健保資料目的外利用之法律爭議--從去識別化作業工具談起

吳全峰[1] 許慧瑩[2]

我國衛生福利部（簡稱衛福部）中央健康保險署（原行政院衛生署中央健康保險局，簡稱健保署）依據相關法律辦理全民健康保險業務，因此擁有全國民眾之納保與就醫資料，並於 1996 年委託國家衛生研究院建置「全民健康保險研究資料庫」，訂定相關申請與使用規定，釋出資料提供醫療政策與公共衛生研究應用；自 2011 年起，衛福部進一步依據「國民健康資訊建設計畫」建置「加值應用協作中心服務平台」（現為衛生福利部資料科學中心，簡稱資科中心），持續提供申請者於該中心獨立作業區進行跨資料之加值應用。然而，相關資料之釋出卻引起侵害民眾資訊隱私與隱私自主之疑慮，相關爭議包括告知後同意之欠缺、作業程序是否公開透明、新舊法之適用爭議、公共利益之範圍、資料技術面（去識別化）資訊安全之質疑等，後續並有相關訴訟之提起（參見台北高等行政法院 102 年訴字第 36 號、最高行政法院 103 年度判字 600 號、台北高等行政法院 103 年度訴更一字第 120 號、最高行政法院 106 年度判字第 54 號），並因此促成衛生福利資料釋出程序與標準之變動。

壹、隱私權之內涵

在衛生福利資料釋出供原始目的外利用之爭議中，隱私權為主要之爭議核心。司法院大法官於釋字第 603 號中，已闡釋個人資料應屬個人資訊隱私權之範疇，包括「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」[3]；進一步，在「人性尊嚴與個人主體性之維護及人格發展之完整」之前提下，隱私權之內涵不僅限於個人外在行動自由之保障（隱私自決），亦應包括個人人格內在形成空間之尊重（資訊隱私）[4]，以確保個人人格發展與價值選擇不致因個人資訊之任意收集、處理、利用而受到不當限縮。美國最高法院在 Whalen v. Roe 法院乙案中亦將憲法所保障之隱私內涵進一步區分為「資訊隱私」（information privacy）與「隱私自主」（privacy through autonomy）[5]，前者係指個人資訊不被任意公開之權利（the right to avoid disclosure of certain personal matters）[6]，而後者則屬個人自主決定權力不受任意干涉之權利（the right to make certain important life decisions independent of interference）[7]。雖然我國大法官

---

[1] 中央研究院法律學研究所副研究員、國立台灣大學公共衛生學系兼任副教授、國立陽明大學衛生福利研究所兼任副教授。

[2] 中國文化大學法律學系兼任助理教授。

[3] 司法院，大法官釋字第 603 號，http://www.judicial.gov.tw/constitutionalcourt/p03_01.asp?expno=603

[4] 秋文聰，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，168 期，頁 177（2009）。

[5] Whalen v. Roe, 429 U.S. 589, 599-500 (1977).

[6] Id. at 599.

[7] Id. at 599-600. See also Richard C. Turkington, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. Ill. U. L. Rev. 479, 498 (1990).

及美國最高法院均認為憲法對資訊隱私權之保障並非絕對[8]，並可在經比例原則之權衡下給予適當之管制（regulation）；但其仍須同時衡量被視為隱私權重要利益之資訊隱私與隱私自主（dual privacy interest）[9]，且考量之變因十分細緻，包括資訊內容、可能侵害、資訊安全保護機制等[10]。

但目前政府在公務機關依職權蒐集當事人與衛生福利相關之資料，以提供第三人利用為目的所進行之資料處理與利用之整體政策規劃與執行上，對於哪個環節需要尊重當事人於何種範圍決定是否揭露其個人資料之自主權保障、何種資訊可能與人格形成或人格自由開展密切關聯，卻仍未有充分討論。以法務部法律字第 10303513040 號函釋為例，其主張「如將公務機關保有的個人資料運用技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料，公務機關得自行決定是否公開或提供」[11]，便將公開之資訊是否仍得識別當事人與該資料是否得不經當事人同意便任意處理並公開，混為一談；蓋就前者而言，雖然獨特且個人化（unique and personalized）資訊已被匿名化而使其與當事人間之鏈結中斷，而保障部分隱私利益，但去識別化是否便表示得因此恣意在個人不知情且未同意之情況下將其資料去識別並任意運用在原始同意目的外之用途，卻不無爭議（尤其是牽涉敏感性個資之保護）。在生命倫理（bioethics）之相關討論中，便強調過度重視去識別化（de-identification）之結果，將可能使攸關研究參與者保護之其他要素（包括自主權）被過度簡化甚至忽略[12]。

雖然有關健保資料釋出並提供原始目的外利用之爭議有其重要性，但論點卻也十分繁雜，本文限於篇幅並無法逐一討論，故將討論之議題限縮聚焦於無從識別當事人之概念與去識別化作業工具之討論。

貳、「無從識別特定當事人」之爭議

若暫不考慮提供第三人利用之資料處理目的是否仍處於原始蒐集目的範圍內之爭議，各界更感興趣的是個人資料於何種條件下喪失其獨特且個人化之特徵而不再受個資法所規範。尤其個資法第二條第一款係以個人是否可透過直接或間接方式加以識別作為判斷該資料是否屬個資法所規範之個人資料；法務部法律字第 10303513040 號函釋亦以運用技術去識別化而呈現方式已無從直接或間接識別特定個人，作為判斷資料是否屬個人資料之依據，及是否得逕依檔案法第十八條或政府資訊公開法第十八條規定公開或提供；最高行政法院於 106 年度判字第 54 號判決中亦同樣認為，資料是否屬「個人資料」之判準為資料內容之「去識別化」

---

[8] 司法院大法官釋字第 603 號。See also NASA v. Nelson, 131 S. Ct. 746, 751, 760 (2011).

