Business Better (Season 4, Episode 7): Cyber Adviser – Your Data, My Headache: Consumer Health Data Laws

Speakers: Greg Szewczyk and Kelsey Fayer

Steve Burkhart:

Welcome to Business Better, a podcast designed to help businesses navigate the new normal. I'm your host, Steve Burkhart. After a long career at global consumer products company BIC, where I served as Vice President of Administration, General Counsel and Secretary, I'm now special counsel in the litigation department at Ballard Spahr, a law firm with clients across industries and throughout the country.

This episode is part of our Cyber Adviser series, where we discuss emerging issues in the world of privacy and data security. Today, our lawyers discuss new state consumer health data laws in Connecticut, Nevada, and Washington, highlighting the laws' scope, obligations for regulated entities, and enforcement mechanisms. Participating in this discussion are my Ballard Spahr colleagues Greg Szewczyk, Leader of the Privacy and Data Security Group, and Kelsey Fayer, an Associate in the Privacy and Data Security Group. So now let's turn the episode over to Greg.

Greg Szewczyk:

Hello and welcome to this month's installment of our webcast and podcast series focused on trending issues in privacy and data security. There's never a shortage of timely topics for this series, but this month we wanted to highlight a particularly relevant issue, the new set of state health data laws, two of which go into effect at the end of this month.

And as a reminder, these presentations are not meant to be a full-out deep dive webinar because we don't always have an hour to hear about each development. Instead, these are meant to give a higher-level overview of important laws or developments, so listeners and viewers can assess whether they may need to do that deeper dive.

Before we start, let me tell you who's talking at you. My name's Greg Szewczyk, and I'm the head of Ballard's Spahr's Privacy and Data Security Group. Joining me is Kelsey Fayer, one of the lead associates in our group, who also sits out here with me in Colorado.

To set the stage, it helps to think about where we are in the current state of privacy. If you're watching the webcast, you'll see that on the screen, we have a color-coded map showing a few different types of state laws.

In green, we have states with a comprehensive privacy law that's already in effect. In blue states with a comprehensive privacy law that's passed, but is not yet in effect. In yellow, states with biometric identifier laws. And in red, states with dedicated health data laws that we're going to talk about more today. And for states that have more than one of these laws, it's striped with both colors.

So I think we can go ahead and check the privacy bingo word of patchwork off the list because when you look at it is really a patchwork of laws up here. But I think it's important, even though that's kind of a cliché, to put these new laws into that context because it matters how they're rolled out, enforced, and interpreted.

Health data laws are a good example of that. We have three states that have passed dedicated health data laws or provisions, and that's Connecticut, Nevada, and Washington. And for Connecticut, the expanded health data provisions were actually introduced last year as an amendment to its already passed comprehensive privacy law, but it was amended before it even went into effect.

So that really changes how things are both broadcast from a media standpoint, how they're enforced, and the models that they follow. We're largely going to focus on the Nevada and Washington laws because those are the laws that go into effect at the end of this year, and they're also the laws that follow this new model.

But the Connecticut law also goes to show that we need to stay on top of amendments to existing laws because those don't always get quite as much press and coverage, but they can be equally important to a compliance regime.

So with that, I'll turn it over to Kelsey to start giving an overview of the scope of these laws.

Kelsey Fayer:

Thanks, Greg. These laws apply to what is called regulated entities, which are essentially controllers of consumer health data, which we'll get to in a second, but basically, the organization determining the purposes and means of collection and processing like we've seen in the comprehensive laws, and second, the regulated entities conduct business in Washington Connecticut, Nevada, or provides goods or services targeted to consumers in those states.

So we've understood the second prong to be more broad than it might appear at first glance, especially where a company conducts business online. And with the broad consumer health data definition, which I'll discuss next, companies might not consider themselves healthcare companies, but they could easily fall into the scope of these laws.

So what is consumer health data? These laws cover consumer health data, which definition is broad, as I've already hinted at a couple times. I won't make you wait anymore. It means personally identifiable information linked to a consumer relating to any mental or physical health condition or status, disease or diagnosis, interventions or procedures, reproductive or sexual healthcare, gender affirming care, use or acquisition of medication. And also includes biometric data and precise geolocation information related to a consumer receiving healthcare services or products.

Consumer health data also includes a catchall to include any information that a business processes to associate or identify a consumer with health data that is derived or extrapolated from non-health information. So companies looking to get creative, they've already thought ahead of that.

