论个人医疗信息的匿名化处理制度

——兼评《个人信息保护法》相关条款

李润生*

目次

摘要 构建完善的匿名化处理制度是化解个人医疗信息利用困局的可行选择。匿名化是指通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。按照法定标准匿名加工后的信息不再属于个人信息，从而不再受同意规则之约束。个人医疗信息具有特殊性，既应进行更高标准之保护，又应推动更高程度之利用，有必要予以特别规制。我国《个人信息保护法》关于匿名化制度的规定仍有不少缺憾，首先应当补齐短板，形成制度闭环，完善一般性的匿名化处理制度。在此基础上，我国应对个人医疗信息的匿名化进行特别规制，由政府统一认定汇集和匿名加工个人医疗信息的专门机构，规定更严格的准入标准和工作流程，由认定机构对信息的安全负责，且认定机构自信息控制者接收个人医疗信息时适用默示同意规则。

关键词 匿名化 个人医疗信息 明示同意 默示同意 特别规制

* 北京中医药大学人文学院法律系副教授、法学博士。本文系北京市社会科学基金青年项目“疫情防控视野下互联网医疗法律规制问题研究”（项目编号：20FXC020）的阶段性研究成果。

一、引　　言

我们已进入大数据时代。大数据技术在医疗领域已有广泛应用并带来巨大价值。例如，本次新冠肺炎疫情期间，我国就广泛运用大数据技术对病毒感染者的生活轨迹进行梳理，追踪人群接触史，为精准抗疫提供技术支撑；一位患者曾表示自己并无重点疫区接触史，但经大数据排查，确认其曾经至少接触过三位来自重点疫区的潜在患病人士。〔1〕2020 年 2 月，中央网络安全和信息化委员会办公室专门印发了《关于做好个人信息保护利用大数据支撑联防联控工作的通知》（以下简称《通知》），鼓励各类组织运用大数据技术防控疫情。和 2003 年的 SARS 相比，大数据技术的广泛应用是新时期传染病防控的重要特征。此外，大数据技术在药物开发、辅助诊断、医院管理等领域均有广泛应用。

世界各国均十分重视医疗信息的流通和利用，并通过立法予以体现和引导。例如，日本 2015 年全面修订其《个人信息保护法》的主要目标之一就是“确保个人信息的正当且有效利用从而促进新兴产业的创造、激发经济社会的活力、实现国民生活的富足”〔2〕；2018 年其颁布的《下一代医疗基础设施法》（次世代医療基盤法，Next Generation Infrastructure Act）更是将医疗信息作为重要的基础设施，对《个人信息保护法》所创设的匿名化处理制度进行了针对性改造，进一步便捷了医疗信息的汇聚和利用〔3〕。欧盟《一般数据保护条例》（General Data Protection Regulation，以下简称 GDPR）虽被称为“史上最严个人信息保护规范”，但个人数据〔4〕的流通和利用始终是其追求的核心目标之一。〔5〕美国医疗信息领域的主要规范性文件是健康和人类服务部（HHS）依据《健康保险可携性和责任法》（Health Insurance Portability and Accountability Act，HIPAA）授权制定的《隐私规则》（Privacy Rule）和《资安规则》（Security Rule），其采行了所谓的“下游保护”（downstream protection）模式，即只规制个人医疗信息的使用和披露行为而不规制搜集行为，这为医疗信息的搜集和利用创造了很大空间。〔6〕我国《个人信息保护法》（以下简称《个保法》）已于 2021 年 11 月 1 日起正式实施，该法第 1 条也明确将“促进个人信息合理利用”作为重要的规制目标。正如学者所言，“几乎所有国家和地区都将个人信息的流通和利用作为最终目标”〔7〕。

不过，个人医疗信息颇为特殊，各国一般将其界定为个人敏感信息，给予特殊保护，要求严格适用知情同意规则，这抑制了个人医疗信息的流通和利用。一般而言，搜集和使用个人医疗信息前应征得信息主体的明示同意，默示同意规则不得适用。例如，日本《个人信息保护法》区分了个人一般信息和个人敏感信息，对于个人一般信息的搜集和使用，允许适用默示同意规则（又称选择退出规则，即 OPT-OUT）〔8〕，而搜集和使用个人敏感信息则只能适用明示同意规则（又称选择进

〔1〕 参见王建：《中国利用大数据技术助力疫情防控》，载新华社百家号 2020 年 2 月 11 日，https://baijiahao.baidu.com/s?id=1658206416174721107&wfr=spider&for=pc。

〔2〕 参见日本《个人信息保护法》第 1 条。

〔3〕 岡本利久「次世代医療基盤法について」医療と社会 28 巻 3 号（2018 年）333—338 頁参照。

〔4〕 “数据”和“信息”的含义较为接近，本文中二者通用，不作区分。

〔5〕 参见京东法律研究院：《欧盟数据保护宪章：〈一般数据保护条例〉GDPR 评述及实务指引》，法律出版社 2018 年版，第 15 页。

〔6〕 See Nicolas P. Terry, *Bigdata Proxies and Health Privacy Exceptionalism*, 24 Health Matrix: Journal of Law-Medicine 65－106(2014).

〔7〕 高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期，第 98 页。

〔8〕 OPT-OUT 规则，即选择退出、默示同意规则，是一种默认同意机制，即信息主体不明确反对即推定其同意搜集和使用个人信息。

入规则，即OPT-IN）[9]。美国在一般信息领域，通常允许适用OPT-OUT规则，但在医疗信息领域，《隐私规则》则明确要求适用OPT-IN规则。根据我国《个保法》第14、29条的规定，无论个人一般信息还是个人敏感信息，在处理前均应获得信息主体的明示同意，个人敏感信息的处理更应获得信息主体的“单独同意”，这明显受到了GDPR的影响。总之，各国普遍在个人医疗信息领域确立了明示同意规则，这导致医疗数据的大范围搜集事实上难以执行，或成本高昂，同时，数据体量的局限性又反过来削弱了大数据分析的能力：大数据分析要求样本数据达到必要体量，数据体量越大则数据价值越高，并且呈非线性增长。[10] 显然，这对于大数据抗疫及后疫情时代信息价值的挖掘显著不利。那么，如何破解上述难题呢？如何兼顾个人医疗信息的保护和利用呢？笔者认为，构建完善的匿名化处理制度是一个可行的选择。

本文将首先对一般性的匿名化处理制度进行阐释，进而论证个人医疗信息匿名化处理特别规制的必要性及可行方案，并对我国《个保法》的相关条款进行深入评述、提出完善方案。应予指出的是，本文虽以个人医疗信息的研究为切入点，但其论证路径和研究思路具有一定程度之普适性。

