



EXECUTIVE SPOTLIGHT

ISSUE 2 • FEBRUARY 2021

Protecting “Health-ish” Data: Balancing Innovation and Health Data Privacy



Jodi Daniel
Crowell & Moring



Laura Hoffman
American Medical
Association



Liz Salmi
OpenNotes and Beth
Israel Deaconess Medical
Center



Alice Leiter
eHealth Initiative

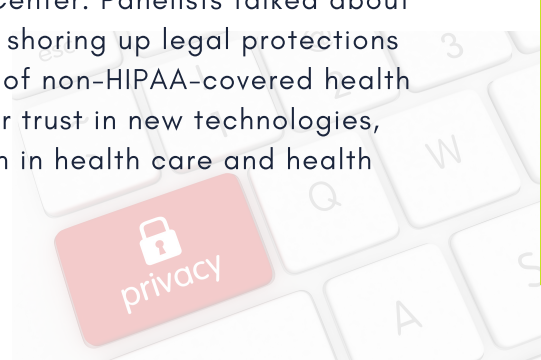
PANEL HIGHLIGHT

ESTABLISHING CONSUMER TRUST IN NEW TECHNOLOGIES

In the featured panel, eHI's Vice President and Senior Counsel Alice Leiter joined Jodi Daniel, Partner at Crowell & Moring; Laura Hoffman, Assistant Director of Federal Affairs at the AMA; and Liz Salmi, Senior Strategist, Research Communication at OpenNotes and Senior Multimedia Communications Director at Beth Israel Deaconess Medical Center. Panelists talked about the challenging balance of shoring up legal protections for the increasing amounts of non-HIPAA-covered health data, establishing consumer trust in new technologies, and encouraging innovation in health care and health tech.

“The lack of significant changes since the HIPAA statute was developed can be seen as both a challenge and as a strong point. Ultimately, HIPAA really did set a common set of rules, a common language and common expectations that have served to enable health technology innovation.”

- Jodi Daniel



Can you give us an overview of the current legal landscape around health data and privacy?

Jodi Daniel: HIPAA is the foundation of health information privacy, security and data use. Although not perfect, it was actually ahead of its time when the statute came out in 1996. The privacy rule was first published in 2000, revised in 2002 and took effect in 2003, before anyone was really talking about privacy, sector-specific data or sensitive data. This was before internet use, smartphones, EHRs and widespread health information breaches.

What helped HIPAA to stand the test of time is that it was designed to be flexible and scalable. The goal was to come up with rules that set a simple baseline guide that everyone could follow; reasonable rules that would be a foundation for what healthcare organizations could do with data and what individual rights there would be. There have only been modest changes since the original rules came out.

The lack of significant changes since the HIPAA statute was developed can be seen as both a challenge and as a strong point. Ultimately, HIPAA really did set a common set of rules, a common language and common expectations that have served to enable health technology innovation.

Although in many ways HIPAA has stood the test of time, there are a lot of things that regulators did not contemplate when we were writing it, such as ability for care coordination, health information exchanges disclosures for social services and social determinants of health, and the widespread uses of data for algorithm development and for machine learning.

So there is still opportunity for improvement, as there are still many limitations, such as the fact that it does not cover all healthcare providers. Self-pay telehealth providers might not be covered by the rules; some behavioral health providers only do self-pay and we are seeing more and more of this happen with concierge practices in healthcare; notably these might not be covered by HIPAA.



Alice Leiter



Jodi Daniel

HHS has come up with two new Rules this year that will be effective later on in 2021: the ONC rule and the CMS Rule. The ONC Rule was adopted under the 21st Century Cures Act and was designed to make some changes to the certification program, including promoting more access to data via APIs, and there are provisions prohibiting the practices of information blocking.

With these new Rules anything that is permitted under HIPAA may become required under information blocking, so if you are allowed to disclose information for treatment under HIPAA and you do not without a reasonable and necessary excuse, you are now in violation of information blocking.

The CMS rule promotes access and interoperability specific to health plans having to disclose claims, encounter data and clinical data that they maintain through a patient access API. For both of these rules the government is strongly promoting the patient's access to their data in machine readable format through APIs using the third party App of their choice.

What are the consequences of a shaky or non-existent consumer/patient trust foundation in considering the proliferation of new technologies?

Laura Hoffman: An example that I come back to time and time again is what happened with digital contact tracing applications particularly last spring and over the summer. There was a great idea and need to try to supplement traditional public health contact tracing due the outbreak of COVID-19 with digital and smartphone applications that can use different functionalities on your phone, such as Bluetooth or GPS, to alert people when they were exposed to COVID.

Unfortunately, what we saw with the early rollouts of those applications was that people did not trust what would happen with the information they provided. Last summer especially we had a lot of heightened tension with respect to law enforcement; there were protests, immigration proceedings and many people were nervous about providing information to government authorities through technology companies.

