值得信賴的健康醫療 AI—從資料共享之治理論起 *

王自雄 **、張腕純 ***

摘要

人工智慧 (Artificial Intelligence, AI) 在健康醫療領域的應用與日俱增，且可能應用的範圍極為多元。惟實際上，健康醫療日常實務的 AI 應用不如 AI 倡議者預期般普及，主要原因來自於人們對 AI 健全性的懷疑，從而無法對 AI 應用產生足夠信賴。目前健康醫療領域 AI 研究多採機器學習 (Machine Learning) 方法，而仰賴大量訓練資料以進行預測。然而，高品質健康醫療資料取得不易，連帶影響 AI 的健全性，進而限制了健康醫療 AI 擴大到日常臨床實務應用的機會。

本文探討值得信賴的健康醫療 AI，先從 AI 偏誤 (bias) 問題切入，說明 AI 可信賴程度與資料之間的密切關係，並以歐盟、OECD 可信賴 AI 相關建議為例，說明資料治理、資料共享生態系對可信賴 AI 發展之重要性。其次聚焦於高品質健康醫療資料取得不易的原因，探討國際社會資料保護意識抬頭，對取得健康醫療資料之影響。最後分享國內、外健康醫療資料共享治理案例，說明如何在信賴關係下形成健康醫療資料共享生態系，間接達到提升健康領域 AI 應用健全性之目的。

目　次

關鍵字：資料共享、資料治理、人工智慧、健康醫療資料、資料再利用

---

*　投稿日：2020 年 11 月 26 日；接受刊登日：2021 年 2 月 15 日。

**　東吳大學法學博士；資策會科技法律研究所數位創新中心主任。

***　資策會科技法律研究所數位創新中心法律研究員。

壹、前言

人工智慧 (Artificial Intelligence, AI) (以下簡稱 AI) 在健康醫療領域的應用與日俱增，且應用範圍多元廣泛，舉凡臨床診斷治療、生醫研究、公共衛生乃至於後勤行政管理等，幾乎各種醫療健康照護之提供或管理面向皆有運用 AI 的可能性。

依據經濟合作暨發展組織 (Organization for Economic Cooperation and Development, OECD) (以下簡稱 OECD) 2020 年提出之「值得信賴的健康領域 AI」(Trustworthy AI in Health) 報告[1]，國際上已有許多健康醫療 AI 潛力應用的研究，如影像組學 (radiomics) 的 AI 應用、遠距遙控機器人手術、臨床決策支援系統 (clinical decision support system) 之改善等，且隨著 2019 年新型冠狀病毒 (COVID-19) 等重大傳染病疫情爆發，生醫與公共衛生領域的 AI 應用更加嶄露頭角。

AI 應用看似潛力無窮，然而實際上健康醫療日常實務的 AI 應用卻不如 AI 倡議者預期般普及[2]，主要原因來自於人們對 AI 健全性[3]的懷疑，從而無法對 AI 應用產生足夠信賴。目前健康醫療領域的 AI 研究多採用機器學習 (Machine Learning) 方法，這些方法多半仰賴大量訓練資料以進行預測[4]。然而，現實世界中，

1 Organization For Economic Cooperation And Development [OECD], *Trustworthy AI in Health* (2020), https://www.oecd.org/health/trustworthy-artificial-intelligence-in-health.pdf (last visited Sept. 4, 2020).

2 *Id.*

3 指 AI 系統能以安全（包括資訊、隱私安全、人身與財產安全等）、可預見的方式運作或表現，且有適當的防護措施以避免預期及非預期的負面影響發生。

4 *Supra* note 1.

高品質健康醫療資料的取得不易，連帶影響 AI 的健全性，進而限制了健康醫療 AI 從小型專案研究擴大到日常臨床實務應用的機會。

本文探討值得信賴的健康醫療 AI，先從 AI 偏誤 (bias) 問題切入，說明 AI 可信賴程度與資料之間的密切關係。其次聚焦於高品質健康醫療資料取得不易的原因，探討國際社會資料保護意識抬頭，對取得健康醫療資料之影響。最後透過國內與國際健康醫療資料共享治理案例，說明如何在信賴關係下形成健康醫療資料共享生態系，進而間接達到提升健康領域 AI 應用健全性之目的。

貳、AI 可信賴程度與資料之關聯

目前健康醫療領域的 AI 研究多以機器學習為主，常見的機器學習方法例如線性回歸 (linear regression)、邏輯回歸 (logistic regression)、決策樹 (decision tree)、主成分分析 (principal component analysis) 乃至深度神經網路 (deep neural networks) 等，通常需藉由大量資料訓練進行分析預測。資料的蒐集、處理及利用成為影響健康醫療 AI 訓練結果的因素。造成 AI 訓練結果產生偏誤的原因，與資料的蒐集、處理及利用息息相關。

一、常見的偏誤類型

健康醫療 AI 研究常見的偏誤類型主要有三種[5]。

(一) 報告性偏誤 (reporting bias)

由於資料被選擇性地揭露或部分資訊被掩蓋，導致研究結果在報告或呈現時，無法完整代表真實世界的狀況[6]。可能發生在臨床資料較易從正面實證研究 (positive research findings) 中取得的情況。因研究參與者在選擇研究主題、設計、執行、分析或揭露研究方法、研究結果時，或許已對資訊進行篩選，而連帶影響 AI 訓練結果。基於正面研究 (positive research) 目的所取得的資料，較可能有重複或過度報告的情況；而基於負面研究 (negative research) 目的所取得的資料，則較可能有遺漏或報告不足的情況[7]。

(二) 選擇性偏誤 (selection bias)

又稱為選樣偏誤 (sampling bias)，指所選取的資料樣本無法準確代表研究目的所涉人口的狀況[8]。使用特定人口群資料集

---

5 *See* J. Raymond Geis et al., *Ethics of AI in Radiology: European and North American Multisociety Statement* (2019), https://www.acr.org/-/media/ACR/Files/Informatics/Ethics-of-AI-in-Radiology-European-and-North-American-Multisociety-Statement--6-13-2019.pdf (last visited Oct. 25, 2020).

