12 條、馬斯垂克條約(Maastricht Treaty)第 8 條第 1 項。

1.電子病歷

醫療照護產業之發展，自傳統疾病治療與預防，已轉為現今之健康保健，電子化醫療資訊範圍亦自電子病歷擴大為電子健康紀錄（electronic health record，EHR）。EHR 系統之建構，除可促進病人安全及與增進醫療照護效率與提升醫療品質外，並可有效支援整體健康照護體系 [18]。因此，系統管理安全性、存取限制是否符合保護個人隱私權與尊重自主權，乃建構系統時除資訊使用之便利性與可交換性兩大要素外，另一不可或缺之要件。前「行政院衛生署」(2013 年 7 月 23 日升格為「衛生福利部」)於西元 2000 年推動病歷電子化相關試辦計畫，而於 2009 年宣告為電子病歷元年，正式開啟我國邁入電子病歷新紀元。電子病歷之發展，除了可以降低醫療資源重複使用之浪費外，並可增加醫療品質及安全，然而，伴隨而來之資訊安全問題，於建構完整醫療紀錄資訊化同時，該如何同步建立完善之資訊保護法制？亦係政府應積極規畫之重點。

2.健康雲

由於資訊通信建設與網際網路使用之普及，前行政院衛生署於 2012 年即規劃辦理「臺灣健康雲」計畫，分為「醫療雲」、「照護雲」、「保健雲」、「防疫雲」四項子計畫，係以透過雲端化概念之運用，使民眾可透過此整合性運用，達到提升醫療品質，促進國人整體健康之目的。雖然雲端科技之使用方便快速，而且即使有資料加密技術，

[18] 前「行政院衛生署」(2007)，《建構以病人為中心之電子病歷跨院資訊交換環境案》，頁 9，台北：台灣醫學資訊學會。

惟資料外洩可能性仍比傳統紙本作業為高，因此，如何提高資訊安全，則有賴政府於推動健康雲時建立適當之管理規範。[19]

3.遠距醫療與健康照護

隨通訊傳播技術之進步，醫療照護結合資訊科技而發展出新興照護模式；依據國際上不同之定義及應用範圍廣度可分為：電子健康照護（E-Health），遠距醫療（Telemedicine）及線上醫療（Cybermedicine or Online Medicine）；此三種不同卻相互交集之領域中，無論係經由網路、電話、信件等各種通訊方式，傳輸個人醫療資訊以達到醫療、保健、諮詢、衛生教育，或偕同會診等目的均可含括其中。雖然科技之發展使健康照護所覆蓋之範圍、場所更廣泛而無所不在，且對民眾可帶來更便利及多樣化之服務，惟隨之而來之資訊保護問題卻可能因法令保護之不足，致民眾之醫療資訊隱私權及自主權受侵害而不自知。

4.巨量資料利用

巨量資料（big data，又稱 megadata 或大數據）之研究，與產業領域上之應用發展係近來熱門議題。我國醫療體系於實施全民健康保險後，已成為單一保險人制度，加以電子病歷實施普及化結果，已然累積相當龐大之電子病歷資料，致我國於醫療照護上推動巨量資料之運用相較其他國家具更大利基。前中央健康保險局（現為衛生福利部

[19] 健康雲的困難與挑戰，DIGITIMES 中文網，http://www.digitimes.com.tw/（最後瀏覽日：09/17/2016）。

中央健康保險署）於 1998 年委託國家衛生研究院建置「全民健康保險研究資料庫」，且於 2000 年起正式對外提供學術研究利用[20]，從此開啟我國醫療照護巨量資料之使用。而前行政院衛生署於 2009 年 3 月 1 日成立資料加值協作中心，並於 2011 年 2 月 1 日開始對外試行營運，繼之，科技部亦於 2014 年通過中央研究院所提出之提升健康照護巨量分析計畫結合醫療雲之建置，行政院亦將針對個資保護、研究成果衍生加值應用等擬訂專法。

二、國際醫療資訊權利保護

醫療資訊電子化已為世界趨勢，而且為了因應醫療資訊電子化後，對於隱私權可能帶來極大之衝擊，因此，各國於建立電子化制度之同時，亦設法建構可提供隱私保護之法制環境。以下即就經濟合作組織、亞太經濟合作組織及美國對於醫療資訊隱私保護之法規制度進行簡介。

（一）經濟合作開發組織（OECD）

經濟合作開發組織（Organization for Economic Co-operation and Development，以下簡稱 OECD）於 1980 年公布一項名為保護隱私與跨境傳輸個人資料之隱私指導原則—「隱私保護及個人資料之國際傳遞指導方針」（OECD Guidelines on the Protection of Privacy and Trans-Border Flows

[20] 非學術界研究類依衛生福利部 102 年 11 月 19 日 1020109741 號函通知「行政院衛生署及所屬機關提供產業界衛生相關資料庫使用作業要點」自即日起停止適用。學術研究類依衛生福利部 104 年 9 月 8 日健保企字第 1040038443 號函：「全民健康保險研究資料庫」加值服務對外開放申請期間至 104 年 11 月 30 日截止。

of Personal Data，1980），成為最受世界各國所認可之實務參考資料，其中所列之八項個人資料使用原則廣受各國或國際組織採用，然此文件並不具約束力；另外，「個人資料保護指令」（Directive on the Protection of Individual with Regard to the Processing of Personal Data on the Free Movement of Such Data，1995）則係由歐盟執行委員會（European Commission），參考 OECD 之八大原則所制定，且要求及約束歐盟會員國於處理個人資料時必須遵循。

自 1980 年以來，直至 2008 年的首爾（Seoul）「網路經濟之未來宣告」，開始提出第一次修正案，因 30 年來個人資料於經濟、社會與日常生活中之地位已然發生巨大改變，因此，2011 年 OECD 資訊安全隱私工作小組（Working Party on Information Security and Privacy，WPISP）遂重新檢視，並於 2013 年公布自 1980 年來第一次之修正版本。該修正版本中兩個主要議題：一、強調藉由以風險管理為基礎之隱私保護於實務上之應用，二、為經由改善「相互間可操作性」(interoperability)建構隱私之全球化。[21]

（二）亞洲太平洋經濟合作會議（APEC）

針對隱私維護與個人資料保護之要求，APEC 於 2003 年成立隱私保護小組，且於 2004 年 11 月正式通過「隱私保護綱領」（APEC Privacy Framework）[22]。此綱領旨在推廣亞太地區之電子商務，以增進消費者信賴及確保電子商務之

[21] Organization for Economic Co-operation and Development, at http://www.oecd.org/ (last visited 09/10/2016).

[22] *See* APEC, at http://www.apec.org/ (last visited 09/10/2016).

發展，而與 OECD 1980 年「隱私保護及個人資料之國際傳遞指導方針」之核心價值相符，並再次確立隱私對個人及資訊社會之價值。APEC「隱私保護綱領」對資訊保護建立：（1）預防損害、（2）告知、（3）蒐集限制、（4）個人資料之利用需合目的、（5）當事人自主、（6）個人資料之完整性、（7）安全管理、（8）查閱和更正、（9）責任等九大原則。

（三）美國

美國關於資訊安全或資訊隱私權之保護，係屬個別立法模式，其中針對醫療機構資訊安全管理及個人醫療資訊保護，影響最大者莫過於 1996 年所頒布之「健康保險可攜性及責任法」（Health Insurance Portability and Accountability Act，HIPAA），以及美國健康及人類服務部（The Department of Health and Human Services，以下簡稱衛生部或 HHS）依據 HIPAA 所頒布之「隱私規則」（Privacy Rule）與「安全規則」（Security Rule）。

1.健康保險可攜性及責任法（HIPAA）

美國國會於 1996 年 8 月 21 日通過 HIPAA 法，此法共包含五大議題，包括：（1）健康保險之存取、承受及續約；（2）防止醫療照護之虛報及濫用；（3）與稅務相關之規範；（4）團體健康計劃之要件；（5）收益之抵銷，其目的在於確認健康保險之承受性、減少醫療照護之詐騙與濫用、保障醫療資訊之安全與隱私、及推動醫療資訊之標準規範。為改善健康照護系統之效能及效率，該法內容亦包含行政程序簡化之部份，要求衛生部須進行包括資料之標

準化，醫療資訊安全之保障，及個人可辨識醫療資訊隱私之保障[23]。

該法之目的在於讓醫療保險團體與個人，能維持醫療保險項目之可攜性與連續性，以達到減少浪費、浮報及醫療保險與醫療照護濫用之目的，且得以強化醫療資訊利用、提供長期照護，以簡化醫療服務行政工作來增加美國醫療照護體系之效率及效益[24]，確保個人於醫療保險之權益及範圍及醫療資訊安全，必須具權限或經同意始能存取[25]。

（1）健康資訊隱私權

醫療健康資訊屬個人隱私之一部而當受到保護，因此，HIPAA 對健康照護提供者及健康保險公司作出規定，對於個人之健康資訊隱私，賦予個人對自己健康資訊之權利[26]，此包括（1）閱覽或取得權、（2）修正變更權及（3）資料受揭露之查詢權。

（2）資料保護原則

HIPAA 針對資訊保護訂定：（1）限制提供給第三者、（2）資訊管理權、（3）訂正、（4）目的限制、（5）直接蒐集、（6）事前通知、（7）正確性、合目的性、現在性、完全性、（8）禁止持有敏感資訊、（9）安全保護措施等九大

[23] The Department of Health and Human Services, at http://www.hhs.gov/ (last visied 03/02/2016).

[24] 宋珮珊（2010），〈個人醫療資訊隱私保護之立法趨勢研究—以美國、加拿大為例〉，《科技法律評析》，5 期，頁 47。

[25] 開原成允、樋口飯雄（2005），《醫療の個人情報保護とセキュリティ》，頁 58-59，東京：有斐閣。

[26] The Department of Health and Human Services, at http://www.hhs.gov/(last visied 03/02/2016).

原則[27]。

（3）資訊安全

HIPAA 保護隱私之措施中，最為核心之概念即係「最小必要性揭露原則」，亦可謂係「比例原則」之體現[28]，HIPAA 對隱私及安全之觀念認為，電子病歷應建立對於維護內容之機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）等要項，以為實施因應措施之最基本需求，亦是安全性機制所提供之基本服務，此三項亦稱為「資訊安全金三角」。

HIPAA 規範資訊之利用與揭露，但是，對於資訊取得之蒐集部分卻未加以規範，此資訊保護設計，亦有學者認為尚未真正完整保護個人隱私，而僅於獲得資訊後之保密所為規範[29]。本文認為 HIPAA 雖僅針對資料利用及對第三方揭露有所規定，而對蒐集部分尚未加以規範，然因已限制第三方揭露，亦間接形成限制間接蒐集，至於直接蒐集部分，於進行說明告知後對當事人進行直接蒐集，當事人亦願意配合提供，實質上已等同獲得當事人之同意，故 HIPAA 僅係於條文中未對蒐集為清楚規範，然實質仍有資料蒐集之限制。

2.可辨識個人身分醫療資訊隱私標準與安全規則

HIPAA 主管機關為衛生部，因健康照護產業複雜性增

[27] 新美育文（2000），〈個人情報保護基本法制大綱－アメリカ・EU との對比〉，《ジュリスト》，39 期 1190 號，頁 100-101。

[28] 洪子洵（2013），〈外國法與我國健保資訊應用之比較－以美國醫療保險可攜性及責任法（HIPAA）為鑑〉，《醫事法學》，20 卷 2 期，頁 36。

[29] Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 387, 400 (2012).

