從人工智慧基本法邁向值得信任的數位健康生態系：健康數據創新治理沙盒之方向初探[1]

劉汗曦*

壹、前言：AI基本法通過後之數位醫療治理新局

一、立法背景：全球AI技術與法制競賽

隨著生成式人工智慧（Generative Artificial Intelligence）等AI科技的爆發性成長，世界各國政府無不積極推動立法以因應此潮流。我國也在2025年12月23日年底，正式三讀通過**《人工智慧基本法》**，宣示性的將台灣帶入AI法制化年代。[2]

雖然這部基本法的通過，可視為台灣AI法制發展的關鍵性里程碑，並且該法的規範目標是期望在產業發展與風險管控之間取得平衡點。[3]但徒法不足以自行，對於涉及高度敏感、生命身體安全的醫療領域資料治理而言，基本法的條文多僅具備宣示性、框架性的骨架規範。具體執行的細節血肉，仍有賴主管機關──衛生福利部──在個人資料保護法、健保資料管理條例、醫療法及人體生物資料庫管理條例等交錯的法網中，織就出一套具體可行的落實方案。[4]

二、核心問題意識：數據孤島與信任赤字

「數據是新時代的石油」（Data is the new oil）。對於AI的發展與應用來說，數據確實是推動這部龐大機器的關鍵燃料。然而，這句來自產業界的諺語很容易讓人們忽略了一些本質上的差異：石油是種天然資源，可以開採與買賣，並且會因為使用而消耗，所以是有稀缺性之交易標的；但個人數據（Personal Data）源自於人的主體，承載了人

＊本文作者係喬治城大學法學博士，陽明交通大學公衛博士，政治大學創新國際學院兼任助理教授，執業律師。

註1：本文改寫自作者2025年12月23日「2025台灣人工智慧及精準醫療之發展暨法治論壇」之專題演講「台灣健康數據治理的現況與挑戰」內容。作者特別感謝主辦單位台灣醫事法律學會及國泰綜合醫院之邀約，與談人姚念慈法官及黃國光牙醫師的評論，以及全國律師聯合會醫藥與健保法制委員會胡峰濱主委的鼓勵。

註2：數位發展部（2025），數位發展部發布「人工智慧基本法」草案，數位發展部全球資訊網，https://moda.gov.tw/press/press-releases/18316（最後瀏覽日：2026/01/12）。

註3：同前註。

註4：同前註。

格權與隱私期待，並且資訊本身可以無限複製、傳輸的特性，一但被濫用風險危害更大，亟需有好的風險控管。

因此有論者以「大樓建設」為喻：若將AI的應用成果視為眾人渴望爬上的大廈頂樓（Penthouse）按鈕，從下而上的各個樓層，如數據品質（Data Quality）、元數據治理（Metadata）、數據血緣（Data Lineage）與所有權模型（Ownership Model），則是讓大樓能夠穩固不搖的基礎建設。[5]欠缺了這些基礎，原先掌握在不同單位、不同部門的數據，就會因為欠缺信任、法規限制等因素而拒絕或無法順利地進行數據整合、交換或共享，而形成彼此隔離、欠缺可交換性「**數據孤島**」（Data Silo）。[6]

以台灣為例，雖然我們擁有舉世聞名的全民健保資料庫，這本應是發展精準醫療與AI模型的巨大優勢。然而遺憾的是，台灣目前的健康數據治理，就面臨著「基礎不穩」的危機。憲法法庭111年憲判字第13號判決（以下簡稱「釋判13號」）就明確指出，我國在健保資料庫之「目的外利用」上，缺乏獨立監督機制，且未賦予當事人退出權（Opt-out），宣告部分違憲。[7]這不僅是法律層次的違憲宣告，從長達十多年的訴訟與公民團體的抗爭中我們可以看出，這是整個台灣社會對於數據治理的「信任赤字」之司法認證。[8]