Finally, and unlike the comprehensive state laws Greg discussed, Washington and Nevada do not have revenue or volume of processing thresholds. This means that any company processing consumer health data in these states is subject to these laws with very limited exceptions. So if your business is not subject to the other comprehensive privacy state laws, don't rule yourselves out of these yet. They have a much broader net.

And now, Greg will discuss the obligations for those companies within the scope of these laws.

Greg Szewczyk:

Thanks, Kelsey. Moving into the obligations, the first one we're going to discuss is requirements for the privacy policy. But before we do, I want to note that under the Washington law, there are different obligations for full regulated entities and small businesses in some instances and also different compliance deadlines. So it's important to assess where your business may fall, for the Washington law, within that scope of a fully regulated entity or a small business.

But moving on to the privacy policy, one of the key most important things to mention is that, at least for the Washington law, there needs to be a standalone privacy policy for health data. So it'll be incredibly easy to immediately tell if a company's compliant.

And we know that both plaintiff's attorneys and regulators monitor website privacy policies to assess compliance on a threshold basis on a regular basis. So making sure that you have that facial compliance is really important to keep you out of the crosshairs of either of those.

With respect to the substance, there's specific requirements about what needs to be identified, like the categories of health data collected, the sources, and the categories of third parties of whom it was shared with.

And those are largely similar between Nevada and Washington, but there are important differences. For example, Nevada law specifically requires that the privacy policy disclose whether any third parties collect health data across internet sites or online services. So some types of ad tech may need to be detailed more than they are in most privacy policies.

And you also need to disclose how you'll notify users of material changes to the policy, which is very topical in light of some of the recent FTC announcements and the Colorado Privacy Act rules, which are changing how companies have traditionally notified users of their privacy policy changes.

If you want to see more on that in the non-health care context or non-health data context, you can go look at the Cyber Advisor blog where we've done some recent blog posts on that.

But the important thing to take away from this is that the separate and distinct privacy policy is going to be new, and it's going to have specific requirements in it, and it's going to be a very low-hanging fruit to judge compliance, so it's something that companies need to be very cognizant of and make sure that they're complying with, including before that March 31st deadline.

Another obligation of regulated entities is the need to obtain consent to collect and share consumer health data. And this consent needs to be specific, meaning it can't simply be part of the general terms of the privacy policy to which the users agree.

Now, there may be instances where the nature of the service or product classifies for an exception to this express consent, but it's an issue that needs to be seriously considered. Because, as we've seen from regulator enforcement sweeps across the various different states, they're looking at these specific consents when it comes to sensitive data already, and we have no reason to believe that that's going to be different when it comes to the regulators who will be assessing the health data logs.

Because, like privacy policies, it's something that is easy to assess. It's something that you can go onto a website, and at most, start to sign up for a product to see if the consent is actually there and if it's in the form that it needs.

To sell consumer health data, there needs to be a specific authorization which goes beyond the specific consent. And when you look at the statutes when it comes to the authorization, there are specific components to what needs to be in that authorization. There's also record retention obligations and the need to provide a signed copy of the authorization to the user. So there are a lot of technical requirements that differ from current standard practices.

And another thing to mention is that this is another area where we expect to see a lot of focus of not just the regulators, but also the plaintiff's bar because we'll talk a little bit later, the Washington law has a private right of action. And, again, these are low hanging fruit issues that will be very easy to tell about compliance.

It's also something that can tie in in ways with various different types of ad tech that are pretty common that companies may not think really fall into some of these categories. But there needs to be a very serious audit of what types of cookies, pixels, and other ad tech's being used to assess whether or not that might trigger the need to obtain this type of consent that wouldn't already be provided on the current interface.

And, with that, I'll turn it over to Kelsey to talk about the obligations related to geofencing.

Kelsey Fayer:

Thanks, Greg. So as Greg just mentioned, the next obligation that companies will have under these laws is around geofencing. And even where a company has obtained consent in the way that Greg just discussed, the laws still prohibit companies from geofencing within 1,750 feet of any person or entity that provides in-person healthcare services for certain purposes.

So these facilities would include physical healthcare centers, reproductive healthcare, mental healthcare facilities. And if a company is seeking to geofence around those areas within that range, they can't do so for the purposes of identifying or tracking consumers seeking in-person healthcare services or products, collecting consumer health data, and sending notifications, messages, or advertisements to consumers related to their consumer health or healthcare services or products.