6 *Id.* at 21. *Also see* Catalogue of Bias: Reporting Bias, CEBM, https://catalogofbias.org/biases/reporting-biases/ (last visited Oct. 31, 2020).

7 此種偏誤也可能發生在原型資料 (prototypical data) 的假設時，例如在形容香蕉時並未註記它的顏色是黃色，因為已想當然爾地認為香蕉是黃色的。

8 *Supra* note 5, at 21-22. *Also see* Catalogue of Bias: Selection Bias, CEBM, https://catalogofbias.org/biases/selection-bias/ (last visited Oct. 31, 2020).

所訓練的 AI 演算法，一旦輸入有別於訓練資料集人口特徵以外的資料時，演算法的運作結果可能產生偏差。舉例而言，依 OECD 調查顯示，目前全球健康領域 AI 研究主要來自於美國、歐盟會員國、英國、加拿大與澳洲等地區，而用以訓練 AI 模型的資料多數來自於西方、較富裕、教育程度較高、工業化程度較高、民主社會的人口群[9]，依此人口群特徵資料所開發的 AI 演算法，若套用於亞洲、非洲或中南美洲等地區人口進行健康醫療預測時，結果可能產生偏誤。此外，使用合成或強化過的資料 (synthetic or augmented data)，亦可能有演算法無法對未來作出準確預測的風險[10]。

(三) 自動化偏誤 (automation bias)

自動化偏誤經常發生在由人類負責監控或觀察決策機器 (decision-making machine) 的情況，是指人類傾向贊同機器所產生的決策，而忽略與機器決策相反的資料或相衝突的人類決策[11]。自動化偏誤會導致決策機器的誤用，例如：過度信賴、監控不足、盲目同意等。例如若電腦輔助偵測系統決策牽涉太多細節，以致放射科醫師難以覺察時，在快速檢查過程中，醫師可能忽略其他與系統決策相反的資訊，傾向直接接受系統決策[12]。

9 *Supra* note 1, at 12.
10 *Supra* note 5, at 22.
11 *Id.* at 35. *Also see* Linda J. Skitka, Automation bias, https://lskitka.people.uic.edu/styled-7/styled-14/index.html (last visited Oct. 31, 2020).
12 *Id.* at 35-36.

除了前述三種偏誤之外，AI 也可能從資料中學習到人類既定的錯誤、偏見、刻板印象及不平等，從而產生演算法偏誤的情況。例如美國一項用以確認病患健康照護需求的 AI 演算法，被認為帶有種族歧視，究其原因在於，該演算法是以健康照護成本作為健康照護需求的預測基礎，而因美國社會對健康照護資源分配不平等，對白人所投入的健康照護成本原就高於黑人，導致該演算法得出「黑人比白人健康而健康照護需求較低」之結論[13]。此外，大部分機器學習的預測模型，是以資料相關性為基礎而非因果關係，因此可能違背人類直覺地將資料相牽連後，推導出荒謬的預測結果[14]。例如預測病患死亡風險的 AI 模型，因為同時患有氣喘與肺炎的病患，比單純肺炎患者受到更多的積極治療，而推導出「同時患有氣喘與肺炎病患的死亡風險低於單純肺炎患者」之結論[15]。

二、提升 AI 可信賴程度之方法

隨著 AI 的蓬勃發展，國際社會近年來不斷倡議發展可信賴之 AI，許多國際組織鑒於造成 AI 偏誤的原因多與資料的蒐集、處理、利用密切相關，因此在所提出的建議中納入資料共享與資料治理議題。

---

13 Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations,* SCIENCE, 366(6464), 366, 447-453(2019), *available at* https://science.sciencemag.org/content/366/6464/447 (last visited Feb. 17, 2021).

14 *Supra* note 1, at 12-13.

15 *Id.*

(一) 歐盟之建議

2019 年歐盟執委會 AI 高級專家小組 (High-Level Expert Group on Artificial Intelligence, AI HLEG) 提出「值得信賴之 AI 倫理指引」(Ethics Guidelines for Trustworthy AI)[16]，認為所謂「值得信賴的 AI」必須以人為本 (human-centric) 並具備三大要件 (component)，包括：合法 (lawful)、符合倫理道德 (ethical) 及健全 (robust)。

至於實際上如何開發一個「合法、合乎倫理、健全而值得被信賴的 AI」，歐盟提出下列七項要求 (requirement) 作為實踐之參考 [17]：

1. 人類主體動因 [18] 與監督 (human agency and oversight)：AI 系統應作為人類自主性 (human autonomy) 與人類決策之輔助，尊重並保護人的基本權利，且需實現人類重要的目標或價值，並由人類加以監督。

---

16 High-level Expert Group On Artificial Intelligence [AI HLEG], *Ethics Guidelines for Trustworthy AI* (2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (last visited Oct. 25, 2020).
該指引所提之值得信賴 AI 架構，包含三大基本要件、四項倫理原則 (包括尊重人類自主性 (respect for human autonomy)、避免傷害 (prevention of harm)、公平 (fairness)、可解釋 (explicability)) 及七項實踐要求，相較於其他國際 AI 倫理相關指引，內容更完整具體，堪為近年來國際 AI 倫理之指標性文件。

