Laura Hoffman, JD, on protecting patients' vaccination data

Watch the AMA's COVID-19 Update, with insights from AMA leaders and experts about the pandemic.

Featured topic and speakers

In today’s COVID-19 Update, during #DataPrivacyWeek, AMA Chief Experience Officer Todd Unger talks with Laura Hoffman, JD, the AMA’s assistant director of federal affairs, about the importance of establishing guardrails for digital vaccination data and how physicians can address data privacy concerns with patients.

Access the AMA's case for privacy by design in app development resource (PDF).

Learn more about AMA's health data privacy framework and advocacy work on the issue.

Learn more at the AMA COVID-19 resource center.

Speaker

- Laura Hoffman, JD, assistant director of federal affairs, AMA

Transcript

Unger: Hello, this is the American Medical Association's COVID-19 Update video and podcast. Today we're talking about data privacy with Laura Hoffman, the AMA's assistant director of federal affairs in Washington, D.C. I'm Todd Unger, AMA's chief experience officer in Chicago. Laura, thanks for joining us.

It's not a Hallmark holiday and I didn't see any cards for this but it is data privacy week. A lot of privacy issues out there to talk about today. Why and how has data privacy become such a concern at this point in the pandemic?
Hoffman: Thanks, Todd, and it's great to be here to talk to you about this. I have to say I'm partial to this non-Hallmark holiday, as you called it. I think it's a great opportunity to talk to listeners about why, as you said, privacy is really rising in the collective consciousness right now, especially in the midst of the pandemic.

I think one thing that's on a lot of people's minds is that there have been increasing calls to you use or to implement what we refer to as digital vaccine credentials. You may have heard them inappropriately called vaccine passports historically but essentially they're a way to prove and document that you have actually been vaccinated. A lot of different states are starting to require these types of credentials to enter restaurants, bars, movie, theaters, that kind of thing. It's an effort essentially to try to help keep the public safe.

Again, obviously people can use their paper vaccine cards to meet a lot of these requirements but there is an increasing desire to digitize this and ensure that that information is legitimate, that it hasn't been a counterfeited paper card and that it's easy for establishments to trust that the credential is actually valid.

Unger: I know here in Chicago, of course, you need to show your vaccine card to be able to eat at a restaurant.

Hoffman: Yep, same with D.C.

Unger: Of course, I'm pulling out my phone a lot to do that.

Hoffman: Yes.

Unger: This idea that we need to move to maybe some different format, given the concerns you just outlined, I mean, these are not new concerns, potentially, and neither is privacy. But we're seeing a lot of privacy concerns, not just here but also with technology and app development. Can you talk about the context in general?

Hoffman: Absolutely. Yes, absolutely. I think a lot of the concerns that we see with apps generally when we talk about privacy carries over pretty cleanly into the digital vaccine credential service world too, that vaccine app world. We've all gotten so used to using apps to do anything from ordering food, to ordering a ride, to checking in to airlines for travel. It seems like it should be this really easy, common sense thing to just pull out an app to verify your vaccine status but unfortunately, the same things, like I said, that we talk about with other apps and other digital technologies when it comes to privacy exist in these vaccine apps as well.

Namely, I don't want to get too technical but a lot of times what happens is these apps are collections of different software that operate together to get us the service that we're after. One thing I would
specifically mention are what are called SDKs, software development kits. They're little pieces of that go into a lot of apps. What they wind up oftentimes doing is pulling data from that app and then sending it back to some unknown third party. Folks may have heard a lot in the news over the last few years about Facebook receiving, for example, a lot of data that individuals weren't aware that Facebook was receiving, they might not have even had Facebook accounts but Facebook has a very broadly disseminated SDK that goes into a lot of different apps and therefore pulls information that people aren't sure and didn't realize that they were actually sharing.

Now, this might seem kind of like, "Well, what's the big deal? Okay, so Facebook gets a little bit of my information," but I think the things that we want to think about are more systemic, they're more global. What happens when Facebook or other data analytics companies start to collect so much data on people that they're able to start slicing and dicing people in different groups? Maybe you've got a group of Christians over here and a group of young Black women over there, and it goes on and on. A lot of times that can be used for good, you can target opportunities at different groups of people, maybe there's a group of people with a certain health condition and you want to try to advertise a new emerging treatment or a drug for a health condition.

The unfortunate case is that that also sometimes flips into the opposite effect, where these opportunities start to be limited by the data that is collected and so certain groups of people do not see the same kinds of opportunities that we all may. I realize that's a big jump from just talking about privacy in apps but I think it's really important that the AMA and others really help the public to know about this and for clinicians to know about this so, that they're able to give good suggestions to their patients about the kinds of health technology that they use.

