Music Intro

Welcome to *A Hard Look*, the Administrative Law Review podcast from the Washington College of Law. We'll discuss how administrative law impacts your daily life—from regulatory actions by agencies, and the litigation over them, to the balance of power over the branches of government. This is *A Hard Look*.

Steven: Welcome to Administrative Law Review's *A Hard Look*. My name is Steven Valentino, your host for Season 3 of *A Hard Look*. Before I dive into our agenda for today, I would like to foremost thank both Sarah Knarzer and Shabbir Hamid for their excellent work in developing this podcast as well as contributing to the many important conversations happening in the world of administrative law. Most of all, I want to thank them for their mentorship and assistance in transitioning into this role. I wish them nothing but the best moving forward in their legal careers.

I am not alone in this endeavor. I will be working closely with Kübra Babaturk, the Technology Editor for Administrative Law Review. We look forward to discussing important topics in administrative law as we curate this next season.

Today, I am joined by Professor Kirk Nahra, Partner at WilmerHale and the Co-Chair of both their Big Data Practice and Cybersecurity and Privacy Practice. In addition to his career as a legal practitioner, Professor Nahra also serves as an adjunct professor at American University's Washington College of Law and Case Western Reserve University. Professor Nahra has been recognized as a leading data privacy professional, with awards from many organizations, including the Vanguard Award from the International Association of Privacy Professionals.

As a disclaimer to our viewers, any views expressed by our guest are that of his own and are not a reflection of that of his firm, organizations, clients, or other parties in which his opinions could be imputed.

On this episode of *A Hard Look*, we will be discussing the Health Insurance Portability and Accountability Act of 1996—or more commonly known as HIPAA. Today, with the help of our guest, we will discuss the law's inception, evolution, and potential for the future.

Professor Nahra, welcome to *A Hard Look*.

Prof. Nahra: Thank you very much for having me. I appreciate the opportunity.

Steven: Well thank you for coming! So, in 1996, Congress decides to pass HIPAA and confer new responsibilities to HHS. What purposes was this law trying to serve?

Prof. Nahra: Sure. So you read the name and its important to focus on the name. It's "Health Insurance Portability and Accountability Act." Portability was the focus of the law. Portability meant, essentially, taking your health insurance with you when you switched jobs. There was a concern at the time—again this is a long time ago in our health system—there was a concern that if people had any kind of pre-existing conditions they would not be able to get health insurance if they went to a new employer. So, the law was intended to address that issue. It has nothing to do with privacy at that point, it has nothing to do with security. And so that's how we start down

this crazy path that ends up today where when people say HIPAA as you say "commonly known as HIPAA," nobody means "portability" they tend to mean privacy. They also tend to often be wrong about what HIPAA in fact stands for on privacy and security, but we can get to that over the course of our discussion today.

Steven: When this law was finally passed, what challenges did HHS face as a governmental organization in trying to implement this legislation?

Prof. Nahra: Sure, so let's talk about this. I know this is an administrative law related podcast, so lets talk about what I think are the key administrative law issues. Going back to the idea of portability. So, the focus of the law was on portability. Everybody in Congress—hard to imagine today—but everybody in Congress essentially agreed that that was a problem that needed to be fixed. So one of the things that Congress often does is they start adding other stuff into bills where there is a key provision everyone agrees on, they start adding other stuff. So, lots of people in the health care industry, and otherwise, originally new HIPAA because of the fraud provisions, the anti-fraud provisions that were in the law. I spent a lot of my early career—you know HIPAA to me meant dealing with anti-fraud issues. Over time it has meant privacy and security. Privacy and security very much comes through the back door. It was a part of something called "administrative simplification." That was the idea—and again, 1996, very beginning of the internet era and the idea that more and more of the health care industry was moving to computers and online. Congress didn't really know what that meant. They thought that if the health care system could standardize certain activity, think a doctor sending in claim to an insurance company and an insurance company paying the claim. If you could standardize those electronic transactions you could make things a lot more efficient, save money, and be more accurate. Great idea, you know, we can debate whether it worked, but great idea. But what then happens from an administrative law perspective is Congress basically said, "if we are going to push all this stuff electronic, shouldn't we think about privacy and security of that data" and at the same time Congress said we don't know what to do about privacy and security of that data. So Congress as a legislative matter basically—in that 1996 law—gave itself three years to pass privacy and security rules. Those of our listeners who are Congressional scholars can probably guess what happened at the end of those three years was nothing at all. And so what happened then was Congress wrote into the law the responsibility on HHS to write privacy and security rules. But the interesting administrative law challenge is that they gave them no instructions of any kind on what those privacy and security provisions would be, other than who could be covered by those rules. And the who could be covered by those rules was dictated by what entities were involved in portability and what entities were involved in submitting standard electronic transactions. So, we end up with a set of privacy rules that is very, it's not narrow, but it doesn't cover all of the health care industry and all of your health data, because there is lots of stuff that wasn't subject to companies and entities that did portability or standard transactions. So, HHS was stuck with basically regulating hospitals, doctors, pharmacies, and health insurers. And they were given no substantive guidance on what to say about those entities and what they could do and how they could protect the data. So, that was the challenge. Originally it was we have an obligation as HHS to write regulations. We have a blank piece of paper where other than

