The Ethical and Legal Privacy in the World of Big Data and eHealth: Are the US and the EU Ready for the Big Change in Healthcare?

Hana You
Yonsei University Graduate School of International Studies (GSIS)

Changes in global health care are occurring with the adoption of big data, and the digitization of health and patient data as traditional paper-based medical records are being switched to electronic health records (EHRs). Although the implementation of EHR systems has incredible potential to improve health management, it has raised significant ethical and legal concerns over data privacy and security, with large volumes of health data becoming available and accessible online. What calls for greater attention is that neither the existing legislative nor constitutional law sufficiently protects health information privacy. The privacy rights for healthcare information and data protection laws are different in the US and the EU and are often inconsistent and fragmented across and within states and nations. This essay examines the ethical and legal privacy concerning big data and eHealth in the US and the EU. It looks at the extent to which the legal frameworks have been established to protect health privacy, questioning whether the existing legislative framework comprehensively covers the facilitation, adoption, and use of big data and EHRs in health care.

Introduction

With the rapidly growing amount of medical data in the world, big data in health care has gained greater attention partly due to the adoption of the Electronic Health Record (EHR) in health care. Big data has been defined in several ways, but it generally refers to enormous data sets with sizes beyond what can be managed by traditional software tools. An example of a big data application in health care is the EHR. The US Department of Health and Human Services (HHS) defines the EHR as follows:

> An electronic record of health-related information on an individual

that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization.[1]

EHRs enhance the health care process by managing health information electronically, improving data availability, and providing more accurate and complete documentation, mainly through longitudinal health records (LHRs). These can track an individual's health history data over time from numerous data sources across the health system.[2] Along with the benefits associated with EHR, there are some risks and barriers that raise privacy concerns. A significant challenge regarding the use of big data in health care is that it is difficult to standardize and form a single large-scale database that is compatible across all nations. Linking data about the same individual from multiple sources is another challenge since traditional health records are stored in various institutions. Additionally, switching to EHR and linkages will require identifiers – such as a patient's name and date of birth – which will increase privacy concerns.[3]

Many national health policies or strategies and data protection laws do not encompass the use of big data and health information in an online environment. Less than one-fifth of countries have reported having a national policy or strategy that regulates the use of big data in health care. Those numbers become smaller when asked about having a national policy or strategy that regulates the use of big data by private companies. Moreover, a survey that asked the EU Member States about barriers to adopting big data for health has shown that a lack of data privacy and security laws is regarded as the top barrier to implementing big data in health care.[4] Based on the results of a global survey on eHealth conducted by the World Health Organization (WHO) in 2012, 70 percent of the 113

1 "Medline/PubMed Search & Electronic Health Record Information Resources," National Library of Medicine (NLM), accessed May 8, 2021, https://www.nlm.nih.gov/services/queries/ehr.html.

2 Shelley Reynolds, "Making sense of information technology," *British Journal of Midwifery* 11, no. 3 (2013), https://doi.org/10.12968/bjom.2003.11.3.11130.

3 Margaret Foster Riley, "Big Data, HIPAA, and the Common Rule: Time for Big Change?" in *Big Data, Health Law, and Bioethics*, eds. I. Glenn Cohen et al. (New York: Cambridge Univ. Press, 2018), 253-54.

4 Who Regional Office for Europe, *From Innovation to Implementation – EHealth in the WHO European Region*, report for the World Health Organization, 2016, 72.

responding countries reported having general legislation that provides a basic right to privacy.[5] However, when asked whether the responding countries have legislation that specifically protects the privacy of the EHR, only 30 percent globally reported having such legislation established.[6]

The right to privacy is recognized as a fundamental human right under Article 12 of the Universal Declaration of Human Rights; however, protection of privacy is not universally guaranteed because it is often based on the actions of governments. For example, the United States Constitution does not explicitly state the right to privacy. Only certain aspects are dealt with by the government and law enforcement, and the privacy rights for healthcare information are regulated sector by sector.[7] The notion of legal privacy can take different forms in different geographical regions and circumstances; however, it can largely be sorted into two scopes. According to William W. Lowrance, the two privacy regimes are (1) broad privacy and data protection regimes and (2) regimes specific to health care, public health, and health research.[8] This essay focuses on privacy issues regarding big data in eHealth from privacy regimes specific to health care. The essay examines the scope of the legal and regulatory framework supporting health information privacy in the US and the EU and the challenges arising from big data and eHealth not covered by the existing legal framework.

