1-16-2021

HIPAA-Phobia Hampers Efforts To Track And Contain COVID-19

Lee Hiromoto M.D., J.D.

HIPAA-Phobia Hampers Efforts To Track And Contain COVID-19

Lee Hiromoto, M.D., J.D.*

Introduction

Passed in 1996, the Health Insurance Portability and Accountability Act (HIPAA)[1] sets privacy standards for healthcare providers, hospitals, and their business associates. No doubt well-intentioned, HIPAA has come to embody a force beyond its original purpose. It has become a boogeyman for those entrusted with health information, even when HIPAA does not actually apply to them. Doctors, information technology specialists, and schools officials walk on eggshells to avoid violating federal privacy law. In the current pandemic, this *fear* of violating HIPAA has created inefficiencies in addressing COVID-19. This essay looks at a few ways that HIPAA-phobia is hampering the flow of information that could help public health teams combat this illness. Finally, the essay explores regulatory and legislative ways to address HIPAA anxiety and its negative consequences.

I. Fear Of HIPAA Can Muzzle Doctors' Ability To Warn The Public Early On

Medical training ingrains in healthcare providers that patient privacy is sacrosanct. So much so, that medical providers will err on the side of the caution when faced with a grey decision to disclose—even if it may benefit public health. During the early days of the pandemic, in March 2020, the following exchange between a doctor and a reporter exemplifies what could have been opportunity spread awareness of where and when the virus may have been transmitted:

Reporter Ike Bendavid: Can we learn more about this patient? I mean, were they active in the community? Where did they travel? There are a lot of people concerned that they are frequenting public spaces in Chittenden County.

* Resident Physician, Department of Psychiatry, Oregon Health & Science University

[1] Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

Dr. Steve Leffler: I want to remind people we are bound by federal law and what we can tell you.[2]

This exchange highlights the instinctive fear that healthcare workers have when revealing information about patients.

At that early stage (this was the *second* patient in the state), members of the public could have used the information to self-quarantine and pursue testing. But Dr. Leffler was reluctant to share information about who might have been exposed, citing "federal law" (implicitly HIPAA). Contact tracing is labor intensive, imperfect, and relies on government efficiency. Publicly notifying potential contacts where and when they may have been exposed would add another layer of notice to those efforts.

Of note, there are exceptions already built into HIPAA that could justify release of a COVID-19 patient's recent whereabouts and activities. One such exception involves public health and the need to identify those who were exposed.[3] Another exception allows disclosure of information when "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public"[4] In this scenario, the doctor could have justified saying more about the patient—one of the first in the state—based on either of these exceptions. But with the specter of HIPAA lurking, he chose not to.

The American approach contrasts with that in Israel, where the government made public where coronavirus cases had been. In one instance in late February 2020, the Israeli government made public the flight he had taken, the toy store he had visited, and even the approximate times he was at the store.[5] This stands in contrast to Dr. Leffler's inability to provide this basic information to the public due to "federal law."

---

[2] Ike Bendavid, *Vt. patient with 2nd COVID-19 case in critical condition*, WCAX.COM (Mar. 12, 2020), https://www.wcax.com/content/news/UVM-to-provide-details-on-2nd-COVID-19-case-NH-reports-6th-case-568739241.html.

[3] 45 C.F.R. § 164.512(b)(1)(iv) (2016).

[4] 45 C.F.R. § 164.512(j)(1)(i)(A) (2016).

[5] *Health Ministry: Israeli with coronavirus visited toy store before diagnosis,* TIMES OF ISRAEL (Feb. 27, 2020). https://www.timesofisrael.com/health-ministry-israeli-with-coronavirus-visited-toy-store-before-diagnosis/.