at the top who it says the rules apply to. That was it. That's all they had. They had to basically invent a privacy and security system from there.

Steven: So taking that sort of open mandate, given by Congress, and given really only the script of who it actually applies to, what did HHS ultimately write? What sorts of obligations were these entities supposed to, to adhere to?

Prof. Nahra: Yeah—and again, this became a really interesting issue—and I'm now. The first draft of those rules came out I think in 1999 and I've been working with these rules since 1999. And so now, we are dealing with a very different system today. You know, all kinds of things are different from 1999. It's often interesting to me how good a job they did, right? You know, making this up as they went along. But there are a couple of really core ideas that I think really are sort of the dominant elements of what HIPAA was. The HIPAA Privacy Rule in particular. So the first point they came up with—let me back up one step—one of the first things that was really important in thinking about these rules was that HHS went into the drafting thinking about two, perhaps, competing goals. One was protecting the privacy of patient information. The second was making sure that the healthcare system still worked well. Those rules could be intentioned, they didn't have to be intentioned, but they wanted to be careful, they wanted to do the best they could to accommodate both of those goals. And so, for example, one of the key principles of the HIPAA Privacy Rule—probably in my mind the most important principal and one that was really sort of groundbreaking in broader privacy law was to say, alright, how we are going to define what you are going to do with what you can do with data is to basically say lets define in the rules what is "normal" in the healthcare system and we are going to make use and disclosure of that information for those normal purposes, we are going to make that automatic. Patient consent really isn't needed for that, consent is essentially going to become automatic. If a hospital or a doctor or a health insurer wants to do something that isn't normal, they have to get the patient's permission. But otherwise, we are going to define what's normal and they did a pretty good job on that, we can debate around the edges, but all that normal stuff happens automatically. That makes the system work much better, much more efficiently, and lots of the goals of the healthcare system are able to be accomplished because they are able to use information for things like quality control and improving how you conduct health care and making sure there is appropriate oversight and things like that. So, that use and disclosure principle is really important. They also made up some other stuff that was really important. For example, they recognized very quickly, in writing these rules, that hospitals and doctors and health insurers used vendors. Everybody has vendors. And HHS is looking at that and saying we do not have any authority over those vendors. We are not allowed to regulate them, they are not defined in the law to be somebody we can regulate. So, they made up this idea of what is called a "business associate"—that's a vendor to a healthcare company—and they made up a way to protect peoples' privacy when data went from the hospital to the vendor. And so they basically imposed on the hospital—who they could regulate—the obligation to have a contract with the vendor—the business associate—that passed through by contract certain privacy and security obligations. So in that sense they were able to allow hospitals and doctors to still use vendors—I mean, they could have prohibited vendors, but that would have been a bigger problem—they let them continue to use vendors, but at the same time they found a way, very creatively, to protect

data reasonably well even though Congress didn't give them any authority to do that. So that's, you know, those were I think the two biggest. They came up with various individual rights, they came up with the idea of privacy notices consumers get, patients get when they go to the hospital. Lots of other key pieces, but again, the sort of governing principle was lets protect privacy pretty well, but lets make sure that we don't do that in a way that makes it hard to operate the healthcare system because it's in the interest of patients to have a well-operating healthcare system. Privacy isn't the only absolute goal, we want to make sure the healthcare system is working well at the same time.

Steven: And you mention that individuals have a piece in this to some extent. What sorts of rights or privileges are within HIPAA at this point in time to regular citizens?