[9] Jessica C. Wilson, Protecting Privacy Absent A Constitutional Right: A Plausible Solution to Safeguarding Medical Records, 85 Wash. U. L. Rev. 653, 671 (2007).

[10] In re Crawford, 194 F.3d at 959; Fraternal Order of Police, 812 F.2d at 110.

[11] 法務部，法律字第 10303513040 號函釋，https://mojlaw.moj.gov.tw/LawQuery.aspx。

[12] K. L. Hudson and F. S. Collins, Bringing the Common Rule into the 21st Century, 373(24)NEJM 2293, 2294 (2015).

作業是否完成[13]，故去識別化（無從識別特定當事人）之內涵以及如何達成去識別化，便成為重要之議題。

一、去識別用語定義之不一致

（一）國內法觀點

但分析相關法律規範與行政法院判決內容，卻不難發現法務部及行政法院雖然肯認資料經「去識別化作業」而不再具個人化屬性，即非屬「個人資料」而不受個資法之規範；但對所謂「去識別化作業」之定義與內涵卻相對模糊且混亂，而進一步導致釋出之資料是否仍屬「可間接識別當事人」之判斷（個資法第二條第一款與個資法施行細則第三條），出現爭議。

舉例而言，歐盟（European Union，簡稱 EU）之個人資料保護規則（General Data Protection Regulation，簡稱 GDPR）[14]便將假名化（pseudonymization，編碼便屬假名化作業工具之一）與匿名化（anonymization）之概念適度區隔，並認為前者因仍可透過與其他資料串接/對照以識別特定個人[15]，故被視為可識別資料（information on an identifiable natural person）[16]，而在利用上需遵守以下原則：可供對照以識別當事人之資訊需隔離儲存，且所有利用資料者（包括資料管理者（information controller））均不得接觸該資料[17]。相關研究亦指出，是否可得重新識別當事人並不適合單純以去識別化作業之種類做出判斷，而可能需要進一步依資料釋出之類型、數量與範圍做出判斷[18]。我國立法例中，人體生物資料庫管理條例第三條亦將編碼、加密與去連結視為不同之資料處理方式，並認為不同作業程序對能否再識別當事人之難度並非一致，如編碼僅能達到難以辨識個人身分之程度，

---

[13] 最高行政法院認為，「如果該資料內 容已完成「去識別化」作業，「個人」屬性即已消失，不能再視之為新個資法所規範之「個人資料」，而該資料收受者對資料之後續處理及利用，亦不受新個資法之規範。但若未進行「去識別化」作業，或作業不嚴謹，未達成「去識別化」作業應有之實證效用（即徹底切斷資料內容與特定主體間之連結），該收受之資料仍具「個人資料」屬性時，則應依其收受目的是為「處理」或「利用」而受新個資法對應法規範之規制（「處理」行為受新個資法 第15條及第6條之規範，而「利用」行為受新個資法第16條及第6條之規範）」。

[14] Regulation (EU) 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 (General Data Protection Regulation), 2016 O.J. (L 119) 4.5.2016, p. 1-88 (EU), at Recital 26 [hereinafter GDPR].

[15] Emma Swahne, **Data Protection by Design and Default, 64 (Master Thesis,** University of Lapland, 2016).

[16] Article 23 of the GDPR.

[17] Recital 23(c) of the GDPR, "In order to create incentives for applying pseudonymisation when processing personal data, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure, for the respective processing, that the provisions of this Regulation are implemented, and ensuring that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the data shall also refer to authorised persons within the same controller."

[18] Sophie Stalla-Bourdillon andAlison Knight, Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization And Personal Data, **34 Wis. Int'l L.J. 284, 284 (2016). See also** C. Christine Porter, De-Identified Data and Third Party Data Mining: The Risk of Re-Identication of Personal Information, 5 Shidler J. L. Com. & Tech. 3, 3 (2008).

但加密尚須將足以辨識個人之資料/資訊轉化為無可辨識，去連結甚至要求永久無法以任何方式連結/比對。

但在個資法相關規範中，卻未將假名、匿名、編碼、代碼、隱藏部分資料、去識別、去連結等名詞適當定義，在實務及判決中更將這些不同內涵之名詞交互混用，便使得資料在何種條件下可被排除不被視為可直接或間接識別之個人資料出現混淆，導致個人資料保護之混亂與困境。舉例而言，個資法施行細則第十七條便認為「個人資料以代碼、匿名、隱藏部分資料…無從辨識該特定個人」，便屬個資法所謂「無從識別特定當事人」，而無視代碼、匿名與隱藏部分資料等不同作業方式之內涵並不完全相同，對個人人格發展與價值選擇之影響程度亦可能有所差異，過度簡化且均一地將不同去識別化作業工具做相同處理，對於個人隱私權保障並不適當。且參照個資法施行細則第三條之規定（「…得以間接方式識別，指保有該資料…須與其他資料對照、組合、連結等，始能識別該特定之個人」），以代碼為處理作業後之資料應仍屬可間接識別（因其雖不能直接識別，但仍可與其他資料對照、組合、連結後識別特定個人，內涵與人體研究法所稱之「編碼」相近），但細則第十七條卻又認定資料若以代碼處理後便屬無從直接或間接識別個人之資料，兩者顯然有所矛盾。換言之，因不具特定個人屬性資料與個人資料為二個相對應之概念，在瞭解何謂不具特定個人屬性資料進而不適用個人資料保護法前，應先行確認其定義；但個資法相關規定卻對於例示之去識別化作業工具（代碼、匿名、隱藏部分資料）之操作型定義、施行方式、資料狀態、與去識別化概念之關聯性，未有說明或回應，甚至與個資法其他條文或其他法規相矛盾，導致在確認不具特定個人屬性資料（去識別化資料）上出現挑戰。