加，加以健康資訊技術及交流之進展，使健康資訊機密性之保護將具更大挑戰，因此，議會於 HIPAA 法案中之「行政程序簡化條款」（simplification provision），授權予 HHS 部長制定頒布相關條款。2002 年 HHS 部長頒布行政命令「可辨識個人身分醫療資訊隱私標準」，資訊「安全規則」亦於 2003 年接續頒布；「隱私規則」與「安全規則」之目的，非僅為維護資訊主體之隱私與自主權利，亦同時兼顧資料之利用，尤以醫療照護方面使用之方便性與效能，此制度之設計與我國「個人資料保護法」之立法意旨較為相似。

（1）隱私規則

「隱私規則」之主要目的，在於定義限制個人受保護之健康資訊，於何種情況下可被責任主體所使用與揭露。原則上，除「隱私規則」中允許揭露或要求揭露，或已獲得資訊主體之書面同意，否則責任主體不可使用或揭露[30]；至於要求揭露情況僅限於兩種情形：（1）因當事人或代理人之要求而對其揭露、（2）為犯罪調查、檢視或強制執行而提供予衛生部。

規則中關於醫療資訊揭露之規定，係以事前告知為原則，惟於特別情況下可不需經由事前告知或同意而逕行揭露，告知之內容必須包括：（1）涵蓋機構對受保護健康資訊之使用與揭露方式、（2）涵蓋機構對維護隱私所負之法律責任，公告執行隱私保護之作為且遵循公告內容、（3）個人之權利，包含感覺其隱私權受侵犯時向衛生部及涵蓋主體所提之申訴。

[30] 45 C.F.R. § 164.502(a).

（2）安全規則（Security Rule）

「安全規則」之主要目的，則係於保護個人健康資訊之隱私，同時亦提供涵蓋機構可採取新科技，以改善病人照護之品質與效能。「安全規則」除資訊機密性之要求，可支持「隱私規則」禁止不當使用與揭露原則外，另亦提供維持資料完整性與可用性之目標。

「安全規則」要求涵蓋機構必須維持合理、適當之措施以保護 ePHI(electronic protected health information，以電子保護之健康資訊)，此包括行政保障、物理保障及科技保障，其中尤以涵蓋機構必須做到[31]：（1）於產生、接受、儲存或傳輸 ePHI 時，必須確保資訊之機密性、完整性與可用性；（2）保護資訊之安全或完整性，免於受到合理可預測之威脅；（3）保護資訊免於合理可預測之違規使用或揭露；（4）確保員工均能遵循規定。

雖然「安全規則」內容列出責任主體必須遵循之基本原則，然亦同時考量各機構之規模大小差異性甚大。因此，允許責任主體可依據機構大小、能力、資訊基礎建設、執行資訊安全之成本，以及對 ePHI 可能風險之機率，彈性決定施行之方式[32]，惟倘機構狀況改變，即須重新檢視與調整機構之資訊安全措施[33]。

3.經濟與臨床健康資訊科技法（HITECH）

於隱私與安全保障中，與 HIPAA 相較，HITECH 法則

[31] 45 C.F.R. § 164.306(a).
[32] 45 C.F.R. § 164.306(b)(1)& (2).
[33] 45 C.F.R. § 164.306(e).

加重違反規定行為時之處罰及增加通知義務，強制要求須通知因而受影響之個體 [34]。另者，於 HIPAA「隱私規則」其適用範圍僅係被涵蓋機構，而不包含商業夥伴，雖「隱私規則」有間接要求商業夥伴之安全措施，然僅可要求涵蓋機構以契約規範商業夥伴遵守「安全規則」；而 HITECH 則將商業夥伴含括在內，倘有違反，其處罰規定亦適用於商業夥伴，此規定加重商業夥伴之法律責任，而補強 HIPAA 醫療資訊隱私之保護；其修正重點包括 [35]：（1）加重處罰－HITECH 加重 HIPAA 行政罰鍰與刑事處罰、（2）違反規定之通知義務、（3）對商業夥伴加重要求、（4）增加行為義務。

三、我國醫療資訊權保障

於資料保護規範與措施中，為免人格權遭受侵害，並促進個人資料之合理利用，尤以資料之蒐集、處理或利用，必須遵循許多原則，此一則係源自法治國家依法行政原則之要求，再者係源自對當事人「資訊自主權」與「資訊隱私權」基本權利之保障。

對於資料保護之原則與例外規定，因現代民主法治國家，多數行政行為均係由法律、行政命令（包含法規命令及行政規則），以及自治法規等成文法予以規定，藉以落實

[34] 參閱美國精神科協會執業機構網站：http://www.apapracticecentral.org/legal/technology/hitech-act.aspx，該篇內容係 2009.2.刊載於該學會網站（最後瀏覽日：06/12/2016）。

[35] 楊智傑（2014），〈美國醫療資訊保護法規之初探—以 HIPAA/HITECH 之隱私規則與資安規則為中心〉，《軍法專刊》，60 卷第 5 期，頁 110-113。

依法行政原則。惟法規範中仍有諸多原則及例外規定，例外係為凸顯原則之存在，然而，例外規定過多則可能變成原則，導致原則反成例外，此時即無原則可言，因此，應採「例外嚴格解釋」（Exception est strictissimae interpretationis），且不得類推適用，否則例外既可不受原則規制，原則亦被破壞殆盡。故對資料保護之法規範，至少應具完整、正確、直接、公開、教示、責任、必要及目的拘束等之原則，且不得與一般法律之比例原則、必要原則、禁止不當結合原則與目的拘束原則相牴觸，否則即嚴重違反「法治國家原則」之要求[36]。

因應個人資料保護之發展趨勢與要求，學者認為，於相關法規範中，除依循一般法律原則外，對資料保護之特定原則，條文中應具體包括限制蒐集原則（又稱直接原則）、內容完整正確原則、目的拘束原則、安全保護措施原則、公開原則、個人參與原則（又稱當事人權利原則）、責任原則，及必要原則與闡明原則，且基於原則與例外關係，對其例外規定應明確，且適用時應嚴格解釋之[37]。

（一）個人資料保護法

我國於 2010 年全面修正電腦處理個人資料保護法並改名為個人資料保護法，於 2012 年公布施行。其中與醫療資訊相關之第 6 條規定，敏感性資料原則上禁止蒐集、處理或利用，惟第 1 項但書亦規定於「法律明文規定」、「公務機關執行法定職務或非公務機關履行法定義務所必要」、「自行

[36] 許文義，同前註 1，頁 157-160。
[37] 許文義，同前註 1，頁 203。

公開或其他已合法公開」、「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要」等 4 款例外情況可蒐集、處理或利用，然該條文因未與該法同時施行，直至 2015 年再度修正時亦尚未施行。

2015 年個人資料保護法進行修正，同時亦將尚未施行之第 6 條一併進行修正，增列「為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施」及「經當事人書面同意」兩款為可蒐集、處理或利用之例外條款，同時亦對第 4 款「統計或學術所必要之資料」需進行去辨識之處理程序，修正條文於 2016 年 3 月 15 日施行，醫療資訊之蒐集利用終有所依循。

（二）民事法

醫療資訊權利於民事實體法之實現，主要表現於侵權行為與契約責任而衍生之損害賠償。民法第 195 條[38]，將「隱私」列為人格權之一種，醫療資訊為敏感性資料自屬隱私權範圍之一部，如不法侵害隱私，即使為非財產上之損害，亦得請求賠償相當之金額，倘若因病歷資料洩漏而造成隱私權侵害，被害人除可依侵權行為請求非財產之損害外，亦可請求相當慰撫金之賠償。

（三）刑事法

我國刑事法規，無論實體法抑或程序法，均有針對涉及醫療資訊權利之保護規定，於刑事實體法部分，刑法第

[38] 1999 年民法第 195 條修正理由：「一、第一項係為配合第十八條而設，原條文採列舉主義，惟人格權為抽象法律概念，不宜限制過嚴，否則受害者將無法獲得非財產上之損害賠償，爰擴張其範圍，及於信用、隱私、貞操等之侵害」。

316 條洩漏業務上知悉他人秘密罪，此條文處罰之行為主體為醫師、藥師、助產士、心理師等，或其業務上佐理人等之醫療人員，如有無故洩漏病人之醫療資訊，將科以刑責。

至於刑事訴訟法第 182 條則明文規定，醫師等醫事人員於業務上知悉之他人秘密（病情），若未得本人同意，縱使司法機關傳喚要求醫師等職別之人員作證時，該員可拒絕證言之。

（四）醫事法

1.醫療法

關於醫療資訊權利之保障，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。」；違反者依同法第 103 條可處 5 萬元以上 25 萬元以下罰鍰。此外，為尊重病人對病情資訊瞭解之權利，第 74 條明文規定病人得申請病歷複製本。

2.醫事人員法

於各類醫事人員法中，對於因業務而知悉他人醫療資訊亦有保密義務規定，如醫師法第 23 條、法醫師法第 21 條、心理師法第 11 條、呼吸治療師法第 16 條、語言治療師法第 15 條、護理人員法第 28 條及聽力師法第 15 條；然同屬醫事人員，於藥師法、職能治療師法、物理治療師法、牙體技術師法、醫事放射師法、醫事檢驗師法等卻無如同前述之相關保密義務，因此，倘前開人員違反保密規定，則適用醫療法第 72 條，依醫療法第 103 條處 5 萬元以上 25 萬元以下罰鍰。

3.醫院電腦處理個人資料登記管理辦法

此辦法係依電腦處理個人資料保護法（個人資料保護法前身）及其施行細則相關規定於 1996 年所訂定[39]，其中涉及資訊權利者為第 8 條之醫療資訊調閱請求權，及第 11 條資訊安全管理義務規定；關於資訊查詢、閱覽及製給複製之請求權，於第 9 條除外規定：（1）有妨礙業務執行之虞者、（2）有妨害第三人重大利益之虞者、（3）申請書件未齊備者、（4）其他與法令規定不符者。此排除條款中，除第 3 款程序不完備及第 4 款違反法令規定尚屬合理外，較為爭議者為第 1 款妨礙業務執行與第 3 款妨害第三人重大利益，然而個人資料保護法通過施行後，該查詢調閱與複製請求權之限制，與個人資料保護法第 3 條意旨相悖，故應予廢止。