Prof. Nahra: Regular citizens, sure, the average patient. So, I mean a couple of things. One, your information is protected according to these rules and you don't really have to do anything about it. So, when you go to the doctor, there are certain things the doctor is able to do with your information, but they are generally things that you would expect the doctor to be able to do. I mean, if I gave you a list and I said "here is the fifteen things the doctor is able to do, do you think that all fifteen of those are normal?" You might not agree in any random sense, but you know that the doctor is going to use your data to treat you. You know that the doctor is going to get paid and has to submit a claim to the insurance company. You know that the doctor more accurately, you know, more appropriately the hospital has an accounting department, they have a quality department, they have to hire new doctors, they have to defend litigation. They have to do stuff to run a business as well. So, you know as a patient if you pay attention to the notice that's handed to you, you know sort of what the doctors and hospitals can do and its generally normal stuff. That's a kind of right, its again just sort of automatic. You have a right to get a notice, everybody gets a notice, hardly anybody ever reads the notice, you don't have to read the notice, because the rules are automatic. You have a right to what is called access of your information. You get a copy of your information if you want it. You don't have to ask for it, you aren't required to get it, but that's become an increasingly important right over time, particularly as records become more electronic. People have lots of different healthcare providers and they are able to now—it doesn't always work perfectly—but in general, you have the right to make sure that your data if you switch doctors or you need or go to a specialist or you've moved locations or whatever, you can move your data from one doctor to another. That's a really important right and something that is in the news today because HHS is really trying to make sure that is working well. You have a right to correct records, it's called "amend records." You don't get to say "oh, please delete the fact I had that condition or whatever" but if it really wasn't you, you get to amend it. There are some others, some complicated rights in particular situations. If you are in a domestic abuse situation there are certain rights that you have to make sure your information is held in particularly careful ways. It's a generally pretty good system that lets people, I think gives them rights in situations where they want to exercise it. Now again, that puts a burden on the individual to know that they have the right and then choose to exercise it. The domestic abuse is a good example. There is a very particular process, the average person doesn't know that process exists. That presumably means the average victim of domestic abuse doesn't know that that exists. That's a bit of a problem. I'm not sure HHS can necessarily solve

that, but again, they've done a good thoughtful job. Keeping in mind, blank piece of paper, Congress said nothing whatsoever about individual rights and HHS has done a pretty good job on that.

Steven: Now that we've evaluated HIPAA in its original conception and its subsequently promulgated regulations, lets transition to 2009. In 2009, Congress passed the Health Information Technology Act—or HITECH as its often colloquially referred to. What substantive changes manifested as a result of this legislation?

Prof. Nahra: Sure, so, so Congress is great at the acronyms.

Steven: Laughter.

Prof. Nahra: That's probably their single best skill is coming up with good acronyms and the privacy field in particular has a lot of really good ones—the CAN-SPAM law for emails and stuff. HITECH was a part of a much bigger law. It was part of the overall economic stimulus act that came in at the beginning of the Obama Administration that included road building and stuff like that. And there was a piece that was tied to the healthcare industry. And the idea—the motivating factor—was to try and motivate doctors and hospitals to implement electronic medical records, with the idea, and again, the system would work better if we had these sort of electronic medical records that could be standardized, could be shared if needed, could be more accurate, etc. And they economic stimulus part was basically the government was going to pay doctors and hospitals to implement electronic health records. So, Congress is going to do that and at the same time they say well, lets see what we should do about the privacy and security rules because we are now going to encourage people to have more and more electronic records. You could debate whether it made sense to add obligations while you were at the same time trying to encourage them to implement these records, but that's a different issue. So, HHS had an opportunity, based on the legislation, to go in and write new rules to both implement the legislation, which is a more traditional administrative law function. They also had the chance to just rewrite the rules. What they ended up doing was pretty much just implementing the legislation. So, that meant the legislation said that these business associates—who I mentioned earlier, the vendors—now can be subject directly to the law because they changed the statute. HHS couldn't do that in the regulation but Congress made most of the HIPAA privacy and security rules applicable to these vendors. They also created security breach notification obligations. So if your medical records are subject to a security breach, you get notice. HHS looked at the rules more broadly. They didn't do much to the rest of the rules. I kind of wish they had done a little bit more active work on, they had a chance to revise the rules. And frankly, you said the law was passed in 2009, the rules didn't go into effect until about four years later, more than four years later. And so, I think it was a little disappointing that they didn't do more with the opportunity that was presented to them. Lessons learned from the HIPAA rules, etc. There wasn't all that much that happened as a result of that law. But again, that's all in effect now. It's all one set of HIPAA privacy and security rules, subject to the same entities generally, adding in the business associates, and now we are navigating a variety of other changes in the healthcare system that we are trying to figure out how to manage those across both HIPAA and a wide variety of other rules because one of the things that has become noticeable in the last few years is

how much health information exists in this country that isn't regulated by the HIPAA rules, and that's really generating a lot of the attention today.