二、匿名化处理的概念阐释和效果评述

论证匿名化处理机制的可行性，我们首先需要深入分析匿名化处理的法律概念和法律效果。

（一）匿名化处理的法律概念阐释

何为“匿名化”（anonymization）？我国《个保法》第73条第4项规定：“匿名化是指个人信息经过处理无法识别特定自然人且不能复原的过程。”日本《个人信息保护法》第2条规定：“匿名化信息是指按照规定的方法对个人信息进行加工后获得的无法识别特定个人，并无法得到恢复的信息。”可见，两国关于“匿名化”的界定基本一致。学界也持类似观点，例如，有学者认为，“匿名化信息是指该信息先前得以用之辨识特定个人，但经匿名化处理后，此个人辨识性不再可能，而此辨识之不可能原因在于将所有可连结至特定个人之资料，皆永久去除”。[11] 总之，匿名化信息有两个核心特征：一为无法识别出特定个人，二为识别性资料被永久删除而无法回复。

若要真正理解“匿名化”，必须将其与相似概念进行比较。欧盟GDPR除规定“匿名化”外，[12]还界定了“隐名化”（pseudonymization）的概念，“隐名化是一种使个人数据在不使用额外信息的情况下不指向特定数据主体的个人数据处理方式，若该处理方式将个人数据与其他额外信息分别存储，凭技术性和组织性措施无法指向一个可识别或被识别的自然人”。[13] 这基本等同于我国《个保法》第73条第3项所界定的“去标识化”概念，“去标识化是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程”。去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。[14] 可见，“隐名化”强调的是“不借助额外信息的情况下无法识别出特定个人”，即排除个人信息的“直接识别性”，而“匿名化”则进一步要求排除个人信息的“间接识别性”，即参照比对额外信息后仍无法识别出特定个人。此

〔9〕 OPT-IN规则，即选择进入、明示同意规则，是指除非获得信息主体的明示同意，不得搜集和使用个人信息。

〔10〕 参见吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016年第7期。

〔11〕 参见张陈宏于《中原财经法学》2018年第40期所发文章。

〔12〕 See GDPR Preface(26).

〔13〕 See GDPR Article 4.

〔14〕 参见《信息安全技术 个人信息安全规范（GB/T35273－2020）》第3条。

外，“隐名化”并不要求将识别性资料永久删除，而允许以代码或假名替代，因此，“隐名化”又被称作“假名化”。〔15〕 总之，“隐名化”是一种可逆的去连结化，而“匿名化”则是一种不可逆的去连结化，“隐名化”的去连结程度低于“匿名化”。

美国《隐私规则》则使用了“去识别化”(de-identification)的概念。“去识别化信息是指无法识别出特定个人且没有合理理由相信可以被用来识别出特定个人的信息。”〔16〕具体判定标准为：一位具有统计学与科学背景且知道如何对个人信息去连结的专家出具书面分析意见认定，该信息被第三者取得后，将其单独或与其他合理方法可取得的信息比照后，只有非常小的风险可以识别出该信息所连结的主体。〔17〕 此外，《隐私规则》还设定了安全港(safe harbor)规则，即只要去除十八种识别性资料，即为去识别化信息。〔18〕 这十八种资料几乎包含了所有我们能想到的识别性资料。正如学者所言，虽然《隐私规则》没有特别强调必须将识别性资料永久删除，但其对信息去连结化程度的要求已经十分接近甚至超过“匿名化”了。〔19〕 因此，“去识别化”的实效基本等同于“匿名化”。

学者对多个国家的相关概念进行仔细分析后，做了如下区分和界定：(1) 匿名化(anonymized)信息，是指将识别性资料不可逆转地删除的信息；(2) 隐名化(coded or pseudonymized)信息，是指识别性资料被代码或假名替代而非永久删除的信息；(3) 去识别化(de-identified)信息，是指将识别性资料按照《隐私规则》设定的标准去除的信息。〔20〕 这和上述分析基本一致，具体比较请参见表 1。厘清上述概念对于我们进一步讨论匿名化处理的法律效果非常重要。

表 1　三种概念的比较

概　念	含　义	识别资料是否永久删除	去连结化程度要求
匿名化(anonymization)信息	按照规定的方法对个人信息进行加工后获得的无法识别特定个人并无法得到恢复的信息	是	无法直接或间接识别出特定个人
隐名化(pseudonymization)信息	按照规定的方法对个人信息进行加工后获得的不借助额外信息便无法识别出特定个人的信息	否，以假名或代码替代	无法直接识别出特定个人
去识别化(de-identification)信息	按照《隐私规则》设定的标准去除识别性资料后得到的信息	未明确要求	无法直接或间接识别出特定个人

〔15〕 参见张陈弘：《个人资料之认定——个人资料保护法适用之启动阀》，载《法令月刊》2016 年第 5 期。

〔16〕 See 45 C.F.R. § 164.514(a).

〔17〕 See 45 C.F.R. § 164.514(b)(1).

〔18〕 这十八种识别性资料为：(1) 姓名；(2) 所有比州单位还要小的地理位置；(3) 所有与个人有直接连结的数据元素(除了年份)；(4) 电话号码；(5) 传真号码；(6) 电子邮件信箱；(7) 社会安全号码；(8) 医疗记录编号；(9) 健康照顾计划受益人编号；(10) 账户号码；(11) 证书号码；(12) 车辆识别和序列编号；(13) 设备识别或序列编号；(14) 网页网址；(15) 通讯协议位置编号；(16) 生物识别资料；(17) 全脸照片或其他可比较影像；(18) 任何其他独特可识别的号码、特征或编号。See 45 C.F.R. § 164.514(b)(2)(i).

〔19〕 See David M. Parker, Steven G. Pine, Zachary W. Ernst, *Privacy and Informed Consent for Research in the Age of Big Data*, 123 Penn State Law Review 703 - 732 (2019).

〔20〕 See Mark A. Rothstein, Bartha Maria Knoppers, Heather L. Harrell, *Comparative Approaches to Biobanks and Privacy*, 44 Journal of Law, Medicine & Ethics 161 - 172(2016).

（二）匿名化处理的法律效果评述

目前来看，各国个人信息保护法的规制对象仅为个人信息，非个人信息不适用个人信息保护法，也就是说，非个人信息的搜集和使用不受同意规则的约束。例如，日本《个人信息保护法》第1条规定："本法规制政府和企业等处理个人信息的行为。"欧盟GDPR第1条规定："本条例制定与个人数据处理相关的自然人保护规则及个人数据自由流动的规则。"我国《个保法》第3条也规定："在中华人民共和国境内处理自然人个人信息的活动，适用本法。"那么现在的问题是，匿名化处理后的信息是否就不再属于个人信息了呢？

这需要进一步考察个人信息的定义。日本《个人信息保护法》第2条规定："个人信息是指可直接或与其他信息简单容易地比对后识别出特定个人的信息。"我国《个保法》第4条规定："个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。"可见，各国关于个人信息的定义中均包含了"直接识别性"和"间接识别性"的要件，只有同时排除"直接识别性"和"间接识别性"的信息，才属于非个人信息。应当说，通过匿名加工程序去除个人信息的"直接识别性"较容易实现，但问题是，能否由此去除个人信息的"间接识别性"呢？笔者认为，这需要继续考察下面两个问题，即"间接识别性"标准的设定和辅助性制度的保障。

