Balancing Health Privacy, Health Information Exchange and Research in the Context of the COVID-19 Pandemic

Leslie Lenert, MD, MS[1] and Brooke Yeager McSwain, MSc, RRT[2]
[1]Medical University of South Carolina, Charleston, SC and
[2]South Carolina Childrens' Telehealth Collaborative
Charleston, SC 29425

Abstract

The novel coronavirus COVID-19 infection poses serious challenges to the healthcare system that are being addressed through the creation of new unique and advanced systems of care with disjointed care processes (telehealth screening, drive-through specimen collection, remote testing, telehealth management, etc.) However, our current regulations on the flows of information for clinical care and research are antiquated and often conflict at the state and federal level. This paper discusses proposed changes to privacy regulations such as the Health Insurance Portability and Accountability act (HIPAA) designed to let health information seamlessly and frictionlessly flow between the health entities that need to collaborate on treatment of patients and, also, allow it to flow to researchers trying to understand how to limit its impacts.

Author contact information:

Leslie Lenert, MD, MS, FACP, FACMI
Assistant Provost for Data Science and Informatics
Medical University of South Carolina
135 Cannon Street, Suite 405J
Medical University of South Carolina, Charleston, SC 29425. Author contact information: Lenert@musc.edu

The COVID-19 response imposes unprecedented challenges on our healthcare system. To address these challenges, the health information needed to safely care for a patient needs to flow across provider platforms in a given region without impediment. For example, patients may first be screened by one organization utilizing telehealth, obtain testing at a “drive-through” collection site run by a second institution, have tests performed by one of multiple clinical laboratories with novel testing capacity, obtain follow up through primary care or other case management methods at a different institution, and be hospitalized at locations with sufficient capacity, not necessarily related to any prior providers in the information chain. This process is illustrated in Figure 1. Successful care in this complex, ad hoc system will require safe, secure, and standardized health information exchange, through point-to-point (such as Direct) and hub-and-spoke models (such as a Health Information Exchange (HIE) Organization). However, the current mix of state and HIPAA privacy regulations poses a confusing maze of barriers to effective HIE for patient care. Urgent action is necessary to ensure regulations that are designed to preserve privacy and move toward a more balanced footing that emphasizes continuity of care.