17 *Id.* at 14

18 human agency 亦有翻譯為「人類主體動力」或「人類能動性」。簡言之，係指人類作為主體出於自由意志作出決定並加以實踐的能力。根據歐盟「值得信賴之 AI 倫理指引」，AI 系統應被用以支持使用者的主體動因 (user's agency)，以促進民主 (democratic)、繁榮 (flourishing) 及平等 (equitable) 社會之形成。

2. 技術健全且安全 (technical robustness and safety)：AI 系統之開發應採取風險預防方法，將非預期的損害降到最低，以保護人類身體與心理的完整性，故開發過程中應特別考量資料與系統安全遭受攻擊的復原能力 (resilience)，透過備援計畫確保系統發生問題時仍維持一般安全性，並確保 AI 系統能作出準確判斷，且輸入相同條件的資訊能產出相同或類似的結果。

3. 隱私與資料治理 (privacy and data governance)：AI 系統可能對個人隱私產生影響，應在 AI 系統生命週期過程中尊重個人隱私與資料保護。此外，由於資料的使用對 AI 系統的效能至關重要，良好的資料治理，包括資料品質、資料完整性之確保及資料近用管理等，亦能避免損害發生。

4. 透明性 (transparency)：為能追蹤、解釋 AI 系統所作成的決策，AI 系統相關的要素，包含資料、系統本身與營運模式 (business model) 等，皆需將透明性納入考量，例如資料的蒐集、標註乃至演算法之使用等重要環節，應作成紀錄並加以保留。

5. 多元、不歧視、公平 (diversity, non-discrimination and fairness)：AI 系統可能因所使用的資料帶有人類無意中形成的偏見、資料不完全、資料治理不良等因素，產生不公平或歧視的決策結果，因此 AI 系統生命週期過程中，應有多元包容的視野、通用無障礙之設計及利害關係人之參與。

6. 環境與社會福祉 (environmental and social well-being)：AI 系統生命週期中應關注到永續發展、環境友善、社會影響與民主等面向。

7. 可歸責 (accountability)：應建立機制確認 AI 系統在開發、部署與使用前後之責任，透過稽核強化 AI 系統可信賴程度。另為盡量降低 AI 系統的負面影響，應做到識別、評估、紀錄與通報，並對可能受影響之人給予救濟或尋求賠償之管道。

(二) OECD 之建議

OECD 在「值得信賴的健康領域 AI」報告[19] 中提到，當前全球健康領域的 AI 應用尚有待發展的空間，實際上大部分健康領域的 AI 屬於弱 AI (artificial narrow intelligence)，用以解決非常特定的問題或完成非常特定的推論任務，較難擴及訓練模型以外之領域。造成 AI 難以廣泛應用到醫療與健康照護日常實務的主要原因有三：第一，現實世界中 AI 演算法的健全性備受質疑；第二，高品質健康資料的匱乏；第三，政策與監管的真空狀態，因此大幅限制了利用制度或人力實現 AI 潛力應用的可能性[20]。

為了增進健康領域 AI 的健全性，擴大健康醫療 AI 之應用，OECD 提出五點建議，其中特別提到「透過安全、公平、合法

19 此報告為近年來少數與健康領域 AI 倫理相關之國際文件，內容不僅呼應 2019 年 OECD 理事會所提之 AI 建議 (OECD Council Recommendation on Artificial Intelligence)，亦作為 2020 年 6 月 G20 數位經濟任務小組 (Digital Economy Task Force, DETF) 人工智慧對話 (AI Dialogue) 的背景文件 (background paper)。

20 *Supra* note 1, at 11.

及符合倫理的資料共享，育成 AI 數位生態系」的重要性[21]。為更有效改善 COVID-19 等全球性傳染病、罕見疾病之預防或治療，不免需藉由資料共享方式增加AI訓練資料的廣度與代表性。然而，健康資料多屬敏感個人資料 (下稱個資)，個人隱私以及病患、公眾、資料控管者與其他利害關係人缺乏信賴，是健康資料共享再利用的主要障礙。OECD 認為健康資料治理框架應強調透明、公眾溝通與利害關係人之參與。在宣揚健康資料運用益處的同時，應先做好資料安全維護與風險管理，以扭轉利害關係人或公眾認為「健康資料共享再利用必然會犧牲個人隱私與資料保護」之想法[22]。

參、資料保護法制對健康醫療資料取得之影響

由於高品質及具代表性的資料，有助於提升 AI 準確度、降低偏誤風險、發揮 AI 預期效用，「資料的取得近用」隨著 AI 的蓬勃發展變得更為重要。尤其在面對全球性傳染病疫情、重大或罕見疾病時，AI 研發者對健康醫療資料共享有迫切渴求，重要資料的來源或許不僅限於單一機構、地區或國家。然而，在資料驅動經濟時代下，掌握資料幾乎等同於掌握了競爭優勢，不少機構、地區或國家採行資料保護相關政策或法制，以維護既有的競爭優勢，使得資料共享更加困難。此外，隨著全球隱

21 *Id.* at 16-20. 五點建議包括：1. 透過安全、公平、合法及符合倫理的資料共享，育成 AI 數位生態系；2. 落實以價值為基礎 (value-based) 的 G20 AI 原則 (G20 AI Principle)；3. 建立「值得信賴的 AI」相關法規及指引，形塑政策形成之環境；4. 培育人才，為健康領域勞動市場之轉型儲備能量；5. 有策略且永續地投資 AI 研究與發展。

22 *Id.* at 16.