1. "间接识别性"标准的设定探析

信息"间接识别性"标准的设定是个复杂且易生争议的问题。应当说，在信息技术高速发展的当下，完全排除信息的"间接识别性"几无可能。〔21〕根据学者的研究，即便按照《隐私规则》设定的严苛标准删除所有十八种识别性资料，这种信息仍有0.01%到0.25%的可能性被重新识别。〔22〕在一个案例中，哈佛大学拉坦亚·斯维尼（Latanya Sweeney）教授仅使用出生日期、性别、选民登记标识符及保留在出院记录中的邮政编码等公开信息，便确认了时任马萨诸塞州州长威廉·威尔德（William Weld）的健康记录，斯维尼教授坚信，在大数据时代和大数据技术下，完全不可识别的数据是不存在的。〔23〕因此，各国均设定了适当的标准对信息"间接识别性"的范围进行限定。据笔者研究，各国主要通过主客观相结合的标准进行限定：主观标准解决以谁的识别能力作为判断基准的问题，客观标准解决信息自身的去连结化应达到何种程度的问题。下文详述之。

（1）主观标准探析

综合来看，主要有以下三种代表性的主观标准。其一，"一般人标准"，即以社会一般多数人的识别能力作为判断基准，不要求具备任何特殊的主观条件，仅以社会平均识别能力为基准。如果按照社会平均条件无法从中识别出特定个人，则该信息不属于个人信息。这种标准大大限缩了个人信息的范围，有利于信息的流转和利用，但显然对信息主体的保护不够周全。其二，"信息处理者标准"，即以信息处理者的识别能力作为判断基准。亦即，信息是否具有间接识别性，应从信息搜集和使用者的主观条件出发，本无一致性标准，应在个案中审查判断。例如，医疗机构搜集和利用信息时，应以医疗机构的识别能力作为判断基准；制药公司搜集和处理信息时，则应以制药公司的识别能力作为判断基准。因此，不同处理者掌握的资料数量和性质不同，必然会产生不同的识别结果，这也导致了认定的相对化问题。信息处理者通常具有较强的识别能力，这事实上扩大了个人信息的范围，提升了保护标准，也为信息利用预留了必要空间，较好地平衡了保护和利用之间

〔21〕 See Parker, Pine, Ernst, *supra* note〔19〕.

〔22〕 See Sharona Hoffman, *Citizen Science: The Law and Ethics of Public Access to Medical Big Data*, 30 Berkeley Technology Law Journal 1744－1805(2015).

〔23〕 See Parker, Pine, Ernst, *supra* note〔19〕.

的关系。这是目前的主流标准，日本、美国和我国台湾地区等均采此标准。[24] 其三，“任何人标准”，即以任何人的识别能力作为判断基准，只要任何人基于其主观条件得以从信息中识别出特定个人，则该信息为个人信息。这大大扩展了个人信息的范围，是一种很高的保护标准，同时也增加了个人信息匿名化处理的难度。欧盟 GDPR 即采此标准，正如其在序言中所言，“为判断自然人身份是否可识别，需要考虑所有人包括信息处理者及其他任何人是否能够直接或间接识别出特定自然人”。[25] 不过，此种标准对信息流动和利用的阻碍较大，除欧盟外，鲜有其他国家或地区采用。

（2）客观标准探析

综合来看，主要有以下两种代表性的客观标准。其一，“容易照合标准”，即若与其他资料简单容易比对后可识别出特定个人，则为个人信息，否则即不属于个人信息。日本采此标准。其二，“合理可能标准”，即通过任何可能、合理的手段（all the means reasonably likely to be used）比对分析后可识别出特定个人，则为个人信息，否则即不属于个人信息。欧盟、美国等采此标准。

从字面上看，依据“合理可能标准”认定的个人信息范围要宽于“容易照合标准”，不过，这种程度上的差别，一则很难衡量，二则在实践效果上已十分接近。例如，欧盟和日本在个人信息保护的互认谈判中并未将客观标准的差异作为谈判要点，双方争论的焦点在于前述主观标准的差异，日本为弥合双方分歧而专门制定的补充细则也未提及客观标准的调整，欧日顺利达成了个人信息保护的互认协议。[26] 可见，各国在信息“间接识别性”的客观标准上并无实质不同。下文即以“合理可能标准”一并论述。

（3）评述

各国均通过主客观标准对信息的“间接识别性”进行限定。就主观标准而言，“信息处理者标准”虽然无法避免认定的相对化问题，但由于较好地协调了保护和利用之间的关系，且适应了个案灵活审查的需要，目前仍是主流标准；就客观标准而言，各国的规定虽然存在文字上的差异，但实践效果并无多少差别。综上，目前信息“间接识别性”的主流判断标准为“信息处理者能否通过合理、可能的手段识别出特定个人”。由此，个人信息的范围得以限定，经由匿名化处理将个人信息转变为非个人信息成为可能。前述标准也成为信息匿名化处理的指导标准。不过，个人信息范围的压缩和匿名化信息范围的扩张，可能引发保护不周的担忧，这便需要其他辅助性制度的保障。

2. 辅助性制度的保障探析

辅助性制度的实施是匿名化处理达至预定效果的制度保障，其中，尤以禁止再识别制度为重。日本《个人信息保护法》第 36 条第 5 项规定，匿名化信息的处理者和接收者不得再次识别信息中的特定个人，违者将承担行政或刑事法律责任。英国《数据保护法》也明确将“故意或重大过失从匿名或化名数据中重新确认个人身份的行为”认定为犯罪。[27] 禁止再识别义务从制度上阻断了匿名化信息被再次识别之可能，也为信息主体提供了更周全的保护。

此外，日本《个人信息保护法》第 36 条第 3、4、6 项还规定，匿名化信息的处理者负有安全维护、明示、公开等义务，即应当采取适当的安全维护措施，防止匿名化信息被泄露或违法利用；应当将匿名化信息的加工方法、流向等公开，接受公众监督；应当向接受匿名化信息的第三者明示，其应

〔24〕 参见范姜真微：《大数据时代下个人资料范围之再检讨——以日本为借镜》，载《东吴法律学报》2017 年第 2 期。

〔25〕 See GDPR Preface(26).

