

「智慧醫療與資料科學研究倫理與法律」紀要（中）

～ 臺大醫院倫理中心研究倫理研習會

整理 / 臺大醫院倫理中心 吳紫瑜、戴君芳

2023 年 12 月 8 日，臺大醫院於兒醫大樓 B1 講堂舉辦「智慧醫療與資料科學研究倫理與法律」研習會，邀請多位在醫療倫理及法律領域的重量級專家學者，就「智慧醫療研發趨勢與倫理考量」、「省思智慧醫療應有之法制典範革新」、「層級化的生醫個資利用法制」、「動態同意之實務與法律」、「資料科學研究之倫理審查思維」等議題進行研討。在前一期（2024 年 6 月第 2 期），我們已摘要「智慧醫療研發趨勢與倫理考量」、「省思智慧醫療應有之法制典範革新」講題之精彩內容，本期將針對「層級化的生醫個資利用法制」、「動態同意之實務與法律」兩個議題進行整理，業經講者確認內容，提供給讀者參考。

肆、層級化的生醫個資利用法制：演講者陽明交通大學法律學院院長陳鈺雄教授

111 年憲判字第 13 號「健保資料庫案」，可能成為帶動個人資料(簡稱個資)利用的法律發展及未來設立專責機關的契機，以應對數據驅動與數位醫療發展可能面臨的情況。在實務上，申請數位醫療相關計畫的 IRB 許可時，常會涉及或參照國外個資法中的相關主張，如歐洲通用資料保護規則（General Data Protection Regulation, GDPR）。例如，當個人資料僅進行假名化處理而未去連結時，仍需獲得當事人同意才能使用，甚至連進行去連結的行為本身也需得到當事人同意。然而，各國個資法對於這些處理手段的要求及條文解釋存在差異，在法律層面及個資概念上值得我們進一步探討。

我國憲判字第 13 號提及，「但由相關法制整體觀察，卻未見立法者依所保護個人資訊隱私權與利用目的間法益輕重及手段之必要性，而為適當權衡及區分，一律

未許當事人得請求停止利用」。意謂在個資利用上，需要進行層級化的思考。判斷層級化的標準，基本上運用比例原則。比例原則有三個要素：

1. **Purpose test (目的性原則)**：必須具有公共利益，而非只因為機構是公部門機構。
2. **Necessity test (必要性原則)**：必須是必要的手段，例如免除同意是達到目的所必要，無其他替代方案，不免除同意則研究可能無法進行。
3. **Balancing test (狹義比例原則)**：公共利益大於個人隱私權。

比例原則在不同國家的認定上實際上存在差異。以 2005 年南韓和台灣對於民眾取得國民身分證是否需要按捺指紋的問題為例，兩國的大法官均認為指紋屬於敏感個人資料，應適用比例原則。然而，兩國的判決結果卻恰恰相反。南韓認為：指紋在處理大量犯罪案件或無名死者時，其公益性超過了對個人隱私權的限制，符合比例原則。而台灣則認為這樣的措施過於嚴苛，不符合比例原則。顯示比例原則在具體個案中，各國對於利益衡量的看法有所不同，從而導致個資法上的差異。各國對於不同類型的生醫個資，也有層級化的看法與其認定標準，依資料敏感度大致可分為以下三種：

1. **健保資料 (Health Insurance Claim)**：屬於低敏感程度的生醫資料，因資料揭露的訊息較少。例如，可能知道做了 X 光檢查，但不知檢查內容；知道進行了肝臟測試，但無法取得測試數據。在某些國家，如德國這類資料有時可以免除知情同意。
2. **電子病歷 (Clinical Data)**：電子病歷因資料量龐大，多數國家通常採取選擇退出 (opt-out) 的方式。例如，英國有相關的 opt-out 規範，而澳洲則使用雲端平台，允許用戶選擇是否允許特定機構獲取研究資料。對於資料匿名化的部分，大多數國家並不要求在進行匿名化處理前需獲得同意。少數國家如日本，根據《次世代醫療基盤法》，要求醫院在進行資料匿名化處理前需先通知病人。如果病人在通知後的一段時間內未提出退出要求，醫院才能進行匿名化處理並加以應用。目前我國尚未有關於選擇退出相關的法律規範，因此在 IRB 的審查過程中，無法要求研究者使用這種方式來取得同意。
3. **特殊型態生醫資料**：屬於高度敏感的生醫資料，包括基因體資料 (如全序列基因體資訊)、心智資料，以及像愛滋病、SARS 等致命性傳染病。由於這些資料涉及的風險較高，許多國家原則上會採取積極同意的方式。