（五）特殊醫療用途之資訊隱私保護

1.醫學研究

醫學之進步有賴於不斷之研究與試驗，醫學研究類別中，大致可分為統計分析、不牽連到人類或生命個體的實驗室（in vitro）研究，及與生命關連之生物體（in vivo）研究等三類，其中人體研究方面，對研究對象權益之侵害可能為最大，且與人格權、人性尊嚴息息相關之人體試驗，於我國已有醫療法、人體研究法[40]與人體生物資料庫管理條

[39] 參閱醫院電腦處理個人資料登記管理辦法第 1 條。

[40] 人體研究法之適用範圍，參閱 2011 年人體研究法第 1 條立法理由：「人體研究之範圍極為廣泛，基於人體試驗及人體生物資料庫研究等已有法律規定，為釐明法律適用關係，爰訂定第二項規定。例如人體研究屬人體試驗者，應依醫療法有關人體試驗之規定；屬人體生物資料庫者，應依人體生物資料庫管理條例

例等法規，以及人體試驗管理辦法、藥品優良臨床試驗準則」與藥品優良臨床試驗規範等法規命令以作規範，對於研究對象之權益保護可謂相當完整，亦符合《紐倫堡守則》（Nuremberg Code）[41]及《赫爾辛基宣言》（Declaration of Helsinki）[42]精神。

依據人體研究法第 4 條之定義，蒐集病人醫療資訊而進行分析之研究，係屬人體研究之範圍，應受該法之規範而優先適用。而同法第 12 條第 2 項規定研究計畫，應依審查會審查通過之同意方式及內容，取得研究對象之同意，惟屬主管機關公告得免取得同意之研究案件範圍者，不在此限。因此，前行政院衛生署於 2012 年 7 月 5 日公告得免取得研究對象同意之人體研究案件範圍[43]，共有四種情況可免

之規定」。

41 《紐倫堡守則》是一套人體試驗之準則，是成於第二次世界大戰之後的紐倫堡審判的結果。具體地說，該守則是由於納粹於戰時對人類進行不人道的實驗而來。法官們也發表了他們對人體試驗的意見。1947 年 4 月，Dr. Leo Alexander 向戰爭罪行議會（Counsel for War Crimes）呈交了六點方案為合法的醫學研究取義。在裁決中這六點被接納了，另外也加了四點。而這十點方案便成了《紐倫堡守則》的條文。

42 1964 年「世界醫學會」發表《赫爾辛基宣言》，作為進行人體試驗的規範。美國的衛生部所頒發的法則：Code of Federal Regulations Title 45 Volume 46link（45CFR46），是為管理在美國由聯邦政府資助的實驗，該法則即是以紐倫堡條文和其有關連的赫爾辛基宣言（Declaration of Helsinki）為基本。

43 參見行政院衛生署 101 年 7 月 5 日衛署醫字第 1010265083 號公告：「研究案件符合下列情形之一者，得免取得研究對象之同意：一、公務機關執行法定職務，自行或委託專業機構進行之公共政策成效評估研究。二、自合法之生物資料庫取得之去連結或無法辨識特定個人之資料、檔案、文件、資訊或檢體進行研究。但不包括涉及族群或群體利益者。三、研究屬最低風險，對研究對象之可能風險不超過未參與研究者，且免除事先取得同意並不影響研究對象之權益。四、研究屬最低風險，對研究對象之可能風險不超過未參與研究者，不免除事先取得研究對象同意則無法進行，且不影響研究對象之權益。」

除取得同意之限制：第一項為執行法定職務；第二項為研究之資料已去連結，不屬於個人資料的範圍；第三項與第四項則係於研究風險、資料主體權益及研究所能獲取之公共利益間尋求一平衡點，對於資料主體之資訊權利已有衡平之考量。

關於人體研究之規範，若規定過於嚴苛，可能有礙醫學之進步，對我國醫療科技之發展，或醫療品質之提升將有不利之影響，然若規定過於寬鬆，對人民之隱私權與人格權之保護復嫌不足，故兩者間之平衡，為相關法規制定時尚須審慎為之。另外，關於研究行為，主管機關應採鼓勵、開放之態度以協助研究行為之進行，惟對研究進行中相關資料之管理與監督，則須採最嚴格之標準，要求研究者或研究機關需採行一定之管理規格，以保護個人資料之隱私安全。

2.遠距照護

我國遠距照護相關法制化，遠落後政府與民間於遠距照護產業發展之速度，因遠距照護實非醫療法規範之醫療行為，因其所蒐集、紀錄之醫療資訊僅適用個人資料保護法，而不受醫療法所規範，於政府 2006 年開始推動遠距照護後 8 年，衛生福利部終於 2014 年公布遠距照護個人資料安全維護指引以作為個人資料保護法[44]之補充規定，強化當事人同意、目的內使用及資訊安全措施等規定，為日漸風行之遠距照護資料安全維護提供準則方針。惟該指引僅係行政指導性質，亦非創設遠距照護服務業務所需之審查項

[44] 衛生福利部 103 年 11 月 5 日衛部照字第 1031561844 號訂定全文 7 點。

目，是否具有實質約束力仍依個人資料保護法規定。

參、以 HFMEA 檢視我國現行醫療資訊隱私保護

我國對於資訊隱私之保護，係採集中立法方式，規定於個人資料保護法，然而對醫療資訊保護之相關法規範則散於民法、刑法、醫療法、個人資料保護法及關於各醫事人員等法律，而無單一專法進行系統性規範。依個人資料保護法施行細則第 12 條第 2 項第 3 款規定，機構對於個人資料需進行風險評估並建立管理機制，而醫療資訊為敏感性資訊，係隱私侵害高風險對象，故更需進行系統性風險評估。

自法律風險管理角度言，經營者不應忽略法律與企業間之依存性，且應設法將法規範融入經營策略中，若能預先充分了解未來的司法風險，並為適法之規畫，當可防範不法行為之發生。誠然，風險之態樣固多，於研究該風險時，應自定量方法研析，其所占之比值、發生法律風險之機率，及法律風險於風險損害之比重，以建立客觀數值，強化管理之信實度[45]。

因我國醫療資訊之儲存、傳遞模式已朝向電子病歷、雲端儲存邁進，為瞭解我國對醫療資訊權利之保護現況，本文將嘗試運用健康照護失效模式與效應分析（Healthcare Failure Mode and Effect Analysis，簡稱 HFMEA）方式，針對現實醫療資訊之蒐集、處理及利用等各步驟進行系統性

[45] 施茂林（2013），〈法律風險管理體用矩陣與連動議題之研究〉，施茂林主編，《法律風險管理跨領域融合新論》，頁 17、21，台北：五南。

檢視，藉以觀察可能發生之隱私權及自主權侵害，且對照現行法規之要求與保障，據以了解現行法規範之缺失。

一、失效模式與效應分析於健康照護

（一）失效模式及效應分析簡介

失效模式與效應分析（Failure Mode and Effect Analysis，簡稱 FMEA）係源於 50 年代由美國格魯曼（Grumman）公司所提出，並將其運用於飛機可靠度設計改良之參考。當時，因飛機系統複雜性，並為預防因飛機裝置失效而發生事故，FMEA 之運用成功，導致降低事故發生機率，因此廣受航空與國防產業之採用，進而漸漸發展成安全性與可靠度之設計模式，以期可增加產品品質，降低不良問題之發生。[46]

FMEA 係一種預防流程失效之系統性分析方法，將各主流程或子流程進行系統性分析，以檢視該流程是否可達所應有之功能，經由團隊運作及腦力激盪方式，逐步偵測流程中包括系統、過程、環境、設備或人為所可能造成之潛在失效模式，以及可能影響之結果，並針對某些高風險係數項目進行重新設計或修正，以期對機構造成影響之關鍵失效模式，及其伴隨之風險效降至最低。

FMEA 具失效模式（Failure Mode）、失效影響（Effects of Failure）與失效原因或機制（Causes／Mechanisms of Failure）等三個核心元素。失效模式係指流程或產品失效

[46] 任秀如（2013），〈醫療失效模式與效應分析〉，朱樹勳編，《醫療機構品質與病安管理—理念與實務》，頁 311，台北：華杏。

之表現形式或狀況，失效影響則指失效模式會造成對安全性、產品功能影響，而失效原因即係使產品發生失效之（根本）原因。由各失效原因分別去評估該事件發生之可能性（發生率）、該事件發生後造成影響之嚴重度，及是否可能偵測事件發生之可偵測度等三個因子，以三維風險分析進行風險優先級數（Risk Priority Number，RPN）計算；發生率、嚴重度與可偵測度三個因子並非完全獨立互不影響，例如當事件之發生可容易被偵測時，事件之發生率或嚴重度即可降低。FMEA 之目的在於可事前做好風險評估，對可能之風險危機設計屏障，以減少不良事件之發生並降低損害，將風險控制於機構所能容許之最低風險。

（二）健康照護失效模式及效應分析（HFMEA）之發展

健康照護失效模式及效應分析（Healthcare Failure Mode and Effect Analysis，HFMEA）為美國醫療機構評鑑聯合會（Joint Commission on Accreditation of Healthcare Organization，簡稱 Joint Commission 或 JCAHO）所提出，係從工業界引入 FMEA 模式修改而來，並由美國國防部「國家病人安全中心」所研發，將 FMEA 三維風險分析簡化為二維風險分析，此保留嚴重度與可能性以計算風險優先級數，再透過決策分析以決定改善對策進行之順序。

HFMEA 之應用以醫療照護流程之核心為主，所分析對象包括醫師、護理、醫技、行政等職別人員個別或整合參與之醫療照護相關之流程，目的在於提高病人安全、降低病人之傷害，使病人於醫療照護過程中，能夠得到最大的保護。

本文採用之 HFMEA，所分析者係流程中所有可能發生之失效模式，進而解析可能原因及可能造成之影響，以流程中可能造成之缺失為觀察，討論人員之疏失、環境之不良或設備之失誤，亦即行政流程之疏失而非法規缺失，惟於流程分析中，除失效模式、原因及失效影響外，尚有該流程之管制方式，藉由對照管制方式之有無或管制要求，可了解該失效原因是否與管制方式不足或缺失有關，或藉由管制方式之優化以達降低行政流程缺失問題，故亦影響到法制之問題。為瞭解常規醫療作業上，現行法規於醫療資訊所能提供之保障及是否會造成相關作業困擾，本文除將失效影響設定為隱私權侵害外，與一般 HFMEA 所進行之方式相異者，即更強調流程失效與管制方式之關聯性，以達分析法規保護之目的。