〔26〕 参见刘静怡：《浅谈 GDPR 的国际冲击及其可能因应之道》，载《月旦法学杂志》2019 年第 3 期。

〔27〕 参见英国数字、文化、媒体和体育部（DCMS）编：《英国新数据保护法案：改革计划》，邓辉译，载《中国应用法学》2017 年第 6 期。

负担与提供人相同之义务等。其他国家和地区或多或少也有类似的规定，如欧盟GDPR规定，信息控制者应采取必要的技术性和组织性措施保障匿名化或隐名化信息的安全；[28]《资安规则》规定，信息控制者应采取行政、技术和物理空间保障措施维护去识别化信息的安全。上述制度进一步提升了匿名化信息的安全性。

综上，通过限定信息"间接识别性"的标准，信息控制者完全可以将个人信息加工为非个人信息，辅助性制度的实施则进一步保障了匿名化信息的安全。由此，按照法定标准加工处理后的信息便成为法律意义上的非个人信息，从而得以豁免同意规则的适用。这为个人信息的利用提供了很大空间和便利。

（三）我国《个保法》相关条款评述

如前所述，我国《个保法》对匿名化的概念和法律效果进行了明确规定，和国际保持了接轨。但是，《个保法》并未规定匿名化处理所应达到的标准，即信息"间接识别性"的标准，学界对此也缺少关注。这导致匿名化处理制度缺乏统一、清晰、可预期的实施标准，容易导致法律适用的犹疑和困难。

而且，《个保法》关于辅助性制度的规定也相当单薄。《个保法》第51条[29]规定了信息处理者的安全维护义务，但仅列举了五项安全维护措施，过于简单，有待进一步扩充和细化。《个保法》第7条[30]原则性规定了处理个人信息的公开原则，但这是否意味着信息处理者有义务将匿名化信息的加工方法、流向等向社会公开以接受公众监督，不无疑问。更重要的是，《个保法》并未规定禁止再识别制度，无法对匿名化信息的控制者和接收者形成有效威慑，无法从制度上阻断匿名化信息被再次识别之可能。《个保法》也未规定匿名化信息流通中的明示义务，无法确保后续接收者负担相同之义务，无法保证匿名化信息流通链条的安全和稳定。

总之，我国《个保法》所规定的个人信息匿名化处理制度尚未形成逻辑闭环，《个保法》只规定了匿名化处理制度的起点和终点，但如何从起点走到终点、如何破除路途中的荆棘和障碍，尚缺乏清晰完整的实施路径，这很可能会抑制匿名化处理制度的实际运转效果。

三、个人医疗信息匿名化处理的特别规制：必要性证成和比较法经验

上文探讨的匿名化处理的一般原理和规则，个人医疗信息当然也适用。现在的问题是，有无必要对个人医疗信息的匿名化处理进行特别规制？如有必要，当如何规制？有无可资借鉴的域外经验？

（一）必要性证成

应当说，个人医疗信息具有特殊性。个人医疗信息是个人因生病医治等产生的相关记录，包括病症、住院志、医嘱单、检验报告、护理记录、用药记录、生育信息、既往病史、家族病史、传染病史等，这是最敏感的个人信息，关涉个人最重要的人格利益，一旦泄露或再次识别将对个人产生重大影响。例如，本次疫情期间，部分"新冠肺炎"患者的医疗信息被泄露，这使他们遭受了无端的歧视

〔28〕 See GDPR Preface(29).

〔29〕《个保法》第51条："个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：(1) 制定内部管理制度和操作规程；(2) 对个人信息实行分类管理；(3) 采取相应的加密、去标识化等安全技术措施；(4) 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；(5) 制定并组织实施个人信息安全事件应急预案；(6) 法律、行政法规规定的其他措施。"

〔30〕《个保法》第7条："处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。"

和偏见，有人甚至收到了辱骂威胁短信，严重影响了正常生活，“污名化”问题引起了社会的广泛关注。〔31〕就此而言，对个人医疗信息进行匿名加工应秉持更高之标准，确保更高程度之专业化，谨防被再次识别。同时，个人医疗信息也关乎公众最重要的健康利益，最大限度地推动个人医疗信息的利用是各国的共同目标。利用医疗信息进行大数据抗疫，正是我国迅速控制疫情的两大原因之一。〔32〕疫苗研发、药物开发等也需要医疗信息的支撑。应当指出，并非所有的个人敏感信息都具有重大的公共利用价值，正如我国《个保法》第28条所界定的，“敏感”本身强调的是“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害”，而非其利用价值；和个人医疗信息相比，本条所列举的“宗教信仰、特定身份”等个人敏感信息难言具有重大的利用价值。诚然，部分个人敏感信息如个人金融信息、个人征信信息等也具有重要的利用价值，甚至是公共利用价值，但其所代表利益的性质和强度很难与个人医疗信息相提并论。个人医疗信息的利用直接关乎传染病防控、药品研究、医疗新技术的开发应用等最重要的公共利益，直接关乎国民的生命健康。例如，各国近年来都非常重视医疗人工智能的研发和临床应用，原因在于，医疗人工智能在疾病的诊断和治疗领域显示出巨大的潜力和优势，可以为患者提供更准确和个性化的诊疗服务，可以显著提升医疗效率、降低医疗成本、有力化解困扰各国的医疗可及性和公平性问题，简言之，可以极大地增进公共健康利益，而医疗人工智能发展的重要基础就是个人医疗信息的流动、汇聚和利用。〔33〕可见，个人医疗信息具有独特的公共利益属性。当然，这并不排斥在个人金融信息等领域借鉴个人医疗信息的规制经验，只是需要更充分的成本收益分析。就此而言，我们应当创造条件加速个人医疗信息的流通和汇聚，充分挖掘数据价值，增进国民健康。一方面需要提高个人医疗信息的保护标准，另一方面又要推动个人医疗信息更便捷之利用，这种看似矛盾的诉求，对个人医疗信息的匿名化处理提出了特别的要求。

显然，一般性的匿名化处理制度无法彰显个人医疗信息的特殊性，无法达成上述目标。因为，若要提升个人医疗信息的匿名化处理的保护标准，就必须在组织机构、人员资质和工作流程等各个环节进行革新，而非只是停留于纸面上的高标准；若要提升个人医疗信息的利用效率，就必须简化流程，加速信息的流通和汇聚，既要破除障碍，又要增加激励，尤其需要政府的积极干预和介入，分摊部分成本，为社会创造更友好的个人医疗信息利用环境。因此，我们有必要在制度层面进行革新，确保个人医疗信息的匿名化处理兼顾高标准保护和高水平利用的双重目标。那么，如何才能实现呢？日本的经验可资参考。

（二）日本《下一代医疗基础设施法》的经验探析

为进一步推进医疗信息的利用，充分挖掘医疗数据的社会价值，日本于2018年颁布了《下一代医疗基础设施法》（次世代医療基盤法），全称为《有助于医疗领域研究开发的匿名加工医疗信息法》（医療分野の研究開発に資するための匿名加工医療情報に関する法律）。该法将医疗信息视作未来医疗发展的关键基础设施，并通过对《个人信息保护法》设置的一般性的匿名化处理制度进行针对性改造，实现对个人医疗信息的特别规制，在提供有效保护的前提下进一步助推医疗信息

〔31〕 参见甘怡群：《新冠肺炎患者治愈后，该如何正确面对复工复产？》，中央纪委国家监委网站百家号2020年4月8日，https://baijiahao.baidu.com/s?id=1663400626015970275&wfr=spider&for=pc。