同意權的考量因素

根據 GDPR 第六條規定目的的相容性，即二次利用的目的必須與最初收集的原始目的具有相容性。有些因素可能與當事人的利益產生衝突。例如，透過罪犯的日記發現其犯罪行為，這與當初撰寫日記的目的相悖。在這種情況下，除了考量目的的相容性外，還需考量公共利益的因素。目的的相容性不是一種絕對原則，而是需要在公共利益的框架下進行評估。GDPR 第五條(b)89 條第一項指出，「為達成公共利益之目的、科學或歷史研究目的或統計目的所為之進階處理，不應視為不符合原始目的(目的限制)」。因此，學術研究通常都符合目的的相容性原則。此外，GDPR 中也提到了資料保存的規範。如果原始目的已經達成，但資料有其他合法的進階利用目的，例如學術研究，則可以在符合 GDPR 規範的前提下，延長資料保存的時間，以便用於學術或其他合法目的。

在生醫領域中，同意權的本質是一個值得深入探討的議題，究竟同意權應該被視為個人權益，還是集體權益？有些資料是屬於個人化的，例如醫療健保資料和臨床資料，但與基因體相關的資料或研究結果可能會對特定群體產生效益，這就涉及集體同意權的問題。顯著的例子包括《人體研究法》第 15 條中，其中規定「以研究原住民族為目的者，除依第十二條至第十四條規定外，並應諮詢、取得各該原住民族之同意；其研究結果之發表，亦同。前項諮詢、同意與商業利益及其應用之約定等事項，由中央原住民族主管機關會同主管機關定之」。意味這個利益的本身屬於全體權益而非個體權益。

哈佛大學法學院 Glenn Cohen 教授對於同意權，提出了「分享義務」(Duty to Share) 的觀點。Cohen 教授主張，對於電子健康紀錄，當政府或醫療機構為了促進公共利益且在確保不為再識別的前提下，個人對其健康照護資料並不擁有所有權。這裡所指的不為再識別行為，指的是法律上的去識別化。相較之下，台灣所談及的去連結或假名化通常僅涉及資料本身的狀態，並未考慮到契約條款加入後，整體環境下的假名化。在所有的個資法中，包括 GDPR 等，皆未對個資的所有權進行明確定義。普遍的認知是，個人對於資料本身並不擁有所有權，而是擁有隱私權。Cohen 教授認為，個人資料本身的價值並不高，其真正的價值在於資料經過聚合後所顯現出的群體價值，而健康資料的特性，其公益性遠大於個人去識別後的資料價值。Cohen 教授並提出了「社會對等性」的概念，認為個人資料提供者可能因為自己提供的資料而受惠。科學的進步以及個人醫療資料的產生，都是建立在健保和醫

療體系所提供的資源之上。取得個人醫療資料的過程中，所獲得的實質上並非資料本身，而是依賴於累積知識所形成的診斷。因此，從社會對等性的角度來看，Cohen 教授主張應承擔「Duty to Share Health Data」。

獨立監督機制

當數位資料在不同機關之間流轉時，必須依賴可信賴的機制以確保資料的安全和正當性。憲法判決第 13 號中則強調「獨立監督機制」在資料移轉過程中的重要性，判決指出此一獨立監督機制之目的在於確保個資蒐用者對於個資之蒐用，均符合相關法令之規定，以增強個資蒐用之合法性與可信度。判決提及審酌事項尤應包括特予注意個案利用之申請，其具體情狀是否合於比例原則。此判決旨意並非要設立獨立專責機關，而是要建立一個獨立監督機制，以確保個資的使用符合相關規範和比例原則。個人認為 IRB 即為一種獨立監督機制，但憲法判決第 13 號對於 IRB 的角色並未提供較為充分的說明，而歐盟則使用「Research Ethics Committee」來指代類似的機構，歐盟的研究倫理委員會多數設置於機構外，屬於政府層級，具有官方色彩，其主要功能是監督是否存在實驗偏差行為，以及審查個案是否符合比例原則。