私保護與資訊自主權意識抬頭，多數國家定有隱私或個資保護相關法制，而健康醫療資料往往被認為是與隱私高度相關的敏感個資，因此在健康醫療資料的蒐集、處理、利用上，需謹慎依循法律規範，亦連帶影響健康醫療資料之流通。

一、資料在地化 (data localization) 要求

資料在地化[23]是常見的資料保護手段之一。國家藉由法制要求資料必須儲存在其管轄領域內，甚至限制資料僅能在其管轄領域內蒐集、處理和儲存，主要目的在保護國家重要利益[24]。不少國家將健康醫療及個人隱私視為重要利益，針對健康醫療等敏感資料，將資料在地化要求納入相關法律規定，進而影響健康醫療資料的跨境取得。

---

23 資料在地化 (Data localization) 與資料滯留 (Data Residency)、資料主權 (Data Sovereignty) 概念極為近似，因此經常被相互混用。惟亦有論點將三者依限制的寬嚴程度作概念細分：

1. data residency：指政府機關或私人機構明確指定資料需儲存在所選擇的地理區域內。
2. data sovereignty：指國家透過法律要求資料必須在特定地理區域內蒐集、處理和儲存。
3. data localization：指國家透過法律要求資料的建立和儲存僅能在國境範圍內，或要求資料跨境傳輸之前需在國內保留資料的複製本。

See Benjamin Vitaris, Data Residency: Meaning, Laws, & Requirements (July 30, 2020), https://permission.io/blog/data-residency/ (last visited Nov.5, 2020).

24 *See* Lothar Determann, How Data Residency Laws Can Harm Privacy, Commerce and Innovation- and Do Little for National Security, World Economic Forum (Jun. 9, 2020), https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/ (last visited Nov.6, 2020).

例如澳洲 2012 年個人健康紀錄法 (My Health Records Act 2012) 規定，持有健康紀錄或能存取健康紀錄相關資訊的系統營運商 (System Operator) (包括登記註冊的資料庫營運商、入口網站營運商或服務提供承包商)，不得在澳洲境外掌握或持有健康紀錄、處理健康紀錄相關資訊，亦不得使他人在澳洲境外掌握或持有健康紀錄、處理健康紀錄相關資訊，除非健康紀錄不包含個人可識別資訊 [25]。加拿大聯邦政府雖無資料在地化要求，但部分省分的法律卻有資料在地化相關規定，如加拿大英屬哥倫比亞省 (British Columbia) 的「資訊自由與隱私保護法」(Freedom of Information and Protection of Privacy Act) 規定，除非資料當事人同意或法律另有規定，公務機關必須確保所監管的個資僅儲存在加拿大，且僅能在加拿大被近用 [26]，該法所指之公務機關包括英屬哥倫比亞省的健康照護機構 [27]。又如阿拉伯聯合大公國在管制健康領域資通訊技術使用之 2019 年第 2 號聯邦法 (Federal Law No.2 of 2019, on the Use of the Information and Communication Technology (ICT) in Health Fields) 規定，除非健康主管機關允許，否則健康資訊及國家提供健康服務之相關資

25 *My Health Records Act 2012* (Cth) s 77 (Austl.).

26 Freedom of Information and Protection of Privacy Act, R.S.B.C, 1996, c 165, s 30.1 (Can.).

27 *Id.* schedule 1.

料不得在國外儲存、處理、產生或傳輸到國外[28]。

二、其他個資保護要求

自 1980 年 OECD 提出八大隱私保護原則[29]至歐盟 2018 年施行一般資料保護規則 (General Data Protection Regulation, GDPR)[30]以來，國際社會在個資保護規範上已逐漸形成共通性原則。儘管不同國際組織或國家所提出的原則略有差異，但核心原則不外乎資料蒐集、處理及利用之「目的特定」、「資料蒐集最少化」、「資料當事人資訊自主權保障」、「資料安全維護」等。

有些地區縱使並無資料在地化要求，但因健康醫療資料屬於個資範疇，資料之蒐集、處理與利用必須遵循個資保護相關規範，而增加健康醫療資料共享再利用的法遵負擔。如歐盟

28 *See* Els Janssens and Kellie Blyth, UAE Issues Law to Protect Health Data and Restrict Its Transfer Outside the Country, Baker McKenzie (Mar. 20, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/03/uae-issues-law (last visited Nov. 6, 2020); *also see* Federal Law No.2 Issued on 06/02/2019 on the Use of the Information and Communication Technology (ICT) in Health Fields, art. 13, https://elaws.moj.gov.ae/UAE-MOJ_LC-En/00_Health/UAE-LC-En_2019-02-06_00002_Kait.html?val=EL1 (last visited Nov. 6, 2020).

29 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Nov.23, 2020).

30 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119)1.

GDPR 雖無資料在地化要求，但在資料跨境傳輸方面採取原則禁止例外容許之規定，如欲將歐盟境內的健康醫療資料傳輸到歐盟會員國以外之第三國，該第三國需獲得歐盟資料保護的適足性認定 (adequacy decision)[31] 或採取 GDPR 規定的適當保護措施 [32]。又以我國個人資料保護法 (下稱個資法) 為例，雖無資料在地化之要求，但規範上除了參考國際規範前述幾項核心原則，更將健康醫療資料列為特種個資，較一般個資蒐集、處理、利用之要求更為嚴格，有關病歷、醫療、基因、健康檢查等資料，除非符合法律規定的例外情況，否則不得蒐集、處理或利用 [33]。

此外，健康醫療資料的共享再利用經常牽涉到「資料蒐集目的轉換」之問題。健康醫療資料的原始蒐集目的，一般是出於病患就醫診療或健康檢查，但健康資料之共享可能是為了 AI 研發等原始蒐集目的範圍以外之應用。儘管許多地區法律定有資料目的外利用 (或再利用) 之相關規定 [34]，但實際上要符合法律規定，通常需耗費一些法遵成本。例如以「資料當事人同意」作為資料目的外利用之法律依據時，需考量資料當事人行使同意的方式，包括知情同意 (informed consent) 或概括同意 (broad consent)、口頭同意或書面同意，以及如何確定資料當事人所為之同意出於自由意志、如何處理資料當事人事後撤回同意等事