〔32〕 另一原因为政府的有效防控措施及民众的配合。参见《西媒分析为何亚洲控制疫情强于欧洲》，载参考消息网，http://column.cankaoxiaoxi.com/2020/0325/2405721.shtml。

〔33〕 参见李润生：《论医疗人工智能的法律规制——从近期方案到远期设想》，载《行政法学研究》2020年第4期。

的流动和利用。〔34〕

1. 日本《个人信息保护法》下匿名化处理制度的局限性

日本《个人信息保护法》专节规定了匿名化处理制度。根据该法规定，个人信息按照规定的措施匿名加工后，便成为法律意义上的非个人信息，不再受同意规则之约束。同时，匿名化信息的处理者负有禁止再次识别、安全维护、明示、公开等法定义务，这提升了匿名化信息的安全性。

不过，就个人医疗信息的搜集和使用而言，上述匿名化处理制度仍有较大的局限性，主要表现为以下三点（注：鉴于医疗机构是个人医疗信息最重要的原始搜集者，下文主要以之为例进行介绍）。首先，医疗机构在为患者提供诊疗服务的过程中搜集了大量的个人医疗信息，若要将该等信息自行或提供给他人二次利用，为豁免明示同意规则之适用，则应进行匿名化处理。但是，医疗机构自身通常缺乏相应的技术能力，需委托专门的匿名加工事业者进行处理，这便形成了委托代理关系，匿名加工的最终责任仍由医疗机构承担，这抑制了医疗机构对外分享信息的动力。其次，各医疗机构即使愿意在匿名化处理后对外提供医疗信息，但由于需要各机构分别委托匿名加工、分别转移信息，这便削弱了信息流通和汇集的效率，不利于大数据技术的应用。最后，由于政府未对匿名加工事业者的资质进行统一认定，医疗机构需自行判断受托者是否适格，这无疑增加了医疗机构的风险，抑制其对外分享信息。〔35〕

2. 日本《下一代医疗基础设施法》的改造

针对前述问题，日本《下一代医疗基础设施法》进行了巧妙的改造，从而化解了难题。

第一，规定由政府对处理个人医疗信息的匿名加工事业者统一进行资质认定（以下简称“认定事业者”），由其专门负责个人医疗信息的匿名化处理。〔36〕为保证认定事业者有充分的能力提供高标准的保护，《下一代医疗基础设施法》从组织体制、人员、信息、事业运营计划、安全管理等五个方面设定了严格的认定条件，例如，在组织体制方面，要求认定事业者建立保持医疗信息处理透明度和安全性的适当体制；在人员方面，要求认定事业者的技术人员充分理解医疗信息的安全标准和规格，并具有加工和管理医疗信息的高度专业性；在安全管理方面，要求认定事业者确保其匿名加工主干系统与互联网等开放网络彻底分离，并建立多层次防御体系（包括日志监测、可追溯性确保、第三方认证等），等等。〔37〕由此，医疗机构可以安全便捷地选择合作机构。

第二，规定由认定事业者而非医疗机构承担个人医疗信息匿名加工的最终责任，医疗机构和认定事业者之间的法律关系由委托代理关系转变为信息转让关系，认定事业者由此获得医疗信息法律上的控制权，可自主加工和管理医疗信息，自行决定医疗信息的转让对象。〔38〕由此，医疗机构的法律风险转移至认定事业者，从而排解了医疗机构的疑虑。

第三，规定认定事业者从医疗机构等信息控制者处受让个人医疗信息时适用默示同意规则，除非信息主体明确向认定事业者表示反对，则推定其同意个人医疗信息的转移和匿名加工。〔39〕根据《个人信息保护法》的规定，个人医疗信息的目的外利用适用明示同意规则，医疗机构将其提供诊疗服务时搜集的患者医疗信息转移给认定事业者显然属于目的外利用，而《下一代医疗基础

〔34〕 参见范姜真微：《日本次世代医疗基盘法之简介》，载《月旦医事法报告》2018年第10期。

〔35〕 宇賀克也「行政法の論点第9回：次世代医療基盤法の施行」国際文化研修26巻1号（2018年）32—33頁参照。

〔36〕 参见日本《下一代医疗基础设施法》第8条。

〔37〕 参见日本《下一代医疗基础设施法》第9条。

〔38〕 宇賀克也「行政法の論点第9回：次世代医療基盤法の施行」国際文化研修26巻1号（2018年）32—33頁参照。

〔39〕 参见日本《下一代医疗基础设施法》第30条。

设施法》则将其改造为默示同意规则。由此，认定事业者可以便捷地从各医疗机构广泛接收个人医疗信息，这大大提高了信息流通效率，并将分散的医疗数据汇聚成医疗大数据。此外，认定事业者还可根据制药公司、研究机构等后续利用者的需求进行定制化加工，提高信息的可用性。日本匿名化处理制度的变化请参见图 1、图 2。

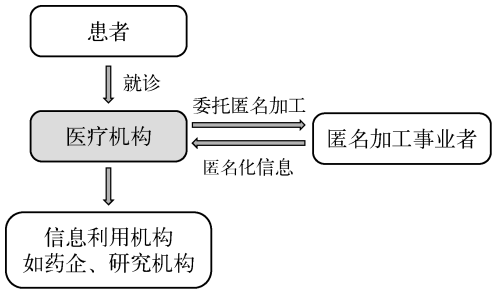

图 1 《个人信息保护法》下的匿名化处理制度

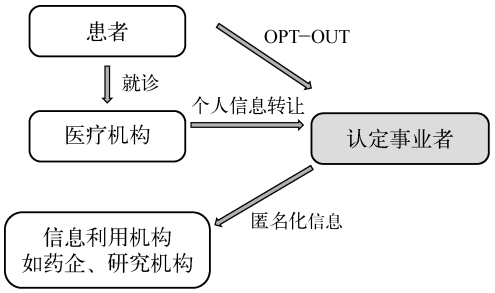

图 2 《下一代医疗基础设施法》下的匿名化处理制度

3. 评述

日本《下一代医疗基础设施法》对个人医疗信息的匿名化处理进行了特别规制。认定事业者制度的建立，辅之以默示同意规则的运用，既提高了个人医疗信息匿名化处理的标准，又促进了个人医疗信息的流动和汇聚，还解放了医疗机构。这是一种更高层次的保护和利用之间的协调共生关系，是不以保护水平的降低为代价的更便捷之利用。就此而言，日本经验是一种跳脱出“保护抑或利用”的零和博弈思维的理想规制路径。而且，《下一代医疗基础设施法》的改造并未根本改变现有制度框架，只是针对个人医疗信息进行了特殊规定，制度改造成本总体可控，是一种兼具经济理性的规制方案。当然，高标准保护和高水平利用是一个相对的概念，其主要参照物为《个人信息保护法》所创设的一般性的匿名化处理制度，《下一代医疗基础设施法》通过巧妙的设计同时提升了个人医疗信息的安全性和流动汇聚效率。这种溢出价值的成本事实上是由政府机关承担的，即政府通过投入必要的公共资源创造了理想的使用环境。就此而言，高标准保护和高标准利用看似对立，实则可以通过适当的规则设计协调共生。而且，始终应明确的是，《下一代医疗基础设施法》是通过对匿名加工过程的控制来实现释放个人医疗信息利用潜力的目标的，虽然包括个人医疗信息在内的个人信息经匿名加工后即转变为非个人信息，从而豁免《个人信息保护法》的适用，但诚如前述，不同范式的匿名加工制度本身对信息处理的影响是不同的，更何况，并不存在绝对意义上的匿名化，只能通过对人员、流程等的严格管控尽量提升信息的安全性。