（三）健康照護失效模式及效應分析（HFMEA）流程簡介

於失效模式與效應分析之進行步驟中，須先發掘流程中潛在失效模式，並檢視此失效模式可能造成之影響，本文即將潛在失效影響設定為患者醫療資訊隱私權或自主權侵害，並就侵害之嚴重度、發生率來進行風險危害分析（Hazard Analysis），訂定風險評估表，並同時檢視現行規範是否能適當有效保護醫療資訊權利，且依據風險評估表計算風險優先級數，依據嚴重度及 RPN 值來決定改善之優先次序。

HFMEA 進行之五大步驟[47]：

1、選擇需要檢視之流程：以選擇高風險流程優先進行。

[47] 同前註，頁 312-333。

2、組成團隊：團隊成員必須與作業流程有相關業務關係。
3、繪製流程圖：繪製所要分析之目標流程，對於複雜之流程可先將主流程細分為數個次流程，再將各個次流程展開，至於展開之程度，則由團隊成員共同討論與確認流程之正確性是否與實務作業相符。
4、進行危害分析：列出每一個次流程或步驟所有可能之失效模式，以決定每一個失效模式之嚴重度及發生可能性，並計算其風險優先級數。
5、擬定行動與量測：針對造成失效模式之原因擬定行動策略，並針對改善後再進行量測，比較改善前後之風險。

二、以 HFMEA 檢視醫療資訊權之侵害

雖然 HFMEA 適用係出於作業程序之分析檢討，惟本文嘗試將醫療資訊之蒐集、處理、利用轉化成作業流程，將部分作業流程步驟進行檢視，以了解於現行法制管理下患者之醫療資訊權利可能受到之侵害，及對機構運作可能造成之風險，並建立風險評估表，以評估資訊權利受侵害之可能性及嚴重度，進而計算風險優先級數，並對應相關法規，將法規範作為流程之管制，以為系統性、全方位檢視，藉以發掘現行法規不足之處。

傳統上 HFMEA 之進行，係針對作業流程（程序）中可能出現之錯誤進行系統性檢視，此錯誤可能係人為疏失，亦可能為系統錯誤，系統錯誤主要為管理或作業標準不當，管理規範之依據即是來自於外部法規，完善的法規範

可使機構政策的制定有所據，而降低錯誤的發生。本文將錯誤所引發之效果，亦即失效之影響，侷限於隱私權或自主權侵害，且將系統錯誤由內部管理，延伸至外部法規，藉此檢討我國對於醫療資訊權利保障之缺失，以尋求更完善保障。

基於保密原則，試以隸屬某醫療體系之區域教學醫院，有關其醫療資訊作業部分流程為例，進行失效模式與效應分析檢討；團隊成員含醫師、護理師、資訊工程師、醫療事務室（主掌業務包含健保申報、病歷管理）、醫管師及工安人員。

（一）繪製作業流程

關於醫療資訊整體作業，依據個人資料保護法對於資料作業之介面，可分為蒐集、處理及運用三個主流程，此作業流程之繪製，即以此三個主流程所延伸（見圖一），於三個主流程中，尤其資訊蒐集和運用，於作業中必須含括內部作業流程及對第三方之資訊揭露，因此，將部分作業流程區復分為醫院內部流程及內部流程兩部分進行；內部流程係指醫院內關於病歷資料之建立、蒐集、儲存、修正、調閱及銷毀等步驟，除醫療目的外，尚包含教學與研究。

三大主流程下尚有數項次流程，本文將針對流程中易侵害資訊隱私權，或資訊自主權之高風險流程進行分析與檢討。

圖一、醫療資訊相關作業流程

（資料來源：著者自編）

1.資訊蒐集

病歷資料之建立基礎為資訊蒐集，蒐集方式可分為直接蒐集與間接蒐集，依據蒐集過程中所涉及之適法性、合宜性與正確性以決定將進行分析之流程；直接蒐集部分，因需病人配合方可進行，因此較無權利侵害之可能，而間接蒐集則可能發生當事人不知或未充分了解之問題。因此，將對內部資料庫讀取與外部資料庫讀取的作業步驟來進行流程檢討。

2.資訊處理

依個人資料保護法第 2 條，資料處理係指資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送，於資訊處理流程中最重要者為 HIPAA 所強調之資訊機密性、完整性與可用性。其中高風險之流程有資訊查訊、資料存取輸出及刪除等流程，為本文選擇優先進行分析。

3.資訊利用

醫療資訊於醫療機構內部之使用包含有蒐集目的之醫療行為使用，及因應醫療法第 67 條第 3 項製作各項索引及統計分析，至於非醫療行為或醫療法製作病歷目的以外之利用尚包含教學、研究、司法、商業保險投保給付、社會保險（如健保、公保、勞保、農漁保等）使用等等，而經由醫療機構取得個人醫療資訊做再利用者，其中以健保資料庫之使用爭議最大。另外研究與遠距照護，雖有其醫療上之目的，惟非屬醫療行為之一部分，亦屬隱私侵害高風險之流程。

（二）建立風險評估表

本文採用健康照護之失效模式分析，為嚴重度與可能性二維分析，以計算出風險優先級數（Risk Priority Numbers，RPN）；將嚴重度與可能性分別評定後，將評定之嚴重度與可能性分數相乘即可得 RPN 值。

1.建立風險矩陣－嚴重度

計算風險優先級數因子之一，為發生事件時所可能造成之嚴重度。嚴重度之評比內容可包含失效影響程度範圍、可能出現之傷害程度與財產損失等；惟本文中所探討者係資訊權利侵害時所可能造成之影響，因此，評比之原則係依據失效模式所造成資訊侵害之族群範圍（例如僅單一個案受影響，或罹患某種疾病或接受某種治療之患者等某一特定族群），與可能散布之程度（例如僅特定個人或機構內部人員得知病人資訊，或已為第三人所得知，或已散布於眾造成當事人人格受具體之侵害），以及是否可能面臨行政、民事或刑事訴訟來評比嚴重度；評比之依據有侵害結果、範圍與工作人員影響三面向，同一事實於三個面向中可能造成不同之評分，最終將以最嚴重之分數採計。共分為十個等級，以下為嚴重度評比的標準與分數的列表（如表格一）：

表一、嚴重度評比

嚴重性–S 評比			
級距	評比原則		
	工作人員影響	侵害結果	影響範圍

1-2	不受影響	造成可能隱私侵害	個別病患
3-4	機構內部懲戒	造成隱私侵害為僅內部人員所知	單一特定族群
5-6	行政罰	造成隱私侵害為內部人員及當事人所知但不為其他第三人所知	多個特定族群
7-8	民事賠償	造成隱私侵害為第三人所知	不特定族群（非全部但無法確認影響範圍）
9-10	刑事罰	造成隱私侵害致生損害	全部

（資料來源：著者自編）

2.建立風險矩陣—可能性

計算風險優先級數之另一項因子，為失效模式可能發生之機率與可能性。就醫院內發生之狀況，或其他機構是否曾發生此類失效模式，來評比發生機率（如表格二）。

表二：可能性評比

可能性—P 評比		
級距	評比原則	
1	可能性極微小	國內外從未發生過
2	可能性微小	
3	有可能發生	國內從未發生過而國際上已有案例
4	近年內曾發生	
5	一年內曾發生過 1 次	國內無案例而國際上已有不少案例
6	每半年至少發生一次	
7	每季至少發生一次	國內有一兩案而國際上已有不少

8	每月至少發生一次	案例
9	每週會發生	國內已有不少案例
10	天天會發生	

（資料來源：Joint Commission Resources[48]）

（三）危害分析

1.資料蒐集

資料蒐集所分析之流程乃病人於就診時，為建立病歷資料所需而進入機構內部資料庫、醫療體系事業群內部資料庫，或連結外部資料庫蒐集相關資料時之流程。依現行個人資料保護法規定，縱使係進行醫療行為而需蒐集利用個人醫療資訊，仍需病人有效之授權同意，故僅需不符合現行法規要求，即屬隱私侵害。在資料蒐集流程中，以未取得病人授權即進入外部資料庫蒐集患者就醫資料的作業步驟之 RPN 值最高，而此失效模式的原因除了缺乏適當的安全管控措施外，背後隱藏的問題在於形式上不符合現行個人資料保護法的規定。而其餘 RPN 值較高的失效模式，也多屬不符合法規要求，例如同意書之填寫、說明內容不符要求或是授權範圍不明確等。

2.資料處理

醫療資訊經由蒐集並建立病歷後，會進入儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送等資料處理各項流程，於各項處理流程中，將依據對資訊機密性、完整性與可用性之保障以考量資訊隱私管理之侵害可能，此部分的流程分析所得之 RPN 值較高的失效模式在

[48] Joint Commission Resources , at https://www.jcrinc.com (last visited:6/30/2017).

於非進行醫療行為時，進入資料庫查詢資料之管控問題，例如密碼管理不當。

3.資料利用

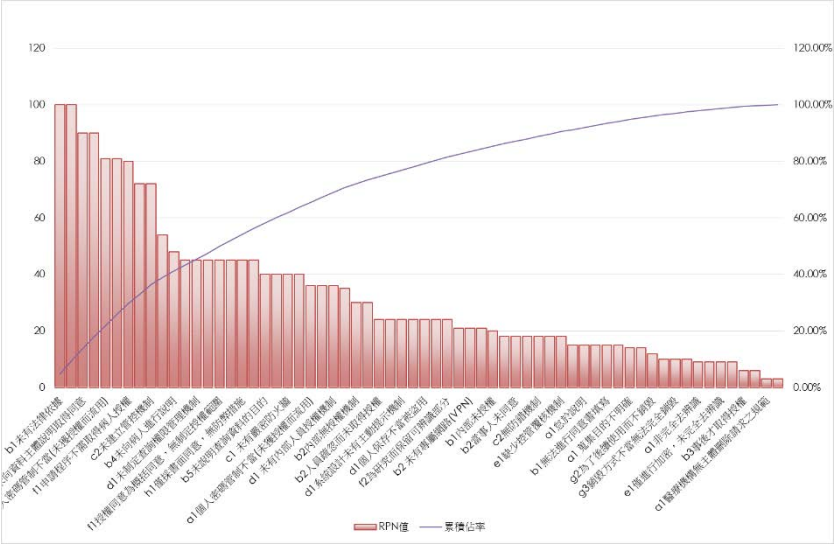
所謂利用係指資料於處理以外之使用，病歷建立之目的係基於醫療行為之進行，至於其他非醫療行為而使用病歷資料之情形，則有各項行政通報、司法調查、商業保險查詢、社會保險使用，及教學研究、遠距照護等特殊目的之使用。其中最具爭議者乃健保機關將健保資料提供健保資料庫作為學術或非學術之使用；此外，因關於研究與新興之遠距照護，相對侵害隱私可能性較高，故優先納入分析之對象，惟需注意者，雖部分流程未納入分析討論，例如傳染病通報流程，尤以人類免疫缺乏病毒感染之通報與保護流程、或司法協助等非當事人同意之利用，雖具公共利益內涵與法律上之授權，而符合「個人資料保護法」資料利用之規定，然其本質上仍有權利衝突問題，要非全無資訊利用與隱私保護衡平問題產生。

