Context Sensitive Health Informatics: The Role of Informatics in Global Pandemics
R. Marcilly et al. (Eds.)

doi:10.3233/SHTI210627

Legal Matters: The Legal Context of Health Informatics in Global Pandemics

Bonnie KAPLAN [a]
[a] *Yale University, New Haven, CT, USA*

Abstract. Law and regulation have not received much attention as part of the context shaping and being shaped by health informatics. Telemedicine, data, devices and software, and electronic health records (EHRs) are examples of how technologies are affected by privacy, intellectual property protections, and other law and regulation.

Keywords. Health informatics, law, regulation, telemedicine, privacy, medical devices, software, electronic health records, privacy, vendor contracts, intellectual property, ethics, ELSI, COVID-19

1. Introduction

In a time of COVID-19, ethical, legal, and social issues related to health informatics are increasingly apparent, social determinants of health are glaringly relevant, access to care is difficult, and the need for data to track and treat public health crises is abundantly clear. Even though healthcare is among the most regulated sectors, the *legal* part of ethical, legal, and social issues has not received the very welcome attention paid to the ethical and social, yet as policy advocates recognize, law and regulation are significant to the context of health informatics.

Health informaticists have been grappling with ethical, legal, and social issues (ELSI) for about a half-century.[1] Legal scholars, too, have discussed many of the issues, albeit from a different perspective and over a shorter time period. These scholars and new law school initiatives in digital health, artificial intelligence, robotics, privacy, disparities, and Big Data have been producing legal analyses and recommendations relevant to health informatics. With contact tracing and vaccine passports, as well as various algorithmic and digital developments, they have been paying even more attention.

This paper sketches how policy, law, and regulation contribute to the context of health informatics. Telemedicine, data, devices and software, and electronic health records (EHRs) in the US serve as examples of how technologies are affected by privacy, intellectual property protections, and other law and regulation. I discuss the role of law as part of the context of health informatics by putting together these four examples in one paper. They are drawn primarily from my own health informatics publications because those include numerous citations and an extensive reference list is beyond the page limits of this paper.

2. Telemedicine

Regulatory changes contributed to the astronomical increase in telemedicine use during the first months of the COVID-19 pandemic.[2] To facilitate access to care and data, US regulations and enforcement regarding reimbursement, privacy and data sharing, licensing, credentialing, supervising non-physician providers, and previously established doctor-patient relationships were relaxed. As this is being written, it is predicted that these policies will continue and that telemedicine will remain popular. Patients like the convenience and administrators and vendors like the economics.

As with the regulatory environment, broadband policies also affected telemedicine's uptake. Technology infrastructure may not seem related to health policy, yet funding affects its availability for healthcare. Lower income and rural patients without technologies for video had telephone visits,[3] so were less able to meet the widely recognized standard of care of telemedicine being equivalent to in-person visits.[2] Though voice visits are preferable to no healthcare at all, policy regarding technology and access contribute to disparities regarding access related to locale, income, and also to disabilities. Hearing, speech, dexterity, cognitive, and vision impairments create difficulties with telecare, likely more so with voice-only care.[3, 4]

3. Health Data

Privacy has gotten extensive and widespread discussion with growing public attention to social media and smartphone apps. Much discussion focuses on intrusive marketing and targeted advertising, secretive data collection, both business and governmental surveillance, and unsuspected use of data for automated decisions affecting all aspects of our lives. These kinds of concerns influence attitudes towards vaccine passports and contact tracing for COVID-19 control. The privacy regulatory environment in regards to healthcare contributes to how and why these issues arise.

Data privacy in the US is regulated, when it is regulated, by sector. Different national laws pertain to financial data, health data, student data, genetic data, etc. Where data originate affects how privacy is regulated nationally. (State laws are different in each state.) The Health Insurance and Portability Act (HIPAA) governs clinical data generated by "covered entities" (generally, health care providers). Research involving human subjects is regulated through the Federal Policy for the Protection of Human Subjects, known as the Common Rule, which covers data protection for healthcare research subjects. Both require that people give permission for identifiable data to be released; both specify how data are to be de-identified or anonymized for purposes for which permission is not required, thereby implicitly defining "privacy" in terms of identifiability, permissions, and kinds of data. Neither protects de-identified data, even when combined in ways that may lead to re-identification or implicating people other than the ones represented in the data. The two sets of rules may be difficult to reconcile with each other and with other regulations. Data governance regimes juggle these differences with the result that privacy regulation impedes data sharing for research, public health, and patient care, while not much protecting patient privacy.[5-7]