（三）欧盟和美国的制度介绍和比较

欧盟 GDPR 规定了统一的匿名化处理制度，并未区分对待个人医疗信息。应当说，欧盟为匿名化处理设定了很高的标准，即“任何人标准”，只有当任何人基于其主观条件无法从信息中识别出特定个人时，方可认定为匿名化信息。这大大压缩了匿名化信息的空间，不利于信息的利用。总体来看，欧盟的匿名化处理制度更偏向信息的保护而部分牺牲了信息的利用。这在疫情期间表现得尤为突出。为解决疫情防控中个人医疗信息的利用难题，欧盟被迫授权各成员国采取紧急立法措施，适当降低保护标准，允许有关部门搜集和使用未经匿名化处理或未达匿名化标准的个人医疗信息。〔40〕

〔40〕 The European Data Protection Board, *Statement on the Processing of Personal Data in the Context of the COVID - 19 Outbreak*, Adopted on 19 March 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

美国没有统一的《个人信息保护法》，采分散立法模式，其在医疗信息领域的主要法律文件为《隐私规则》和《资安规则》。应当说，和其他信息领域相比，《隐私规则》设定了较高的保护标准。就个人医疗信息的去识别化而言，《隐私规则》设置的判定标准和安全港规则更加严格，例如，该安全港规则规定，只有移除全部18种识别性资料的信息方为去识别化信息，而在其他信息领域则通常只要求移除其中的一部分。〔41〕因此，从国内横向比较来看，个人医疗信息无疑享受了更高的保护标准。但是，从国际比较视野来看，由于《隐私规则》和《资安规则》采行了所谓的“下游保护”模式，即只规制个人医疗信息的使用和披露行为而不规制搜集行为，而且私人也无法据其提起诉讼，因此，美国的个人医疗信息保护水平较之欧盟、日本等明显更低。〔42〕正如学者所言，美国在个人医疗信息领域事实上秉持的是“积极利用主义”的理念，〔43〕欧盟法院甚至在2015年以美国的保护标准过低为由，判决美欧之间达成的个人信息交换的安全港协议无效。〔44〕

可以说，就个人医疗信息的匿名化处理而言，欧盟和美国事实上仍然游移于“零和博弈”的迷局中：欧盟偏向了保护而抑制了利用，美国则偏向了利用而降低了保护水准，只有日本的制度设计较好地兼顾了保护和利用。

（四）我国《个保法》相关条款评述

我国《个保法》并未针对个人医疗信息的匿名化进行特别的制度设计，这无法彰显个人医疗信息的特殊性，很难同时实现高标准保护和高水平利用的双重目标。而且，就笔者对我国实践状况的观察，各类机构普遍降低了对个人医疗信息的保护水准。以各主要互联网医疗平台的隐私权政策为例，《阿里健康法律声明及隐私权政策》〔45〕开篇即规定，“一旦您开始使用阿里健康提供的各项产品或服务，即表示您已充分理解并同意本政策”，结合该文件之后的规定，阿里健康几乎可以在提供服务的过程中不受限制地搜集和使用用户的医疗信息。这与“明示同意”的要求差距较大。针对个人医疗信息的二次利用，文件虽明确规定“会事先征求您的同意”，但就用户而言，事实上无法知晓，更无法掌控，实际执行状况也不容乐观，再次打开阿里健康APP时收到的各种莫名的“定制”推送就是一个例证。《腾讯微医隐私权政策》〔46〕《好大夫在线隐私保护政策》〔47〕《丁香园隐私政策》〔48〕等与阿里健康的规定大同小异。显然，这种宽松的实践状况是以个人医疗信息保护的严重不足为代价的，非长久之计。此外，参照日本的经验，我国也会面临日本在《下一代医疗基础设施法》出台前所面临的类似问题：由于政府未对匿名加工事业者进行专门认定、未设定更高的准入门槛，个人医疗信息的高标准保护难以真正落地；个人医疗信息的控制者尤其是医疗机构承受着繁重的法律负担，缺乏对外提供和分享医疗信息的动力；由于缺乏类似认定事业者之类的中间机构，医疗信息的流动和汇集效率受到抑制，难以满足大数据技术处理的需求。总之，我国《个保法》

〔41〕 See Heather L. Harrell, Mark A. Rothstein, *Biobanking Research and Privacy Laws in the United States*, 44 Journal of Law, Medicine & Ethics 106－127(2016).

〔42〕 See Terry, *supra* note〔6〕.

〔43〕 参见王立梅：《健康医疗大数据的积极利用主义》，载《浙江工商大学学报》2020年第3期，第34页。

〔44〕 See Rothstein, Knoppers, Harrell, *supra* note〔20〕.

〔45〕 《阿里健康法律声明及隐私权政策》，载阿里健康官网2019年9月27日，https://www.alihealth.cn/privacy.html。

〔46〕 《腾讯微医隐私权政策》，载腾讯微医官网2021年11月4日，https://www.guahao.com/agreement/privacy。

〔47〕 《好大夫在线隐私保护政策》，载好大夫在线官网2019年12月9日，https://www.haodf.com/info/privacy_policy.php。

〔48〕 《丁香园隐私政策》，载丁香园官网，http://www.dxy.cn/pages/sitedeclaration.html（最后访问时间2020年7月18日）。

的制度设计无法实现针对个人医疗信息的特殊规制目标，甚至可能引发“双输”的结果，既无法扭转“弱保护”的现状，又削弱医疗信息的利用效率，这值得我们警惕和反思。

四、个人医疗信息匿名化处理制度的构建：具体方案及论证

如前所述，我国《个保法》所规定的匿名化处理制度仍有不少缺憾，有必要进行针对性的完善。笔者认为，我国首先应当完善一般性的匿名化处理制度，形成逻辑闭环，打牢根基；在此基础上，我国可借鉴日本经验，对个人医疗信息的匿名化处理进行特别规制，既提升个人医疗信息的保护标准，又促进更充分便捷之利用。