（四）結果與優先改善項目

完成失效模式風險優先級數（RPN）計算後，將各失效原因之 RPN 值彙整，並繪製 RPN 之柏拉圖（如圖二），總 RPN 值為 2104。將各項失效模式與失效原因歸納分類，吾人可發現以安全管理措施問題最劇，其中包括資訊安全管理之科技保障措施不足、資訊安全管理之內部授權相關問題等共占 53.3%；授權同意相關的問題占 36.9%次之，其中包括就醫時醫師登入資料庫查詢電子病歷資料或雲端藥歷、進行研究時申請健保資料庫之授權同意、研究時授權

解除等問題至於針對健保資料庫資料問題則占 9.5%，此涉及目的外利用問題，而此部分係單項風險優先係數最高部分，亦值得進一步研究。

圖二 失效原因 RPN 值



（資料來源：著者自編）

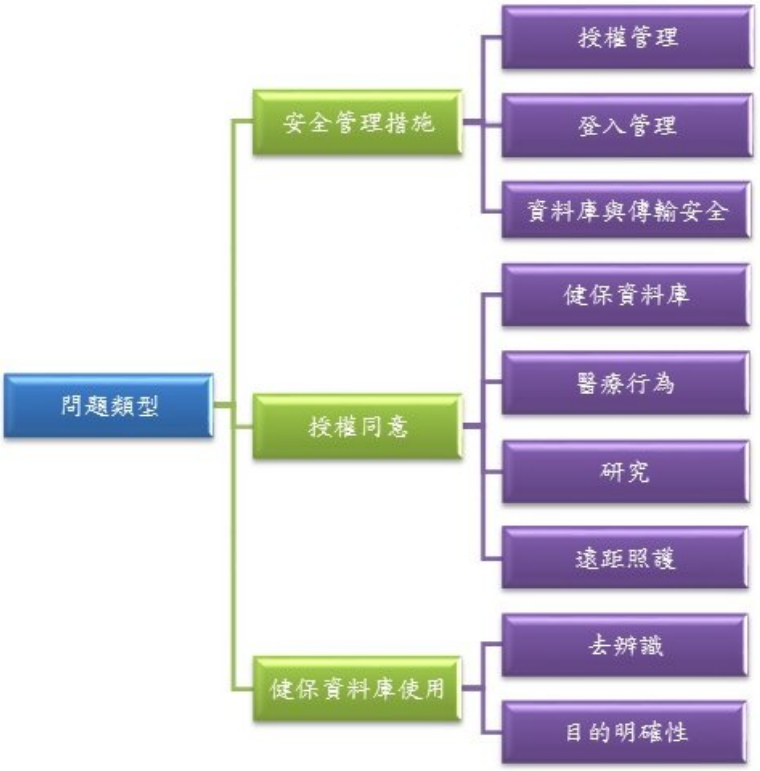
優先改善項目部分，依 80/20 法則以決定優先改善項目[49]，經計算，RPN 24 分以上累積占率達 81.46%，總分為 1714。就優先改善項目進行分析，其中仍以資安管理問題最多，占 52.41%；其次為授權同意問題，占 35.86%；而健保資料庫使用問題，占率提高至 11.67%。

[49] 美國 J. M. Juran 將柏拉圖運用在品管領域，關鍵重要的少數，瑣細的多數(vital few，trival many)

肆、強化醫療資訊權利保護

依 HFMEA 分析，於資料蒐集、處理及利用之流程可能發生侵害資訊權利之失效模式中，可歸納出其主因係安全措施規範無一標準（占 53.3%），說明同意及授權無明確（占 36.9%），及健保資料庫利用之問題（占 9.5%)等三大類（整理如圖三）。

圖三 問題類型分析



（資料來源：著者自編）

一、安全措施

依個人資料保護法第 6 條、第 18 條及第 27 條規定，無論公務機關或非公務機關均需有適當之安全措施，而此安全措施，係指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，所採取技術上及組織上之措施而言[50]。於安全管理措施中居最重要地位者，乃存取控制，且於醫療機構內存取過程中，最易發生病人病歷資料隱私權受到侵害。資訊持有者對於機構內資訊存取之管理措施，主要在於資訊存取流程當中，對於接觸資訊之人員所作之身分、存取範圍及使用資訊時間或地點之授權等安全機制。此外，資訊正確性與即時更新與否，亦為減少醫療失誤要素之一。

（一）問題分析

對醫療資訊之保護，有賴於機構對於資訊安全風險管理之落實，與政府高密度之法規管制。於影響隱私權之失效模式中，安全性管理問題所占比例達 53.3%最高，基此，即可知安全管理措施之重要性，而落實安全性管理，除資料持有管理者須善盡機構本身之企業責任外，更需仰賴法規以為外部之規範指引，故自律與他律缺一不可。

於安全管理措施問題中，依失效原因之性質再予以類別化，將發現以授權相關管理問題（如圖四），例如人員資格管理、資料範圍管理等，與內部授權相關之授權管理問題最多，其約占三成；次者係資訊系統登入管理問題，約

[50] 參閱個人資料保護法施行細則第 12 條。

占兩成；查核與資料庫安全防駭或傳輸安全保護問題則各占一成；可辨識資料去連結問題占 7.5%，其他資料正確性或完整性維持約占 5%；此外有 16.8%為如雲端藥歷查詢等系統登入安全管理問題，因此類問題本質為授權同意問題，將併於以下之授權同意一節討論。

圖四 安全措施問題之類別

（資料來源：著者自編）

授權問題所涉及者為資訊安全金三角中之機密性問題，其包含內部人員可能接觸個人資料時，如何進行個別授權之行政保障，對於機構內部授權，或當事人之外部授權，如何進行安全查核、如何確保依授權目的、範圍或時限處理利用個人資料之科技保障；至於資訊系統登入方式、資料庫或網路安全，亦為資安機密性問題，即需仰賴科技保障；另外，資料更新、毀損或刪除，則係資安完整

性與可用性問題，其在於機構資訊安全管理系統是否建立流程，是否有風險管理及措施，至於辨識之問題，則涉及機密性與可用性。

雖前述問題多屬機構內部管理，惟倘若法規未對機構做出適當、明確之規範，將難以落實資訊安全管理。關於安全管理措施，雖於個人資料保護法規範要求，無論公務機關或非公務機關，均須實施安全管理，然於施行細則中對安全措施之要求僅作例示參考，欠缺系統性與完整性之安全建置規定，於資訊安全管理上似略嫌不足，且僅於第 48 條規定，對未實施安全管理措施之非公務機關有罰鍰之規定，然對公務機關則無相關處罰規定，僅於造成當事人隱私侵害時方負賠償責任，此將大為削弱對機構設置安全管理措施之強制力，而間接弱化資訊保護之目的。

（二）標準化與資訊安全

所謂資訊安全，乃依 ISO/IEC 27001 及我國國家標準 CNS27001 之定義，為「保存資訊的機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）」，而此定義亦為美國衛生部訂定之資訊「安全規則」(Security Rule)所要求之基本義務；標準化之於資訊安全，除可為內部建立資訊安全管理之參考依據外，於網通科技發達之今日，依國際標準所建立之資安系統，始可確保跨域資訊流通時之安全性、機密性，以維資訊當事人之隱私安全。

資訊隱私安全管理國際標準首推 ISO/IEC 27000 系列及 BS 10012 兩類，而 ISO 29100 則係協助建立隱私框架，對於

國際標準，標準法第 3 條之定義為「由國際標準化組織或國際標準組織所採用，可供公眾使用之標準。」，由此可知，我國承認國際標準組織所建立之標準，並足以為大眾所採用與信賴。

ISO 27000 系列係為資訊安全管理相關之一系列標準，其中包括資訊安全管理要求之 ISO 27001、資訊安全作業實施要點之 ISO 27002、資訊安全管理系統實施指引之 ISO 27003，量測指引之 ISO 27004，與資訊安全風險管理等共超過十項之標準；ISO 27001 建構了安全管理系統之標準，於執行面上 ISO 27002 則提供廣泛複雜之指導標準，且部分國家亦採此通則標準以為該國之醫療照護資訊安全規範，惟通則性標準尚非完全適用於醫療照護資訊，故於累積經驗後，適用於醫療照護資訊安全管理之 ISO 27799 標準亦應運而生，ISO 27799：2008 係將 ISO 27002 使用於健康資訊安全管理之標準專章，依循該標準非僅可保持資料之機密性與完整性，且仍可維持醫療資訊系統之運用。目前已有許多國家將 ISO 27002 做為健康資訊科技安全管理指引，例如澳洲、加拿大、法國及英國等，而 ISO 27799 即係蒐集利用該等國家於處理個人健康資訊安全中所獲得之經驗，作為 ISO 27001 之配套文件，惟 ISO 27799 實非取代 ISO 27002，而係補充此類較通則性標準。

ISO 29100 國際標準對資訊與交換技術系統（information and communication technology，ICT）中之個人可辨識資訊（personally identifiable information，PII）提供高階之保護框架，此隱私框架可助機構確認隱私安全保

護需求，ISO 29100 提供些可辨識個人資訊之標誌，此類標記可提供有用訊息以進行自然人之辨識，其可單一項目即可清楚進行個人辨識，例如社會安全號碼、護照號碼、銀行帳戶、電話號碼等或資料中可連結至該等項目而進行辨識，某些則可經由數個項目之組合而進行個人辨識，藉由 ISO 29100 所提之個人可辨識資料標誌，可提供機構或主管機關或法院來判斷個人資料保護是否完備，是否有隱私洩漏之虞，或去連結程序是否完備達到匿名之效果。

BS 10012 源於英國 1998 年資料保護法（The Data Protection Act 1998，簡稱 DPA），BSI 英國標準協會於 2009 年 6 月正式發佈 BS 10012：2009 個人資訊管理系統（personal information management system，PIMS），該標準具體說明對個人資訊管理系統之各項要求，並依據完整之 PDCA 循環流程，建立出一套完善個資保護框架和符合實務需求之個人資訊管理系統 [51]。「經濟合作暨發展組織」OECD 所揭示之保護個人資料八大原則，則轉化為控制措施，無論係自 OECD 隱私保護指導方針，或 BS 10012 之原則觀之，除要求資料持有者之保護責任外，皆更強調個人資料之自主控制與合理利用。

自個人資料保護法角度觀察，新版個人資料保護法要求保護個人資料之蒐集、處理、利用及國際傳輸，而 ISO 27001 所著重之部分多數在於個人資料「處理」階段，其主要要求係資訊管理安全，而自 BS10012 之原則以觀，除要

