Podcast Transcript

Dobbs on Demand: Healthcare Privacy on the Line in a New Legal Setting

Date: August 4, 2022

Guest: Kimberly Gordy; Aleksandra Vold, **Host:** Amy Kattman

Run Time: 21:42

For questions and comments contact:

Kimberly Gordy

Partner
Houston
T: 1.713.646.1360 | kgordy@bakerlaw.com

Aleksandra Vold

Partner
Houston
T: 1.312.416.6249 | avold@bakerlaw.com

Kattman: Since the recent *Dobbs* decision which overturned *Roe v. Wade*, companies have been impacted nationwide and have several new legal angles to consider as it relates to their employees and their businesses. With that in mind, we've created a new podcast series, *Dobbs* on Demand, designed to help you navigate this new and evolving landscape. We'll feature partners from our Labor and Employment, Employee Benefits, White Collar, Digital Assets and Data Management, and Healthcare practices as we break down the top issues and changes in law. I'm Amy Kattman, and you're listening to BakerHosts.

On this episode of *Dobbs* on Demand, we will discuss several legal perspectives that employers should consider in light of the *Dobbs* decision. Our guests today

are Kimmy Gordy and Alex Vold, partners in our Digital Assets and Data Management practice and members of our *Dobbs* Decision Task Force. Welcome to the show, Kimmy and Alex.

Gordy: Hi. Thanks so much for having us.

Vold: So happy to be here to talk about this subject.

Kattman: I understand that in the last several weeks, the U.S. Department of Health and Human Services Office for Civil Rights, or OCR, and the Federal Trade Commission, FTC, have both come out with guidance on reproductive health privacy. Kimmy, I'd like to start by asking a foundational question. Are all businesses subject to the guidance, or does the guidance only cover some of the entities?

Gordy: That is a great question, and it is a source of confusion for a lot of people. Who does HIPAA actually apply to? So, the OCR's jurisdiction is limited to HIPAA covered entities and their business associates, and a covered entity means a healthcare provider, a health insurer, or a health insurance clearinghouse that conducts what is called a covered transaction. And we normally think that this is electronically processing insurance claims or Medicare claims. So, a cash-only provider is not going to be subject to HIPAA, example would be a psychologist that only has her patients pay via Venmo or cash.

A business associate is a company that performs some operational function that involves accessing or processing or viewing protected health information, commonly known as PHI, to a covered entity. So, somebody that you hire to paint the outside of a hospital building or remove shredded garbage would not necessarily be a business associate because they're not accessing and viewing health information. But a food service vendor that comes in and delivers trays to hospital rooms and sees the dietary restrictions could be a business associate, just the way a law firm who may see patient information as a result of helping advise clients on legal responsibilities would be a business associate.

Vold: And so, for the FTC, it has cast a little bit wider of a net with respect to who is subject to their guidance. The FTC is in charge of investigating and prosecuting unfair or fraudulent business practices, among some other things. The FTC though can target really any person or entity that offers goods or services in interstate commerce. So, examples of FTC cases in recent history include an action against a grill maker for allegedly restricting consumers' ability to repair the products that they have purchased. Or an action against a consumer tax preparation service for allegedly misleading consumers that the service was quote, free. So, it is a wider net than OCR's jurisdiction and there can be some overlap particularly with respect to the business associates that Kimmy referenced because they often provide services outside of the hospital setting as well.

Kattman: Let's talk about OCR's guidance first. Alex, what have we heard from OCR regarding patient privacy post *Dobbs*?

Vold: So, we've gotten two privacy-related guidance documents from OCR recently after the *Dobbs* decision. I'll cover the first one, and I'll have Kimmy chime in on the second. So, the first thing we heard from OCR was guidance that, although HIPAA permits the disclosure of PHI to law enforcement and in response to court orders without a patient's consent, that disclosure is not required by HIPAA. Importantly, this is not a new rule. HIPAA has a number of standards that basically dictates when disclosure PHI can be done at all, and then if there can be a disclosure, what parameters exist around those disclosures. Sometimes it requires patient consent, sometimes it requires some power of attorney, and sometimes it requires no consent at all for limited circumstances. And so, some of those limited circumstances have always been those situations where a provider or other covered entity is presented, like I said, with a court order or there is a request from law enforcement.

So, what this guidance essentially did was it just reiterated that no one should read that permissible disclosure without authorization as a required disclosure. So the impact is, as a result, kind of limited to the extent that a covered entity or business associate fights a request from law enforcement or through a court order. The guidance is, I guess, an easy rebuttal to an uneducated litigant who says hey, HIPAA requires this disclosure because it is in response to a court order or in response to a law enforcement request. So the provider, the covered entity or the business associate can say no, look, here is this guidance from OCR. It specifically says it is not required.