Data related to health but collected by social media, fitness and other devices, and smartphone apps generally are not regulated at all. Commercial entities that provide these services are bound by their privacy policies, which are enforced by the Federal

Trade Commission, if enforced at all. People usually are given no choice but to click through consent to an end-user license agreement (EULA) to use the device or participate in social media. EULAs may or may not include a privacy policy that may or may not be honored, and that almost certainly are not widely read or understood.[7, 8]

Data from all these sources are sold and combined in ways that make it easier for even de-identified data to be identified. Data from commercial products are incorporated into patient records, as patient-generated data is recognized to be important for monitoring social determinants of health and real world data, and for better control of chronic disease. Distinctions between the different regulatory categories of data are thus blurred as all data are becoming health data.[8]

Privacy regulation—what is regulated and what is not—has facilitated an active market for all sorts of products and services sold to promote healthy lifestyles, empower people to control their health, enable people to share health-related information ranging from genetics to shopping habits, keep track of children and people with dementia, and improve hearing, limited only by the imagination of creative entrepreneurs. Appealing health-related apps benefit many happy customers and create opportunities for collecting and selling data in ways that can both help and, though legal, harm people.

4. Devices and Software

Technologies now being sold to improve lifestyle and health are popular for good reason. They keep track of voice, breathing, retinal patterns, vital signs, gait, diet, exercise, and sleep patterns. They may help detect potential health problems or enable people to monitor various conditions unobtrusively during their daily routines. They remind people to take medications and alert caregivers if there are problems. Some simply are fun. Most fall outside the scope of health data privacy protections, which are targeted towards patient record information, not daily life activities and measurements. Indeed, most are not regulated at all. The Food and Drug Administration (FDA), which is responsible for overseeing not only medications but also medical devices, does not classify them as such because they are not intended to be used in diagnosis, cure, mitigation, treatment, or prevention of a disease. This means that HIPAA does not apply to them. It also means that they are not vetted by the FDA as being safe and effective.[4,8] Like the market for data, a lax regulatory environment enables commercial health informatics applications to flourish.

Regulation has been more pertinent to software-based devices that clearly are part of clinical settings, what is known as "software as a medical device (SaMD)." The FDA waived the usual regulatory approval process for these and other devices because of the COVID-19 public health emergency. Recently, the FDA proposed ending regulatory review and making that waiver permanent. The new process would make precertification possible for software such as for AI and machine learning. Since 2017, the FDA has been developing a software precertification program to make regulatory oversight of software based medical devices more streamlined and efficient. As with the precertification initiative, the recent proposal was that products substantially like existing products and that rarely are associated with adverse events would not need regulatory review. This includes artificial intelligence programs that physicians can use to help them detect cancers, respiratory diseases, broken bones, and other findings on medical images. Digital devices to be exempted from review include ones that manage the safety of drug infusions, monitor fetal heart rates, and deliver behavioral therapy for psychiatric patients. The intent is to promote innovation and quickly get devices to market, another way the regulatory environment shapes health informatics.[9]

For reasons discussed above for other apps and devices, legal and ethical issues are rampant for COVID contract tracing and vaccine passports promoted for public health and opening up the economy. They raise privacy, safety, efficacy, surveillance, and equity concerns, including geolocation tracking and segregation due to inequities of vaccine and smartphone availability.[10] When predictive algorithms based on machine learning are used, it may be impossible to know just how they arrive at their results.

Another way regulation is relevant to devices and software is through intellectual property law. To reward innovators for new products and services, trade secrets, patents, copyrights, and contracts all prevent disclosure of how these technologies function. Software, especially, is opaque, more so with advances in artificial intelligence and machine learning. Intellectual property protections make it difficult to know what data were used to create models, how they were trained and tested, and, in the case of machine learning, why and how they work. Contracts protect vendor interests with non-disclosure clauses, such as for EHRs, that prevent disseminating knowledge of hardware and software problems.[11]