三、本文主張

本文認為，面對AI時代的挑戰，傳統法制下的數據治理模式已難以為繼。此時主管機關應依照人工智慧基本法之精神，率先建立「風險分級（Risk-based Approach）」制度與「法規沙盒（Regulatory Sandbox）」，解決數據孤島與信任赤字的雙重困境。唯有透過制度設計重建「數位信任（Digital Trust）」，台灣的智慧醫療才能從口號走向實踐。[9]

以下將先爬梳台灣健康數據治理的現況及困境，接著透過以英國為主的比較法經驗來強調透明與問責對信任建構之重要，最後則從「風險分級」與「創新沙盒」的角度出發，嘗試提出建構衛福領域資料治理法制之新方向。

註5：John Wernfeldt, So true-plenty of budget for the PH nothing, LINKEDIN (2025), https://www.linkedin.com/posts/courtlinholt_so-true-plenty-of-budget-for-the-ph-nothing-activity-7404092792152481792-WX1S/ (last visited 2026/01/12).

註6：關於數據孤島在醫療領域的定義與挑戰，參見Edd Wilder-James, Breaking Down Data Silos, HARV. BUS. REV. (Dec. 5, 2016); 亦可參見Fei-Fei Li et al., Artificial intelligence for medicine: Progress, challenges, and perspectives, 26 NATURE MEDICINE 16 (2020)（指出數據孤島是阻礙精準醫療模型訓練的主要技術障礙）。

註7：憲法法庭111年憲判字第13號判決，https://cons.judicial.gov.tw/docdata.aspx?fid=38&id=309956

註8：台灣人權促進會，健保資料庫釋憲案，台灣人權促進會官網，https://www.tahr.org.tw/cases/NHID（最後瀏覽日：2026/01/12）。

註9：關於數位信任的論述，參見：劉汗曦（2022），〈從數位憲政與數位信任看我國健保資料庫的爭議與使用〉，《月旦法學》，331期，第37-53頁，https://tpl.ncl.edu.tw/NclService/JournalContentDetail?SysId=A2023001314

貳、台灣健康數據治理的現況與困境

一、數據治理的斷裂：三個不等式

檢視台灣目前的健康數據治理地景，可以發現明顯在治理規範上之破碎化現象，筆者將其歸納為三個治理上的「不等式」：

（一）「健保資料≠衛福資料」

由於釋判13號之要求，行政院在2025年5月15日向立法院提出「全民健康保險資料管理條例」草案（以下簡稱「健保條例」）。並在國會經過半年的激烈討論後，於12月2日三讀通過並經總統於同月19日公布而正式完成立法。[10]

然而本部健保條例所規範的，只限於「全民健康保險保險人為辦理保險業務，依全民健康保險法所蒐集、處理之資料」，也就是外界俗稱「健保資料庫」（National Health Insurance Research Database, NHIRD）。但實際上學界、甚至產業界更常使用的，是被稱為「資科中心」的衛福部衛生福利資料科學中心之相關資料庫。其中包括了衛福部直屬單位（如醫事司、社保司）與附屬機關（疾管署、國健署、社家署）約百項衛生、社福、統計資料。

這些可以被統稱為「衛福資料」的數據資料，包括出生通報檔、死因統計檔、癌篩資料庫、癌症登記檔、低收入戶及中低收入戶檔、家暴通報明細檔等。然而這些同樣具有高度價值且具敏感性的個人資料，卻不在本次通過的健保條例規範範圍內，因此未來是要類推適用、比照辦理呢？還是急需另外制定一部「衛生福利資料管理條例」呢？仍有待行政與立法機關的後續行動，已解決此一「法律真空」之問題。[11]

（二）「衛福資料≠所有健康數據」

然而，即便是近百個衛福資料庫整合成的資科中心，還是無法涵蓋國人健康數據的全面。例如由人體採集如細胞、組織、器官、體液等生物檢體所構成的「人體生物資料庫」，從2003年中研院開始規劃成立迄今，已經有39個由醫院、學校、機構所設立的biobank，總計收案人數已超過百萬，就是一個非常巨量、價值巨大的健康數據。[12]除此之外，國內各大醫學中心幾十年來累積的病歷相關資料，在幾乎已經數位化、電子化之後，亦是另外一塊極為可觀的健康數據。[13]