Unger: I think your example of Facebook is a good one. There's a lot of concern about how that data is shared. I think if you have an iPhone, you've seen a little popup, that'll say, "Allow this app to track across other apps." That is, a big concern, data privacy also a focus of certain organizations. Even now, I was surprised, I looked at my portal for the health system that I go to and I saw an aggregation of all my shots, vaccines. I didn't know how that happened. I'm glad that it is but at the same time, it kind of fits in with what you're saying, that in the background, which is a lot of what happens in apps or digital marketing. There's a lot of stuff going on, a lot of data being shared.

When we focus on this credentialing, the vaccine credentialing arena, let's talk a little bit more, you talked about some of the downsides.

Hoffman: Sure.

Unger: You're starting to point out where segmentation can occur for good and bad.

Hoffman: Yep, exactly.
Unger: It's just that maybe we didn't give permission for that to occur. Talk a little bit more about that.

Hoffman: Yeah, exactly. I mean, clearly we want to encourage the use of health apps, for example, for consumers to access their own medical information, to be able to see what vaccines they've received over the years and send that to their new physician if they move across the country. We want to make these kinds of apps workable and functional for patients. At the same time though, however, we want to ensure that there are certain safeguards put in place.

For example, we actually wrote to the federal government last year, and to the State Governor's Association, I believe also at the end of last year and tried to pull out some key protections that we think should be included in the development of apps and how they basically govern the data that they collect.

Unger: What specifically would those safeguards be?

Hoffman: Yeah, so things like minimizing the amount of data that's actually collected. Let's say, for example, you're using a vaccine app that will keep track of how many COVID shots you've gotten over the months and years. Maybe it shouldn't be asking about where specifically you live or what your other health conditions are or what the medications are that you take. This is a decades-old principle around privacy, is ensuring that you're only collecting and sharing the amount of information that's really necessary to accomplish a particular purpose.

The other kinds of things that we ask for the federal go to do is, again, to make sure that people can always use paper vaccines or vaccination cards rather than an app. Not everyone has a smartphone obviously, not everyone has internet access to be able to use these services, so we wanted to ensure that people weren't left out of being able to participate in public activities, even if they didn't have an app. Then certain other specific things, like maybe you don't need to create an account to use a digital vaccine credential app. Again, minimizing the collection of data that is really required. Then of course just ensuring that people who saw, say you go to a restaurant and they want to check your app, what kind of information is the restaurant then holding onto? Do they need to store all of your information or do they just need to see, "Yep, she's gotten her shots, come on in."

I'd encourage folks to maybe take a look at that letter and continue to pay attention to the kinds of policies that their individual states are requiring for the apps that they're promoting.

Unger: I mean, obviously, in the app marketplace, pretty limited number of key players out there. Any concerns about who's going to have access and control, I guess for lack of better words, in that particular marketplace?

Hoffman: Yeah, for sure. I mean, while not commenting on specific apps, there is absolutely a concern that the more apps that are out there, essentially they are less than regulated. Again, there
aren't any real federal standards around what these apps should and shouldn't do. It would be great to see app stores start to require some of these kinds of standards. I mean, you mentioned Apple earlier, popping up different notifications to their users on the iPhone saying, "Hey, this app might be actually tracking what you're doing when you're looking at something else." I think we need more of that. We need more responsibility from the actual technology developers and vendors to say, "Hey, we recognize that privacy is really important to our users, to clinicians."

In fact, we're just wrapping up a survey right now that we've been working on, talking to patients and seeing how they want their data used and how they don't want their data used. We're going to have more coming from that throughout the year. I can say, as a little sneak peek, I suppose, that basically individuals are really wary of companies getting their personal data. I think that developers would really be wise to pay attention to that and look forward and see, "Hey, what kinds of controls should I be putting my technology to ensure that people are going to want to use them, that doctors will trust them and that we maintain the public trust in trying to use these apps?"

**Unger:** You mentioned earlier in the conversation this idea of segmenting. I think we've faced this issue before, in terms of insurance and things like that, that once people will be able to track certain things about you, there's a chance that there could be equity issues around different kinds of segmentations. Can you talk about what the pitfalls are there?

**Hoffman:** Yeah, absolutely. Again, I love this question. I think privacy is so often thought of as this technical, nerdy, behind the scenes thing but it really is a people issue. It's a human rights issue, it's a civil rights issue. Privacy essentially gives people the autonomy to control who knows what about them. I mentioned earlier, for example, Facebook was, and still does, collect vast amounts of data, slicing and dicing, segmenting this data into different risk groups.