II. HIPAA-Encouraged Reliance On The Fax Machine Slows Down Contact-Tracing

HIPAA has rigorous information security requirements (and correspondingly rigorous penalties) for "electronic" data, which disincentivize the use of electronic communications. However, these rules (Subchapter C of Title 45 of the Code of Federal Regulations) specifically carve out an exception for "transmissions, including of paper, via facsimile, and of voice, via telephone."[6] This is one of the reasons fax machines were estimated to account for 75% of medical communications.[7]

Reliance on the fax machine as a HIPAA compliant mode of communication can hamper efforts to trace COVID-19 contacts. In Hawaii, local media reported that "the state's contact tracing program has relied on two fax machines to receive the thousands of new positive and suspected case reports pouring into its offices."[8] The same article noted that after faxes received, they were then being scanned for a period of time because staff were not aware that digital copies were automatically made.

Similarly, the fax machine has hindered efforts in Texas, where using "faxes to report coronavirus cases in the state *is a way to ensure a person's privacy is protected*." Austin's director of public health is quoted "we have a whole team of people who have to sort through more than a thousand faxes a day," which he described as a "very manual and archaic process."[9] One could imagine a better system—computerized—where the team sorting through stacks of faxes could instead be focused on substantive work like contact tracing.

---

[6] 45 C.F.R. § 160.103 (2014).

[7] Brad Spannbauer, *Does the Fax Machine Still Have A Place in Modern Healthcare?*, HIT CONSULTANT (Aug. 27, 2018), https://hitconsultant.net/2018/08/27/fax-machines-modern-healthcare/.

[8] Marcel Honore, *How Hawaii's Reliance On 'Labor Intensive' Fax Machines Hampers Contact Tracing*, HONOLULU CIVIL BEAT (Sept. 4, 2020), https://www.civilbeat.org/2020/09/how-labor-intensive-fax-machines-hamper-hawaiis-contact-tracing/.

[9] Erik Ortiz, *Amid coronavirus surge, Texas has a contact tracing problem: reporting cases by fax*, NBC NEWS (June 26, 2020) (emphasis added), https://www.nbcnews.com/news/us-news/amid-coronavirus-surge-texas-has-contact-tracing-problem-reporting-cases-n1232212.

To be fair, HIPAA is not the only reason healthcare depends on the venerable fax. Much has been said about the role of economic incentives for healthcare networks and hospitals to create barriers to leaving a given network.[10] But HIPAA's rigorous information security requirements and potential penalties only reinforce the economic incentive to use the fax. For example, the University of Rochester settled a HIPAA violation stemming from loss of an unencrypted flash drive and theft of a laptop for USD $3,000,000.[11]

American dependence on the fax machine contrasts with the high-tech approaches seen in East Asian countries during the start of the pandemic. There, digital contact tracing met with early success.[12] But American healthcare IT, held back in part by HIPAA and its fines, is not there.

III. HIPAA-Phobia Limits Current Efforts To Monitor COVID-19 Spread

In addition to limiting healthcare providers' ability to share data—a context in which HIPAA actually applies—the reputational penumbra of that law has become so large that it has chilled data sharing outside healthcare. Even those *not* covered by HIPAA, like schools, worry about violating it. The text of the HIPAA rules make clear that it only applies to healthcare providers, organizations, and their business associates.[13] Nonetheless, an everyday appreciation for HIPAA's (justifiable) privacy protections has snowballed into a McCarthy-esque situation where officials hold onto information with white knuckles, lest they be accused of violating HIPAA.

---

[10] Alyssa Rege, *Why the US health system still prioritizes fax machines: 7 things to know,* BECKER'S HEALTH IT (Oct. 30, 2017), https://www.beckershospitalreview.com/healthcare-information-technology/why-the-us-health-system-still-prioritizes-fax-machines-7-things-to-know.html.

[11] Press Release, Dep't of Health & Human Serv., Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement (Nov. 5, 2019), *available at* https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html.

[12] Yasheng Huang et al., *How Digital Contact Tracing Slowed Covid-19 in East Asia*, HARV. BUS. REV. (Apr. 15, 2020), https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia.

[13] 45 C.F.R. § 164.500 (2013).