而在台北高等行政法院 103 年訴更一字第 120 號判決中，法院甚至認為資料經過編碼方式加密處理後，便已屬無從直接或間接識別特定個人之資料，「雖然資料保有者仍保有代碼、原始識別資料對照表或解密工具而得還原為識別資料，但只要原資料保有者並未將對照表或解密方法等連結工具提供給資料使用者，其釋出之資料無法透過該資料與其他公眾可得之資料對照、組合、連結而識別出特定個人時，該釋出之資料即屬無法直接或間接識別之資料而達法律規定去識別化之程度」。但編碼是否屬不得間接識別特定當事人之去識別化工具，在個資法架構下已有前述爭議；若再進一步參考歐盟「資料保護指令第29條資料保護工作小組」（Article 29 Data Protection Working Party）於2014年所發布之「第216號有關個人資料匿名技術意見書」（Opinion 05/2014 on Anonymisation Techniques，簡稱WP216）[19]，便可發現編碼（假名化技術）所進行之資料處理，並不被認為屬歐盟所認可去識別之匿名化技術，因其認為編碼技術只能作為減低資料與資料間連結性、減少再識別特定當事人風險之資訊安全措施，資料與資料間之連結仍然存在[20]。最

[19] Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques (hereinafter WP216) (2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last visited Dec. 17, 2017).

[20] Id. at 7.

高行政法院於106年度判字第54號判決中雖然挑戰台北高等行政法院之見解，但其理由僅係因編碼係由資料蒐集者執行，導致其仍掌握還原「資料與特定主體間連結關係」之鑰匙而具「還原」資料與主體間連結之能力；對於「編碼」作為作業工具是否已足以達成個資法去識別化之要求，在個資法規範未有明確定義之限制下，最高行政法院亦未加以深論，殊為可惜。

（二）比較法觀點

另方面，若觀察其他國家個人資料保護法制之發展，不難發現各國對去識別化之內涵與作業工具雖各有不同，甚至有相同名詞但內涵完全不同之情況（如英國與歐盟均使用「匿名化」一詞，定義卻有所差異，詳後述），但均有明確定義以避免概念之混淆；但我國個資法制在納入相關名詞時，卻未進一步考慮各國規範內涵之差異，橫向切割移植之結果，也使得去識別化資料之概念治絲益棼。

以前述 WP216 意見書為例[21]，其認為匿名化係為達成個人資料「不可逆（irreversibly）」無法回復識別狀態的技術[22]；但歐盟個人資料保護指令[23]（1995 Data Protection Directive，簡稱 DPD）對於如何進行匿名化並未加以具體規範，而是聚焦於進行技術處理後之資料狀態（GDPR 並未修正此部分規範），亦即匿名化資料須為以任何可能之合理方式均無法識別個人時方符合規範狀態[24]。舉例而言，資料之匿名化應處理到何程度始符合相關規定，意見書雖例示提供相關匿名技術作業處理工具（如 noise addition、permutation、differential privacy、aggregation、k-anonymity、I-diversity 與 t-closeness），但主要仍以匿名化資料是否符合以下標準作為判斷依據[25]：資料經匿名技術處理後是否仍可能識別特定個人（is it still possible to single out an individual?）、是否仍可連結至個人相關紀錄（is it still possible to link records relating to an individual?）、及是否仍得從相關資訊推斷至個人（can information be inferred concerning an individual?）[26]。若從歐盟之規範反觀我國個人資料保護法律架構，不難發現：（1）我國個資法施行細則第十七條之「匿名」是否即為歐盟規範下之「匿名」，因我國法中對其並未有任何定義，並無從判斷。但從國家衛生研究院（簡稱國衛院）在相關訴訟中所為之主張（稱其所採「假名

[21] Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques (WP216), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last visited Dec. 17, 2017).

[22] Id. at 3.

[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

[24] 需特別說明者為，匿名化屬於對個人資料的處理（further processing），故不僅在進行匿名化前亦須符合個人資料蒐集、處理、保存之相關法制規定，且必須通過目的相容性評估（compatibility assessment）測試。

[25] Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques (WP216), 3 (2014).

[26] 另需注意者為，匿名化技術雖能加強隱私保障，但仍必須認知資料雖已經匿名處理，但仍具有剩餘風險，亦即仍有可能連結至特定個人而成為「一般資料保護規則」所規範之具個人屬性資料，故仍需個案認定並定期檢視。

化」之去識別化作業為「匿名化」之去個人化處理），顯然與歐盟對匿名之概念相違；而在「假名化」與「匿名化」之基本概念與再識別風險並不相同之情況下，將兩者概念混用，對於個人資料保護之強度將可能造成負面影響（如誤認「假名化」與「匿名化」之再識別風險相似，而不適當地對前者採取較為寬鬆之管制策略）。（2）歐盟之「匿名化」概念雖然某種程度相近於我國人體生物資料庫管理條例中所謂「去連結」之概念，但個資法中卻未採「去連結」之概念，而以「匿名」取代，是否有意區隔，亦無從得知。進一步，我國法規範中對去連結之要求是「永久」無法以「任何」方式連結比對可供辨識之特定個人資料，與歐盟認為匿名化僅是「不可逆」無法回復識別狀態（並非「永久」無法識別）之概念並不完全相同；也因歐盟認為在時間、資源、資料種類與數量毫無限制之情形下，匿名化資料仍有再識別之風險[27]，故該意見書建議不使用「匿名化」或「匿名化資料」等名詞，而在規範中採「匿名化工具」作為規範標的，以表現再識別之風險與消除該風險尚需有其他組織或程序之配套[28]。相對而言，我國法規範中「去連結」對再識別風險之標準，顯然較歐盟之「匿名」概念更為嚴格，若直接將去連結概念套用在個人資料保護之實務操作上，是否適當不無討論空間。