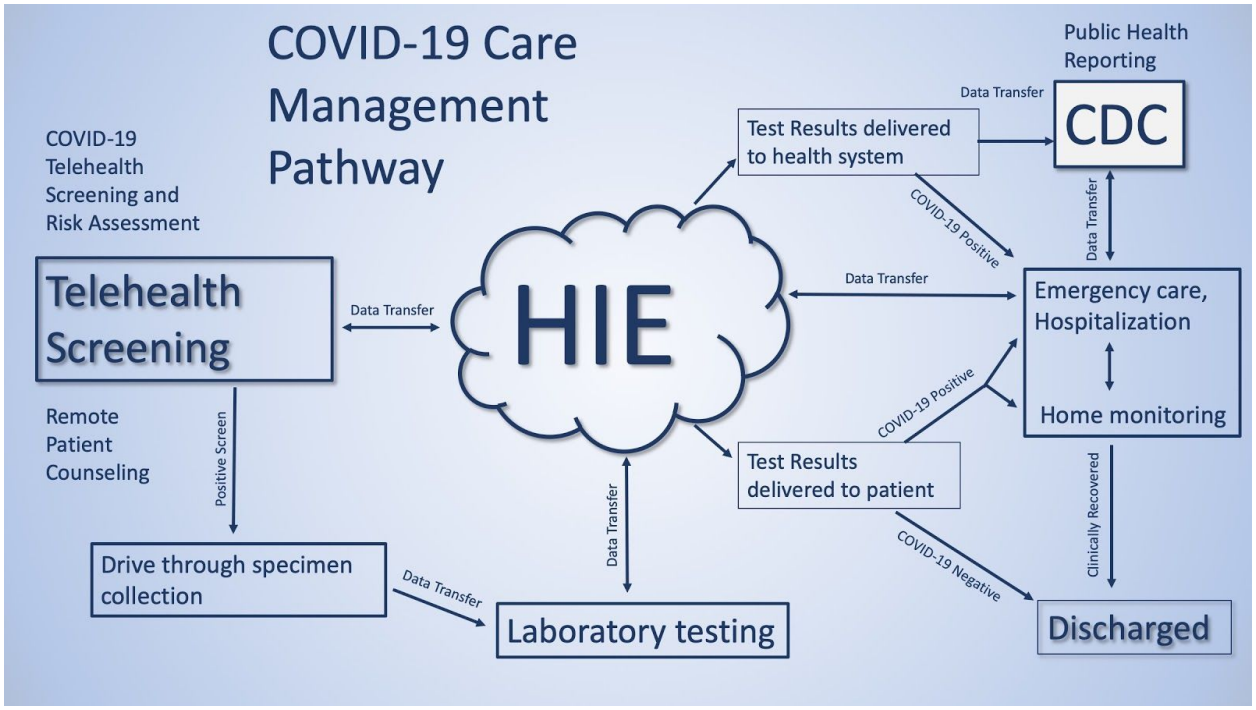

Figure 1. Hypothetical system for screening and care of patients with COVID-19.

In addition, novel approaches to contact tracing using cellular geolocation data and implementation of different types of social distancing strategies, such as workplace and restaurant closures, prohibitions against large public gatherings, and home quarantine, are being applied to manage the pandemic. Research on the effectiveness of controlling the epidemic through advanced contact tracing, social distancing and testing strategies is urgently needed in order to direct policy--but much of this work is limited by current federal requirements for safe harbors regarding anonymization of clinical data. Understanding how specific social

distancing strategies work in different micro-geographies may be accelerated by expanding the “safe harbor” definition to allow researchers a more detailed geographic view. Normally, this would be a “limited” HIPAA data set, which requires both a human subjects expedited review and a HIPAA waiver for research. Loosening the borders of anonymization might allow a broader range of data scientists access to the information without administrative barriers. While such work is possible today, changes to the definition of what protected health information (PHI) is, in the context of this epidemic, could accelerate it. Such changes are possible under the broad powers of the Stafford Act.

The current state of emergency declared by President Trump allows the Secretary of Health to waive certain federal regulations [1,2], such as HIPAA, or to override state laws with more stringent privacy protections of health information exchange, during this emergency period through a Stafford Act declaration. The Stafford Act allows a broad range of powers to the federal government in the setting of this emergency. How should these best be used to remove roadblocks inhibiting care and research? While privacy is normally of paramount importance, this pandemic dictates the creation of new systems of care on an unprecedented scale, as well as the development of cost-effective strategies for reducing transmission through social distancing in a timely way. Both may require rethinking the primacy of privacy of health data.

Is HIPAA the problem?

The rights of privacy we have today are the product of nearly 130 years of layered legislative and regulatory actions, executive orders, and judicial interpretations. This disjointed approach has resulted in the labyrinthine and fragmented array of privacy protections we find ourselves navigating today. And health information and data privacy are no exceptions to that rule. Of particular concern during the challenges of the global COVID-19 pandemic are the barriers created by the patchwork of laws and regulations, and the complexity of HIPAA, particularly as it relates to sharing PHI via either point-to-point or hub-and-spoke HIEs.

HIPAA, passed in 1996 and enacted over the following few years, was written to incentivize the digitization of health information and codify ways in which we protect health data. To that end, its authors created the Privacy and Security Rules in an attempt to presage how digitized data might be vulnerable to unintended sharing with third parties. (DHHS) The Privacy Rule provides the guidelines by which the collection, storage, access, and methods of disclosing data, are handled and was intended to be a uniform regulation for the immediate management of PHI as the workforce transitioned from paper files to digitized records. The Security Rule was written to apply only to PHI transmitted electronically, and while legislators soundly anticipated how future data exchange would occur, the law does not work well with today’s HIEs. This is largely due to misunderstanding at the organizational level about how the law applies to the broad range of data information that can now be shared via HIE, the complexity of which data requires consent, and what liability exists if healthcare entities misinterpret the law.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed with the purpose of promoting the adoption and meaningful use of electronic health records (EHR), and health information technology [3]. HITECH also recognized the accountability of businesses who assist health providers in the sharing of data via EHR, and legally defined the roles of and responsibilities of both healthcare providers and business associates, requiring both contracts, or Business Associate Agreements (BAAs) and direct accountability for compliance with the appropriate sections of HIPAA's Privacy and Security Rules. Further confusing matters, HIPAA, while always intended to function as a federally preemptive law, allows for stricter state laws to supersede the federal statute. And, interpretation and enforcement falls simultaneously to HHS and state attorneys general, who are allowed to prosecute infractions by provider and non-provider organizations, alike.