Some school administrators have been unwilling to discuss COVID-19 cases due to fear of even potentially violating HIPAA. When a staff member tested positive at one elementary school, the superintendent invoked HIPAA to avoid releasing details: "[d]ue to HIPAA privacy laws, the identity of the . . . staff member was not disclosed. The staff member's position in the school was also not disclosed in connection with HIPAA privacy laws."[14]

In the case of the University of Alabama, which had over 1,000 cases during one week across three campuses, guidance was issued to faculty in the English Department that the pandemic makes "ANY reference to student health a potential HIPAA violation."[15] Someone who was exposed in a classroom might want to know about an infected colleague, but the misunderstanding of HIPAA would limit that.

Perhaps more egregiously, lawyers and government officials are not immune from misunderstanding that HIPAA does not reach beyond healthcare. The Attorney General of Louisiana—that state's top legal official—recently cited HIPAA when declaring his opposition to the state health department's release of school-specific coronavirus data. In response to this release, which was ordered by Louisiana's Governor, John Bel Edwards, Attorney General Landry wrote on Twitter: "[S]chools report specific healthcare information on your child without your consent! I believe that this order may be in violation of HIPAA."[16]

And during the recent White House coronavirus outbreak, former press secretary Sean Spicer accused a news agency (via Twitter) of violating HIPAA by reporting about a current staffer's positive test result. Though

---

[14] Linda Murphy, *Fall River schools report first COVID-19 case*, HERALD NEWS (Sept. 21, 2020), https://www.heraldnews.com/news/20200921/fall-river-schools-report-first-covid-19-case.

[15] Meryl Kornfield, *Universities can't use privacy laws to withhold data on coronavirus outbreaks, experts say*, WASH. POST (Sept. 2, 2020), https://www.washingtonpost.com/education/2020/09/02/college-coronavirus-privacy-laws/.

[16] JC Canicosa, *Attorney General Jeff Landry is challenging Louisiana public schools and health department*, LA. ILLUMINATOR (Sept. 26, 2020), https://lailluminator.com/2020/09/26/attorney-general-jeff-landry-is-challenging-louisiana-public-schools-and-health-department/.

the claim is baseless (as noted by one of the law's authors),[17] a public accusation of violating federal law is enough to create a deterrent to information sharing, especially given the power of social media to disseminate incorrect information.

Less data and less transparency make it more difficult for both policymakers and members of the public to make decisions that affect community spread of the pandemic. Should kids (generally or specifically) go to in-person classes at school? Should I go to work if there is a known cluster nearby? Knowing how the virus has spread locally would be helpful to make that call at both the collective and individual levels. But fear of HIPAA makes those with key data unwilling to share.

IV. Short And Long Term Solutions To HIPAA's Chilling Effect On The Coronavirus Fight

Addressing HIPAA-phobia can be done in the short term with executive action, and longer term with statutory reforms by Congress.

Discretionary Enforcement To Promote Data Sharing

Short-term, the executive branch can calm fears over information sharing and technology use by announcing discretionary non-enforcement during the emergency period. One success story comes from the Department of Health and Human Services (HHS), which announced discretionary non-enforcement of HIPAA's data safeguard standards to promote telehealth. Specifically, HHS announced that it would not seek penalties under HIPAA if providers used an application whose information security may not meet HIPAA standards.[18]

---

[17] Zack Budryk, *Shalala corrects Spicer on HIPAA: 'I should know, I wrote it'*, MSN.COM (Oct. 5, 2020), https://www.msn.com/en-us/news/politics/shalala-corrects-spicer-on-hipaa-i-should-know-i-wrote-it/ar-BB19JmkT.

[18] *OCR Issues Guidance on Telehealth Remote Communications Following Its Notification of Enforcement Discretion*, U.S. DEP'T HEALTH & HUMAN SERV. (Mar. 20, 2020), https://www.hhs.gov/about/news/2020/03/20/ocr-issues-guidance-on-telehealth-remote-communications-following-its-notification-of-enforcement-discretion.html.

Per HHS's loosening of rules, "covered health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR [the HHS Office of Civil Rights] might seek to impose a penalty for noncompliance with the HIPAA Rules."[19]

Stories about so-called "Zoom bombing" point out that these everyday voice and videoconferencing applications do not boast ironclad information security,[20] which would make them normally unacceptable under HIPAA. Thanks in part to this change, telehealth went from 0.1% of Medicare primary care visits in February 2020 to 43.5% by April 2020.[21] By easing fears of HIPAA (and multi-million dollar fines), the federal government was able to encourage routine healthcare needs to be met digitally, cutting away some of the bureaucracy that has kept the fax machine around.