But we've seen, just to stick with the Facebook example, the U.S. Department of Housing and Urban Development a couple of years ago filed a complaint against Facebook for essentially not advertising housing opportunities to certain groups of people, largely historically marginalized groups of people, LGBTQ individuals, Black individuals. That is a prime example of saying how when we continually feed so much data almost without thought out into the universe, it can be collected and then framed in a way that can either help people, again, to get that new job or that person might not ever see that job opening because they've been specifically requested to, because based on their demographics, that kind of person is not wanted for this job so don't even show them the advertisement.

It really is this larger at play, where people literally have risk scores and risk profiles developed on them with hundreds and hundreds, if not thousands, of data points. Again, as I mentioned earlier too, this can spill over into not only your own personal demographics, whether it's race, religion, whatever but also health conditions. Things like substance use disorder are historically stigmatized and so you see a lot of employers maybe making hiring or promotion decisions based upon someone's substance use history.
A lot of people aren't thinking when they use health apps that this information is going to wind up in the hands of their either current or perspective employers down the line or life insurers down the line, which could have huge effects for them and their families.

**Unger:** Yes, my former business school professor from a long time ago wrote a very, very thick tome on this kind of surveillance, Shoshana Zuboff, if you are interested in that.

**Hoffman:** Oh, yes, yes. Exactly, exactly.

**Unger:** I think that kind of surveillance and the data economy that we're in right now is a substantial issue for us to contend with. You mentioned, Laura, the survey that the AMA's putting together. Can give us a little bit more, in terms of deep details on when we'll start to see the results of that?

**Hoffman:** Yep, absolutely. We literally just wrapped up the survey this month, in January, and we're synthesizing the results right now. We reached out to over a thousand patients, and again, wanted to just get real data behind what types of companies, what individuals, what purposes are patients most comfortable sharing their health information about? Again, a couple key takeaways I would say is that people were very clear that privacy is a right of theirs, it shouldn't be up for sale. There was a very reaction to data being monetized and commercialized, especially when they aren't aware of it. The other thing had to do with notices of privacy practices and how companies are explaining to individuals what they're actually doing with the data and does that change all the time and people aren't aware of it.

We're pulling that together and we'll be synthesizing that into some broader messaging and speaking to how health systems can help patients and the physicians who work in them provide really meaningful guidance. We want to ensure that's better transparency to patients so they understand what's being done with all the data that is collected by these apps.

The other thing I should mention is, right at the end of 2021, we put out a new resource that's aimed largely at developers to help them think about some of the tools that they can build into their apps, kind of a privacy-by-design perspective. That may also be interesting to listeners to check out. It really walks through the business case for privacy, perhaps getting ahead of federal legislation that might require this eventually anyway but then taking our AMA privacy principles and translating that into technical controls that can help to really shore up the privacy controls that we want to see in these apps.

**Unger:** We'll put some information about where to locate that resource in the description of this particular episode, which I'm sure that is a very, very important resource. Laura, just in closing, what's your advice to physicians out there are contending with these kinds of questions. How do they advise their patients in regard to these kinds of privacy issues?
Hoffman: Definitely. To physicians, I would say research is showing that your patients are going to start coming to you with these questions about apps and what kind of apps are trustworthy and what can be used. We would encourage physicians to talk to their, again, administrators, their IT departments, maybe reach out even to your vendors, your HR vendors and try to get information from them about how they are exploring the privacy and security of the apps that they offer in that EHR ecosystem. I would say they should be prepared to explain to patients how the apps that a health system might offer do protect privacy.

Again, I think it's helpful to all come back to that this is about maintaining trust between the physician and patient as well. If a patient goes to a physician and tells them really trusted, potentially sensitive things, and then they hear about it from somewhere else because it got leaked out through these apps, the patient might think, "Well, why is the doctor sharing this information that I disclosed in confidence?" We want to make sure that physicians feel comfortable in responding to patients and reassuring them that that trusted relationship is there, even if they choose to start to use these apps.

Unger: Laura, thanks so much for joining us and marking this data privacy week with information about how physicians need to be thinking about this important topic. We'll be back soon with another segment for COVID-19 Update. In the meantime, for resources on COVID-19, visit ama-assn.org/COVID-19. Thanks for joining us. Please take care.

Disclaimer: The viewpoints expressed in this video are those of the participants and/or do not necessarily reflect the views and policies of the AMA.