And if we think about how broadly consumer health data is defined, this is another thing to keep in mind with how broadly this could be interpreted in terms of what's prohibited.

Next, we have contracts. So processors can only process consumer health data pursuant to a written contract between the processor and the controller, what these laws call the regulated entity processors, can only process that data if it falls within those limited instructions set out by the controller in the contract. We expect this will be more narrow than the interpretations of processing instructions under the comprehensive privacy laws.

The processors are also required to assist controllers with their obligations under the health laws, which includes assistance with regards to processing consumer rights requests. For example, if a consumer exercises a delete request, then the processor must also honor that. So companies that aren't controllers under these laws still need to be paying attention to what they need to do as processors.

Next, we have employees who are operating under contractual confidentiality obligations. They're limited only to access consumer health data where it is reasonably necessary. Controllers can only authorize access to employees where the consumer health data is necessary to further the purposes for which the consumer provided that consent that Greg talked about for those limited specific purposes. And the other time where employees can access it is only going to be where it's necessary to provide a product or service that the consumer has specifically requested from the controller.

So not a lot of wiggle room in getting creative there with purposes and access from the employees they're trying to... These laws are written in a way that limits what employees at these companies can access consumer health data, and that needs to be tied to the purposes driven by the consumer's consent.

And for the final obligation, we have security measures that the regulated entities and the processors will need to implement. So they're required to establish, implement, and maintain policies and practices for the technical, administrative, and physical security of consumer health data.

As a best practice, companies should already have these, but this is a good time, good opportunity to update those and ensure that it also includes the sensitivity of consumer health data in its risk analysis.

And then, finally, I'll turn to Greg for enforcement.

Greg Szewczyk:

Thanks, Kelsey. The last topic, enforcement. And as you can see if you're watching the webcast, the Connecticut and Nevada laws follow the pretty established practice that we've seen under privacy laws of having the attorneys general enforce under existing UDAP laws.

And those come with teeth as the violations can add up quickly in the context of a website say that is violating these laws. I mean, at 5,000 per violation, at 10,000 per violation, those numbers can really escalate in a hurry.

But the big game changer here is the Washington law, which also has a private right of action. Now, there needs to be actual damages, but those damages can be trebled up to 25,000 per violation. I mean, you think about that in the context of class action and the numbers get big very quickly. And with the attorney's fees baked in as a right, you can be sure that plaintiff's firms are going to be testing every theory you can imagine on actual damages.

And you think back to the early days of data breach litigation, and we saw some very creative and interesting theories as to how you suffer the actual damage and where that goes. And we kind of expect to see a lot of that come up in the following years.

But, in any event, it's going to take years for that litigation to settle on what will or will not constitute actual damage. So there's a big risk in the interim. It just takes that amount of time for the various theories to get tested at the district court level, then get up and down through the appeals levels.

So all of this is to say, take these lawsuits, this law seriously. If there's room for interpretation as to whether or not a collection constitutes a collection of covered health data, it may make sense to err on the side of caution for now, especially as we may see the flood of lawsuits in an effort to try to test new theories.

And that means there's going to need to be changes to existing practices. As Kelsey talked about, there are different contractual requirements than what is typically in contracts with employees, with processors. It might require new documentation or updating the documentation of security practices. And it's necessarily going to require updating policies.

And these are all relatively simple steps that companies that will already be generally complying with the core principles behind the law of not sharing consumer health data may be doing, but they won't have that documentation built in to try to defend against potential litigation.

So taking those steps now might put you in a better position to more efficiently and successfully combat that type of private right of action and potential regulatory enforcement once these laws go into effect at the end of the year.

Thanks everybody for joining us. For those of you on the webcast, we have our contact information up. We also have the link to Cyber Advisor. We will be posting that. If you are listening to the podcast, you can go to www.cyberadvisorblog.com, and you can get some more information. And we look forward to talking to you next month.

Steve Burkhart:

Thanks again to Greg Szewczyk and Kelsey Fayer. Make sure to visit our website, www.ballardspahr.com, where you can find the latest news and guidance from our attorneys. Subscribe to the show in Apple Podcasts, Google Play, Spotify, or your favorite podcast platform. If you have any questions or suggestions for the show, please email podcast@ballardspahr.com. Stay tuned for a new episode coming soon. Thank you for listening.