In a similar vein, the Executive Branch could issue a broader notice of discretionary enforcement as regards COVID-19. Such a policy would apply the looser technology rules to contact-tracing efforts to replace the clunky fax. Similarly, it might offer healthcare providers broader leeway to report public health risks to the public and those in danger, offering that good faith efforts to prevent localized outbreaks will not be punished. Although there already are HIPAA exceptions for public health (noted above), there is little concrete guidance. Faced with a grey choice, providers will therefore choose to err on the side of caution and follow the letter of

---

[19] *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEP'T HEALTH & HUMAN SERV. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (last updated Mar. 30, 2020).

[20] Eric Hamilton, *Zoom Hacking is on the Rise: Here's What You Need To Do To Be Secure*, TECH TIMES (May 12, 2020), https://www.techtimes.com/articles/249572/20200512/zoom-hacking-is-on-the-rise-heres-what-you-need-to-do-to-be-secure.htm.

[21] HHS Issues New Report Highlighting Dramatic Trends in Medicare Beneficiary Telehealth Utilization amid COVID-19, U.S. DEP'T HEALTH & HUMAN SERV (July 28, 2020), https://www.hhs.gov/about/news/2020/07/28/hhs-issues-new-report-highlighting-dramatic-trends-in-medicare-beneficiary-telehealth-utilization-amid-covid-19.html.

HIPAA scrupulously. While lawfulness is noble, this course protects one person's information while that information could help others.

Lastly, such executive action would clearly note that HIPAA does not apply to schools. Ideally, this action would also address that other federal privacy laws like the Family Educational Rights and Privacy Act (FERPA)[22] would also have enforcement deferred in cases of good faith efforts to contain the spread of COVID-19. This would address timidity in releasing data from the virus's spread to educational settings. An executive order may be the best vehicle for such a policy, as there is inter-departmental crossover between HHS and the Department of Education (which handles FERPA matters) and Justice (responsible for criminal enforcement).

Longer Term Reform

Longer term, policymakers might look at revisiting HIPAA to reflect those changes in enforcement in statute. Public health emergencies could allow for more explicit waivers of HIPAA and FERPA to the extent reasonably aimed at fighting the spread of illness. Digitization would be encouraged, instead of disincentivized, as current law does (with carve-outs for analog communication). Such changes would change the current perception and climate of fear as regards potential HIPAA violations, facilitating the flow of public health data. Good faith would be the presumed basis of adjudicating alleged HIPAA violations, with penalties reserved for the worse offenders.

A statutory solution would differ from discretionary non-enforcement, as is currently happening with looser HIPAA enforcement as regards telehealth. Discretionary non-enforcement is transient and could change through executive action. Statutory change, on the other hand, would be the default rule and give actors (doctors, school leaders, IT specialists) more certainty that they will not run afoul of some law, rule, or regulation and fall victims to America's politico-legal bureaucracy.

[22] 20 U.S.C. § 1232g (2018); 34 C.F.R. pt. 99.

Conclusion

Medical privacy is undoubtedly an important interest. But it does not exist in a vacuum. The world is currently facing its greatest public health challenge in over a century. Efforts to contain the coronavirus, pending a vaccine or cure, can benefit from the free flow of data to policymakers and the public. Individual citizens can make better decisions with more information. Public health agencies can do better contact tracing when they are free to use digital technology. However, some data-holders are squeamish to release it for fear of violating HIPAA and incurring penalties. This misunderstanding of HIPAA is compounded when officials invoke the law to avoid, deter, or criticize disclosures that could help the public make decisions about school and work. Moreover, this fear of the HIPAA boogeyman has sustained technological obsolescence, as seen in the widespread reliance on the fax machine in American healthcare. We have the data and the technology to face the novel coronavirus head-on. The President and Congress can and should take action to make sure that HIPAA-phobia does not hold us back from using them.

Edited by Ben Davisson