另外，隨著物聯網（IoT）與穿戴式裝置

註10：總統府公告，中華民國114年12月19日華總一義字第11400129981號，https://www.president.gov.tw/Page/294/50094（最後瀏覽日：2026/01/12）。

註11：其實衛福部最早於2024年3月1日所提出的為「衛生福利資料管理條例」草案，是將衛福資料涵蓋在內。但送行政院後經過行政院內部討論後，決定限縮適用範圍並同步將名稱變更為「全民健康保險資料管理條例」。參見：衛生福利部，預告制定「衛生福利資料管理條例」草案；衛生福利部全球資訊網，2024年3月1日，https://www.mohw.gov.tw/cp-18-77823-1.html（最後瀏覽日：2026/01/12）。

註12：衛生福利部醫事司，人體生物資料庫設置情形，衛生福利部全球資訊網，https://dep.mohw.gov.tw/doma/cp-3133-12824-106.html（最後瀏覽日：2026/01/12）。

註13：臺北醫學大學數據處，健康數據庫介紹，臺北醫學大學網站，https://ods.tmu.edu.tw/portal_c3_cnt.php?owner_num=c3_69585&button_num=c3&folder_id=4165（最後瀏覽日：2026/01/12）。

（Wearables）的普及，大量的健康數據（如Apple Watch的心律與EKG資料）散落在民間企業、跨國公司或個人手中。這些真實世界數據（RWD）對於訓練高品質醫療AI至關重要，但目前仍缺乏有效數據整合與治理之架構。

（三）「個資主管機關≠獨立監督機制」

當然，論者或許會認為，個人資料保護法（以下簡稱「個資法」）應該可以作為治理之框架與問題的答案。然而這一層曖昧不明的法治面紗，某方面已經被釋判13號所拆穿…現行個資法本身，並不等同於一套合乎憲法保障民眾資訊隱私權之獨立監督機制。

特別我們可以看到，雖然個資法修法後將主管機關從國發會轉為個人資料保護委員會這個專責機構，但該專責機構的籌備處牌子一掛掛兩年以上，組織條例卻仍然躺在立法院不知道何時能夠通過、何時能夠施行。[14]更重要的是，即便是現行個資法組織條例草案能通過，依照該草案所規劃的人力與資源，實在很難倚賴該機關來承擔所有健康數據利用的獨立監督重責大任。[15]而是有賴於真正進行健康資料搜集、處理、利用的單位，如各學術機構或醫療院所建立倫理委員會一般，自行建構一套獨立的資訊治理監督機制，該機制並應接受外部的規範約束與查核監督，方能更有效的執行法遵、保障權益。

二、信任赤字的實證觀察：三個本土案例

事實上，前述所提到的幾個治理斷裂，並非僅存於學理上的分析與討論。近年來發生的幾件重大社會爭議，就是民眾對於健康數據利用上的信任赤字實例。

（一）憲法訴訟案：對「目的外利用」的集體焦慮

早在2012年，台灣人權促進會等民間團體便發起「還我資訊自決權」運動，質疑健保署在未經當事人同意下，將全民健保資料以抽樣檔案光碟釋出等方式，提供給學術機構進行研究。[16]這場長達十年的法律戰，最終在2022年迎來釋字13號判決。雖然大法官肯認了個資法條文適用的合憲性，但也嚴厲指責現行法制缺乏「獨立監督機制」及未能給予民眾「退出權」，導致民眾對於自己的數據如何被使用、流向何方一無所知、並無法

註14：行政院（2023），行政院會通過「個人資料保護法」第1條之1、第48條、第56條修正草案，行政院全球資訊網，https://www.ey.gov.tw/Page/9277F759E41CCD91/fec13417-8626-466f-a59d-cclaaee75a25（最後瀏覽日：2026/01/12）。