[51] 參閱英國標準協會網站：http://www.bsigroup.com/（最後瀏覽日：09/13/2016）

求資料持有者之保護責任外，皆更強調個人資料之自主控制與合理利用。

（三）小結

1.法規之檢討

2010 年我國制定個人資料保護法並於 2012 年施行，該法對公務機關或非公務機關於資料保管上，均訂有安全措施規定[52]，法務部則於 2012 年依該法第 55 條之授權訂定施行細則，關於安全措施內容，該細則第 12 條第 2 項則列出 11 款內容提供機構參考，各款內容乃基於與國際接軌，並以 P-D-C-A 方法論建立[53]。本文認為該條文內容確實將資訊安全國際標準之精神與概念納入，然細究其法規內容，則僅將國際標準規範之條文標題寫入，恐僅具資訊保護之外觀，而缺少實質性提高資訊保護之效果。

而該細則第 12 條所云「所欲達成之保護目的間，得包括下列事項」，條文中所指之所欲達成保護目的，係為誰所欲？倘為國家所欲達到之資訊保護目的，則應於母法中予以明確標準。如以個人資料保護法觀之，保護之目的應係第 1 條所提之「避免人格權受侵害」，然此目的誠屬空泛，尚難使蒐集處理或利用醫療資訊之機構能有所依循，倘該目的所指，非為國家之資訊保護目的，而係機構之資訊保護目的，則個人資料保護目標將不一致。有關目的強度之不同亦將影響維護資訊安全必要之措施設置，此為其一；

[52] 關於安全措施之規定，如個人資料保護法第 6 條第 1 項第 2 款所稱適當安全維護措施、第 18 條所稱安全維護事項、第 27 條第 1 項所稱適當之安全措施。

[53] 參閱個人資料保護法施行細則第 12 條立法理由。

再者，安全措施應有必須符合與得符合之差別，方能使資訊安全得到一定之保障以符合保護之目的，例如第 2 款「界定個人資料之範圍」應由法規命令明定之，而非由機構界定，機構僅需依循法規命令，進行所持有資料之盤點，及是否讓該資料列入保護之範圍，而第 4 款「事故之預防、通報及應變機制」涉及損害發生後之減少傷害，第 10 款「使用紀錄、軌跡資料及證據保存」涉及證據保全與責任認定問題，此兩款規定應列入必要之措施，不應僅係「得包括」，而第 9 款之資料安全稽核機制，應要求包括外部稽核，以確認資訊安全管理系統運作之無虞，此為其二；此外，該項各款之規定僅為「使各企業得參考所列之 11 款內容，考量組織規模與保有個人資料之數量或內容，依比例原則建立技術上與組織上之措施。」，而非明確規定機關組織應建構之安全措施[54]，個人資料保護法施行細則，其法律位階屬於法規命令[55]，依大法官釋字第 367 號解釋之意旨，授權命令應就執行法律有關之細節性、技術性之事項訂定，但不可逾越母法規定之限度，然以立法理由觀之，「得參考」、「考量組織規模……依比例原則建立……」等語詞之使用，該項各款之規定僅具建議性質，而非賦予法律上強制力以督促機關組織實施應有之安全管理，亦即該項僅

[54] 參閱法務部 101 年 9 月 26 日法令字第 10103107360 號令公布電腦處理個人資料保護法施行細則修正說明。

[55] 行政程序法第 150 條：「本法所稱法規命令，係指行政機關基於法律授權，對多數不特定人民就一般事項所作抽象之對外發生法律效果之規定。法規命令之內容應明列其法律授權之依據，並不得逾越法律授權之範圍與立法精神。」

具行政指導之事實行為效力[56]，縮減法規命令應有之強制性法律效力功能。

2.資訊安全管理標準之法制化

個人隱私權之保護周全與否，主要依賴法律涵蓋密度而定，無論 ISO 27001 抑為 BS 10012 之資訊安全管理，皆應以法律規定為依歸，亦即於法律許可範圍內，機構可裁量資訊安全之層次，個人資料保護法對資訊保護之規定應更明確，而非僅於資訊權利受損時處以懲罰，且應加強處理資訊之機構於內部管理之義務，方可落實保護資訊權利。自標準化之制定以觀，其攸關著經濟順利發展與否，倘標準化之制定可達保護公眾利益目的，政府則應容許甚至鼓勵制定該標準[57]，而資訊安全管理標準之法制化，亦復如此。蓋將標準法制化後，機構將有所依循及拘束，故本文建議持有管理特種資訊之機關，應賦予更重責任，將個人資料保護法施行細則第 12 條內容，列為允許進行特種資料蒐集、處理與利用之必要條件，輔導進行標準化之認證，經由常規之查核，以確保安全維護措施之正常運作。

建構安全資訊系統，有賴於管理者之支持與決心，於 ISO 27002、ISO 27002、或 ISO 27799 中皆強調此重要性，此要件非僅適用於機構，亦適用於政府對資訊安全管理之政策，參考國際標準方法、原則與框架，將其應用於資訊保護規範，將有利於資訊安全需求與保護標準之一致性，

[56] 行政程序法第 165 條：「本法所稱行政指導，謂行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為。」

[57] Carl Shapiro & Hal R. Varian, INFORMATION RULES-A STRATEGIC GUIDE TO THE NETWORK ECONOMY, 302-306 (1999).

則他律與自律之連結亦更為緊密，將可營造更讓人民信賴之資訊安全環境，方可達到個人資料保護法第 1 條促成個人資料合理利用之目標。

3.改善後之查核

落實資訊安全管理標準化，建立符合國際標準要求之管理系統，於 HFMEA 資訊安全問題類別中，總 RPN 值由 1122 降低至 438，改善率為 61%，而依八二法則選取之資安問題類別項目，總 RPN 值則由 899 下降至 291，改善率為 67.6%。

二、授權同意

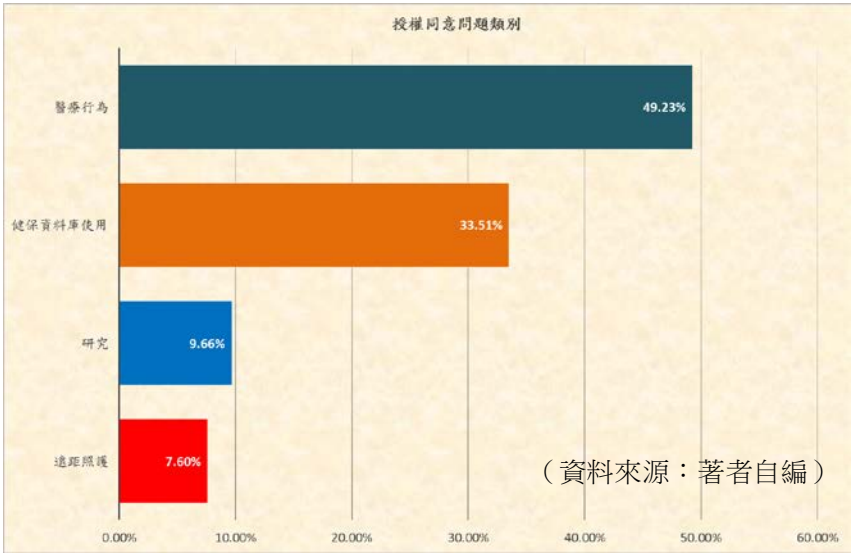
醫療行為過程為一互動、持續性之動態活動，於醫療資訊之蒐集上，通常難以先行確認所需資料之範圍，僅能採取概括同意，或事後同意方式[58]，以滿足形式上之授權同意，甚或診療過程中醫師僅表示「我查一下你先前的紀錄」後，如病患未立即表示拒絕即會著手進行資料查詢，更遑論先予進行說明再取得書面同意。我國個人資料保護法，對於進行醫療行為時所需之資料蒐集並無特殊規定，現行法規是否適合醫療行為進行之需要，是否能兼顧醫療行為所必需之資訊蒐集，以滿足醫療品質與正確性，且符合病患對隱私權與自主權之期待？

[58] 因個資法對「當事人書面同意」之要件，既無立法解釋，亦無立法意旨說明，故亦有學者自刑法對「同意」之概念及要件規範中分析，認為當事人之「同意」必須於行為前明示或從具體行為可得知，始有可能阻卻違法，若事後再表示承認或允許者，則不能發生承諾之效，只有經當事人事前同意，資料蒐集、處理或利用方有其合法性。參閱許文義，同前註 1，頁 239。

（一）問題分析

授權同意之相關問題，包含醫療照護、健保資料庫使用、研究與遠距照護等項目，於進行時之同意。由 RPN 分項類別之占率排序（如圖五）可知，為進行醫療行而蒐集、利用醫療資訊時，所造成之授權同意問題最高，其中多屬醫療資訊之間接蒐集，例如由雲端藥歷取得過去與現在用藥、經由電子病歷平台查詢他院紀錄、同醫療體系內之醫院進行跨院查詢、甚至為院內資料庫查詢，此占 49%；其次為健保資料庫使用時當事人同意問題，整體占率為 33.5%，該部分主要涉及健保資料目的外使用與資料去連結問題。其餘與研究相關之授權同意約占 10%，遠距照護資料取得之授權同意占 7.6%，研究與遠距照護之授權問題因各失效原因之 RPN 值均小於 24。

圖五 授權同意問題之類別



（資料來源：著者自編）

於個人資料之蒐集、處理與利用上，當事人同意之意義在於表彰個人對於個人隱私之自主控制，此乃隱私保護之基礎；我國關於資訊蒐集使用告知或同意，係採法律保留方式，由立法者先行制定，故需受較高密度保護規範。於醫療行為進行時，充分蒐集醫療資訊，為進行正確診治之必要過程，然一般醫療行為蒐集醫療資訊之過程，由 HFMEA 結果分析，有將近四成係因違反同意規定，而侵犯現行所賦予個人之資訊權利，此為除安全管理措施外，占率次高部分。故，如何調和資訊權利與順行醫療行為，並可兼顧隱私與醫療品質，實為不容忽視之課題。

（二）醫療行為之授權同意

關於進行醫療行為時，醫療資訊之蒐集與利用規定，個人資料保護法並無如同美國「隱私規則」中直接明列醫療行為可

免為當事人同意之規定，究竟於進行醫療行為時，欲合法蒐集利用病人醫療資訊之程序，應適用個人資料保護法第 6 條第 1 項但書中哪一款規定？如何踐行其合法程序？

關於病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料等，屬於敏感性資料，對其資料之蒐集、處理或利用，依 2016 年 3 月施行之個人資料保護法第 6 條第 1 項規定：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限」。

醫療機構於進行醫療行為時，欲合法蒐集利用醫療資訊，除第 6 條第 1 項第 6 款當事人同意外，是否可適用第 2 款規定而免為當事人授權同意？其關鍵乃於執行醫療行為是否符合法定義務。醫師法第 21 條僅規定「醫師對於危急之病人，應即依其專業能力予以救治或採取必要措施，不