Steven: So now that we sort have discussed this package that is HIPAA, both the privacy and security elements and who they pertain to, what does enforcement look like? How is HHS actually ensuring compliance with these obligations—to what extent are covered entities maybe liable to the government for breaches of data privacy?

Prof. Nahra: Sure, so enforcement is again sort of an interesting issue with HHS because as I said earlier when they were writing the rules, they wanted to make sure that privacy was protected, but that the healthcare system still worked well. When the rules first went into effect, the government was actually very concerned that if they were too aggressive in their enforcement that doctors and hospitals would stop sharing information and out of nervousness and precaution, that would actually be bad for both patients and the system. So, early on the government went out of its way to basically say look, we are not trying to hammer people, you know, we want to help, we want to guide, we want to educate, we want to fix, and that is going to be our enforcement approach. So for the first several years of HIPAA, there was no enforcement. Consciously, intentionally, there was no enforcement. And again, they wanted to make sure that the normal appropriate information flow still happened. So, then we get to a point in time where they start slowly, but surely, to start doing, to start doing enforcement. I made a joke when I first started doing some of this enforcement work where the, I said "the Obama Administration was going to be more active on enforcement than the Bush Administration had been" and a couple years into the Obama Administration I was totally right! The Bush people had done one case and the Obama people had done two.

Steven: Laughs.

Prof. Nahra: And that's more than one!

Steven: We're doubling!

Prof. Nahra: We're doubling! Yeah, it's a 100% increase. But, so I don't think HHS does anything to ensure compliance from all the covered entities. I don't know there is any rational, reasonable way for them to do that. At the same time, what they generally do now, I think they do reasonable and thoughtful enforcement. They have to know about something, they don't really have any way to just randomly show up and just start asking questions. They don't have resources for that and I'm not sure if that would be appropriate. They learn about situations from a variety of ways, one of the HITECH requirements we talked about a minute ago was the data breach notification. If a company has a data breach, a HIPAA regulated entity has a data breach involving more than 500 people, they have to tell HHS about that—and that means HHS investigates that matter. That's one source of reporting—they also see reports in the newspaper, they see media exposure, etc. So, they can do investigations and they do investigations regularly. I have lots and lots of clients who have been investigated under the HIPAA rules. At the same time, they recognize that most of these rules should not be held to perfectionist standards. Particularly the Security Rules. You cannot have perfect security, they know that. So, when they go in and do enforcement what they want to learn is what did the company do from the

beginning? Did they try reasonably hard to do the right thing? That's part of their analysis. Then, when the security breach happens, how did they handle it? Were they prepared? Did they handle it well? Did they do the notice right? Did they mitigate the harm? Did they do things to deal with the breach appropriately? And then they want to know did you learn lessons? And so one of the things I always tell my clients is "look, they are going to knock on your door, but its going to be three to six months after your breach happens." I want my clients to be in a better place three to six months later than they were when the breach happens. And that being in a better place is not a negative, that's the expectation. You should learn lessons, you should improve. And so HHS's enforcement, and again, you can criticize this, there are reasonable ways to criticize their enforcement, but they have focused their attention on, I don't know, I'll say sort of three categories. There are repeat situations, where a company has had the first, second, third, fourth, fifth problem and at some point they are going to get a penalty. It's not the first time, it might not be the second time, but after that, you know. Or repeated problems that weren't fixed. The same kind of problem that comes up more than one time and they didn't fix it. So those are the two categories that constitute most of the penalties. There are a handful of situations where they do things like send a message. I use an example, there was a case where a hospital filmed a reality TV show in the hospital, and you know, there were newspaper reports and basically an elderly woman was watching the show and sees her husband die on television. It's like his face was blanked out, but she knew, and you can't do that. And HHS went after that hospital, even though it was the first time they had a problem, sending a message saying "don't do this." Don't film these shows in your hospitals. There is now an aggressive action by HHS on patient access, which is people making requests for their records and hospitals or doctors not giving them. HHS is going after them even though they are small dollar cases because they want to send a message that this is really important. So, absolutely you could criticize saying there should be more enforcement. I'm not personally sure it's a fair criticism because in general I think they've done a really good job, they've done a thoughtful job, and as I said, they are not looking to nail people, they are looking to fix and educate and guide, and they want to do enforcement against people that really haven't tried and really haven't done a good job.