5. Electronic Health Records

It is by now common knowledge in health informatics that electronic health records have significantly changed clinicians' work while improving some aspects of care and being detrimental to others. The regulatory environment contributed to this phenomenon. EHRs are not regulated, except in so far as the meaningful use/promoting interoperability criteria for certification and reimbursement reporting requirements are ways to regulate.[8] Without incentives and penalties established by the federal government to promote adoption of electronic health records through the 2009 HITECH Act, electronic health records likely would not be as widely used as they now are. Incentive payments based on certification and meaningful use criteria emphasized some areas of functionality, which necessarily diverted attention from others. Although there are many benefits of current systems, among the pitfalls are increasingly arduous and clinically irrelevant documentation requirements that take time away from patient care, which, together with alert fatigue, contribute to burnout, and have motivated physicians to leave practice or influenced their choice of specialty.[12] There has been little attention to interoperability (one of the reasons why EHRs have been promoted), to usability, and to compatibility with clinical thinking and workflow, although all are getting more attention than previously.[11] Further, as mentioned above, intellectual property protections included in vendor contracts contribute to continued concerns. It is impossible to consider virtually any aspect of electronic health records that is not influenced by regulation and its (un)intended consequences.

6. Conclusion

The Context Sensitive Health Informatics conference call notes that COVID-19 made it clear that health informatics innovations need to bridge time and space with infrastructure that supports the healthcare management of populations at a macro level while also providing the necessary support for front line care delivery at a micro level, all while insuring quality and safety. Law and regulation are crucial to shaping, and themselves are shaped by, these efforts. They are part of the context of health informatics.

References

[1] Goodman KW. Ethics in health informatics. Yearb Med Inform. 2020(EFirst). https://doi.org/10.1055/s-0040-1701966.

[2] Kaplan B. Revisiting health information technology ethical, legal, and social issues and evaluation: Telehealth/telemedicine and COVID-19. Int J Med Inf. 2020;143(November):104239. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2020.104239.

[3] Kaplan B. Ethical, legal, and social issues pertaining to virtual and digital representations of patients. In: Hsueh P-YS, Wetter T, Zhu X, editors. Personal health informatics: Reimagining consumer health informatics for precision medicine and healthcare. Cham: Springer; forthcoming.

[4] Kaplan B, Ranchordás S. Alzheimer's and m-health: Regulatory, privacy, and ethical considerations. In: Hayre CM, Muller D, Scherer M, editors. Everyday technologies in healthcare. Boca Raton, London, New York: CRC Press; 2019. p. 31-52. http://ssrn.com/author=2307861.

[5] Kaplan B, De Muro PR, Goodman KW, Pasquale FA, Talmon J, Winkelstein P. Data governance dilemmas for research and clinical care. AMIA Annu Symp Proc. 2014. http://ssrn.com/author=2307861.

[6] Kaplan B, Davidson EJ, Demiris G, Schreiber R, Waldman AE, Rethinking health data privacy. AMIA Annu Symp Proc. 2019. http://ssrn.com/author=2307861.

[7] Kaplan B, with appendix by Monteiro APL. PHI protection under HIPAA: An overall analysis. In: Dallari AB, Monaco GFC, editors. LGPD na saúde (LGPD applicable to health). São Paulo: Editora Revista dos Tribunais (Thomsom Reuters); 2021. p. 61-88. http://ssrn.com/author=2307861 and https://www.livrariart.com.br/lgpd-na-saude/p.

[8] Kaplan B. Seeing through health information technology: The need for transparency in software, algorithms, data privacy, and regulation. JL & Biosci. 2020. https://doi.org/10.1093/jlb/lsaa062.

[9] Kaplan B. Regulation of software as a medical device: Opportunity for bioethics. Hastings Center Forum; 2021 [updated March 1, 2021]. https://www.thehastingscenter.org/regulation-of-software-as-a-medical-device-opportunity-for-bioethics. Accessed March 1, 2021.

[10] Clayton J, Humell A, Pervaiz S, Cahn AF, Manis E. The good, the bad, & the invasive: The impact of vaccine registries, day passes, & passports. Surveillance Technology Oversight Project; 2021 [updated June 2, 2021]. https://www.stopspying.org/vaccineapps. Accessed June 3, 2021.

[11] Koppel R. Uses of the legal system that attenuate patient safety. DePaul L Rev. 2019;68(2):273-90.

[12] Hoffman S. Healing the healers: Legal remedies for physician burnout. Yale J Health Pol'y L & Ethics. 2019;18(2):56-113. https://digitalcommons.law.yale.edu/yjhple/vol18/iss2/2.