值得進一步探討的是：IRB 組織的結構與組成方式，是否具備審核個資和資安的專家。在美國《健康保險流通與問責法》(HIPAA) 的法律規範中，除了 IRB 角色外，另設有 Privacy Committee；在以下四種情況下，可以免除法定同意：

1. 獲得 IRB 同意和 Privacy Committee 同意 (比例原則)
2. 研究前的準備 (比例原則)：資料僅用於準備機構間之研究契約或為研究做類似的準備工作，比如招募受試者。在此情況下，研究人員不得從醫療機構中移走任何受保護的病歷資料，並且受保護病歷資料對研究目的是必要的。
3. 亡者的個資：根據 HIPAA 規定，人死後 50 年內其個資仍受隱私保護，若能獲得家屬同意，則不受此限制可以進行相關研究。
4. 高度假名化的資料 (Limited Dataset) (匿名化的實質等同)：部分研究可能需要連結性資料來證明研究對象的身份，因此無法完全去除識別，在這種情況下，即需使用高度假名化處理來保護資料的隱私。

匿名化的實質等同

假名化是否可以免除同意，涉及到資料與病人之間的關聯性。以一個著名的

John Moore 案為例，在案件中 Moore 在接受加州大學洛杉磯分校醫療中心的白血病治療時，他的癌細胞被發展成一個細胞株，由醫師和該醫院及大學進行商業化並從中獲利數百萬美元。Moore 隨後提起訴訟，主張對這些檢體擁有所有權，經加州最高法院裁定：醫院和研究人員從 Moore 的血液和組織樣本中獲得的商業產品不屬於 Moore 的個人財產，Moore 也無權分享這些商業化產品或研究所帶來的利潤。法院認為，考慮到生醫研發充滿風險，個資尚未被商業性利用之前，沒有任何人擁有所有權。從權力分立角度來看，此問題應由國會而非法院來決定。法律對於個資的保護在於隱私權而非所有權。

假名化對隱私的影響，在於可能發生的再識別行為，造成對病人的隱私造成侵害的風險。如果在特定的使用環境和法律約束下，能夠有效防止再識別行為的發生，那麼假名化和匿名化對隱私的影響其實是等同的。過去在台灣的相关討論中，未充分考慮假名化與環境中匿名化及法律上匿名化條件的結合。例如，在封閉的環境中，若僅允許查看結果而無法接觸原始個人資料，也無法將資料帶走，這樣的運作模式可以有效防止數據串接，從而顯著降低再識別的風險。在此情況下，該環境可能可以在法律上被視為等同於匿名化。

聯邦學習 (Federated learning) 在國內常被認為沒有同意權的問題，對於強調同意權重要性的人來說，即使資料僅在醫院內部進行處理，若資料尚未匿名化，仍需獲得當事人的同意，包括醫院內部的研究也不例外。這樣的要求會影響聯邦學習的實際應用。新的隱私強化技術能否合法利用，取決於我們對匿名化的定義是否能達到實質等同的標準，而不再需要獲得當事人同意的情況下進行合作。此外，這也取決於對比例原則的判定，即再識別風險是否可以降低到實質等同於匿名化的程度。

根據美國 HIPPA 規定，去連結資料的標準包括「不得再還原回溯至個人」包括「技術上不得再識別」以及「法律上不得再識別」兩種情形。HIPPA 定義，當去除所有 18 種識別因子後，符合法律上的去識別標準； Limited Dataset 的定義則為去除 16 種識別因子，可保留兩種識別因子事做連結，但 Limited Dataset 資料僅能用於特定用途，例如醫療機構的運作、公共衛生或其他研究，並且使用者必須簽訂資料分享契約，簽契約負有不得再識別義務、任何拿到該資料的下一手也會遵守相同的承諾、不得連絡病人、採用資安保護、資料外洩時有通報義務。這些法律規範使得