得無故拖延。」；醫療法第 43 條則規定：「醫院、診所遇有危急病人，應即依其設備予以救治或採取一切必要措施，不得無故拖延」。至於對一般病人之診療行為並無規定，即使係危急病人，醫師應進行救治之規定，究係法定義務抑是強制締約？若從醫師法與醫療法之法體系、立法沿革與比較法制之經驗等以觀，對於危急病人之救治並非醫師之法定義務，而係強制締約義務，依舉重以明輕原則，一般診療行為更非醫師之法定義務，而醫師之救治義務非法律上之法定義務，僅係醫師執業之道德義務。

據上所述，依個人資料保護法第 6 條第 1 項規定，醫師進行醫療行為時，蒐集利用病人之醫療資訊並無執行法定義務之適用，因此，於進行醫療行為時之蒐集利用醫療資訊行為，仍須取得病人之書面同意，方符合個人資料保護法規定，而於取得同意前，因無個人資料保護法第 8 條第 2 項免為告知之適用，故須依第 8 條第 1 項之規定內容進行告知。

（三）小結

1、調和資訊使用與資訊自主

關於強化授權同意之改善對策，以醫療行為之資訊失效影響而言，似乎緣於法規上之無法適從，究竟醫療行為目的內之資料蒐集處理應採書面同意？或視為允許之意思表示，甚至為履行契約所必須而無須當事人之授權同意？倘以隱私權絕對之標準觀之，個人自主權之保障將優先於其他利益－包含公共利益或當事人利益，惟隱私權於我國雖屬基本權利，然仍屬相對性權利，於一定情形下可限制之，因此 HFMEA 之失效影響須與實際社會生活調和，即須

法規之明文規定，方解決法適用上之問題。

本文認為，醫療資訊因醫療行為而生，醫療行為復為滿足當事人健康需求而為，醫療資訊之蒐集利用，於本質上就不應與非醫療行為等同看待，惟個人資料保護法，對於敏感性資料之管制，似忽略此基礎關係，而把公務機關進行法定職務，統計研究等屬於醫療資訊建立所得之附加利益優先於進行醫療行為之主要利益，將醫療行為與其他業務如私人保險業務等同視之，完全忽略醫療資訊存在之原因與核心價值。

是以，醫療行為應當列為個人資料保護法第 6 條第 1 項但書除外條款之首位，於一般就醫情況，當事人至機構求診，於診療過程中提供自身疾病狀況等資料，或接受檢查等過程，於醫師法或醫療法中均規定須說明，方符合個資蒐集利用說明之要求，且當事人配合進行之行為，應足以之推定當事人同意係基於醫療行為之需要，故機構可蒐集利用醫療資訊。倘將醫療行為完全排除於須當事人同意外，如有隱私權侵害可能之疑慮時，此推定同意或擬制同意之形式，對於干擾醫療行為進行之影響甚微，而推定同意或擬制同意之立法，卻保留當事人撤銷同意之權利，至於緊急情況當事人意識不清，如非屬當事人意願之就醫情況，則適用緊急避難法理，以免除取得同意之義務，此方可兼及隱私權與醫療行為進行之順遂，至於資訊蒐集之最小需要原則，並不適用正當醫療行為進行時，以避免資訊完整性缺失，增加醫療不良之風險。

2、改善後檢討分析

若採行修訂醫療行為蒐集利用醫療資訊之規定，授權同意相關類別之總 RPN 值由 776 降低至 145，改善率為 81.3%；依八二法則篩選之授權同意類別，總 RPN 值由 615 降低至 15，下降率達 97.6%。無論係將醫療行為列為排除條款，或採推定同意之認可，或以契約之責任義務以放寬醫療資訊於醫療行為之蒐集利用，或為利益權衡考量及民眾之期待，應係可採之方式；雖 RPN 值下降達到預計目標，然於放寬簡化醫療目的使用程序下，對機構之安全管理措施要求應同時提高，並針對違反保密義務加重處罰，以平衡資訊管理或使用者之權利與義務。

三、目的外使用與明確性原則

健保資料庫之使用有其必要性，且需符合增進公共利益與資料活用之目的，就適法性而言，詳列資料使用目的之範圍內容，以杜絕爭議，此即須立法予以明確化。基此，事先之說明同意，或去辨識使資料成為數據，將自主權為合憲性之限制以達公共利益，且能兼顧隱私權等等，於目的外使用時，其適法性問題才能有所依循。

我國實施全民健保迄今，其龐大的健保資料，包含國民完整之健康資料、疾病、治療等重要且敏感資訊，行政機關持有此等資料時，當善盡管理職責並審慎使用此資料庫，亦須將資料處理過程及運用資料方式公開、透明化，以減少民眾對公務機關之疑慮，進而提升民眾對於政府保障隱私權的信心。

（一）問題分析

現行健保資料庫之設置，有財團法人國家衛生研究院「全民健康保險研究資料庫」，及衛生福利部「健康資料加值應用協作中心」，健保資料庫使用之最大爭議，係於此些特種資料蒐集目的是否符合明確性原則[59]與比例原則[60]，及資料利用是否合於蒐集之特定目的？另者，資料庫內容提供予第三者之法源依據為何？此爭議問題已有人民團體提出訴訟案[61]，藉以凸顯隱私權與自主權所存在之爭議問題。

可再進一步探究者，係健保署將資料傳輸至國家衛生研究院健保資料庫，或衛生福利部健康資料加值協作中心，對於個人資訊隱私侵害問題，主要地可能涉及不當揭露予第三方、資料被濫用及法律未有明確依據等問題，除了目的明確性問題外，資料去連結之處理是否符合法規標準，亦可能造成隱私受到侵害之原因。

另者，當個人資料將其內容中可辨識特定個人部分去除，或使該部分無法與其他資料進行連結以辨識特定個人資料後，所呈現者則僅剩數據，此已無法與特定個人相連結，自然亦與個人人格權無關，任何自然人資料如與特定個人間無最低限度「可辨別性」之連結性，此部分資料即應稱之為「統計數據」[62]，係屬新修正個人資料保護法第 6

[59] 行政程序法第 5 條：「行政行為之內容應明確。」

[60] 行政程序法第 7 條：「行政行為，應依下列原則為之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。」

[61] 請參閱，臺北高等行政法院 102 年度訴字第 36 號判決。

[62] 蕭奕弘（2012），〈論個人資料保護法的法制性問題〉，《成大法學》，23 期，頁 162-163。

條第 1 項但書第 4 款中，所提及之「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人」，故相關健保資料庫之資料處理是否符合該規定，亦值得重新檢視。

（二）健保資料庫使用

2012 年行政院衛福部依全民健康保險法第 16 條第 2 項，制定全民健康保險保險憑證製發及存取資料管理辦法，以為健保 IC 卡管理之規範，該辦法第 2 條明文規定，健保 IC 卡僅限於保險對象於保險醫事服務機構作醫療使用，於此範圍外之使用則均可能屬違法使用。此外，全民健康保險法第 16 條所授權之範圍，係對於健保 IC 卡之發給、資料存取與運用、使用管理及其他與健保 IC 卡有關事項，所上傳資料之使用並未於授權範圍內，然全民健康保險保險憑證製發及存取資料管理辦法第 15 條卻列舉上傳資料可利用之範圍，此部分因非授權範圍，且其第 4 款將利用範圍擴大至非健保業務，依該辦法第 15 條之規定，即已涉及逾越法律明確授權範圍之問題。

除了健康保險之相關業務外，中央健保署為達成國民健康資訊建設計畫（National Health Informatics Project，NHIP），遂成立「健康資料加值應用協作中心」，將全民健康保險所蒐集之個人就醫及醫療相關資料，提供予財團法人國家衛生研究院建置「全民健康保險研究資料庫」，以對外提供資料做為學術研究或生技相關產業發展之用，此就原資料蒐集目的為觀察，無論係為提供學術研究使用，抑或促進生技產業之發展，皆非健保相關業務，實屬特定目的外之利用。

醫療資訊為敏感性資料，原則上不得蒐集、處理或利用，然個人資料保護法第 6 條第 1 項但書，亦賦予衛生福利部或國家衛生研究院，可進行醫療或病歷資料之蒐集、處理和利用之權源。無論衛生福利部或國家衛生研究院所取得之健保資料，係來自醫療機構所提供而非來自當事人，因此，依個人資料保護法第 9 條規定，須盡告知義務並明訂告知之事項，惟上開情形已遁入其所列舉之 10 款不需告知例外。須注意者，前述規定均係針對蒐集目的內之使用所為，而目的外之使用，於公務機關須符合第 16 條但書規定，非公務機關則須符合第 20 條第 1 項但書規定，且此兩條文均將第 6 條之敏感性資料排除在外，因此，病歷或醫療資訊依個人資料保護法規定，無論公務機關或非公務機關，均不可進行蒐集目的外之使用。

新修正個人資料保護法第 6 條第 1 項但書第 4 款，所提及之「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人」，由該款規定推知，個人資料之處理須達無從識別之程度，始屬非個人資料保護法所保護對象，惟此處所指之無從識別究應達到何程度，需達到永久不能以任何方式連結或是僅為難以辨識即可，於母法及施行細則中均未有所規定。然而人體研究法第 4 條與人體生物資料庫管理條例第 3 條，皆要求去辨識或去連結，須達「永久」、「不能」以「任何方式」連結比對，倘僅為難以連結、辨識，則尚不符人體研究法與人體生物資料庫管理條例對去辨識或去連結所要求之程度。

（三）小結

1、目的外使用須符合明確性原則

大法官釋字第 603 號解釋指出，資料庫之建立須基於特定重大公益之目的、以法律明定其蒐集之目的、與目的有密切之必要性與關聯性，並應明文禁止法定目的外之使用、採取組織上與程序上必要之防護措施[63]。亦即，即使係基於重大公共利益目的下，對於隱私權之限制亦須符合明確性原則，並採適當防護措施以保障當事人之資訊自主權與隱私權，如此，方能合乎憲法保障基本權利之本旨，亦即對個人可辨識之資料使用，立法者須明確定義使用的目的，並限制其使用範圍。德國法院更進一步認為，於電子資料處理上之可能風險，行政單位間應禁止合作使用個人資料[64]；對於資訊蒐集使用之公益與個人資訊隱私權間之平衡，許宗力大法官與曾有田大法官於同號解釋之協同意見書中，亦對舊個人資料保護法所謂基於公共利益或為國家安全等理由，而將資料作目的外之使用提出批評，並要求公務機關對於個人資料之蒐集使用更應該確守明確性原則，避免使用空泛、概括之理由作為目的外使用之依據。