而相同之「匿名」概念，在英國在內化歐盟個資保護指令為其內國法並發行相關指引時，卻採與 WP216 意見書建議不盡相同之立場（主要原因可能在於英國對於 WP216 所建議之匿名化標準，係針對資料管理者或資料蒐集者而設置，有不同見解，詳後述），而在英國資訊專員辦公室（Information Commissioner’ s Office，簡稱 ICO）於「匿名：管理資料風險實作指引」 （Anonymisation: Managing Data protection Risk Code of Practice）中在介紹經眾多匿名化技術後的資料就像頻譜一樣分散著不同的風險，將編碼或隱藏部分資料亦含括在匿名之概念內[29]，導致「匿名化」之內涵較歐盟所指涉者更為廣泛。雖英國對匿名化之解釋似與我國實務上之認知較為相近（如國衛院便認為其所蒐集之健保資料經過代碼或移除部分資料及屬匿名之去個人化處理[30]，另如法務部於 105 年 4 月 8 日法律字第 10503505760 號函檢送「公務機關利用去識別化資料之合理風險控制及法律責任」之研析報告則認為資料以代碼等雙重加密方式去識別化即屬「可匿之擬匿名化資料」），但是否便能因此主張我國個資法之「匿名化」概念係採與英國法制類似較為寬鬆之架構，不無疑問；主要原因在於，個資法施行細則第十七條係將代碼、匿名、隱藏部分資料等去識別化作業工具並列，暗示法律體系有意將前述去識別化作業工具加以區隔，而無法將「代碼」或「隱藏資料」逕自納涵於「匿名」之概念下。也因此，實務上將代碼與匿名之概念混用，但個資法上又將其區隔，此矛盾便導致在個人資料保護之論述上，出現字意混淆且概念衝突之狀況。

---

[27] Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques, 7 (2014).

[28] Id.

[29] UK ICO, Anonymisation: Managing Data Protection Risk Code of Practice, 36 (2012), available at https://ico.org.uk/media/1061/anonymisation-code.pdf (last visited Dec. 17, 2017).

[30] 台北高等行政法院 103 年訴更一字第 120 號判決。

再以，最高行政法院認為「基於『個人資訊隱私權』之考量，而徹底排除特定主體之個人資料，其手段太過，有礙於公益之實踐」，其論述基本上並無太大爭議；但此見解卻似乎暗示不應有徹底排除特定主體個人資料之去識別化方式，亦即我國法中不存在歐盟所謂「不可逆（irreversibly）」無法回復識別狀態的匿名技術（因其基本上要求徹底排除特定主體個人資料），而僅接受類似英國所主張之「可匿之擬匿名化資料 」方式進行去識別化。但若依最高行政法院之見解，則個資法施行細則第十七條之「匿名」概念便難以解釋，因個資法規範若無意且不能要求完全排除特定主體個人資料，則匿名之概念將變成與代碼、移除部分資料相近，則法條上刻意將這些概念區隔之意義將不復存在。且最高行政法院之論述亦可能過於倉促，而忽略即令英國將假名視為匿名工具之一，仍不排除完全可以去除個人資料之嚴格匿名作為去識別化作業工具（亦即假名雖可為匿名之工具，但仍不可逕將假名等同於匿名）；且亦忽略歐盟於特定狀況下的確規範需採嚴格定義之「匿名化」作業工具後方可提供資料，而其所例示之匿名技術作業處理（如 differential privacy）便係嘗試在法律要求需徹底排除特定主體個人資料之前提下，仍得以提供資料分析完整性之作業工具。

前述匿名與假名概念之混雜僅是一例，若再將各國對編碼、隱藏部分資料、去識別、去連結等不同概念納入，其所構成去識別化作業工具之架構將更為複雜，且定義各異；若我國法未能將不同去識別化作業工具做細緻定義與區隔，或將各國名詞翻譯後再混用，便可能導致行政機關與法院在個人資料保護之執行與判斷上，出現相互矛盾之論述。

二、去識別化內涵之空白

（一）國內法觀點

除前述去識別化作業工具之定義區隔不夠明確外，我國個人資料法律規範對去識別化之內涵亦存在概念上之空白。以台北高等行政法院 103 年訴更一字第 120 號判決為例，法院雖認為去識別化程度應綜合考量個人資料類型、敏感性程度、對外提供資料之方式、引發他人重新識別之意圖等因素進行整體風險影響評估，但對去識別化內涵、去識別化與風險控管之區別卻又加以混用：如（1）法院認為含有個體性、敏感性之擬匿名化資料仍可被視為去識別化資料[31]。但若資料在專屬代碼、雙向加密後仍具備個體性特徵，實難謂其已符合個資法所謂去識別化之定義，而仍應被視為個人資料；且即令判決中採用法務部見解創設「可匿之擬匿名化資料」之名詞，但因其本質仍屬假名化資料（pseudonymised data）[32]，自應屬落入個資法施行細則第三條之間接識別。但法院將匿名化（法務部定義為對