在此需要说明的是，从现有条款来看，我国《个保法》显然更多借鉴了欧盟 GDPR 的条款，那为何又要在匿名化制度领域吸收日本经验呢？这是否会引发体系性冲突呢？笔者认为，欧盟 GDPR 和日本《个人信息保护法》在很多方面具有共通性，同属统一立法模式，均对个人一般信息和个人敏感信息进行区别规制，对匿名化的概念和法律效果等的认知也相仿。简言之，二者并不存在根本冲突，我们在个人信息处理规则、个人权利等方面学习欧盟，并不妨碍我们在匿名化制度领域借鉴日本经验。应当说，日本《个人信息保护法》更加重视匿名化制度的建构，希望借此平衡个人信息的保护和利用，并特设专节予以详尽规定，《下一代医疗基础设施法》更是针对个人医疗信息的匿名化进行了特别规定，以兼顾高标准保护和高水平利用。可以说，在匿名化领域，日本的制度设计更加精细务实，更值得我们参考借鉴。而且，日本《个人信息保护法》具有鲜明的行业化规制倾向，即针对不同行业授权不同行业组织出台细化的保护标准，〔49〕以契合行业的特殊需求，《下一代医疗基础设施法》本质上就是一种行业标准，这与我国《个保法》所设计的部门分工协作的模式及《数据安全法》所倡导的行业安全的理念〔50〕高度契合。就此而言，我国在个人信息尤其是个人医疗信息的匿名化处理上借鉴日本经验具有合理性和正当性。

（一）打牢地基：完善一般性的匿名化处理制度

针对匿名化处理标准的缺失和辅助性制度的罅缝，《个保法》应予针对性的修改。这也是实现对个人医疗信息特别规制的前提。当然，由于《个保法》刚刚出台，短期内再次修改的难度较大，故笔者建议，我国可考虑先以部门规章或国家标准的形式弥补制度漏洞，积累实践经验，待修法条件成熟后再纳入《个保法》。

首先，我国应增加关于个人信息匿名化处理标准的规定，应采主流标准，将“信息处理者能否通过合理、可能的手段识别特定个人”作为判定标准。这是各国或地区普遍采行的标准。虽然该标准也有其自身问题，但相对而言，较好地兼顾了个人信息的保护和利用，是一种更加平衡的认定标准。“一般人标准”保护标准过低，几乎未曾被正式立法采行过；“任何人标准”界定范围过宽，容易诱发过度保护进而抑制利用，欧盟在 GDPR 实施两年后的评估报告中也进行了反思：“任何人标准”对个人信息的保护范围过宽，这对欧洲数字经济是一种复杂而沉重的消耗，而且，该标准还导致欧盟在匿名化、隐名化等制度执行层面缺乏明确性。〔51〕 因此，我国应注意吸取欧盟的经验教

〔49〕 参见范姜真微：《匿名加工资料制度之创设——因应大数据时代日本个人资料保护法之新进展》，载《东海大学法学研究》2020 年第 5 期。

〔50〕 参见《数据安全法》第 6、10 和 21 条。

〔51〕 See Eline Chivot, *Two Years On, the GDPR's Flaws Show Why the EU Should Avoid Additional Rules*, Center For Data Innovation(June 24, 2020), https://datainnovation.org/2020/06/two-years-on-the-gdprs-flaws-show-why-the-eu-should-avoid-additional-rules/.

训，在个人信息的认定标准上，理性分析、辩证取舍。

其次，我国应对个人信息匿名化处理的辅助性制度进行更加系统明确的规定。第一，增加关于“禁止再识别制度”的规定，信息处理者及后续接收方不得再次识别信息中的特定个人，违者将承担行政甚至刑事责任。这将形成有力的制度威慑。如前所述，技术上完全彻底的匿名化难以实现，有学者更是直接将其称作“美丽的神话”（beautiful myth）〔52〕，因此，在限定匿名化处理的法律标准后，我国有必要从制度上阻断匿名化信息被再次识别之可能，以填补技术意义上有限匿名化的缝隙。个人信息匿名化之“不能复原”，既包括技术上之“不能复原”，亦包括法律上、制度上之“不能复原”，二者结合方能构建完整的防护网。第二，充实和细化安全维护措施，建议由国家网信部门尽快牵头起草实施细则，落实《个保法》第51条第6项所称的“法律、行政法规规定的其他措施”。《个保法》第51条仅列举了五项安全维护措施，明显不足。部分已出台的国家标准中包含了更详细全面的安全维护措施，可资参鉴。例如，《信息安全技术 健康医疗数据安全指南（GB/T 39725－2020）》针对个人健康医疗数据列举了众多安全维护措施，具体包括境内存储、身份鉴别、访问控制、分类分级、权限管理、质量管理、元数据管理、存储介质管控、加密设置、备份恢复、审计、销毁等等，《信息安全技术 个人信息去标识化指南（GB/T37964－2019）》则对去标识化这一安全措施的目标、原则、过程、方法和模型等进行了细致的规定。上述国家标准均为推荐性标准，无强制约束力。第三，我国应在《个保法》第7条规定的公开原则的基础上，具体规定信息处理者负有将匿名化信息的加工方法、流向等向社会公开、接受公众监督的义务。社会监督可有效配合行政监督，也可促使信息处理者形成自我约束机制，推动匿名化信息更加规范、有序的利用。第四，我国应增加关于明示义务的规定，匿名化信息的处理者应向接收者明示其负担相同之义务，包括禁止再识别、安全维护、公开等义务。明示义务的设置将使匿名化信息的流通链条更加完整可靠，确保其全流程安全，也可将禁止再识别、安全维护、公开等义务真正贯彻落实于流通链条的各个环节、各个主体。

需要说明的是，我国《个保法》所规定的“个人信息处理者”的概念具有特殊性，需要在规则设计和法律适用时予以注意和协调。我国《个保法》只规定了“个人信息处理者”，即“在个人信息处理活动中自主决定处理目的、处理方式的组织、个人”，而未像欧盟GDPR一样区分“控制者”和“处理者”。结合GDPR第4条的定义可知，《个保法》所规定的“个人信息处理者”更接近于GDPR所规定的“控制者”，而GDPR所规定的“处理者”则更接近《个保法》第22条个人信息委托处理条款中的“受托方”。日本《个人信息保护法》也只规定了“个人信息处理者”的概念，根据该法第2条的规定，“个人信息处理者是指正在将个人信息用于业务的主体”，可见，日本法上的“个人信息处理者”更加强调加工处理个人信息的状态，事实上涵盖了GDPR下的“控制者”和“处理者”的概念，由此我们也更容易理解该法第23条的规定，即个人信息处理者在使用目的范围内委托他人处理个人信息时，该受托人亦属于“个人信息处理者”。当然，这只是不同国家和地区在概念界定上的不同选择，不构成制度借鉴的绝对障碍，只是要求我们在规则设计时予以厘清和协调。例如，在我国《个保法》语境下，禁止再识别义务不但应适用于“个人信息处理者”，还应适用于“受托方”及其他后续接收方；公开义务和明示义务应一并适用于“个人信息处理者”和“受托方”；下文所称“认定机构”，事实上已经具有了较大的自主权，应属“个人信息处理者”而非“受托方”；等等。

〔52〕 See Ira S. Rubinstein, Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 703－710 (2016).