The Ambiguity of Privacy and Confidentiality in Health Care

Defining privacy is complex and challenging. There is no universal consensus that defines privacy and the right to privacy in its legal context. Alan Westin defines privacy as the claim of an individual or group to arbitrate for themselves about how and to what extent information is shared with others.[9] Lawrence O. Gostin defines privacy as one's claim to limit access by others to some parts

5 WHO Global Observatory for eHealth, *Legal frameworks for eHealth: Global Observatory for eHealth series – Volume 5*, report for the World Health Organization, 2012.

6 Ibid.

7 Mary F. E. Ebeling, *Healthcare and Big Data* (New York: Palgrave Macmillan, 2016), chap.3, 49-66.

8 William Lowrance, *Privacy, Confidentiality, and Health Research* (New York: Cambridge, 2012), 36.

9 Alan F. Westin, *Privacy and Freedom* (New York: Ig Pub., 1967), 7.

of his/her private life.[10] Generally, most definitions of privacy are not adequate to specifically cover privacy in health care or online platforms. For this essay, based on O. Gostin's research, we define privacy as "an individual's claim to control the circumstances in which personal health information is collected, used, stored, and transmitted."[11] More often than not, privacy is interpreted as confidentiality, even though the two have essential differences. Confidentiality is an individual's claim to handle information disclosure within relationships of trust between individuals respectfully.[12] Confidentiality is a form of health information privacy that emphasizes the relationships of trust between individuals in an intimate relationship, such as those between a physician and patient.[13] Confidentiality becomes tied with ethical issues in health care for traditional reasons concerning the role of trust in personal information disclosure, the fear of discrimination, and for contemporary reasons such as greater accessibility to information via the Internet.[14]

The Complexity of Privacy with Big Data in Health Care

EHRs complicate the issue of privacy and confidentiality since medical information is shared through the Internet. Additionally, the EHR can exchange patient data outside the healthcare delivery system, which means data sharing across multiple organizations is possible.[15] Although health care information is primarily transmitted between authorized users, mainly healthcare providers, it is essential to note that the collected data may not solely be limited to medical purposes. This implies medical information is electronically stored and is available for purposes other than those it was initially obtained for, that is, secondary uses. Such secondary data uses may involve personal, public, and commercial purposes (e.g., the development of new drugs, treatment, and marketing) by health and non-

10 Lawrence O. Gostin, *Public Health Law: Power, Duty, Restraint* (California: Univ California Press, 2008), 316-7.

11 Ibid.

12 Lowrance, *Privacy, Confidentiality, and Health Research*, 33.

13 O. Gostin, *Public Health Law*, 316.

14 James Anderson and Kenneth W. Goodman, *Ethics and Information Technology: A case-based approach to a health care system in transition* (New York: Springer, 2002), 2.

15 Ramona Nelson and Nancy Staggers, *Health Informatics: An Interprofessional Approach* (St. Louis, Missouri: Elsevier Mosby, 2014), 88.

health providers.[16] With goals specifically including protecting and promoting public health, there will probably be a gradual integration of individuals' health records within an expansive public health information infrastructure.[17] There is no doubt that big data in health care will catalyze this assimilation.

Health Privacy Laws of The US and The EU and Their Challenges

In the US, the legislation relevant to EHRs is the Health Insurance Portability and Accountability Act (HIPAA), signed into law in 1996 by President Bill Clinton. It aims to protect patient's health information from unauthorized disclosure or use in any form. Broadly, the HIPAA privacy rule is designed to establish national standards. Although the US attends to privacy through various methods, its privacy or data protection law is not consistent according to the Constitution, which does not explicitly address information privacy.[18] Thus, apart from the HIPAA, the Privacy Act of 1974 covers the use of personal information collected by federal agencies, and the Freedom of Information Act of 1966 provides public access to the individual's records.[19] However, most health information is collected, stored, and handled by private organizations not subject to these laws. Because of the absence of comprehensive legislation that governs the privacy and security of EHRs, there are fewer incentives for organizations to make investments in enhancing their security. Instead of having a coherent system, privacy protections in the US have referred to statutes, guidance, and professional and business self-regulation that are inconsistent and fragmented across and within states. Furthermore, private health organizations, having competitors in the field, are reluctant to share proprietary information with other entities, as they see little or no incentive when making their database available to others.[20]

The HIPAA law regulates much from US national standards, but there are still ambiguous and controversial aspects of its coverage at an entity and individual level. In her book, Sharona Hoffman offers a critique of the narrow definition of the "covered entities" as HIPAA does not apply to every person who may monitor or use health information, thus, not

16 Anderson and Goodman, *Ethics and Information Technology*, 64.

17 Roger S. Magnusson, "The Changing Legal and Conceptual Shape of Health Care Privacy," *The Journal of Law, Medicine & Ethics* 32, no. 4 (2004): 686.