[31] 如高等行政法院認為「…風險檻值相對較低，其資料去識別化之程度可相對放寬，可提供含有個體性、敏感性之擬匿名化資料，亦即可採取「可匿之擬匿名化資料」方式進行去識別化（即以專屬代碼、雙向加密或其他 技術處理，使處理後之編碼資料無從識別特定個人，惟原資料保有者保留代碼與原始識別資料對照表或解密工具〈鑰匙〉之方式）」（底線為作者所加）。

[32] 法務部 105 年 4 月 8 日法律字第 10503505760 號函。

任何人而言均無法採取任何合理可能方法識別特定個人）與擬匿名化（法務部定義為以編碼或別名取代識別符之可逆去識別化作業工具）後之資料均一地視為個資法中不可直接或間接識別之資料，某種程度反映出法院對去識別化內涵之認知似不同於個資法規範去識別化應達到「無從以直接或間接方式識別個人資料」之認知。或如（2）法院主張「風險檻值相對較低，其資料去識別化之程度可相對放寬」，並認為可因此提供含有個體性、敏感性之擬匿名化資料。但去識別化程度與內涵應為固定標準（無從直接或間接識別特定當事人），反而是去識別化作業工具可能有不同之風險門檻，而需進一步針對再識別風險較高之作業工具要求搭配其他風險控管措施。舉例而言，因假名化之再識別風險較高，GDPR 之立法理由便要求資料管理者需採取技術及組織上措施以確保 GDPR 去識別化規範之具體落實[33]，而不是如本判決倒果為因地將去識別化程度與風險檻值鏈結，甚至由後者決定前者之內涵。

最高行政法院於106年度判字第54號判決中雖某種程度挑戰高等行政法院之判斷，並認為健保署去識別化作業模式並不足以到達「完全切斷資料內容與特定主體間之連結線索」之程度，故「個人資料」屬性尚未被全然排除[34]，而仍屬受個資法規範之個人資料；但其卻又認為去識別化功能作用僅限於「確保社會大眾…不會從資料內容輕易推知該資料所屬之主體」，並以此為基礎主張「去識別化」實證效用強度要求應與「去識別化」作業設置目的區隔。惟就後者而言，去識別化實證效用強度是否可清楚地與去識別化目的加以區隔，不無爭議；而此爭議，同樣還是與我國個資法對於所欲達到之「去識別化」內涵為何不清楚有關。詳言之，不同去識別化作業工具所涉及之實證效用強度本就有所不同（如代碼之去識別化實證效用強度便較差異隱私（differential privacy）為差），但較差之實證效用強度並不代表其去識別化之功能不夠充分；蓋不同社會對於個人資料應去識別化到何種程度始能稱為不具個體性之資料，可能因社會價值而有差異，若對於個人資料之運用持較寬容態度之社會，便可能容忍實證效用強度較弱之去識別化作業工具（如代碼），反之則否。也因此，去識別化實證效用強度是否充分，便應取決於我國個資法對去識別化內涵之想像與其法規範之目的，而不宜貿然將兩者切割或逕自排除特定要件（連續不當之私人資訊探究行為）作為檢視去識別化實證效用強度之依據。但包括我國法規範或行政法院均未就此議題（尤其是去識別化之內涵）作更為深入之討論，也因此使得特定去識別化工具是否符合法規範中去識別化之要求，出現爭議：如最高法院106年度判字第54號判決便載明上訴人係爭執健保資料之「『加密』，充其量僅為以一組特定之亂碼取代個人身分證號的『假名化』處理，而非真正『無從識別特

[33] Recital 23(c) of the GDPR。

[34] 最高行政法院主張，「資料實際上是一種訊息，應與訊息載體分離看待。而所謂「原始資料」其實僅是儲放資料(訊息)之載 體，因此載體即使留在原處，載體內之訊息已透過轉換載體之方式，而脫逸被上訴人之控管，並為輔助參加人衛福部所控管，只要輔助參加人衛福部之內部單位公務員，有「還原」資料與主體連結之可能，對輔助參加人衛福部而言，該資料仍未「去識別化」，而屬「個人資料」。」

定當事人』之『去識別化』」[35]，甚至認為鎖定特定主體以主動搜尋與該主體身分有關之資訊應作為測試去識別化效用強度之可能選項之一；但健保署卻認為健保資料經過個人身分證字號加密程序、刪除個人出生日(僅有出生年月)已符合新個資法對於去識別化之要求，最高行政法院亦認為上訴人所提之測試方式已超過「去識別化效用強度」之法定標準範圍。而其間之爭執便在於上訴人、健保署、法院對於去識別化內涵之想像並不相同，上訴人似認為去識別應屬對任何人均屬無法直接或間接識別，健保署則認為可逆向回復個人資訊之專屬編碼技術處理已符合去識別化之內涵，法院則似主張去識別化之內容仍應有其界線（不包括應排除鎖定並主動搜尋特定主體資訊之侵害方式）。但類似對去識別化內涵之見解歧異，並未在個資法規範或法院判決中獲得解決。

另需特別說明者為，GDPR 第 4(1)條對個人資料之定義，不僅包括可直接識別之個人資訊（如姓名、身分證號等），亦包括可間接識別個人之資訊（如生理、心理、基因、經濟、文化或社會認同（social identity）資訊[36]；我國個資法第二條第一款似亦採類似之定義（個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料）。但在行政法院在相關判決中，似乎均認可健保署將「直接」可識別個人之資料移除或編碼即可，而可「間接」識別個人之資訊是否被移除或做特殊處理（如以不具個別事件特性之聚合統計資料提供），則似乎並不成為法院判斷該處理後資料是否仍屬可識別資料之判斷標準，此是否代表法院對「不可識別」之內涵有不同於個資法之判斷，不得而知。舉例而言，最高行政法院在 106 年度判字第 54 號判決中，對於處理後資料是否具可識別性之判斷，著重在可還原資料與特定主體間連結關係之鑰匙所屬（若資料蒐集者未持有，便被認為屬不可識別之非個人資料）；但該處理後資料資料是否包含其它可間接識別個人之資料（如健保署釋出予國衛院或衛福部之資料中均仍包含個別事件（individual event）之資料，如身份屬性、投保狀態、就醫紀錄等[37]），似乎非最高行政法院所關心之爭點。但此爭點卻攸關我國個資法判斷資料是否屬個人資料之去識別化內涵範圍，似有必要進一步釐清。