（二）筑好高楼：对个人医疗信息的匿名化进行特别规制

如前所述，一般性的匿名化处理制度无法适应个人医疗信息的特殊规制需求，无法实现高标准保护和高水平利用的双重目标。我国有必要对个人医疗信息的匿名化进行特别规制。

突如其来的疫情进一步凸显了构建个人医疗信息匿名化处理制度的重要性和紧迫性。大数据抗疫是我国迅速控制疫情的重要原因之一，大量的个人医疗信息在疫情期间被各类主体搜集用于疫情防控，“健康宝”“精准复工平台”等工具成为生产生活的标配，促进个人医疗信息更便捷之利用以支持疫情防控成为社会共识。当然，为防止无序利用、过度利用损害个人权益，理应提高个人医疗信息的保护标准，防止出现个人利益和公共利益的失衡。个人医疗信息匿名化处理制度的构建，正当其时。

诚然，各国已经为基于疫情防控目的而利用个人医疗信息提供了部分便利。欧盟 GDPR 第 9 条规定，若“数据处理为在公共健康领域维护公共利益之必要”，则可不经信息主体的同意。日本《个人信息保护法》〔53〕、美国《HIPPA 隐私规则》〔54〕也都有类似的规定。我国《个保法》第 13 条也将“应对突发公共卫生事件所必需”规定为处理个人信息（包括个人医疗信息）的正当性基础之一。但是，公共健康目的不可无限扩大，应有合理边界。“目的明确”是个人信息保护的基本原则（《个保法》第 6 条），疫情防控属于概括性目的，必须细化为“明确、清晰、具体”的个人信息处理目的，如疾病治疗、患者追踪、病毒溯源、隔离管理、疫苗研究等。而疫情期间部分个人医疗信息的利用行为已然超出特定目的范围，例如，部分互联网医疗平台将基于“义诊”而搜集的患者信息用于社区管理，甚至将其用于广告推送、用户画像和信用评价等。个人医疗信息的搜集对象也应受到限制，《通知》即明确规定，“收集对象原则上限于确诊者、疑似者、密切接触者等重点人群”，但实践中已远远超出这一范围。而且，疫情期间沉淀的大量珍贵的个人医疗信息，在后疫情时代仍然具有重要的利用价值，“一删了之”恐怕并非最优选择，在进行严格的匿名化处理后实现二次利用，应当作为一个合理的选项。总之，构建专门的个人医疗信息匿名化处理制度，为信息主体提供更高标准的保护，同时有力推进个人医疗信息的流动和汇聚，创造更大更安全的数据利用空间，是实践之需、时代之势。

笔者认为，我国应借鉴日本经验，构筑我国的个人医疗信息匿名化处理制度。我国可考虑在《个保法》之外直接制定针对个人医疗信息的单行法，也可考虑先由相关部门制定针对个人医疗信息的部门规章或国家标准，积累经验，待条件成熟后再上升为法律。

就具体内容而言，首先，我国应规定由政府统一认定汇集和匿名加工个人医疗信息的专门机构（以下简称“认定机构”），规定更严格的准入标准和工作流程，具体可从人员资质、组织体制、安全保障体系等方面进行限定。应当说，个人医疗信息的特殊性赋予更高强度之政府干预以正当性，正如我们在其他医药领域所呈现的那样，医药卫生关乎患者生命健康和基本尊严，始终是一个强监管领域。为提高医疗信息的安全性、推动其更高程度之利用，投入更多的政府监管资源是合理且必要的，应由医药卫生部门和网信部门协同推进认定机构的管理工作。而且，以认定机构这一中间平台为抓手推进数据治理，在网络时代更加务实可行，正如我们通过强化对基础性互联网平台的监管以推进网络良治一样（《个保法》第 58 条）。从既往经验来看，我国政府完全有能力平稳有序地推进认定机构的监管工作。

其次，我国应规定由认定机构统一对个人医疗信息进行汇集、加工和转移，并对信息的安全负

〔53〕 参见日本《个人信息保护法》第 23 条。

〔54〕 See 45 C.F.R. § 164.512(b).

责，且认定机构自医疗机构等信息控制者处接收个人医疗信息时适用默示同意规则。应当说，在对认定机构实施强监管的基础上，赋予其更重要的法律角色理所应当，如此也可缓解医疗机构等对外分享医疗信息的压力和顾虑。同时，以认定机构为中心搭建医疗数据池，可大大提升医疗信息的流通和汇集效率，形成真正意义上的医疗大数据。很多时候，我国医疗机构并非排斥医疗信息的流动和共享，只是囿于法无所依及随之而来的责任风险，畏惧数据的外流。〔55〕我国也可考虑建立对外分享个人医疗信息的激励机制（包括经济激励及其他激励措施），赋予信息分享者各类优先权及优惠机制，进一步推动医疗信息的流通和利用。〔56〕此外，由于强监管框架的完整布局，个人医疗信息的匿名加工及后续流通环节得到了较高程度的安全保障，默示同意规则的适用具有坚实基础，这也将保证个人医疗信息匿名化处理制度的高效运行。应当指出的是，此处默示同意之内容限于针对个人医疗信息的匿名化处理活动，而非及于所有类别的处理活动。正是由于匿名化标准的提高及匿名化信息全链条的安全保障，才有默示同意规则适用之可能。其他种类的个人信息如人脸识别信息能否同样适用默示同意规则，除提高安全保障水平、创造先决条件外，还应进行谨慎的价值衡量和规则设计，毕竟并非所有种类的个人信息均像个人医疗信息一样指向生命健康利益。

Abstract Building a systematic mechanism of anonymization is a feasible way to resolve the utilizing dilemma of personal medical information. Anonymization is the process of letting personal information unidentified and unrecovered by technical means. The information is no longer personal information through the process of anonymization and thus not bound by the rule of consent. Personal medical information is unique which calls for both a higher standard of protection and a higher degree of utilization. It should be regulated particularly. Our Personal Information Protection Law is defective and we should make up for defects to construct a more complete general system of anonymization. On this basis, we ought to regulate the anonymization of personal medical information particularly. Our government should authenticate the specialized institutions that are responsible for collecting and processing personal medical information at a higher level, and in the meantime, authenticated institutions apply to rule of implied consent when receiving personal medical information from the controllers.

Keywords Anonymization, Personal Medical Information, Express Consent, Implied Consent, Special Regulation

（责任编辑：曹博）

〔55〕参见高富平：《论医疗数据权利配置——医疗数据开放利用法律框架》，载《现代法学》2020年第4期。

〔56〕参见蔡培如、王锡锌：《论个人信息保护中的人格保护与经济激励机制》，载《比较法研究》2020年第1期。