Steven: So we've been thinking about the administrative nexus and then we also have these private citizens, do they, are they afforded a private cause of action under HIPAA?

Prof. Nahra: No. Clearly no. There is no private right of action under HIPAA. There is a particular process for complaints with the entity, there is a process for complaints with the government, etc. So there is no private cause of action, that's a hot button issue in the national debate that is going on right now that's not unique to healthcare, but in a general national privacy whether there should be a private cause of action, but HIPAA did not create one. Most of the federal laws that have been passed on privacy do not create a private cause of action. So, a consumer can't sue under HIPAA, for violating HIPAA, but now, there are lots of creative theories that people have been trying to use to bring lawsuits based on essentially HIPAA violations. There has been some success, modest success, on trying to use HIPAA as essentially a tort standard of care. This is the, you know, standard of care that a hospital should engage in if they do something that didn't live up to the HIPAA standards, maybe I can sue them for some common law tort. That hasn't worked, I mean again, there has been some success there, but its

not a big deal situation and it doesn't tend to be, it doesn't tend to be a class-action situation. Those often work better in the individual situation where a particular person was harmed by a particular, you know, particular bad thing that a hospital or a doctor did.

Steven: Shifting gears a little bit and thinking about the broader present context of the world we live in now, COVID-19 has certainly challenged a lot of administrative thinking, among other things. How has it impacted HIPAA? Have we seen any shifts with HIPAA? Does it apply even?

Prof. Nahra: Yeah, so the short answer, I'll give you a little bit of a longer answer, but the short answer is that HIPAA is almost never relevant to virtually any COVID question you're going to ask. In particular, when an employer early on in COVID was trying to figure out what they could share about employees who tested positive with other coworkers and stuff, HIPAA was essentially never relevant to that. If your employer now says you need to represent that you haven't had COVID or you need to report your COVID status or you need to report your vaccine status there is no HIPAA issue with that anywhere, despite what you read on the internet, despite the fact there are people screaming "it's a HIPAA violation." If somebody asks at a press conference whether a quarterback for any football team is vaccinated and they say "no, I'm not going to tell you that because it's a HIPAA violation," that's just wrong. It's just not a HIPAA violation.

joint laughter

Prof. Nahra: It has nothing to do with HIPAA. So, one of the things COVID has done, which I think is really important, is that is has flagged a big gap in HIPAA. There is lots of health information because of COVID, but essentially none of it is regulated. Again, we can imagine some scenario where its right, but almost all of the things we have been focusing on, none of its regulated by HIPAA. And again, that's not inherently a good or bad thing, it's just a fact. It's not part of HIPAA, and so we have all this healthcare data that is in fact unregulated by at least the federal laws. And so, we have to figure out what to do about that, but it, again, it's not a HIPAA issue because of the limited scope of what HIPAA does.

Steven: So, additionally, we are also kind of living in a moment where HIPAA might change a little bit. We noticed during the Trump Administration that HHS issued a notice of proposed rulemaking proposing to amend how coordinated care and how other social services might be implemented for HIPAA disclosures of protected health information, and recently, under the Biden Administration we've seen an extension for comments, I believe through March. What is this proposal seeking to do? What's it seeking to change?

Prof. Nahra: Well, there are two major topics of the proposed rulemaking at this point. One has to do with the patient access right I was talking about earlier and making it better and cleaner and easier. I would say it's a series of small fixes to deal with a broader question, and I think there is lots of support for that generally, I don't think that's particularly a partisan issue. I expect a lot of that is going to go into effect eventually. The other stuff is more complicated. And again, it's raising some questions because of the limited scope of HIPAA. One of the things that the healthcare system has learned over the last twenty years, when you say it, it shouldn't be surprising, but we've learned that one of the reasons you might be sick is that you don't have