（二）比較法觀點

若再從各國規範觀察，亦不難發現各國對去識別化之內涵界定亦非完全相同。詳言之，資料若不具獨特個人屬性便應非屬個人資料而不受個資法所規範，應屬各國在個人資料保護上所共通之基本原則。如美國「健康保險可攜與責任法」（Health Insurance Portability and Accountability Act of 1996 Privacy Rule，簡稱 HIPAA）

[35] 103 年訴更一字第 120 號判決。

[36] Article 2 of the GDPR, "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[37] 在歐盟規範下，此類與個別事件相關之資料（如個人之通勤紀錄），仍被視為屬可識別之個人資料，詳下節說明。Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques, 9 (2014).

便規範完成安全港（safe harbor）條款[38]或專家決定（expert determination）之去識別化（de-identified）程序[39]後之資料，已非屬受 HIPAA 保護之健康資料[40]；歐盟 GDPR 立法理由中亦說明，經匿名化（anonymous）之資料若達無法連結特定個人之程度，亦即以一切合理方法（all the means reasonably to be used）都無法與特定個人連結（relate），便非 GDPR 之規範對象[41]。

但進一步檢視前述美國與歐盟之規範，卻不難發現其對於所謂無法識別特定當事人之判斷標準並非完全相同：如美國之安全港條款便規定若去除十八項可識別資料（identifiers）便可被視為去識別資料[42]，但相較於美國對於去識別化採合理標準（reasonable level of justified confidence standard），歐盟對於再識別化風險卻採更為嚴格之認定，並因此影響 GDPR 對去識別化資料之判斷[43]。此差異植基於美國與歐盟對於隱私權（包括資訊隱私與隱私自主）之基本價值判斷並不完全相同：美國隱私權保障之核心在尊重個人自主，歐盟則將重心放在保障人性尊嚴[44]，故後者對去除個人資訊之方式與相對應之管制模式便採取較為嚴格之立場[45]。但我國對於個資法規範下去識別化（無從識別特定當事人）之內涵卻未加以細緻規範或討論，導致應以較為寬鬆或較為嚴格之標準判斷特定去識別化作業工具是否符合我國法規範所設定之立法目的，無從界定。

---

[38] 45 CFR §164.514(b)(2)(i).

[39] 45 CFR §164.514(b)(1), "Implementation specifications: Requirements for de-identification of protected health information.Acovered entitymay determine thathealth informationis notindividually identifiable health informationonly if: (1)Apersonwith appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i)Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify anindividualwho is a subject of the information; and (ii)Documents the methods and results of the analysis that justify such determination."

[40] 45 CFR §164.502(d)(2), "Uses and disclosures of de-identified information.Health informationthat meets thestandardandimplementation specificationsfor de-identification under§ 164.514(a) and (b)is considered not to beindividually identifiable health information,i.e.,de-identified."

[41] Recital 26 of the GDPR。

[42] 45 CFR §164.514(b)(2)(i), "The following identifiers of theindividualor of relatives, employers, or household members of theindividual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code … (C) All elements of dates (except year) for dates directly related to anindividual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age … (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health planbeneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code…."

[43] Chris Achatz and Susan Hubbard, US vs. EU Guidelines for De-Identification, Anonymization, and Pseudonymization, 20 No. 11 J. Internet L. 1, 7-8 (2017).

[44] Avner Levin and Mary Jo Nicholson, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground, 2(2) U. Ottawa Law & Tech. J. 357, 357 (2005).

[45] Id. at 390.

且若進一步檢視 HIPAA 之規範，針對受保護健康資訊（protected health information，簡稱 PHI）之使用與揭露，其雖不使用「匿名」或「假名」而單純使用「去識別化」之概念（類似我國個資法規範），但其對去識別化內涵之處理卻相對我國個資法規範更為細緻，包括需具有統計或科學原則、專家核決以確認收受者對經處理後資料僅有非常微小再識別風險、刪除十八項可識別資料、適用主體（covered entity）之責任等[46]。

相較美國 HIPAA 具體規範去識別化之定義、方式與結果，歐盟具體規範資料經匿名處理後須達無法回復連結至特定個人之要件，我國個資法對於去識別化內涵之想像卻相對簡單，僅強調無從直接或間接識別，並於施行細則第三條對間接識別做出簡單定義，並無法真正處理去識別化之複雜內涵，遑論將去識別化之內涵與社會對隱私權之價值加以鏈結；行政法院在處理類似之概念上雖然嘗試進一步補充去識別化概念之內容，但卻有認為去識別化需「到達『完全切斷資料內容與特定主體間之連結線索』之程度」（106 年度判字第 54 號判決）、有認為去識別化「[毋需]徹底排除特定主體之個人資料…[以免]有礙於公益之實踐」（106 年度判字第 54 號判決）、有認為「可匿之擬匿名化資料」（如專屬代碼或雙向加密等保留代碼與原始識別資料對照表或解密工具之方式）亦屬去識別化（103 年訴更一字第 120 號判決），其間對「去識別化」之概念似非完全一致。