31 Council Regulation 2016/679, art.45, 2016 O.J. (L 119) 1, 61-62.

32 Council Regulation 2016/679, art.46, 2016 O.J. (L 119) 1, 62-63.

33 我國個資法第 6 條。

34 常見的資料目的外利用（或再利用）之規定，諸如資料當事人同意、科學研究或統計所必要、公共利益等，但不同國家或地區對資料目的外利用的細部規定不盡相同。

項，採取適當措施。倘所需資料量龐大、所涉資料當事人人數眾多或資料使用目的多元，法遵與風險控管的成本或許會相對增加。

肆、健康資料共享治理案例

近年來不少健康醫療領域的研究者，開始思考、建構不同型態的資料共享模式，以因應資料保護法制所帶來挑戰，增加資料應用的機會。除了在傳統集中化資料庫模式下強化資料蒐集與近用之管理措施外，面對資料在地化的挑戰亦發展出分散的聯合式資料系統 (distributed federated data system) 治理模式。

一、　國內案例—醫療影像資料庫資料共享再利用之治理

(一) 背景

鑒於高品質醫療影像資料得之不易，我國科技部於 2017 年推動「醫療影像之巨量資料建立與應用研究」專案計畫 (下稱醫療影像專案)，集結國立臺灣大學、臺北榮民總醫院、臺北醫學大學三大醫療團隊之專業智慧，進行心、腦、肺等醫療影像標註，從而建立我國首座本土跨醫療院所之醫療影像資料庫，作為國內健康醫療 AI 研究的基礎建設，促進國內健康醫療 AI 發展，幫助醫師加速影像判讀及提升診斷的一致性與精準度、縮短病人就醫檢查時間，提升國內醫療品質[35]。

35〈加速醫療影像 AI 發展 再創台灣優勢 科技部啟動台灣首座跨醫療院所之醫療影像標註資料庫〉，科技部，https://www.most.gov.tw/folksonomy/detail?article_uid=9eafcc53-50c3-4803-aff6-fa578c25b1f7&menu_id=9aa56881-8df0-4eb6-a5a7-32a2f72826ff&l=ch（最後瀏覽日：2020/11/18）。

醫療影像資料庫是採取集中化方式，將三大醫療團隊所標註的醫療影像資料，匯集至國家實驗研究院國家高速網路與計算中心 (下稱國網中心)，供其他研究者近用。為此，科技部成立巨量資料應用研究計畫推動辦公室[36]，並與三大醫療團隊組成工作小組，針對「資料建置與標註」、「資料格式與標註工具」、「資料共享再利用法制」與「資料庫維運模式」四大面向，共同研議兼顧資料應用需求、資訊安全與適法可信賴之配套作法。因應資料應用需求，以及我國個資法對病歷、健康檢查或醫療等特種個資蒐集、處理、利用之規範，在建立資料庫的過程中，待解決的主要議題有：資料標註品質之確保、資料共享之隱私保護、資料利用目的轉換之適法性。各工作小組透過長期的溝通討論後，逐步形成一套資料共享之治理做法。

(二) 資料共享治理做法

1. 資料標註品質之確保

標註品質的好壞，將直接影響到未來資料用於 AI 訓練的準確度。為確保所標註的影像能符合健康醫學臨床相關 AI 研究與應用需求，醫療影像資料庫所建置的資料，是在三大醫療團隊專業醫師的帶領下完成影像標註。同時，考量到不同醫師對於影像的標註和解讀不盡相同，資料建置與標註工作小組亦透過「同儕審查」及「專家諮詢」機制，確保資料標註的正確性與完整性。

36 科技部巨量資料應用研究推動辦公室是由工研院產業科技國際策略發展所、工研院巨量資訊科技中心、資策會科技法律研究所團隊合作組成。

2. 資料共享之隱私保護

醫院端保有的醫療影像資料，除單純影像之外還包含影像註解 (image annotations)、從影像所得出的發現結果、解讀、診斷、病患資訊及其他額外詮釋資料 (metadata) 等，其中不乏有可識別個人之資料。因此，資料格式與標註工具小組建立了「兩階段資料去識別化」機制[37]，作為降低潛在隱私洩漏風險的安全措施之一。第一階段去識別化機制在處理「資料從醫院端匯集至國網中心」之隱私風險，以達到資料無法「直接識別」特定個人為目的，考量後續資料可用性並保留資料當事人行使退出權限之可能性，針對不同欄位的資料採取適當的去識別化方法；第二階段去識別化機制則在處理「資料從國網中心端提供使用」之隱私議題，主要目的在降低資料被「間接識別」之風險[38]。

3. 資料利用目的轉換之適法性

為達成醫療影像資料共享再利用之目標，除以資料去識別化作為安全維護措施之外，亦須符合我國個資法對資料利用目的轉換、資料當事人資訊自主權保障等法遵要求。醫療影像資料庫的資料，來自於醫院病患就診所產生的病歷、健康檢查或醫療資料，匯集至資料庫供研究利用，則涉及資料利用目的轉換之問題。依我國個資法規範，醫療影像資料庫建置情境下所

37〈科技部「醫療影像之巨量資料建立與應用研究專案計畫」共用資料庫之法規議題問答 (Q&A)〉，臺北醫學大學校級人工智慧醫療研究中心，https://aimc.tmu.edu.tw/Front/Page.aspx?id=FRMe0Fal1RU=（最後瀏覽日：2020/11/18）。