註15：行政院（2024），行政院會通過「個人資料保護委員會組織法」草案，行政院全球資訊網，https://www.ey.gov.tw/Page/9277F759E41CCD91/747cda78-926f-4205-99b3-1a735fc1b97b（最後瀏覽日：2026/01/12）。

註16：台灣女人連線（2022），〈這「健保」料，按怎判？──在釋憲前夕，破全民「利用」？〉，台灣女人連線官網，https://twl.twh.org.tw/article/zhe-jianbao-liao-anxuanpanzaiji-poquanmin-liyong（最後瀏覽日：2026/01/12）。

行使資訊自主權來退出，形成了「強迫全民參與研究」的違憲實務。[17]這樣的集體焦慮其實並未隨著草案的推出以及通過而停止，相反地，民間團體對於現行的條例與實務操作，仍抱持著許多的不了解、不信任之批判。集體性的資料濫用焦慮，並未能隨著憲法訴訟案的宣判或管理條例的通過，而有太多正面的溝通與良性的互動。[18]

（二）次世代基因定序給付爭議：變相的「不當聯結」

承前所述，如果我們說健保資料庫案有其歷史脈絡甚至是共業，那麼2024年爆發的NGS給付爭議，或許可以說就是這樣信任危機的火上加油。2024年5月，健保署宣布對癌症病患的次世代基因定序（NGS）檢驗來納入健保給付。[19]這項原本自費需要數萬元以上費用的檢測，原本是可以嘉惠每年約2萬名以上癌友的德政。

但在健保署的給付相關會議上，機關首長卻才告知該政策施行其實隱含了一項附帶條件：要求申請給付的民眾必須簽署同意書，將其基因檢測結果上傳至健保署指定資料庫，否則將不予給付。[20]可以想見，此舉立刻以起民間團體代表的激烈反彈，被批評是一種「給我基因，不然免談！」的霸王條款。[21]事實上，從行政法原理來看，這樣的要求可能有違反「不當聯結禁止原則」的情況。因為將「社會保險給付權」與「提供研究資料義務」掛鉤，實質上是利用病患在經濟與健康上的弱勢地位，迫使其交出高度敏感的基因資訊。這不叫「知情同意（Informed Consent）」，而是一種不當壓力下的非自願性同意。

雖然最後在輿論壓力之下，健保署修正規定，不要求民眾提供同意書，並且改為僅上傳不含基因原始數據（Raw Data）的病理報告，且將目的限縮於給付審查，但此事件已再次重創了政府與民眾關係中，對於健康資料治理的脆弱信任基礎。[22]

（三）健保署個資疑似外洩案：說明的缺席

2023年初爆發了一件震驚全國的健保資料

註17：憲法法庭111年憲判字第13號判決，
https://cons.judicial.gov.tw/docdata.aspx?fid=38&id=309956

註18：公民行動影音紀錄資料庫（2024），「健保資料庫案後續修法座談會」，公民行動影音紀錄資料庫網站，
https://www.civilmedia.tw/archives/113104（最後瀏覽日：2026/01/12）。

註19：中央健康保險署（2024），〈健保給付次世代基因定序（NGS）〉，中央健康保險署全球資訊網，
https://www.nhi.gov.tw/ch/cp-14565-e02e0-3255-1.html（最後瀏覽日：2026/01/12）。

註20：中央健康保險署（2024），全民健康保險醫療服務給付項目及支付標準共同擬訂會議113年第2次會議紀錄，中央健康保險署全球資訊網，
https://www.nhi.gov.tw/ch/cp-14472-7f258-2771-1.html（最後瀏覽日：2026/01/12）。

註21：楊惠君、陳弘美（2024），〈次世代基因定序納健保，數據上傳引發「拿個資換給付」爭議〉，報導者，
https://www.twreporter.org/a/opinion-ngs-testing-for-cancer-covered-under-health-insurance（最後瀏覽日：2026/01/12）。