三、去識別化之相對性

進一步，與去識別化內涵類似之討論則是去識別化之相對性，亦即就去識別化之判斷，究應從何種角度或何種標準判斷該處理後資料已達無從識別特定當事人（即去識別化實證效果應為對任何人均無法再識別，抑或僅資料蒐集者或第三人無法識別即可）。緣我國個資法對於第六條、第十六條與第十九條均有「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」之規定，但究竟資料經處理後係應以何人之角度或標準判斷該資料已達無法識別狀態，本法與施行細則均無相關定義。高等行政法院在 103 年訴更一字第 120 號判決中則主張「是否無從辨識該特定個人，應以資料接收者之角度判別揭露之資料是否具有直接或間接識別之可能」；最高行政法院於 106 年度判字第 54 號判決似亦持相同之見解，認為資料蒐集者若仍有「還原」資料與主體連結之可能，該資料便不能被認為屬資料內容與特定主體間連結徹底切斷之去識別化資料，但若僅資料釋出者單方掌握還原能力，則可被視為符合去識別化標準。

但行政法院之判斷並未真實反映此議題之複雜性。以歐盟WP216意見書為例，其便認為DPD之「合理可能再識別手段」（all the means likely reasonably to be used to identify the natural person）應指該處理後之資料對資料管理者或第三者而言是否已達到無法直接或間接識別特定個人之程度[47]（GDPR中亦延續此概念[48]）；而此

---

[46] CFR §§164.514 (c) - (h).

[47] Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques, 9 (2014).

[48] Recital 26 of the GDPR, "…To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. …".

判斷標準（匿名化係指該資料對資料控制者與第三人均屬無法識別）便與最高行政法院之見解（去識別話係指該資料對資料搜集者屬無法識別即可）不同。詳言之，WP216意見書主張，即令資料管理者已將某批資料集（data set）之可識別資料移除或編碼，但若其仍掌握該批資料集匿名化前之個別事件（event-level）原始可識別資料，該批已處理後之資料集仍將被認定屬個人資料而非匿名資料[49]；只有在資料管理者將該資料集之原始可識別資料刪除、或將原始可識別資料轉為聚合（aggregate）資料且個別事件無法再被識別（individual events are no longer identifiable）時，該批資料集始得被視為匿名資料[50]。舉例而言，若個人通勤之移動資料被蒐集後，資料控制者將直接可識別之資訊移除並提供給第三人利用，該處理後之資料集是否可逕被視為匿名資料？WP216意見書認為並不一定，而主張若前述過程中資料管理者（或任何第三人）仍可近用（access）原始可識別資料，則該資料集（包含個人通勤紀錄）仍將被視為可識別個人資料[51]；除非資料管理者刪除該批原始資料，並僅提供該批資料集之聚合統計資料予第三人（如X站於星期一之通勤人數較星期二增加160%），該經處理後所產製之資料方符合匿名化資料之定義[52]。

進一步，GDPR 認為假名化資料（資料管理者仍可透過連結額外資訊比對出特定個人資訊）並不被視為屬匿名化資料（經處理資料須對資料管理者或第三人而言均已切斷所有與可識別資料之連結）[53]，已如前述；換言之，最高行政法院在 103 年訴更一字第 120 號判決中以還原處理後資料（與個人資料連結）能力是否僅限資料釋出者單方擁有，作為判斷該處理後資料是否已屬去識別之標準，顯然便較 GDPR 之標準更為寬鬆。但須特別說明者為，在歐盟規範下，雖然要求匿名化之判斷應考量所有可被資料管理者或第三人用以直接或間接識別自然人之合理可能手段（若非合理可能之再識別手段則非 GDPR 所欲規範者），但亦說明在考量該再識別手段是否為「合理可能（reasonably likely to be used）」須考量所有客觀因素，如進行再識別所需花費費用、時間，及進行資料處理時之科技發展狀況與可得技術[54]。

最後，檢視歐盟法院在 Patrick Breyer v. Bundesrepublik Deutschland（有關動態 IP 位址是否屬個人資料之爭議）乙案之判決內容，亦可發現各國對去識別化之相對性有不同認知[55]。在本案中，主要爭點為：對網站控制者而言，在第三人（ISP

---

[49] Article 29 Data Protection Working Party, Opinion 05/2014 on anonymization Techniques, 9 (2014).

[50] Id.

[51] Id.

[52] Id.

[53] Recital 26 of the GDPR.

[54] See id, "… To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. …"

[55] Opinion of Advocate General Campos Sánchez-Bordona delivered on 12May 2016(1) Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland (Request for a preliminary ruling from the Bundesgerichtshof (Federal Court of Justice, Germany)), http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5ee615ecdad1f44e2850989689e0