access to good food or you don't have access to good housing. Ok, again, that doesn't seem like, that doesn't seem that hard, but we haven't really thought about that in the healthcare system. So, one of the questions is with the social service agencies, how is a hospital allowed to share information, for example, with a food bank about a patient who doesn't have access to food? Again, it's a fair question, and its an appropriate question or the healthcare system. The proposal is basically to make it easier for the hospital to share information with somebody like a food bank. Again, I understand that approach, but at the same time when you think about how HIPAA works, the food bank isn't part of HIPAA. The food banks not a hospital, the food bank isn't a doctor, the food bank isn't a health insurer. And it's not a vendor working for them, and so, when you make it easier to share that information with the food bank, you're essentially saying that information is going from being regulated by HIPAA to not being regulated by HIPAA. And so it's not a privacy-neutral calculation. You may decide it's worth it, one alternative is ask the patient if its ok. You don't need a rule change to ask the patient if its ok. You could do that today. So, basically, that situation is arising in situations where you either don't want to ask the patient or the patient has said no. I'm not sure that's a privacy win. I think that is a complicated issue. How much more sharing do we want to have? The purpose of those proposed rules is to encourage more sharing of information with more people. If you're being treated by one doctor for, you know, you have a cholesterol issue, and you also go to a psychiatrist when you have depression, and it would help the first doctor to know that you were being treated for depression, do we want to put the burden on you, the patient, to tell your doctor? Or do we want to make it much easier and really encourage the psychiatrist to share that information with your doctor? Again, there are healthcare system reasons to encourage that sharing, but the easiest way to do that that doesn't impose on privacy rights is to ask the patient. And the rules—the proposals—are designed to sort of allow more of that without getting the patient involved. I think that's a much trickier policy question, I'm not sure where that is going to end up.

Steven: I think its interesting too because in the larger policy context as well we've seen, as you've helped us illustrate, HIPAA is actually more narrow than I think a lot of people understand it to be.

Prof. Nahra: Yes.

Steven: And even in my own understanding of it, its much more narrow than I anticipated. But thinking about the larger policy debate about privacy generally, what have we seen HIPAA do well? What are its shortcomings?

Prof. Nahra: Well the well. I think the well is that idea of normal uses. I mean, one of the big debates in privacy law is what is the role that the consumer should play in dictating how businesses can use their information? And right now, in most settings, outside of the healthcare field, you know, you go to a website today and there is a privacy notice at the bottom of the website page that is perfectly available to you if you want to choose to read it. I don't know that you are going to understand any of it, and I can bet that you didn't read it. And if you go to fifty websites there is zero chance that you are reading fifty privacy policies. So, you have rights as a consumer today, but those rights are sort of meaningless because the privacy policy says we are going to do anything we want to do, anything we are allowed to do by law, and you agree by

proceeding with this website and you don't know that, and you don't have really any way to check on that. HIPAA changed that approach. What HIPAA did is it said alright, we aren't even going to bother with that. We are going to give you the notice, but we don't care if you read it because we are going to tell the doctors and the hospitals and health insurers 'here is a limited set of things you are allowed to do with this data. That's it. That's all you're allowed to do. If you want to do something else, then you need to go to the patient and ask their very specific permission. But its very affirmative permission, it's very specific permission. I think that system works really well in the healthcare system. The question for the broader national debate is how do we define what is normal and typical and common for not only a hospital, but for a bank, and for the Gap, and for a technology website and for ESPN and for Target, etc. That's really hard. The concept of defining by context or by commonality, or by expectations, that's a really good, I think that is a really good example. I like the HIPAA Security Rule in general, which is designed to be a process security rule. They recognize that if you set out very specific requirements in the rule, you'd have to change those all the time because security and technology changes all the time. So instead what they did was they built in an approach to how you think about security and a process you have to go through, which the process doesn't change over time, what you are applying it to changes over time, but it's sort of a perfect rule to keep up with these technological changes because it makes you think about every new change as it happens. I think that works really well. HIPAA also has a very strong approach on what is called "de-identification." Which is the idea of removing identifiers from your medical records so that it's no longer identifiable. Its data about a person, but I don't know that it's Steven or it's Kirk, it's just some person. And there is lots of uses for that data in the healthcare system for research and analytics and a variety of other things, public health. And it has a really good approach to that issue. So those are some of the big, some of the big sort of wins—all of which were drafted again, were drafted by HHS on a blank piece of paper. All of that was made up, Congress had nothing to do with any of that.

Steven: It seems like the work of some clever engineering in the administrative, branch to take care of that. Curiously we have seen HIPAA inform a larger policy debate. For instance, California has implemented state statutes regarding medical information and other privacy protections for its residents. Taking this context and thinking more broadly to a national law, how has HIPAA helped inform this debate?