註22：吳亮儀（2024），〈NGS檢測納健保5/1上路健保署：不強制簽署同意書〉，自由時報，
https://health.ltn.com.tw/article/breakingnews/4651813（最後瀏覽日：2026/01/12）。

疑似外洩中國案件。根據媒體報導，健保署前主秘涉嫌長期外洩民眾個資至中國。雖然後續調查似乎顯示，並未有整套資料流出的情況，但「內鬼」疑雲已讓民眾對國家掌管的大型資料庫的資安防護能力產生根本性的懷疑。[23]更重要的是，對於根據《個資法》第12條第1項，公務機關知悉所保有之個人資料被竊取、竄改、毀損、滅失或洩漏時，應通知當事人。但事發迄今已經超過三年，身為健保個資主體的全國2300萬民眾，除了在案發數天後在健保署官網能看到一篇簡要回應、一個月後目睹署長火速被更換之外，並沒有得到任何關於此事的任何通知與進一步消息。[24]這種做法先不論是否有嚴守個資法之規範，對於原本就已因為健保資料庫訴訟案、憲法判決而搖搖欲墜的資料治理信任關係，更因為「說明的缺席」而雪上加霜。

參、他山之石：透明與信任的比較法觀察，以英國為例

面對這種信任危機，我們不應陷入資料利用之「完全開放」與「完全封閉」的二元對立。事實上，他山之石可以攻錯，在比較法上英國國民健保署（National Health Service, NHS）歷經推動Care.data等國民電子健康資料利用計畫失敗後，記起教訓後所發展出的一套治理模式，是值得台灣在重新贏回民眾信任上來加以借鏡。[25]

一、信任的社會學與法律定義

要解決信任問題，先要理解什麼是信任。社會學家Piotr Sztompka定義：「信任是對於他方將來未知行為的一種賭注（Trust is a bet about the future contingent actions of others）」。27Rachel Botsman則認為：「信任是一段與未知自信相處的關係」。[27]

在法律上，學者Ari Ezra Waldman提出了「隱私即信任（Privacy as Trust）」的理論。他主張，隱私法不應僅聚焦於「資料的遮蔽或去識別化」，而應聚焦於「保護與修復信任關係」。當民眾將數據交給醫院或政府時，是基於一種對特定目的與保護義務的信賴；一旦這個信賴被打破（例如目的外利用於商業行銷），即便數據經過加密，隱私權益實際上已受侵害。[28]

二、英國NHS模式的啟示：細節的透明

英國NHS England在處理健康數據共享時，在記取先前的失敗教訓而加以改革後，展現

註23：公視新聞網（2023），〈健保署前主秘涉外洩民眾個資檢調搜索約談3人〉，公視新聞網，https://news.pts.org.tw/article/619347（最後瀏覽日：2026/01/12）。

註24：中央健康保險署（2023），「關於健保資料庫資安事件之說明」，中央健康保險署全球資訊網，https://www.nhi.gov.tw/ch/cp-1358-2d6e2-3255-1.html（最後瀏覽日：2026/01/12）。

註25：Janos Meszaros & Chih-hsing Ho, Building Trust and Transparency? Challenges of the Opt-out System and the Secondary Use of Health Data in England, 10 EUR. J. RISK REG. 720 (2019).

註26：Piotr Sztompka, Trust: A Sociological Theory (1999)

註27：Rachel Botsman, Who Can You Trust? (2017).

註28：Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age (2018).

了高度的透明治理（Transparency），民眾可以利用的公開註冊資訊上清楚地看到詳盡的資訊。[29]我們以NHS提供數據給諾華藥廠（Novartis）進行乳癌研究的一個案子為例（以下簡稱「諾華案」），其公開內容之詳盡，與台灣僅公告簡略清冊的做法形成強烈對比：[30]

（一）具體的法律依據

明確列出資料處理符合UK GDPR第6(1)(f)條（合法利益）與第9(2)(j)條（公共利益、科學研究目的）。這要求資料控制者必須先進行「合法利益評估（Legitimate Interest Assessment）」。