18 Lowrance, Privacy, *Confidentiality, and Health Research*, 47.

19 Anderson and Goodman, *Ethics and Information Technology*, 70.

20 Molla S. Donaldson and Kathleen N. Lohr, eds, *Health Data in the Information Age: Use, Disclosure, and Privacy* (National Academy Press, 1994), 31.

protecting all health information.[21] The HIPAA privacy rule covers entities such as healthcare insurers, providers, clearinghouses, and their business associates. Thus, its jurisdiction does not cover government entities, website operators, and private data collectors.[22] This means that HIPAA does not protect personal health data collected by social media firms. Moreover, data collected from unregulated domains, such as de-identified data, patient-generated data, and non-regulated entities (e.g., pharmaceutical companies), are not subject to health information privacy laws.[23]

The EU implemented the Data Protection Directive to regulate the processing of personal data.[24] Although the EU has taken initiatives to promote big data in health care and develop a comprehensive policy strategy across nations, there are still obstacles; gathering health data across countries is not systematized, nor do they have a shared integrated structure.[25]

European countries have all adopted EHRs in differing ways, and thus it is challenging to transfer medical data from one country to another within the EU.[26] While the US privacy legislation is "sector-specific" within its states, the EU privacy law is rather "omnibus" and coherent within its countries and regions.[27] However, there is a notable contrast between the EU and the US privacy laws regarding data mobility across nations and states.[28] The EU Data Protection Directive of 1998 requires member states to prevent the transmission of health information to non-EU countries that do not have laws

21 Sharona Hoffman, *Electronic Health Records and Medical Big Data* (New York: Cambridge University Press, 2016), 181.

22 Ibid.

23 Jane H. Thorpe and Elizabeth A. Gray, "Big Data and Public Health: Navigating Privacy Laws to Maximize Potentials," *Public Health Rep* 130, no. 2 (Mar-Apr 2015): 171-175.

24 Karim Abouelmehdiet al., "Big data security and privacy in health care: A Review," *Procedia Computer Science*, 113, (2017): 73-80.

25 Sebastian S. Vega, Adria Haimann and Elias Mossialos, "Big Data and Health Care: Challenges and Opportunities for Coordinated Policy Development in the EU," *Health Systems & Reform* 1, no. 4 (2015): 285-300.

26 Charles Auffrayet al., "Making sense of big data in health research: Towards an EU action plan," *Genome Medicine* 8, no. 71 (2016): 1-13.

27 Ebeling, *Healthcare and Big Data*, chap. 3, 49-66.

28 Ibid.

with an equivalent level of privacy protection.[29] This kind of directive eliminates the exchange of data between the US and the EU states. In contrast, under US law, most personal data can be transferred outside national boundaries.[30]

Collaboration, Combination, and Refinement between the US and the EU privacy laws

Since the notion of what constitutes personal or private information is different from culture to culture and change over time, there is a contextual aspect of privacy that needs to be considered along the conditions in which data has been privatized. Big data contains personal and sensitive data, and, depending on the context, non-sensitive data can turn into sensitive data.[31] Much of the privacy legislation in the US and the EU may serve as models for other countries, particularly for developing countries. Further research could examine how privacy legislation built around big data and eHealth is carried out in developing countries through the legal architecture of their boundaries.

Big data is challenging existing paradigms for governing, using, and managing data in health care. There is a need to develop and reform policies and laws in health care that can allow synergies between health and data to maximize the potentials of big data. One of the key barriers to developing big data policies and regulations in healthcare is that the US and the EU have different data protection laws. Also, there is no one big data exchange ecosystem that integrates and connects all nations. Existing legislation and legislative infrastructure will require ongoing collaboration, combination, and refinement concerning the health privacy of EHRs and big data to deploy these frameworks in developing countries. There is a definite need for new legislation to establish privacy guidelines ready to face the digital world.

29 Anderson and Goodman, *Ethics and Information Technology*, 72.

30 Ebeling, *Healthcare and Big Data*, chap. 3, 49-66.

31 United Nations Development Group, *Data Privacy, Ethics and Protection: Guidance note on big data for achievement of the 2030 agenda*, report for United Nations, 2017.