Again, that was never the language anyway. But importantly the guidance does not create grounds for circumventing these types of requests, which we got a lot of questions about from our covered entity and business associate clients. There was a callout by OCR saying that you don't have to, you're not required to respond. And they said, okay great, how? How do we fight with it, these requests, or how do we come challenge them? That is not something OCR provided in this document. There are, based on the state that an entity is in, there are procedural legal grounds to avoid responding or try to quash these types of requests. But that, those avenues have not changed based on OCR's guidance.

Gordy: The other piece of guidance that came down was directed specifically at the nation's 60,000 retail pharmacies, which is really the hub of where most Americans get their prescription medications. So that is your Walgreens, your CVS, your pharmacies inside the Target. The OCR made clear that a pharmacy's refusal to dispense a correctly prescribed medication, because that medication could also be used for abortion-related care or is being used for abortion-related care, will be considered a discriminatory act. And so why does this apply to your average grocery store pharmacy?

Well as a recipient of federal funding, primarily Medicare, retail pharmacies are prohibited from discriminatory practices, and that includes discrimination on the basis of gender, sex, race, all your typical protected classes. That also includes discrimination on the basis of pregnancy or a pregnancy-related condition. And a pregnancy-related condition is one that is early pregnancy, caring for someone after a pregnancy, caring for someone intending to be pregnant. The guidance

carved out several scenarios in which conduct by a pharmacy or behavior of a pharmacist, which then gets transferred to the pharmacy from a liability perspective, would be considered discrimination.

So the first example is if a pharmacy refuses to fill a prescription or a medication needed to manage a pregnancy loss, whether unintended like a miscarriage or intended like an abortion procedure, including something like antibiotics because it could also be used to terminate a pregnancy, OCR is going to treat that as discriminatory conduct on the basis of sex. Similarly, if a pharmacy refuses to dispense a medication, the popular example right now is methotrexate because that is a drug used to treat a lot of autoimmune conditions, one primarily being rheumatoid arthritis but it also is used for lupus, a variety of other things. But it can also be used for pregnancy termination purposes. That will also be considered discriminatory conduct but on the basis of disability because that medication was prescribed and needed to treat a condition that is a recognized disability. It meets the definition of a disability under federal civil rights law.

So, what this guidance is really saying, it is not earthshattering. It is not creating any new rules. But it is telling pharmacies, it is putting them on notice that if your pharmacist or a pharmacy tech says, we're not going to stock medications that could be used for abortion. Or we're going to question a patient and then not dispense a prescription because it had something to do with abortion, that could definitely be considered discrimination.

Kattman: The guidance from the OCR doesn't create any new right of privacy or administrative penalties that weren't there before. Do we expect that to come, Kimmy?

Gordy: Well, you're correct. The guidance does not create new penalties or rights. It simply sets out their intent to enforce these rights using the tools OCR already had at its disposal. But it is worth noting that there are some calls from pro-choice lawmakers to amend HIPAA to further restrict when PHI can be disclosed without patient consent. And this could look like, it could come a couple ways. It could look like a blanket prohibition on the disclosure of sensitive data without patient consent. And sensitive data is something, of course, that is open to interpretation. Or it could be a prohibition on disclosing data related to reproductive care without patient consent, which would be more narrow, more easily defined and understood. And I think given the right climate, I think a narrow amendment to address these issues is certainly possible.

In January of 2020, the prior administration amended HITECH, which is HIPAA's sister statute, to include consideration of recognized security practices as a mitigating factor when determining fines and other penalties for violation of HIPAA's breach notification rule. And this tells us that a discreet amendment is not beyond the realm of possibility here, but it definitely would probably take a little bit of political jockeying to get something through. So, I don't know when we would expect that but it is certainly not off the table.

Kattman: For non-HIPAA covered entities, what has the FTC said about privacy issues post *Dobbs*, Alex?

Vold: The FTC recently came out with a public letter that, really for the first time, addressed false claims about data deidentification or data aggregation practices by website operators or app companies. Just a quick side note, HIPAA, as we've been talking about, which covers only a small slice of this population of businesses, provides very specific rules about what constitutes deidentified data. Either the removal of 18 specific data elements, all 18, or getting an expert opinion that for a particular data set that has been cleaned of some but maybe not all of the 18 identifiers, that the risk is, and I'm quoting here, very small, that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify an individual who is a subject of the information. Essentially, it is unlikely, quite unlikely, that given how much data has been removed from a data set that anyone could say oh, this must be Alex Vold.