The resulting morass of multiple and overlapping state laws [4], which have since been written, and re-written, to define the protection, consent for, and transfer of specific kinds of health data (mental health, substance abuse treatment, care for sexually transmitted diseases, etc), are often more stringent than HIPAA. This tangle of federal and state laws makes identifying and complying with general information exchange and consent laws an onerous undertaking [5], frequently leading organizations to the conclusion that data sharing via HIE is legally and financially so difficult as to often be prohibitive. In an emergency setting, we need to drastically reduce the barriers to frictionless HIE: one law of the land for COVID-19 related data.

The President's Stafford Act declaration opens the door for the federal government to provide technical, financial, and other generally defined assistance to states and local municipalities during an emergency and can trigger other public health emergency response authorities. However, in order for the Secretary of Health and Human Services (HHS) to exercise waiver authority under Social Security Act Section 1135 (which allows the Secretary to temporarily waive or modify certain Medicare, Medicaid, SCHIP, and HIPAA requirements), there must be a public health emergency determination under Section 319 of the Public Health Service Act, as well as a presidential declaration under the Stafford Act or the National Emergencies Act.

To enable the efficiencies of rapid communication of required health data that a pandemic response necessitates, we must consider what actions could be taken to waive the current tangle of legal barriers to HIE use while concurrently ensuring the privacy of individual health information.

Three possibilities meet these requirements and should be immediately considered for use in the current state of emergency response:

The first and most decisive action is the enactment of HIPAA's complete federal preemption of all other data sharing and consent laws. This approach may appear extreme but it holds the most promise for balancing the needs of immediate sharing of information, appropriate protection of PHI, and presenting a clear and definitive statement to healthcare providers and the general public, alike. Specifically, for the duration of the health emergency, the HIPAA

standard of no requirement of patient consent to transmit health information on COVID-19 infection status, risk factors, treatments, and recovery status between healthcare providers caring for an individual with suspected, active, or recovering COVID-19 infection, whether point-to-point, or through an HIE Organization, as defined by HIPAA, should be the rule of law for the nation, overriding more restrictive state laws. Requiring patient consent is burdensome and it has been shown that, regardless of method, substantial numbers of patients do not consent. Additionally, research demonstrates racial and ethnic disparities in consent [6], which, in this circumstance, could lead to inequity in care.

Second, the Office of Civil Rights (OCR) should create a Safe Harbor business associates agreement (BAA) that covered entities and other supporting organizations can rapidly adopt for HIE about COVID-19. Under HIPAA, HIE through a Health Information Organization (HIO) requires a BAA. Such agreements govern how information will be used, stored, and reused by parties that hold information prior to forwarding to another organization and differences vary widely between organizations' legal preferences. A covered entity's BAA with an HIO will vary depending on a number of factors, such as the electronic HIE purpose which the HIO is to manage, the particular functions or services the HIO is to perform for the covered entity, and any other legal obligations an HIO may have with respect to the PHI. Disagreements between organizations on content of BAAs or preferences for their own existing documents are a major barrier to operationalization of HIE between clinical entities. A default safe harbor BAA designed to discourage unnecessary variation, and that specifies how an HIO must protect the information while supporting exchange for clinical care and public health purposes, would accelerate the creation of new partnerships that will create the alternative systems of care shown in Figure 1.

Third, an important component of HIPAA is the concept of transmission of the minimum necessary information between covered entities. The Office for Civil Rights should issue guidance that once again clarifies that there is no requirement for minimal information in exchange of data for care of patients. In addition, they should clarify that transmission of minimal information does not apply to public health entities during this crisis. Public health officials should have unfettered access to EHRs of patients with COVID-19 infection for rapid development of guidelines for case investigation and patient care.

Geotracking, geocoding and age coding

In addition, we need better tools for contact tracing and for study of transmission during the pandemic. Public health needs the ability to link medical records of COVID-19 patients to their cellular devices and obtain the histories of their movements prior to diagnosis and of other persons whose cellular devices indicate they came in proximity of these persons. Persons coming in close proximity to known COVID-19 patients could be informed by public health, through their devices, self quarantine, obtain testing if symptomatic and contribute to containment. Taiwan successfully applied this approach as part of a Big Data strategy to slow transmission of the virus [7]. The approach is also being tested in Israel [8]. Currently, public

health does not have authority to access cellular providers' data for this purpose. They need immediate access to this data along with cloud-based tools to integrate this data for the complex analytics required for the Big Data approach. A comprehensive database for a region should be developed and the approach evaluated for its usefulness for future outbreaks.