Prof. Nahra: Well actually, that's a tough question—and to some extent, and I'm not sure HIPAA has informed that debate very much. One of the things that is curious to me about both the state laws so far and the major federal bills is that most of them have essentially exempted people covered by HIPAA. They have exempted people covered by any of the major federal laws. So that is actually leading to lots of confusion today—and you mention the California law, so let's talk about that for a second. The California Consumer Privacy Act, if you are a California resident, today, under that law, your medical information is protected by at least six different sets of requirements, depending on who has your data. There is HIPAA, its exempted from CCPA if you are covered by HIPAA. There is a California medical privacy law. If you are subject to that law, you are not subject to CCPA. If you are a part of clinical research, you are not part of CCPA. If you, then there are people who are subject to CCPA, but that excludes nonprofits, lots of healthcare entities are nonprofits and patient advocacy groups, etc. and if it's

employer-related information it's not subject to CCPA. So, I look at CCPA as an example and say no reasonable California person could understand that. They can't possibly understand that when the doctor has information it's subject to one rule, when a mobile app has it its subject to a different rule, when a website has it it's a third rule, if I'm involved in research it's a fourth rule, if I give my COVID data to my employer it's a fifth rule, and if it happens to be a patient advocacy group, that's a sixth rule. That makes no sense to me. At the same time, healthcare businesses are struggling with that, and again, we can decide not to have sympathy for them, but it makes it harder to do your business. You have to think about who your customers are, who your business partners are, what your data sources are, and it just makes the whole process much more complicated. I've been saying in some of my presentations recently that I think current privacy law, particularly related to healthcare, but not only related to healthcare, is currently bad for consumers and bad for businesses. The only people it's good for right now are privacy lawyers, and I'm happy to be one, and I'm not going to complain about that, you know we are not a protected class that really should be given a lot of additional authority. Right now, it's just too confusing. So, the federal law right now is continuing that trend. It's going to say, we are going to have a baseline federal law, but if you are subject to any of the other laws, you're not a part of the federal law. I'm not sure that's the best approach. I am increasingly of the view, you know, lots of debate on this, I am increasingly of the view that having a single law—I don't really even care what it says—but having a single law would be better for both consumers and businesses because we would have a target to shoot at. We know what we are doing and we can tailor our activities to that law, and again, maybe bad for privacy lawyers at that point, but we wouldn't spend just so much time just figuring out how all these things fit together, which I don't think is really a productive use of anyone's time. Again, perhaps other than my time.

joint laughter

Steven: Thank you Professor Nahra for joining me on the first episode of Season 3 of *A Hard Look* and sharing your expertise and insight in helping parse and explain HIPAA. Do you have any final comments for our listeners?

Prof. Nahra: Couple things. Make sure you spell HIPAA right. I tell my students that if they spell it wrong on the final exam I will fail you. There is only one "P" in HIPAA. It is astonishing to me how many people get it wrong, and if you're on the internet, the people that get it wrong are really loud and aggressive about how wrong it is, and so the substance underlying it is also probably wrong. That's a key one, you're advertising things you don't know what you're talking about when you misspell it. At the same time, do—consumers and individuals should be aware that HIPAA is not a general overall health information privacy rule. It protects certain information when it's held by certain people for certain purposes. And so, if you are dealing with a mobile app, if you are posting your medical conditions to your Facebook account or on Twitter or whatever, you need to recognize that is probably not protected by HIPAA. If its protected, if at all, by the same rules that apply to what magazines you bought or whether you bought a pair of jeans last month. So that is, and you said earlier Steven, that that is sort of a common error, and it is a common error. People think it applies where it doesn't. And so, think about where it applies,

be protective of your own healthcare information, you probably have to be less worried about that in the core healthcare system. Pay more attention to it outside the core healthcare system.

Steven: I will always remember the "P" stands for "portability!" Especially after today. Thank you again Professor Nahra. I want to take this time to thank our guest, Professor Nahra, the American Bar Association's Administrative Law Section, the Administrative Law Review, and Technology Editor Kübra Babaturk for all of their help, resources, and platforms to make this podcast a continued presence and contributor to the larger discussions in the world of Administrative Law. Thank you all for listening and we will see you all on the next episode of *A Hard Look*!

Music Outro

End.

Professor Nahra has provided some extra links for those seeking to learn more information about the subject matter of today's episode.[1] [2] [3] [4] [5]