This is a critically important take away from that experience, which is we can come up with all sorts of innovative technologies that will both make life easier for patients and help to improve the public health of our nation, but if that trust factor is not there and there is no understanding from the very beginning about how one's data will be used so that a person can feel comfortable with the given current social contracts and conditions, then those innovative technologies are not going to be used, there will not be uptake and there will not be improvements in health.



How does this notion of effective education and communication and transparency come into play when establishing trust?

Liz Salmi: Historically health systems get to decide what people can see and not see in their patient portals.

When patients can receive the transparency and ability to see visit notes from their visits, the patient stands to benefit; they better understand their clinicians, they trust their doctors more, they can remember what was said, and they are more likely to take their medications as prescribed.



Jodi Daniel: I am a privacy lawyer and I still click 'I agree' to things without reading through them because you need the service and so you'll agree to them, which is concerning as the consent model is only a layer and not the sole privacy protection. In my view, it puts too much of the onus on the consumer, patient and individual to understand their rights and understand how their data can be used.

What are your thoughts on the balance that needs to be struck between giving people more access and the fact that we do not quite have the right privacy protections in place, and how we should walk that fine line?

Liz Salmi: I think when people are really sick and scared privacy goes out the window. One's thought process is "I don't care I'll post my stuff on the Internet if that means that I'm going to get to talk to the person I need to talk to."

That said, there are no levers for the patient to control how much of their data they are giving access to, which is very much needed.

Laura Hoffman: The thinking that we need to get all the data out there and then worry about privacy later is backwards thinking, and it is the opposite of what we are talking about in terms of laying foundations that incorporate privacy by design and the consumer's best interests.

While it is likely true for most patients and most people that when they are sick they want their information shared immediately and with anyone who wants to look at it, we need to also be thinking about people who do not want to make that choice or who could be harmed if that choice is made for them and when their information is shared in ways that they are not comfortable with.

We are not all evenly situated. I as a relatively young white female in the US will probably be treated much differently than a young black female who lives in a different area and does not have the same level of income that I do. When you put those two people side by side and they are looking for health or life insurance later on for themselves or for their children, or trying to get a job, or find a new place to live, all of their information is out there, amassed by data aggregators and compiled by people creating risk scores for all sorts of things.

These are the harms that we need to be thinking about as we work on privacy policy, to protect against these inequities, while still creating pathways for people to be informed as they choose to share their information.

Jodi Daniel: I want people to feel confident sharing their health information while knowing that there is going to be basic protections against some of those harms. They need to feel comfortable sharing the information that will help them receive treatment, without being worried about the scenario of somebody who will come back to haunt them down the road, because they did not have a choice of both getting the best care and also protecting themselves against those harms.

Laura Hoffman: We need better ways to select and share pieces of information. In the same way that access versus privacy should not be competing against each other, we should not continue to always be faced with this all versus nothing type of sharing paradigm, we need to think about better ways that technology can help patients and clinicians do that.



Should the onus for protecting the consumer health data be placed on the companies, such as through adoption of eHI and CDT's Consumer Privacy Framework for Health Data?

Laura Hoffman: I will selfishly say I hope so but the cynic in me says that a lot of companies like to talk about how they want to do this and how they value doing it, but when it comes time to actually do it, they may not.

[Pew Charitable Trusts recently commissioned a survey] which showed that consumers did not really understand that HIPAA does not apply to most applications even though they desired to use those applications.

Most respondents in that survey said that they would look to their clinicians to help provide guidance to them on the applications that they should select to manage their health information. While we certainly love that patients will look to their physicians for that guidance, at the same time it is really hard for any loving and giving clinician to know the ins and outs of every application their patient might bring to them.

Having some sort of trusted system and framework that not only sets guidelines but is backed by an enforcement mechanism for accountability, will fortify everyone's confidence. I think that clinicians would find it very helpful to have some sort of body they can look to for a universal industry standard and code of conduct for privacy of consumer health information on third party applications.

Jodi Daniel: What we saw with the model privacy notice is that Apple actually used it while others did not because they did not have to. While maybe there is an advantage to having a badge of privacy protection, it was not enough for companies to pursue this and potentially expose to the world what they are really doing with consumers' data.

The value to companies cannot just be because they want to be a good player, it has to be because doctors are going to refer patients to companies who are on that privacy protective list, which provides a benefit that they see in in terms of dollars, and greater use of their product over somebody else's.

Companies will then want to be on such a list, so the uptick will very much depend on what the consequences are of doing it versus not doing it, and I think there has to be some positive incentives or disincentives to not following a universal code of conduct.

Liz Salmi: I have noticed that there are a couple of privacy framework or pledges being developed over the past year and I have participated on some panels and similar discussions where I have asked, who is going to hold everybody accountable when they have made these pledges? Who enforces this? I as a consumer need clarity on how many pledges I would need to be familiar with, or who has the better pledge that I need to you know, and which seal of approval should I recognize?

I would love to see it become organized in such a way so that I will not need to keep reeducating myself about everybody's different plans and there is a universal policy or standard for everyone to abide by which will simply what the consumer needs to know and understand.



info@ehidc.org
202-624-3270
www.ehidc.org