38 資料格式與標註工具小組在推動辦公室的協助下，訂有跨研究團隊資料共享之隱私安全規範，說明醫療影像資料二次去識別化處理程序。

能適用的資料目的外利用依據，主要有二：(1) 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[39]；(2) 經當事人書面同意[40]。法制工作小組審慎考量此二款規定及資料當事人資訊自主權之保障後，建立了「資料當事人動態同意機制」及「資料申請審查模式」。

資料當事人動態同意機制包含三大構成要素：(1) 資料當事人書面同意之取得或資料再利用之補充告知[41]；(2) 當事人撤回同意 (withdraw consent) 或選擇退出 (opt-out) 之機會；三、資料利用情形之資訊回饋。為落實此機制，醫療團隊不僅印製紙本同意書或須知寄送給資料當事人，使其知悉資料匯入國網中心供他人學術研究利用之訊息，更藉由建立網站或資訊系統等方式，回饋資料利用相關資訊給當事人，使當事人能隨時了解專案內容、醫療影像資料利用情況與成果、查詢撤回同意或選擇退出

39 我國個資法第 6 條第 1 項第 4 款。

40 我國個資法第 6 條第 1 項第 6 款。

41 依資料原始蒐集方式而有不同：

1. 專案開始推動後所新蒐集的資料：提供當事人書面須知與同意書，告知當事人專案研究目的、內容及撤回同意的行使方法，以取得資料可用於醫療影像資料庫學術研究利用目的之同意。
2. 專案推動前已存在且曾獲得資料當事人概括同意用於學術研究目的之資料：對資料當事人進行補充告知，提供書面須知，使當事人更了解醫療影像資料庫學術研究目的之資料再利用訊息，並提供撤回同意的行使方法。
3. 專案推動前已存在但未得到資料當事人同意用於學術研究目的之資料：對資料當事人進行補充告知，提供書面須知，使當事人知悉專案研究目的、內容、醫療影像資料庫學術研究目的之資料再利用訊息，並提供選擇退出的行使方法。

的聯繫管道並能更便利地行使權利[42]，以確保符合國、內外個資隱私規範中，當事人資訊自主、透明性等原則。

建立「資料申請審查模式」之目的則在確保資料庫的近用能合乎醫院在同意書或須知中對資料當事人之承諾。法制工作小組更研擬了醫療影像資料申請使用暨審查作業相關規範[43]，明定資料申請使用之目的與條件，並設立醫療影像資料管理審查委員會，就資料提供使用進行把關[44]。

42 三大醫療團隊採掛號信方式分批完成當事人同意書與須知寄送，依各醫療團隊不同類型資料集個案統計，至 2020 年 4 月底，當事人選擇退出的比例最高約 1.9%。扣除選擇退出部分，三大醫療團隊累計可使用資料個案數為 8,057 個（每個個案不僅有一張影像），合乎預期提供使用之資料量。

43〈醫療影像資料申請審查試辦作業規範〉，國網中心醫療影像資料庫，http://lions.nchc.org.tw/files/1%E9%86%AB%E7%99%82%E5%BD%B1%E5%83%8F%E7%94%B3%E8%AB%8B%E5%AF%A9%E6%9F%A5%E8%A9%A6%E8%BE%A6%E4%BD%9C%E6%A5%AD%E8%A6%8F%E7%AF%84.pdf（最後瀏覽日：2020/11/18）。

44 醫療影像資料申請審查試辦方案自 2020 年 4 月正式啟動，截至 2021 年 1 月為止，已有 13 個研究團隊通過醫療影像資料使用申請審查。現階段國網中心已陸續開通使用權限，供通過審查之研究團隊使用資料，資料使用成果將待開通使用後每半年追蹤觀察。

二、國際案例—聯合式健康資料系統之治理

(一) 背景

世界經濟論壇 (World Economic Forum, WEF) 自 2018 年 7 月至 2020 年 7 月推動「打破健康資料藩籬專案計畫」(Breaking Barriers to Health Data Project)[45]，目標在測試如何藉由分散的聯合式資料系統，共享基因等敏感健康資料，精進罕見疾病的診斷治療，並建立明確的治理模式，優化系統運作的效率、確保病患隱私及資料安全，且期望能在跨國之間永續運行。聯合式資料系統的技術原理是利用多方互聯結點(multiple interconnected nodes)，透過應用程式介面 (Application Programming Interfaces, API)，將分散於不同地理位置的資料系統與資料格式安全地開放近用。利用共通的網路架構，使各節點在隱私、安全、身分認證 (authentication) 和稽核特性 (auditing features) 等方面有共通的設定，進而促使各節點資料庫遵循相同核心原則與規則 [46]。

不少國家或機構因健康資料的敏感性，採取資料在地化政策，而聯合式資料系統可使健康資料在不搬離國內或組織內部的情況下，增加被近用的機會。雖然近年來聯合式資料共享模式的倡議逐漸增加，但實際上不同機構團體之間如何成功建立

45 *See* Breaking Barriers to Health Data Project, World Economic Forum, https://www.weforum.org/projects/breaking-barriers-to-health-data-project (last visited Oct. 29, 2020).

46 *See* World Economic Forum [WEF], *Sharing Sensitive Health Data in a Federated Data Consortium Model: An Eight-Step Guide* (2020), http://www3.weforum.org/docs/WEF_Sharing_Sensitive_Health_Data_2020.pdf (last visited Oct. 25, 2020).