在美國使用個資相對較為便利，儘管技術上可能無法實現完全的去識別化，但透過法律約束，能夠實現實質上的去識別效果。

另以歐盟法院判決為例，該案件涉及金融領域而非生醫個資，但金融資料也具有相當的敏感性，並且法院在判決中明確闡述了“去識別化”的定義。該案件為2014年歐盟通過《單一決議機制條例》後，該條例建立「單一清算委員會」(SRB)，負責處理西班牙大眾銀行的破產清算工作。SRB將一些資料假名化後，交給勤業眾信事務所進行分析。部分股東和債權人對此表示不滿，認為此資料分享行為應取得他們的同意，因此向主管機關提起訴訟。法院裁定，假名化資料的再識別風險應從資料接受者的角度來判斷。如果假名化的編碼未被公開，且接受資料的機構無法再識別，則該資料仍被視為個人資料，但可視為匿名化資料，此見解與HIPAA去連結的定義相符。法院也指出，不得再識別有兩種情形，包含法律上不得再識別和技術上不得再識別，並認為兩種均屬匿名化資料。

未來對於匿名化或去識別化的定義應考慮使用環境與法律約定。對於我國未來在個人資料利用方面，將提供更好的參考和指導。

伍、動態同意之實務與法律：演講者陽明交通大學醫學院副院長 吳俊穎教授

人工智能科技在醫療領域引入，引發了對病患知情同意問題的討論。人權團體正在推動「動態同意」(Dynamic Consent)，認為這種方式能更充分地保障病人的知情同意權。在探討其適切性之前，需先了解相關研究類型及法律規範的程度。

「人體研究」不僅涵蓋臨床實驗、新藥開發、新醫療技術或醫療器材的研究，還包含人工智能和智慧醫療的應用，涉及原始醫療資料的蒐集或次級醫療資料的利用。此外，其他非醫療領域的研究，例如犯罪學、心理學和法學等，也同樣納入此範疇。這些研究可以根據其對健康權和生命權侵害的程度，以及對自主權的侵犯程度來進行分類。

需要進行干涉 (Intervention) 的研究，不論是醫學試驗中的人體試驗，或是非醫學相關的試驗，對於健康權和生命權的潛在侵害，通常遠大於純粹的資料庫分析。資料庫分析可細分為原始資料庫及次級資料庫兩類。原始資料庫的收集包含人臉辨識、肢體動作監測、智慧手錶血糖監控等；而次級資料庫則涵蓋醫院電子健康紀錄、醫院資料庫分析；同樣是資料庫分析，對於健康權、生命權的侵犯可能性極

小，但對自主權的侵犯風險，原始資料庫的蒐集還是遠大於次級資料。根據對於自主權、健康權 / 生命權侵害可能性越高，應有更高的法律規範的密度。然而，實際情況中，台灣對於人權侵害風險較高的領域立法雖較早，但相應的規定卻往往較為寬鬆。

人體研究範疇及規範密度：

以下依據重要法條進行人體研究範疇及規範密度的探討：

1. 人體研究範疇

人體研究法第一條：「為保障人體研究之研究對象權益，特制定本法。」此法旨在保護人體研究對象權益，而非僅針對以論文發表為目的的研究進行規範。從法學角度來看，智慧醫療中如人臉辨識等臨床應用，即使是以人體為研究對象，也必須受到相應的法律規範。

人體研究法第四條將人體研究定義：「指從事取得、調查、分析、運用人體體或個人之生物行為、生理、心理、遺傳、醫學等有關資訊之研究。」Google 資料庫中的研究，例如人員移動分析、廣告試驗中使用不同字體、顏色和位置的點擊率測試，均可視為人體研究。這類研究並非僅限於醫療領域，而是所有以人體作為研究對象的實驗都應被視為人體研究。

2. 規範密度

人體研究法第二條：「人體研究應尊重研究對象之自主權，確保研究進行之風險與利益相平衡，對研究對象侵害最小，並兼顧研究負擔與成果之公平分配，以保障研究對象之權益。」人體研究法強調，除了尊重研究對象自主權外，還必須確保研究結果及其利益分配的公平性。需要區分研究的公益性或私益性，明確研究結果的分配方式是平均分配予研究對象，還是歸於研究者，並依此制定不同的規範密度。

人體研究法有不同規範的密度，具體表現在個人資料保護法第六條的敏感性個資上。通常，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。而公益或是學術研究機構，得有相對寬鬆的規範，可基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，取得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資料。