（二）明確的預期效益（Expected Benefits）

不同於台灣僅列出研究題目，英國要求申請者必須論述該研究具體能帶來什麼公眾利益。例如諾華案中，明確指出研究將協助政策制定者改善HR+/HER2-轉移性乳癌的治療路徑與資源分配。這體現了數據利用的「正當性（Justification）」。

（三）嚴謹的技術規範

諾華案中也詳細揭露了數據將儲存於AWS雲端，且分析人員僅能透過雙重驗證（MFA）的VPN進行遠端存取，數據不落地等資安細節。

（四）退出機制（National Data Opt-out）

最關鍵的是，英國建立了國家級的資料退出機制。若民眾已選擇退出（Opt-out），其數據就會從研究資料集中被移除，不會被傳輸給藥廠。

三、對比台灣的改進空間

反觀台灣，目前健保署雖然有對於利用健保資料庫的申請案，公開「審核通過案件清冊」。但細觀其內容，僅列出計畫名稱、申請人與機構（例如：某大學申請「建立全方位臨床數據關聯模型」）、計劃委託單位、申請檔案（編號）等。民眾實際上是無法從中得知：為什麼要把資料給這個單位？法律依據為何？他們拿了哪些資料？對社會有何具體貢獻？資安如何控管？這種資訊的不對稱，正是不信任滋生的溫床。[31]

對此本次新修訂之健保資料管理條例第14條第3項即明定：「主管機關或保險人對於依第十一條第一項申請利用，應定期公開核准案件數、清冊、利用結果報告及其他相關資訊」。並且在立法說明中指明「第四項定明主管機關或保險人應定期公開核准案件數、清冊、利用結果報告及其他相關資訊，以落實健保資料目的外利用之**公開透明、公眾監督及社會信任**」。[32]

這樣的改革方式，可以說是往透過公開透

註29：NHS England, Data Uses Register, https://app.powerbi.com/view?r=eyJrIjoiOWEwZGY3ZmQtNTJiYS00M2RmLWEyNzgtZDUyNjgzN (last visited 2026/01/12).

註30：中央健康保險署，「全民健康保險保險人對外提供資料作業要點及相關申請資訊」，中央健康保險署全球資訊網，https://www.nhi.gov.tw/ch/cp-18263-17998-3966-1.html（最後瀏覽日：2026/01/12）。

註31：同前註。

註32：總統府（2025），「全民健康保險資料管理條例公布令」，總統府全球資訊網，https://www.president.gov.tw/Page/294/50094（最後瀏覽日：2026/01/12）。

明來強化問責監督，以取得、維繫民眾的信任的方向前進，應予肯定。不過實際情形如何，仍然有待於施行細則公布、實際運行情形明朗後，再行評估。

肆、建構衛福領域資料治理的「風險分級」與「創新沙盒」

面對上述困境，本文建議衛福部應跳脫傳統管制思維，採取「雙軌制」的改革策略：

一、導入「風險分級」治理架構

醫療AI的應用可能光譜極廣，從低風險的行政流程優化（如AI協助掛號排程、病歷輸入）到高風險的直接進行臨床診斷（如AI判讀腫瘤影像），不同類型應用其對病患權益的影響截然不同。我們不應以一套標準管制所有應用。因此比較可行的做法，應該是參考歐盟《人工智慧法案》（EU AI Act）的分類邏輯，制定醫療AI的風險分級表：[33]

（一）高風險AI

直接涉及醫療診斷、治療決策或生理監測之AI。此類系統應強制進行「演算法影響評估（Algorithmic Impact Assessment）」與「數據來源合規性審查」，確保訓練數據的代表性與無偏見，並需落實「人類在迴路（Human-in-the-loop）」的監督機制。