So, the FTC however, has not ever promulgated similarly strict rules or guidance. The last time the FTC actually discussed deidentification was in 2012, when in its privacy report it said that companies have to quote, achieve a reasonable level of justified competence that data cannot reasonably be used to infer information about or otherwise be linked to a particular consumer. So, no expert opinion, no specifics about what identifiers must be removed. So, all that the FTC said with that is that the companies have to take reasonable steps to ensure deidentification. Deidentification is in the eye of the beholder, I guess at that point. Folks that have not kind of been presented with a HIPAA-esque rule set might think that name alone, if I take that out might be sufficient to deidentify data. When really, if you're the only 36-year-old in a rural Wisconsin town making over $300,000 a year and are female, they may be able to figure that out. Individuals may be able to correlate all of that nonspecific name information to a particular person.

So, against that backdrop, the FTC said on July 11 that companies that state in their privacy policy or their terms of use policies, that they will not use non-deidentified data. Or in other words they will only reuse deidentified data or some similar claim. They better be sure that that is true, or FTC will come after those companies. They said, you will be hearing from the FTC. So, the FTC in this letter didn't ever say *Dobbs* or abortion, although they did highlight reproductive health information as being particularly sensitive. And so, between the timing of the letter and that reference, I think we can logically understand that it naturally flows from *Dobbs* and where we are now in the post-*Dobbs* digital economy. So, companies that collect data, particularly health-related data, need to take a very close look at their privacy policies and terms of use to see what they're saying to their consumers and users about data deidentification or data reuse or data aggregation, and then make sure that they can back up those statements with their data practices, with their deidentification practices.

And again, it is tough because we don't have a particular set of rules like we do in HIPAA to say this will be sufficient in the FTC's eyes if we were challenged on

our deidentification. There are many companies out there that assist with deidentification, and particularly apps in that health space that collect fertility data and any kind of reproductive health information really need to be careful. Because I think this is going to be a new avenue of enforcement for the FTC in the coming years, and it is not outside of what they've done previously. They had a settlement with a period tracking app about their sale of data when they said they were not selling data. So, it is not, it is really not jumping into completely new territory for them. This is a continuation and a good reminder to companies that the way they represent their use of data really needs to jive with consumers' expectations in what they are doing internally.

Kattman: Alex, do you have any final thoughts on health information privacy for covered entities and their business associates for our listeners today?

Vold: Yeah. You know, we are getting a lot of questions that struggle with the hypothetical situations and how a business covered entity, business associate will respond or what liability might be incurred as a result of this future hypothetical situations. Those are obviously entity-specific questions and strategy specific to each individual entity. But one of the most consistent themes in our advice is to have discussions with business partners around central issues related to the treatment of or request for reproductive health information before the day those hypothetical questions come into reality. So, in other words, a covered entity may be finalizing its own stance on how it will deal with a governmental request, for instance. That includes patient records that have in them abortion-related services.

But if they share patient information, patient records with business associates, which many do lawfully for a number of very legitimate reasons, and if they don't convey that stance to a business associate who might also be or maybe solely be subject to that same request, that business associate may not act in a way that is aligned with the covered entities' newly created stance on these types of issues. A lot of, I shouldn't say a lot, sometimes there is specific language in business associate agreements or contracts that discuss responses to subpoenas, et cetera. But they're generally not incredibly robust and certainly were not contemplating this type of issue at the time they were written, at least to the extent they were written before *Dobbs* came out.

So just making sure both for covered entities and business associates, they should really work together to assess and understand and align. And really the business associate is only permitted to use PHI in a way that their contract with a covered entity dictates. And so the covered entity really does get to call the shots in these situations. But also, with respect to instances where covered entities are transferring patient information to a business associate, they should work together to assess whether they want all of the information that they previously were sending to a business associate to go over to that business associate any more. And generally providers and other covered entities are very good at assessing what is the minimum necessary amount of information that needs to go to a vendor in order to have that vendor provide the services. But they may just reassess what matters to them for those services, and they may not want to

provide reproductive health information to a vendor in order to circle the wagons around reproductive health privacy and be able to control the flow of that information to a third party should a request come.

Those questions and the processes around maybe filtering data or blinding data or removing data is again, super situation specific. There are some limitations, technical and legal, that may prevent full removal or full blinding, but if it is important to either entity having those conversations, being open to others' viewpoints and really understanding how you can walk together and continue to be on the same page is so important especially where we really do not have a patchwork of ideologies around this from governments from state to state.

Kattman: Thank you so much for joining us today, Alex and Kimmy.

Vold: It has been our pleasure.

Gordy: Thanks so much for having us.

Kattman: If you have any questions for Kimmy and Alex, their contact information is in the show notes. For more information on the impact of the *Dobbs* decision, visit the Post-*Roe* Resource Center on bakerlaw.com and check out all *Dobbs* on Demand episodes by subscribing to BakerHosts wherever you get your podcasts. Tune in to our next episode where attorneys from our Healthcare practice will discuss the regulatory implications to be aware of since the *Dobbs* decision.

As always, thanks for listening to BakerHosts. Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of the participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.