國外法條概念亦是如此。以被認為最嚴格的個人資料保護法 GDPR 為例，其第 89 條規定：當研究旨在追求公共利益的科學研究時，這些研究可以在一定程度上不

受 GDPR 中許多個人資料保護規範的限制。GDPR 上路後，受罰對象多為商業團體如 Google 和 Facebook 等，這些公司在收集和交易個人資料後進行販賣等行為，通常被認為是無效的同意。這表明不僅僅是進行研究的活動需要遵循人體研究法或個資法，商業團體的活動也同樣須受到相關規範的約束。

何謂「同意」？

GDPR 定義「同意」必須是出於自願的、具體的、知情的，並且明確表示意願。進行任何研究的更改，包含更改研究目的、方法，皆必須進行告知。知情同意有三大要件：

1. 告知：

研究者以研究對象可以理解的方式，提供充分醫療資訊。判斷基礎：研究參與者獲得與充分而正確與研究相關的資訊，從而得以對自身的研究參與行為做成決定。

2. 能力：

研究對象具有足夠的理解與判斷能力判斷基礎：研究參與者是否真正理解其所參與之研究的研究目的、研究方法、可能的研究結果、可能的？

客觀因素如年齡和是否喪失行為能力等，都可以用來判斷一個人是否具備理解研究內容的能力。倫理審查委員會（IRB）或類似機構可以評估這些因素，以確保參與者能夠理解研究的目的、風險，並且在知情的情況下給予同意。

研究主題必須清晰地表達，舉例來說，以“肝癌手術前影像 AI 分析以預測病患預後”為例，研究者需要具體說明使用的是哪種機器學習方法。此外，必須確保病患能夠充分理解這些方法的基本概念和研究過程。例如，研究中如果涉及判斷肝臟纖維化的程度並區分肝硬化，則需向病患解釋這些診斷標準之間的區別，以確保他們對研究內容有充分的了解，病患才能在完全知情的基礎上給予同意。

3. 自願：

研究對象不受身體約束、心理威脅、及資訊操控，而自發性的做成意思決定。知情與同意需同時達成，只有在對象能夠理解所提供的資訊並且明確同意的情況下，同意才被視為有效。

動態同意法律規範密度與實務困境

「動態同意」並不等同於「數位同意」。數位同意僅是與書面同意採用不同型態的執行方法，介面由原來的紙本形式更改為數位方式簽署同意書，提供更便捷的溝通操作流程。動態同意是指在付諸實施之後，因應研究細節的不斷變化(如特定目

的、特定方法、特定操作流程、相關的風險以及預期效益等)，據此進行重新告知並不斷滾動地進行「動態特定同意」。

「動態同意」相對於「概括同意」及「特定同意」，其規範密度因法律針對侵害可能性的不同而有所區別。過去，在原始資料庫或是次級資料庫的蒐集，簽署同意時多採用概括同意，授權機構和研究者使用資料。資料庫分析隨時可能出現許多新的研究方法、目的和方式。對於比較高風險的醫療行為、人體實驗等，涉及自主權或傷害的可能性，則需要特定同意。而動態同意的法律密度則遠高於特定同意，因只要研究方法、目的等發生變更，就需持續不斷地進行特定同意，屬於最嚴格的法律規範密度。

現今要求風險較低的次級資料研究採用動態同意，實際上是倒置了法律規範密度。動態同意實務面與法律面的困境，主要在於加諸學者與產業界過重之程序負擔，實際上有其窒礙難行之處。從病患角度來看，參與者可能缺乏足夠的專業知識和經驗來完全理解相關說明，可能會盲目同意，導致同意結果自始無效。此外，參與者在同意研究後，若需要不斷地反覆接受告知和重新同意，將會造成無窮無盡的困擾，並可能促使他們行使退出權。

AI 智慧快速發展，且會從速醫療產業界，此時法律如何規範此大數據與智慧的發展是非常重要的議題，故對此研究結果公平之分配性，會決定法律規範的密度。同時對於健康安全侵犯的可能程度，也是規範密度重要的考量，動態同意不同於數位同意，以動態同意規範大數據及人工智慧的發展，顯然違反法律規範密度的原則。