World Medical Journal

Health Privacy Law: Getting the Balance of Interests Right

Edward S. Dove

In terms of scale, scope, and pace of change, health information — and the frameworks governing its protection—are daunting subjects to confront. As everyone knows, health information collected from and about us (which may be broadly defined to include our genetic relatives) is used to diagnose and treat us. The provenance and curation of this information, however, can be mystifying. The information may come from our own medical files, but it may also come indirectly from the data of hundreds of thousands, if not millions, of other people based on clinical audits, observational research, clinical trials, and data linkage studies. In England, for example, the National Health Service (NHS) holds medical records of more than 65 million people — practically the entire population in the nation — dating back for decades [1]. It is uniquely valuable in holding cradle-to-grave information on a national population, and a much-desired "treasure trove" that tech and pharma companies, unfriendly foreign governments, and others would love to access.

But that desired enhanced access is, thankfully, protected around the globe, albeit to varying degrees, by various normative frameworks, including laws. Medical confidentiality is an ancient ethical, professional, and legal obligation that health professionals and researchers alike owe to their patients and participants, respectfully. To focus on ethical codes, the Hippocratic Oath advises doctors that whatever they *"may see or hear in the course of the treatment or even outside of the treatment in regard to the life of [patients], which on no account one must spread abroad"*, they will keep to themselves, *"holding such things shameful to be spoken about"* [2]. The Declaration of Geneva obliges doctors to *"respect the secrets that are confided in [them], even after the patient has died"* [3]. Finally, the medical research-orientated Declaration of Helsinki demands that researchers take *"every precaution […] to protect the privacy of research participants and the confidentiality of their personal information"* [4].

If we also look to specific texts from the professional regulators around the globe, as well as national, regional, and international laws, there is in fact a panoply of precepts and rules governing what health professionals may do with the things they see, are told, write down, and share with others. If a health professional breaches a patient's confidentiality, we can be relatively confident that there will be, at least in principle, some form of sanction, be it from the professional's employer, a regulator, or a court of law. And yet, sometimes health professionals, employers, and governments alike fall short in respecting the reasonable expectations of patients and participants regarding the protection of their health information. Box 1 presents details about the "health privacy law," an emerging cognate area of law comprising three distinct legal frameworks.

Box 1. A Primer on Health Privacy Law [5]

Health privacy law is an emerging cognate area of law comprising three major legal frameworks: confidentiality law, privacy law, data protection law, and laws governing access to health records. Depending on the jurisdiction in question, these legal frameworks may be conjoined or separate, and in some rarer instances, non-existent (e.g. some jurisdictions still have not passed data protection laws that address health information). It is the corpus of laws and legal norms that govern 1) the collection, storage, and use of information relating to a person's or group of persons' physical or mental health, including the provision of health care services, which reveal information about one or more persons' health status, and 2) the spatial and decisional aspects concerning one or more persons' health, such as reproductive choices and end-of-life decision-making.

World Medical Journal

Confidentiality law is the legal framework that protects information disclosed by one party to another. In the health context, classically this would be medical information confided by a patient to one's doctor. Unlike privacy law and data protection law, it is primarily concerned with rules around protecting and sanctioning wrongful disclosure of health information rather than rules governing its collection.

Privacy law, in its broadest understanding, is the corpus of laws and legal norms that govern the collection, storage, and use of personal information, as well as the dimensions of private life of individuals (what might be termed our 'intimate lives') and, more provocatively, groups and communities.

Data protection law is primarily shaped by statute. It largely comprises a set of legal rules that aims to protect the rights, freedoms, and interests of individuals whose personal data are collected, stored, processed, disseminated, or deleted. Its principal purpose is to facilitate flows of personal data across organizations and countries, while at the same time ensuring fairness in the processing of data and, to some extent, fairness in the outcomes of such processing.