（二）中與低風險AI

僅用於行政輔助或者加速，且不涉及直接醫療行為、取代醫療人員角色者，可採較低密度的上市前資格取得與上市後進行監測的模式，以鼓勵創新。

這樣的分類與模式，將有助於避免「一刀切」的過度管制扼殺產業發展。

二、創設「醫療AI治理沙盒（Regulatory Sandbox）」

現行的《個資法》等法規對於大數據分析與AI模型訓練等新興科技應用，在規範上並不完備。實務上往往令保守謹慎的產業界與學界卻步，或使其被迫遊走在法律灰色地帶。本文認為，在《人工智慧基本法》通過後我國應考慮推動專法，責成衛福部成立專責的「醫療AI創新治理沙盒辦公室」。

「沙盒」的概念不應僅限於技術測試，更應是用來測試「法律與治理模式」的實驗室。在沙盒內，我們可以測試以下創新機制：

（一）動態同意（Dynamic Consent）

利用區塊鏈或App技術，讓民眾可以隨時檢視誰在申請使用其數據，並動態地給予或撤回同意。這比傳統的「概括同意」更能落實資訊自主權。[34]

（二）資料利他（Data Altruism）

註33：Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), O.J. (L. 1689) (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

註34：吳俊穎、楊增暐（2023），〈研究參與者動態同意的實務與法律〉，《台灣醫學》，27(5)，656-664。doi:10.6320/FJM.202309_27(5).0015

參考歐盟《資料治理法》（DGA），建立「資料利他組織」的認證機制，鼓勵民眾基於公益自願捐贈數據，用於罕見疾病或癌症研究，而非單純的商業買賣。[35]

（三）隱私強化技術（PETs）驗證

在沙盒中測試聯邦學習（Federated Learning）或差分隱私（Differential Privacy）等技術，驗證其是否能在不釋出原始個資的前提下，完成AI模型訓練。[36]

這樣的治理沙盒機制，具備「容錯與修正」的功能，能讓監管者在小範圍內評估法規鬆綁的風險，待機制成熟後再修法推廣至全國。

伍、結語：以「數位信任」重塑法制靈魂

一、從功利主義到民主治理

回顧憲判字13號判決，黃昭元大法官在部分不同意見書中留下了發人深省的諍言：「便宜行事的高效率管制，通常是會比層層節制、講究程序、追求共識的民主治理，於短期內產生更大的效益，卻也可能因此失去人民長期、穩定的信任。」[37]

這段話精準地道出了台灣數位健康發展的盲點。過去我們太習慣為了追求效率而犧牲程序正義，認為只要目的是為了「國民健康」或「科學發展」的大義，民眾的隱私權就必然應當退讓。然而，NGS爭議與憲法訴訟證明，這種單面向功利主義的思維在民主深化、依法治國的台灣已過於簡略及粗糙。

二、展望：沒有信任，就沒有精準醫療

人工智慧醫療法制的完善，不能只看技術發展，更需回歸穩固地基的基礎工程建設──「人權」與「信任」。唯有建立一個「值得信任的健康數據治理架構」（Trustworthy Health Data Governance Framework），涵蓋完整的規範範圍（All health data）、透明的利用模式、實質的獨立監督密度，以及完善的主體權利（退出權與回饋機制），台灣的智慧醫療與AI創新才能真正走得長遠。

正如黃昭元大法官所言：「有足夠的信任，留下的人就多了，出走的人也會回來。」[38]唯有各界攜手合作，透過風險分級確保安全，透過沙盒機制鼓勵創新，並以透明治理贏回民眾的信任，才能共同迎接AI創新與治理的新時代。

註35：數位發展部，「數據公益運作指引」，數位發展部全球資訊網，https://moda.gov.tw/information-service/govinfo/administrative-directions/ad-plural-innovation/1419（最後瀏覽日：2026/01/12）。

註36：數位發展部，「隱私強化技術應用指引」，數位發展部全球資訊網，https://moda.gov.tw/information-service/govinfo/administrative-directions/ad-plural-innovation/1419（最後瀏覽日：2026/01/12）。

註37：憲法法庭111年憲判字第13號判決（黃昭元大法官部分不同意見書）。https://cons.judicial.gov.tw/docdata.aspx?fid=38&id=309956

註38：同前註。