Further study of transmissivity of COVID-19 and the impact of public health policies on social distancing are needed. Current approaches for social distancing are having massive economic impacts and yet their effectiveness is not known [9]. To facilitate the study of transmissivity and the risk factors for progression of disease, a loosening of safe harbor parameters of anonymization of data sets (or, conversely, what is considered PHI) may be helpful to allow a broad range of researchers to immediately begin work. This can be done without undue barriers from Human Subjects review of projects, and security requirements that are inherent in work with a Limited Data Set. To that end, HHS could modify definitions of what an anonymized geoentity is. The current standard is an area of 20,000 people, or the initial three digits of zip code. We would propose to decrease this to 50-100 persons, which would bring the level of resolution to the block level (relevant to home quarantine approaches). In addition, dates of medical services, such as admission, discharge or death dates, will be critical to understanding the outbreak. These should no longer be considered PHI, initial work shows that the risks of infection are age-related; therefore, requirements to aggregate ages into a single category above 90 years should be waived.

Conclusions

While the USA's Health Insurance Portability and Accountability Act (HIPAA), as well as state privacy regulations, are foundational in protecting the privacy of health information, they are now significant barriers to creation of ad hoc and novel systems of care and the dissemination of information about an individual's infectious status from one state to another in a mobile population. Entities may need to work together across state lines, and entities that may be unknown to each other at the time of administration of medical services may need to collaborate to effectively care for the patient. Patients may not be able to choose the provider doing follow-up care, and delays and overhead in information transmission might compromise the effectiveness of the care system. Public health needs access to new types of information in cellular providers' data systems in order to drive its response. Further, we need to mobilize the full spectrum of researchers to understand and address the challenges posed by the epidemic. Use of emergency federal powers to create a unified framework for data exchange about the epidemic and research is an essential step toward effective response to the challenges we currently face.

Acknowledgements

The authors wish to acknowledge the participants of American College of Medical Informatics mailing list who participated in early online discussions of concepts found in this paper and the expert editorial assistance of Kimberly Snow. This publication [or project] was supported, in part, by the National Center for Advancing Translational Sciences of the National Institutes of Health under Grant Number UL1 TR001450. The content is solely the responsibility of the authors and does not necessarily represent the official views of the National Institutes of Health.

References

1 Gostin LO, Hodge JG, Wiley LF. Presidential Powers and Response to COVID-19. *JAMA* Published Online First: 18 March 2020. doi:10.1001/jama.2020.4335

2 Robert T. Stafford Disaster Relief and Emergency Assistance Act Fact Sheet | State Public Health | ASTHO. https://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Authority-and-Immunity-Toolkit/Robert-T--Stafford-Disaster-Relief-and-Emergency-Assistance-Act-Fact-Sheet/ (accessed 15 Mar 2020).

3 Office for Civil Rights (OCR). HITECH Act Enforcement Interim Final Rule. HHS.gov. 2017.https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html (accessed 20 Mar 2020).

4 O'Connor J, Matthews G. Informational privacy, public health, and state laws. *Am J Public Health* 2011;**101**:1845–50. doi:10.2105/AJPH.2011.300206

5 Mello MM, Adler-Milstein J, Ding KL, *et al.* Legal Barriers to the Growth of Health Information Exchange-Boulders or Pebbles? *Milbank Q* 2018;**96**:110–43. doi:10.1111/1468-0009.12313

6 Turvey CL, Klein DM, Nazi KM, *et al.* Racial differences in patient consent policy preferences for electronic health information exchange. *J Am Med Inform Assoc* Published Online First: 9 March 2020. doi:10.1093/jamia/ocaa012

7 Wang CJ, Ng CY, Brook RH. Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. *JAMA* Published Online First: 3 March 2020. doi:10.1001/jama.2020.3151

8 Lomas N. Israel passes emergency law to use mobile data for COVID-19 contact tracing. *TechCrunch* 2020.http://social.techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/ (accessed 18 Mar 2020).

9 Cohen J, Kupferschmidt K. Countries test tactics in 'war' against COVID-19. *Science* 2020;**367**:1287–8. doi:10.1126/science.367.6484.1287