In May 2023, it was reported that a "stalker" doctor at Addenbrooke's Hospital in Cambridge, England, accessed and shared highly sensitive information about a woman who had started dating her ex-boyfriend, despite not being involved in her care. The doctor first accessed the hospital's medical records system and subsequently another records system that contained detailed notes of intimate conversations (e.g. her former partner's new girlfriend with her general practitioner about a family tragedy, her child's health). The hospital initially denied that staff could access patients' records through the hospital's medical records system, but in a subsequent meeting with the victim, the deputy medical director acknowledged that her full general practitioner's records were available for staff to access [6]. Many other examples abound, such as concerns about the NHS sharing patients' details with the United Kingdom (UK)'s Home Office (interior ministry) so it could trace people breaking immigration rules, and access to the UK Biobank data from a so-called "race science" research group [7,8].

Coupled with these unfortunately not-so-infrequent instances of putative health privacy violations is a growing sense of disempowerment and bewilderment. This scenario is caused in part by increasingly sophisticated and intrusive technical devices, technological developments, and volume of data linkage activity alongside massive mixed datasets of personal and non-personal data. The vast and growing array of policies, frameworks, laws, and legal agreements that characterize data privacy also influences any confusion or negative sentiment toward the ability of state and non-state actors alike to protect and promote our health privacy.

Indeed, the scale of collection, use, and sharing of all sorts of information concerning each individual seems to be growing exponentially. Data may come from the smartphone apps that can track movement and hence trace the spread of infectious diseases (e.g. coronavirus disease 2019, COVID-19) or document vaccination status. It may come from our visits to the therapist's office for a routine appointment or the hospital for a programmed surgical procedure or outpatient treatment. Data may come from simply relaxing in our apartments, taking the tram, train or bus to work, speaking to Alexa, prompting artificial intelligence (AI) chatbots such as ChatGPT or DeepSeek with health-related queries, and going on Bluesky, X, Instagram or TikTok to post a text or "passively" scroll through reels. Few doubt that there is a daunting amount of information about our lives that is hoovered up by algorithm-powered machines, digital devices, and digital systems, which is then assembled, stored, and manipulated into various datasets, and used in ways by governments, companies, researchers (and sometimes hackers) often beyond our understanding and awareness.

Cutting across this desire for solid protection in the face of mystifying and exponential growth in health information collection and use is the powerful pull of economic growth and societal wellbeing—and as part, medical progress to enable healthy, happy lives. The collection and use of health information (e.g. assemblage into datasets, curation, and making available to others for different purposes) depends on its relatively unencumbered free flow, both within and across national borders. Health privacy law, however, may present barriers, such as strict rules preventing the sharing of vital information

World Medical Journal

across international borders, for scientific research and other bona fide purposes.

The question remains: How do we achieve the balance between 1) assuring patients and participants that their health information is vigorously protected, and sanctions will be applied to professionals and other parties (including governments) who violate that trust; and 2) enabling health information to be used for the individual and public good?

In a recently edited book [9] and forthcoming book entitled Health Privacy Law [5], the author charts how the relatively simple days of easy-to-understand laws protecting medical secrets passed from patient to doctor have transitioned to an incredibly complex interplay of legal frameworks that govern the collection, use, and disclosure of health information concerning individuals and groups (as patients, consumers or research participants). For example, the European Union has complicated interactions between a serious of substantive laws, including the General Data Protection Regulation, the Data Governance Act, the Artificial Intelligence Act, and the European Health Data Space Regulation [10-13]. Aspects of health information impact the immediate individual (to whom the information relates) and may implicate other individuals, which raises under-addressed questions about group (or even familial) rights and interests.

In both of these recent works, the author explains how achieving the balance involves the careful drafting, interpretation, monitoring, and enforcement of legislative instruments, coupled with clear case law and policy documents, and easy-to-understand guidance for health professionals and patients. These efforts can help drive global harmonization and consensus, and prudently shape what may be done lawfully with information concerning our health. Of course, laws and regulations only represent part of the journey to building a culture of sustained protection and promotion of health privacy. Apart from compliance with laws and regulations, health professionals must continue to act virtuously, working with health organizations to develop and practice a culture that supports privacy-promoting compliance systems. Likewise, regulators, including health professional regulators, must possess and hone sufficient skills to evaluate and ensure health privacy is respected; regulators must also have the courage and political support to hold professionals and organizations accountable when privacy violations occur [14].