業者）握有得以識別當事人的其他資訊之情況下，瀏覽者連結該網站的動態 IP 位址是否屬個人資料[56]。如德國政府便採否定見解，認為 DPD 立法理由第 26 條所稱之「合理可能可再識別手段」並非將所有客觀上可能透過第三人持有之資訊而可識別當事人的資料都納入「個人資料」的範疇；其主張因資料管理者（ISP 業者)不能在沒有法律依據下提供可識別資料予第三人，對第三人（網站控制者）而言便沒有其他合理方法可識別對應資料當事人之身分，該資料便非屬個人資料[57]。但奧地利政府及歐盟執委會則採肯定見解，認為 DPD 立法理由第 26 條並未限定當事人可否被識別之判斷係以所有資料均由單一控制者所持有為限，即令第三人僅能從資料管理者處取得經處理（如消除可識別資訊）之資料，但若第三人仍能合法且毋需耗費不成比例之資源或時間便可取得其他其他資訊，以達到再識別資料管理者所提供經處理之資料，則該資料處理者所提供經處理之資料仍應被視為個人資料[58]；換言之，即令 ISP 業者提供之動態 IP 並無可識別之個人資訊，但對網站控制者而言，其取得動態 IP 位址後便可以輕易地與其所擁有之其他資料比對而再識別特定個人，則該動態 IP 位址資料便仍應被視為個人資料。歐盟執委會則更一步說明，若第三人儲存特定資料（該資料本身可能並無可識別性，如動態 IP 位址）之目的便是要再識別該資料當事人，那麼該儲存資料之行為變屬識別資料當事人之合理可能方法，進而使該比被儲存之資料成為個人資料[59]；換言之，若網站控制者儲存動態 IP 位址之目的包括再識別特定個人（如網路攻擊者），則由 IPS 業者紀錄之動態 IP 位址使用者身分自然是識別該特定個人之合理可能方法，故動態 IP 位址在此情形下亦應被認為屬個人資料[60]。

歐盟法院在本案中採肯定見解，且亦認知此問題之複雜性，遂嘗試分別回應各國之意見。但相較而言，最高行政法院在於 106 年度判字第 54 號判決中對於去識別化之相對性卻直接採納行政機關之看法（類似德國政府之否定見解），且未進一步說明其採較寬鬆標準之正當性理由。

舉例而言，健保署雖對提供再利用之健保資料採編碼與雙向加密處理，但仍允許第三人利用健保資料與其他資料庫之資料進行串接比對；最高行政法院在此認為，就健保資料本身之可逆還原原始資料之鑰匙而言，若其係由資料管理者（健保署）所隔離擁有，則該處理後之資料便非屬個人資料，而利用資料之第三人是否可透過資料之串連再識別當事人則非最高行政法院所關心之重點[61]。但最高行政法院在此卻未進一步論述其忽略不同資料庫串連後再識別可能性之理由，導致法院對去識別化相對性之寬鬆立場可能受到挑戰。蓋依歐盟法院在 Patrick Breyer v. Bundesrepublik Deutschland 之論述，便不難發現其主張即令資料有編碼加密（如

4f359.e34KaxiLc3eQc40LaxqMbN4Pa38Te0?text=&docid=178241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=76592

[56] Id. at para. 26.

[57] Id. at para. 33.

[58] Id. at para. 36.

[59] Id. at para. 38.

[60] Id.

[61] 最高行政法院於 106 年度判字第 54 號判決中認為「固然在本案中被上訴人與輔助參加人衛福部間之『去識別化』作業的確有所疏漏(如果沒有疏漏，經過去識別化之健保資料即不再是應受新個資法規範之個人資料，後續法律觀點均屬多餘)，但本院在前同樣指明，此等資料之可識別性已大幅度降低…保密流程只要稍加改進，即可到達新個資法所定『去識別化』之標準。」

健保資料），若仍存在逆向還原之原始識別資料對照表或解密工具(鑰匙)，不論該工具係由資料提供者或資料利用者所擁有，均不能被視為匿名資料，而應仍屬個人資料；歐盟法院之主要理由在於，雖然其認同德國政府所稱，正常情況下資料管理者（ISP 業者）若無法律許可應不能提供資料（動態 IP 位址使用者紀錄）予資料蒐集者（網站控制者），但其亦認知不能亦無法排除資料管理者違法提供資料而導致資料蒐集者得以串連其所擁有之資料再識別特定個人，故只要再識別管道存在，不論實際上受到多嚴格的限制（如逆向還原鑰匙之分離保存），對於資料蒐集者而言仍應視為存在「合理方式」可經由該資料（動態 IP 位址）識別特定個人身分之可能，故相關資料雖經處理卻仍應被視為個人資料[62]。

而再觀察歐盟法院對是否具「合理可能再識別手段」之評斷態度，可發現其並不排除將第三人是否刻意再識別之動機納入對「合理可能再識別手段」是否存在之考量，並認為若第三人儲存特定資料之目的便是要再識別該資料當事人，該資料便應被視為個人資料。但我國行政法院對此卻相對採取較為保守之立場，如高等行政法院便認為去識別化之判斷，應直接排除以對照、組合、連結其他公眾可得資料之方式證明經處理後釋出之健保資料是否仍具有間接識別特定個人之可能（103 年訴更一字第 120 號判決）；最高行政法院亦認為去識別化之架構並不包含「刻意鎖定特定主體並搜尋相關資訊再與處理後健保資料資料連結之方式」（106 年度判字第 54 號判決）。歐盟法院與我國行政法院之立場差異應值得更深入之討論，但因行政法院在判決中並未說明其採此立場之理由，導致無法進一步檢視行政法院之論述是否具正當性。

參、小結

就前述分析不難發現，我國個資法規範架構與行政法院在健保資料案件之立場，對於去識別化之內涵仍存在模糊甚至衝突之見解，對去識別化作業工具亦未有明確定義，其結果便導致我國在個人資料保護上之立場並不一致，並頻頻受到挑戰；而類似之挑戰又將使我國在巨量資料分析時代下，應如何規範個人資料之釋出與利用處於不確定狀態，不僅個人隱私權之保障可能因此受到侵害，需利用健保資料之政策分析或學術研究亦將因此延滯。因此，如何在政策執行與法律操作層面，將去識別化之概念進一步明確化與具體化，實應屬我國個資法未來發展所應思考之方向。

[62] Opinion of Advocate General Campos Sánchez-Bordona delivered on 12May 2016(1) Case C-582/14 Patrick Breyer v. Bundesrepublik Deutschland, paras. 72-74.