聯合式資料系統尚有未明，除了技術上有難度，更大的挑戰在於「如何在不同機構之間形成並維繫透明與信賴的關係」。

藉由「打破健康資料藩籬專案計畫」，幾個澳洲、加拿大、英國與美國的基因資料及健康照護機構[47]，在 WEF 的領導下形成一個「聯合式資料聯盟」(federated data consortium)[48]，期望充分利用聯合式基因資料改善診療結果，增進罕見疾病病患之利益。儘管聯合式資料系統有助於提升資料共享、改善健康醫療服務，運作上但仍需有完善的安全維護措施，並有相關政策以因應惡意行為人或資料外洩等風險，因此在建立資料聯盟之前，需考量如何有效制定並執行資料聯盟之治理架構。

(二) 聯合式資料聯盟之建立步驟

依「打破健康資料藩籬專案計畫」的執行經驗，前述機構主要歷經下列八項步驟，逐步建立出聯合式資料聯盟，以提升不同機構之間的信任與合作。同時透過 WEF 作為公正第三方角色，協助調和不同機構所屬地區資料蒐集相關法規、資源、技術等面向之落差，促進安全、公平、合法資料共享生態系之形成。

1. 建立信任 (establish trust)

儘管可透過技術設計強化資料聯盟夥伴 (partner) 對彼此資料存取行為之信任，但真正值得信賴的資料聯盟，應在成立之初開始建立信任關係。需先選對資料聯盟夥伴，瞭解他方機構

47 包括澳洲 Australian Genomics Health Alliance、加拿大 Genomics4RD、英國 Genomics England、美國 Intermountain Healthcare。

48 *Supra* note 46.

的起源 (origin)、策略目標 (strategic goals) 及取得資料之研究目的 (research objectives) 後，衡量與己方機構目標的對應關係[49]。涉及跨國資料共享時，亦應注意不同地區因文化與價值之差異，對信任與否的評估項目亦不盡相同[50]。此外，考量資料聯盟是定期的夥伴關係，在確認信任關係之後，還需瞭解潛在合作夥伴領導階層的支持程度。

2. 界定問題 (define problem)

聯合式資料系統採取遠距資料近用方式，無須將資料搬離在地儲存空間，可幫助臨床醫師和研究者取得輔助診斷所需之資料。然而，聯合式資料共享方法較適合運用在「利用分散的資料解決明確問題」之情境，故合作夥伴需先共同確認聯合式資料聯盟可解決之問題。

---

49 依 WEF「打破健康資料藩籬專案計畫」之經驗，資料聯盟夥伴關係的確認，並非簡單電話溝通或透過網路快速查核所能達成，過程中需經多次親臨會議 (in-person meeting)。會議應聚焦討論的事項包括：目前各機構所蒐集的資料類型、各機構如何透過行為準則或其他指引文件幫助日常運作、各機構對短期和長期資金的運用是否有任何控制。需先瞭解潛在合作對象的動機、機構優先考慮的事項及資料資產，確保所承諾的行動能在機構優先考慮事項及能力所及範圍內達成。

50 例如北美及歐洲地區傾向資訊公開方式 (openness with information)，且通常採取信任但要查證 (trust but verify) 的策略；東亞地區看重聲譽 (reputation)，傾向要求提供成功事蹟紀錄作為證明；中東與南亞國家則採取查證後信任 (verify then trust) 的策略；拉丁美洲地區則會透過社交與商業互動方式決定共通價值。*See* Jeanne Brett and Tyree Mitchell, Research: How to Build Trust with Business Partners from Other Cultures, Harvard Business Review (Jan. 31, 2020), https://hbr.org/2020/01/research-how-to-build-trust-with-business-partners-from-other-cultures (last visited Oct. 28, 2020).

3. 對準誘因 (align incentives)

擁有資料的機構需分享加入資料聯盟的動機，說明該機構對資料聯盟的潛在貢獻。各機構加入資料聯盟的誘因不同，且實際上，機構加入資料聯盟的誘因和動機，可能遠超過原先設定的目標[51]。為維持資料聯盟的長期發展，機構必須先揭露是否具備維持資料聯盟預期目標之能力，說明該機構目前擁有的資料集特性與未來資料集之蒐集規劃[52]。為明確掌握資料聯盟中可供近用之資料，各機構應說明各自資料庫中已存在的資料類型與數量。

4. 確認資源 (identify resources)

人力資源方面需確認、挑選機構內部菁英團隊，負責資料聯盟的建立與運作，並帶領機構內部跨工作團隊的參與，包括政策與法律團隊、技術團隊、研究或臨床團隊等。

資金方面，需確保有持續參與資料聯盟的資金來源。主要資金花費在確保資料集的建構與可互通、建立並執行 API、管理資料系統更新或改善之技術元件等方面。為確保能長期參與資料聯盟，可建立經濟模型估算參與資料聯盟所產生的利益，並將更換領導階層所帶來的風險納入考量。

51 除了為病患利益改善診斷結果之外，還可能期望藉此拓展機構的國際聲望。

52 藉由未來資料蒐集的結構 (data-collection schema) 與資料集成長軌跡 (growth trajectory) 等資訊，可用以估量機構目前與未來的能力。

5. 識別機構落差 (identify institutional gaps)

各機構內部或許有不同的運作方式，例如在資料蒐集取得資料當事人同意的政策與模式、資料結構規範 (data structuring norm) 等方面有顯著差異，必須在各機構形成夥伴關係的前期及早揭露。

作法上可透過公正第三方組織協助瞭解各機構之間的差異，並引導各機構在資訊透明的情況下進行溝通討論。以「打破健康資料藩籬計畫」為例，WEF 扮演著公正第三方的角色，訪談資料聯盟各機構確認機構間之落差，並提供標準化做法。訪談議題聚焦於三項關鍵領域：1. 資料蒐集與同意規範[53]；2. 運作規範與標準[54]；3. 技術標準[55]。各機構對三項關鍵領域問題的回答，將會構成資料聯盟治理模式的基礎。