Health privacy and its regulation is unquestionably a dynamic, multifaceted field that engenders deep questions about power, control, reasonable expectations, and accountability. The author encourages readers to critically consider the ways in which the ethical, legal, and professional regulatory frameworks in their home jurisdiction regulate flows of health information, whether these frameworks are fit-for-purpose, and whether regulators are robust enough in their monitoring and enforcement. In other words, readers should ask: Are these frameworks attuned sufficiently to the evolving paradigm of large-scale, global, and digital data-driven healthcare and biomedical research? Do they strike an appropriate, proportionate balance between protecting morally and legally relevant interests in our health information, and the interests of society in promoting safe, efficient, and effective data flows? Is there a relative balance of power between relevant stakeholders, or do the frameworks inadequately protect individuals (and groups) from privacy intrusions by powerful actors (e.g. private companies like Big Tech, well-funded scientists, intrusive government bodies)? Should regulators do more, are they properly resourced to do more, and is the political will there?

Fundamentally, as we reflect on the answers to these questions, we should consider how health privacy law can help protect and promote human values, serving the interests of society and furthering our ability to lead healthy, flourishing lives. It is my sincere and admittedly self-interested hope that readers find health privacy law as a matter of profound interest and importance for their practice and for sustaining trust with patients and research participants. The forthcoming book, Health Privacy Law, provides insight into how we can all do better to protect and promote our health privacy in our daily practice.

Special note: This opinion piece is adapted and excerpted from the author's forthcoming book [5], with permission to reprint kindly granted by Edward Elgar Publishing.

World Medical Journal

References

1. Kollewe J. NHS data is worth billions – but who should have access to it? [Internet]. The Guardian. 2019 [cited 2025 Aug 20]. Available from: https://www.theguardian.com/society/2019/jun/10/nhs-data-google-alphabet-tech-drug-firms.

2. Edelstein L. The Hippocratic Oath: text, translation, and interpretation. Baltimore: Johns Hopkins Press; 1943. Available from: https://archive.org/details/hippocraticoatht0000edel/page/n3/mode/2up

3. World Medical Association. Declaration of Geneva [Internet]. 1940 [amended 2017; cited 2025 Aug 20]. Available from: https://www.wma.net/policies-post/wma-declaration-of-geneva/

4. World Medical Association. Declaration of Helsinki [Internet]. 1964 [amended 2024; cited 2025 Aug 20]. Available from: https://www.wma.net/policies-post/wma-declaration-of-helsinki/

5. Dove ES. Health privacy law. Cheltenham: Edward Elgar; 2026.

6. Campbell D. Warnings over NHS data privacy after "stalker" doctor shares woman's records [Internet]. The Guardian. 2023 [cited 2025 Aug 20]. Available from: https://www.theguardian.com/society/2023/may/14/nhs-england-data-privacy-confidentiality-records-addenbrookes-hospital

7. Quinn B. Migrants to get Home Office reference number on NHS England records [Internet]. The Guardian. 2023 [cited 2025 Aug 20]. Available from: https://www.theguardian.com/society/2023/aug/29/migrants-home-office-reference-number-nhs-england-records

8. Burgis T, Devlin H, Pegg D, Wilson J. 'Race science' group say they accessed sensitive UK health data [Internet]. The Guardian. 2024 [cited 2025 Aug 20]. Available from: https://www.theguardian.com/world/2024/oct/17/race-science-group-say-they-accessed-sensitive-uk-health-data

9. Dove ES, ed. Confidentiality, privacy, and data protection in biomedicine: international concepts and issues. Abingdon: Routledge; 2025.

10. European Parliament. 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) [Internet]. 2016 [cited 2025 Aug 20]. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

11. European Parliament. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). [Internet]. 2022 [cited 2025 Aug 20]. Available from: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

12. European Parliament. 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 [Internet]. 2024 [cited 2025 Aug 20]. Available from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

13. European Parliament. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [Internet]. 2025 [cited 2025 Aug 20]. Available from: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

14. Black J. Paradoxes and failures: 'new governance' techniques and the financial crisis. Mod Law Rev. 2012;75(6):1037-63.

Edward S. Dove, *PhD*
School of Law and Criminology,
Maynooth University
Maynooth, County Kildare, Ireland
edward.dove@mu.ie