2、落實個人資料去辨識之妥善使用

倘資料庫之內容能確實去辨識，而非僅以加密變造使

63 大法官釋字第 603 號解釋文末段：「國家基於特定重大公益之目的而有大規模蒐集、錄存人民指紋、並有建立資料庫儲存之必要者，則應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成，具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。主管機關尤應配合當代科技發展，運用足以確保資訊正確及安全之方式為之，並對所蒐集之指紋檔案採取組織上與程序上必要之防護措施，以符憲法保障人民資訊隱私權之本旨。」

64 Douwe Korff, THE FEASIBILITY OF A SEAMLESS SYSTEM OF DATRA PROTECTION RULES, 53 (1999)；轉引自陳起行（2000），〈資訊隱私權法理探討—以美國法為中心〉，《政大法學評論》，66 期，頁 321。

資料難以辨識，除了可以消除民眾對於資料利用之疑慮，亦能確實排除個人資料之範圍，而更符合資料保護與妥善用之目的。

3、改善後分析檢討

落實個人可辨識資料去辨識，及資料使用符合特定目的之限制，改善前後之總 RPN 值由 200 降至 2，改善率達 99%，倘行政機關對個人資料之蒐集利用，能夠依據大法官釋字第 603 號解釋所示，與 ISO 29100 國際標準所強調之透明、公開原則與目的明確性原則，輔以資料利用之最小必要原則，並以去名化取代偽名化，才能於個人隱私保護之前提下，將資料利用最大化之成效。

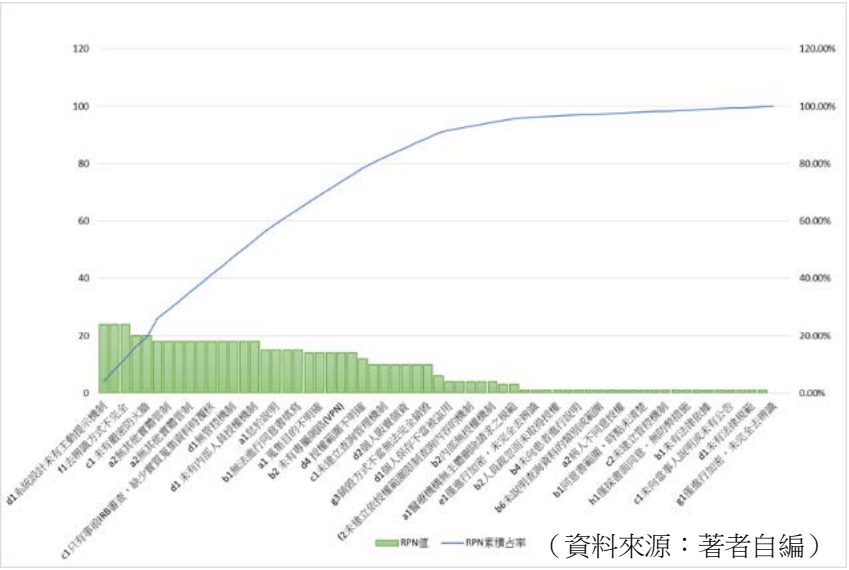
伍、結語

資訊科技之計畫性與經濟性運用，係為有效履行任務之基本要件，於其蒐集運用過程中，一方面帶來便利、迅速性，而有助於提升品質，然另一方面亦相對地引發基本權利侵害之危險。因此，於資料蒐集、處理、儲存、傳輸及利用過程中，如何界定出每一階段其侵害風險之高低，並尋求出解決方法即顯重要課題。

如本文研究，倘依 HFMEA 進行改善建議後，改善後 RPN 值之目標建議降低 50%以上 [65]；本研究所進行分析之流程，總 RPN 值由 2104 降低至 591，此降低 71.9%（圖六、圖七）；改善項目總 RPN 值亦自 1714 降低為 308，更降低高達 82%，此已達改善之目標值，依此進行之改善建議，將可有效減少隱私侵害可能之風險。

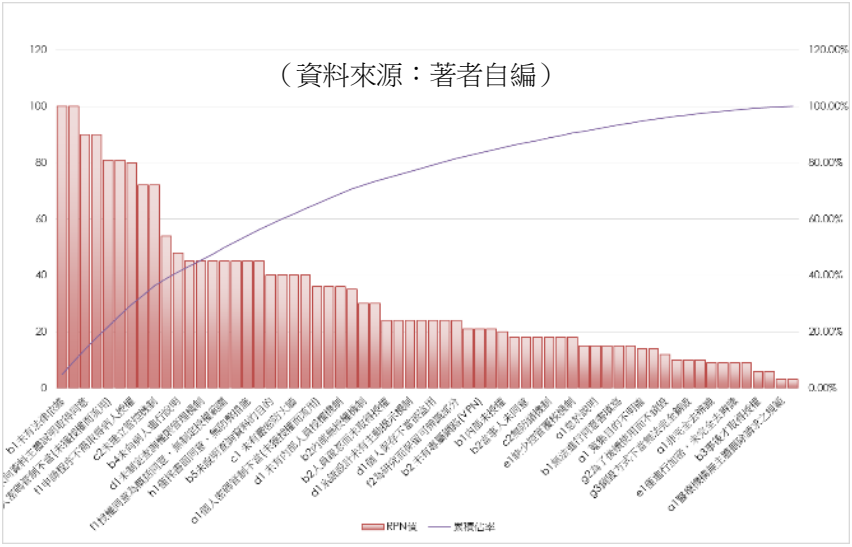
[65] J. DeRosier, E. Stalhandske, J. P. Bagian & T. Nudell, *Using health care Failure Mode and Effect Analysis: the VA National Center for Patient Safety` prospective risk analysis system*, 28(5) JT COMM J QUAL IMPROV, 248-267(2002).

圖六　改善前失效原因之 RPN 值



（資料來源：著者自編）

圖七 改善後失效原因之 RPN 值



（資料來源：著者自編）

法律與企業間之跨領域異業整合，對於問題較易辨明，進而使發生之真相容易釐清，尋找出解決良方。故，科際整合之功效，一則容易釐清問題源頭與關鍵，二則可藉由不同專業激發出加成效果，三則可藉由異業專業人才間之激盪與研發，進而創新與開創，四則可達資源共享之經濟效益。是以，跨專業合作，必能引導個專業化效果[66]。基此，本文即嘗試結合醫療照護失效模式及效應分析（HFMEA）及標準化，檢討並修正現行醫療資訊保護之法規範，藉由作業流程檢視法規之保護密度是否符合人民期待，產業是否已有足以依循之法規範，可做為內部管理品質之標準，藉由標準化之概念補充或修正法規之不足。

依此模式，非僅針對醫療資訊保護可系統性檢視改善現行法規之完整性，亦適用於多項行政法規，例如當前熱門食安問題、地方政府如何落實對個人資料保護之法令制定，皆可藉此模式聚焦立法方向。而醫療資訊之蒐集利用範圍相當廣泛，本文所進行之流程，僅係於一般性運作中之一部分，未來可更加深入討論者，尚有各項行政通報，例如傳染病通報、後天免疫不全症候群通報處理、青少年懷孕通報、人工生殖之通報及資料查詢利用、孕婦產檢資料上傳通報、新生兒先天性異常通報、藥物不良反應通報、司法協助與病人安全通報系統與醫療品質改善等等，皆有涉及個人醫療資訊隱私權之干預問題。

惟本文所採用之 HFMEA 模式，係依機構內實際流程狀況所完成，其中 RPN 排序與分數，於相異機構或不同組

[66] 施茂林，同前註 5，頁 18。

合，極可能產生不同結果，然於現行法規範下，對醫療資訊侵害之可能影響，應無明顯差異。尤以失效模式與原因類別化後再行檢討法規，此更可消除研究中，因對象差異或研究人員差異可能造成之誤差或偏差，所得之結果，當可作為強化資訊保護之參考。

參考文獻

一、中文部分

王勁力（2011）。〈新版個資法的衝擊影響：論我國公務機關對特種個資的管控與監督〉，《科技法律評析》，4 期，頁 63-110。

行政院衛生署（2007）。《建構以病人為中心之電子病歷跨院資訊交換環境案》，初版。台北：台灣醫學資訊學會。

朱樹勳（2013）。《醫療機構品質與病安管理—理念與實務》，初版。台北：華杏。

李震山（2011）。〈論資訊自決權〉，李震山主編，《人性尊嚴與人權保障》，四版。台北：元照。

李震山（2004）。〈法律與生命倫理－以基本權利保障為中心〉，《法官協會雜誌》，6 卷 2 期，頁 65-73。

宋珮珊（2010）。〈個人醫療資訊隱私保護之立法趨勢研究—以美國、加拿大為例〉，《科技法律評析》，5 期，頁 44-63。

芦部信喜著，李鴻禧譯（1995）。《憲法》，初版。台北：元照。

邱文聰（2009）。〈從資訊自決與資訊隱私的概念區分—評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，168 期，頁 172-189。

林子儀（2015）。〈公共隱私權〉，國立臺灣大學法律學院、財

團法人馬氏思上文教基金會編，《第五屆馬漢寶講座論文彙編》，頁 7-64。台北：翰蘆。

洪子洵（2013）。〈外國法與我國健保資訊應用之比較—以美國醫療保險可攜性及責任法（HIPAA）為鑑〉，《醫事法學》，20 卷 2 期，頁 28-45。

施茂林（2013）。〈法律風險管理體用矩陣與連動議題之研究〉，施茂林主編，《法律風險管理跨領域融合新論》，初版，頁 1-56。台北：五南。

許文義（2000）。《個人資料保護法論》，初版。台北：三民。

陳起行（2000）。〈資訊隱私權法理探討—以美國法為中心〉，《政大法學評論》，66 期，頁 297-341。

楊智傑（2014）。〈美國醫療資訊保護法規之初探—以 HIPAA/HITECH 之隱私規則與資安規則為中心〉，《軍法專刊》，60 卷第 5 期，頁 79-116。

蕭奕弘（2012）。〈論個人資料保護法的法制性問題〉，《成大法學》，23 期，頁 141-191。

蕭文生（1990）。〈關於「一九八三年人口普查法」之判決〉，《西德聯邦憲法法院裁判選輯（一）》，初版，頁 288-348。台北：司法周刊。

二、日文部分

開原成允、樋口飯雄（2005）。《醫療の個人情報保護とセキュリティ》，初版。東京都，有斐閣。

新美育文（2000）。〈個人情報保護基本法制大綱—アメリカ・EU との對比〉，《ジュリスト》，39 期，1190 號，頁 94-104。

三、英文部分

DeRosier, J., E. Stalhandske, J. P. Bagian & T. Nudell (2002). *Using health care Failure Mode and Effect Analysis: the VA National Center for Patient Safety` prospective risk analysis system*. The Joint Commission Journal on Quality and Patient Safety, 28(5), 248-267.

Shapiro, Carl & Hal R. Varian (1999). INFORMATION RULES-A STRATEGIC GUIDE TO THE NETWORK ECONOMY. U.S.A: Harvard Business School Press.

Terry, Nicolas P. (2012). *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC Law Review, 385.