53 問題在「瞭解機構如何蒐集資料」，包括：病患是否知悉資料被蒐集的原因、病患是否同意共享資料、病患是否知悉資料被共享的原因、病患是否瞭解資料如何被共享、機構是否將溝通結果適當回傳讓病患知悉、資料蒐集是否遵循既有的法規和規則。

54 關注在「機構如何於資料聯盟中運作」，包括：機構接受資料徵詢 (query) 的對象有哪些、資料使用目的為何、允許回傳資料徵詢的結果有哪些、發生爭議時由誰處理、聯盟加入新成員的門檻。

55 包括如何確保在安全傳輸過程中進行資料徵詢、如何保護病患隱私、所建立的標準是否讓人知悉、管理程序有何地方改變、需達到的可互通性程度（可接觸到 API 或資料集）、確保資料完整性的機制為何、目前如何使資料協調一致。

6. 建立治理模式 (create governance model)

資料治理模式有助於維持並強化資料聯盟夥伴間彼此的信賴，良好的資料治理模式應包含：1. 基本原則，作為引導未來決策或解決疑義之用；2. 明確標準，用以監督日常運作、確保資料聯盟有效啟動，並藉以達成團隊共同目標。基本原則的制定，可先確認機構之間既已適用的資料共享政策是否具有共通性，或參考業界共通原則，例如：歐洲健康資料聯盟普遍適用之資料可查找、可近用、可互通與可再利用 (Findable, Accessible, Interoperable and Reusable, FAIR) 原則。明確標準的建立，目的在維持資料聯盟所有夥伴行為的一致性，包含資料蒐集與同意規範、管理運作規範與標準、技術標準等。

7. 建構資料 (structure the data)

資料必須以「能在聯合式資料系統中徵詢近用之方式」加以組織建構，因此資料聯盟應適用一致的資料建構標準。從前蒐集的資料與近期蒐集的資料，建構方式可能因機構內負責處理資料的技術團隊不同而不一致，且資料若非初次蒐集或以可遠距近用、共享的方式儲存，在建構時可能更為耗時。

8. 部署技術 (deploy the technology)

各機構技術團隊應確保 API 程式的運作，符合資料聯盟治理模式之共通原則與標準，並協助持續改善聯合式資料系統。此外，為有效追蹤利用聯合式資料系統所產生的資料洞見、研究或臨床發現，資料聯盟可建立關鍵績效指標 (Key Performance Indicators, KPIs)，並利用 API 協助追蹤。

伍、 結論

由於機器學習是當前健康領域 AI 訓練的主流，「資料的蒐集、處理與利用」幾乎左右了 AI 的訓練與運作結果，在欠缺適當資料的情況下，AI 的準確度將受到影響而難以發揮預期效用。欲提升 AI 可信賴之程度，需先思考如何降低 AI 偏誤風險，高品質、具代表性的資料，是降低 AI 偏誤風險不可或缺的條件，此論點可從歐盟與 OECD 等國際組織相關建議中略窺一二。例如歐盟將「隱私與資料治理」列為建立值得信賴 AI 的重要實踐要求，認為確保資料品質與資料完整性，有助於提高 AI 系統的效能；而資料不完全或資料治理不良，可能導致 AI 系統產生不公平或歧視的結果。OECD 亦認為安全、公平、合法且符合倫理的資料共享，能提升健康醫療 AI 的健全性進而擴大應用。

然而，健康醫療資料的敏感性使各國採取資料在地化、個資保護等法制政策，大幅降低取得高品質、具代表性資料之機會。資料在地化法制直接限制資料儲存的地理位置阻礙資料流通；又因個資保護規範有許多細節規定，例如目的特定、資料當事人資訊自主權保障等，資料持有者若不了解規範內容恐影響資料共享再利用。不過資料保護法制政策的浪潮，亦帶動有志的健康醫療人員或研究者進一步思考，如何在既有個資隱私保護要求下，突破資料共享的屏障。國內外已有少數跨機構健康醫療資料共享的成功案例可供借鏡，例如：國內推動之集中式醫療影像資料庫及 WEF 推動之健康資料聯合資料系統。

因應個資保護法制下目的特定之原則，健康醫療資料庫的建置，無論是集中式或分散式資料庫，皆需處理資料利用目的

轉換與資料當事人資訊自主權保障的問題。國內醫療影像資料庫採取當事人動態同意機制，除了主動書面通知資料當事人說明資料利用目的之改變，給予資料當事人表達同意之機會及行使退出權之管道，並以資訊回饋方式幫助當事人了解其資料再利用之情況。WEF 聯合式健康資料系統則透過溝通瞭解合作夥伴所持有的資料範圍與特性、如何蒐集資料、如何讓病患知悉資料被共享的原因，建立標準化做法，且以問題解決導向進行資料共享，避免資料再利用目的無限擴張。

面對不同機構在法制政策、技術、人力與經費等面向之落差，國內醫療影像資料庫與 WEF 聯合式健康資料系統之建置，皆組成跨領域工作團隊，且在第三方團隊的協調下，從專案推動開始將個資隱私保護、資訊安全、資料品質、互通性與可用性、資料庫的長期維運等議題納入考量，形成共同遵循的規範或標準。這也凸顯跨機構資料共享再利用的成功要素，不僅是單純資料庫平台或系統本身的開發建置，完整的治理模式更是關鍵，能夠促進資料共享生態系之形成，間接提升健康醫療 AI 發展之健全與可信賴程度。