FOLEY

FOLEY & LARDNER LLP

Health Care Law Today Podcast

Episode 5: Leaks, "Lakes," and Loot: What's the Big Deal About Data?

For this episode, Emily Weber, Foley Partner and member of the firm's Health Care Industry Team, visits with Ian ONeill, General Counsel at Welltok, Inc. They will talk about the challenges of health care data, "data lakes," how mismanaging data can impact your organization, and how to bounce back.

Please note that the interview copy below is not verbatim. We do our best to provide you with a summary of what is covered during the show. Thank you for your consideration, and enjoy the show!

Emily Weber

My name is Emily Weber and I'm an attorney with Foley focusing on transactional compliance and regulatory matters mainly with health care providers, but certainly a lot of data issues with startups, especially in the innovation area. I've been practicing for about 13 years in the area of the health law space. For today's podcast we are going to talk about the challenges of health care data and the challenges in health care, and most importantly, how mismanaging data can impact your organization.

Today, I'd like to introduce Ian ONeill. Ian is the General Counsel of Welltok. Welltok has developed a platform to track and manage consumer health actions. They take a data-driven personalized approach to get consumers actively involved in their health. Ian, it is a pleasure to have you as part of our podcast. Would you like to take a moment to tell us about yourself and a brief introduction to Welltok?

Ian ONeill

Thank you for inviting me. I have been practicing in this space for about 15-16 years now, and I lead the legal operations group over at Welltok, where we have a platform and a push service that effectively uses every kind of follow up communication online. From an online platform, to text messaging, to direct mail, to email marketing, to outbound and inbound phone calls, and sensors, we help consumers take control of their action.

We're a B-to-B platform, primarily working with the providers, with the health care insurers, with Medicare and Medicaid, with different parties that having an interest in reducing what we call the

morbidity curve, which is guiding and being that, if consumers and individuals or patients know more about different determinants, particularly health care situations and health care issues, they can take other control over choices and reduce morbidity curve, which effectively means you can reach the age of 70, 80, 90 without suffering that downward curve in your general well-being and state of health.

Emily Weber

That is fantastic. We're both here in Denver, and it's exciting to be doing another podcast with you again.

Our first question is—and really the issue is that we're going to lay the groundwork for this data discussion, and we want to make sure that we're all on the same page and speaking the same language by identifying the terms so that everyone listening understands data and the rules that govern data—we want to talk about is the general rules of what you can and cannot do with data. Generally, the way I operate is that there's different types of data; there's just data, there's de-identified protected health information, there's protected health information, and then there's personally identifiable information. I know that those are certainly terms we're going to be using today.

Certainly in the PHI and protected health information world, the general rule is that you have to get someone's consent in order to disclose PHI and certainly there's a number of exceptions that allow entities to disclose PHI. The biggest one is, without a patient's consent—and that's for treatment, payment and health care operations issues—but then there's a number of other transactional agreements that you can put in place. You can have an IRB approved research that serves as a privacy board, you could have a limited data set, but the golden rule is that you need to get consent.

And then there's a number of other issues related too; you can have a court order or you can disclose for certain law enforcement reasons. While, I know a lot about PHI, you know more than me certainly about PII and the other data. Are there general rules?

Ian ONeill

With respect to different types of data, obviously PHI is the most essential one. For Welltok, we have fully enriched PHI files, for example, for almost 300 million people, and it’s growing every day. We have full high trust certification, and stock type two certifications, full audits, entire data security team that absolutely can't be undersold on how important that is.

The way I see it though, is that's still only one flavor of data. In today's day and age, data is not only one of the most viable assets, it's one of your most durable characteristics about you in that everything you do, every move you make, every action you take, creates data. All of that is out there, and is a very powerful way to help shape and use and influence the world we're in. For example, at Welltok, we will take PHI for a provider for whom we are providing a platform, and who's various members are using our platform to manage and track certain health conditions. Basically, the way our platform works is we have a system where we create things called action cards, which are really just interactive ways of motivating people to do specific acts. They are based on very deep analytics and social determinants of what we know people are most likely to respond to and the provider will use those to have part of its

population manage their weight, part of the population be more diligent about getting regular screenings for things like mammograms.

Emily Weber

And how do you get that, Ian?

Ian ONeill

That's exactly where I was going with this conversation. To get that type of utility out of data, the PHI is obviously the core of that because the provider has that PHI and they're providing the health management of that individual, but PHI is also limited in that you can only use it for very specific things. If you want to use it going beyond traditional care, and you're not just asking one doctor to give a second opinion, it becomes more restrictive, but if you layer and supplement that PHI with various forms of things like publicly available data so that you know demographics, you know of data you can get from companies like the Experians and Equifax, and Credit Bureaus of the world, you can get things like claims data. You can layer all of these publicly available private data, personal information and PHI and demographics together, and then you can create, what is effectively, an incredibly powerful proxy for just about anybody out there.

That's the day and age we live in and that's why we see these trends of constantly evolving laws trying to stay ahead of us as we realize how much data is not just our identity in the sense of numbers on a piece of paper for identity theft. This is our identity and how we act, who we are, what we do, even down to very tangible results, like would we respond to a certain reward that would incentivize us to go and get our blood glucose checked regularly, would incentivize us to lose 20 pounds, would incentivize us to have regular doctor checkups.

Emily Weber

Or to use this type of medication.

Ian ONeill

Exactly. The best way I'd describe it is not only do we have our own platform, we have lots of what we call connect partners, which are third parties of technology companies, health tech companies that effectively make their offerings and their services available as an integrated offering. Think of it like the iPhone with the app store, but you have lots and lots of different ways in which data is used there. We have folks that come in for prescription medications that will use very precise data to be able to help you and your provider know exactly what the most effective medication would be, not just in terms of how effective it is for you, but how much it's covered by your health insurance plan, how likely you are to take it, how likely it is to interact with other medications you take, how much somebody with your particular background or demographics—maybe your age, your gender, your diet, or anything like that—is likely to take this.

That's just one example where data is a constant flow. We have gone past the stage in just about any health type business, we have gone past the stage where you can compartmentalize it and say, "We only need to worry about PHI," or "we only need to worry about PII," or "we only need to worry about PI," because to get to where we are in the power of data, and to harness it, we have to create this rich data overlay.

As far as laws go—I know we're going to talk about that in a few seconds—it is somewhere akin to Theseus and the Labyrynth to try and analyze these on any given day for a particular purpose.

Emily Weber

I think that's a great segue into saying that, certainly we know about HIPAA and HITAP, and to all of our listeners out there, many who will be in the United States, or certainly here in Colorado, we have our own data privacy law, so I encourage everyone to really look into those state law issues because I think there should more restrictions that are allowed.

There's a lot of case office coming out, and I think University of Chicago / Google case is the most poignant case right now because that really dealt with the issue of data—who says that they own the data, who said that they consented to the data. The point that I'm taking away from that case is, in that event the entities, the defendants in that case are essentially saying, "we complied with law. The fact that the government hasn't kept up doesn't mean that we didn't comply with law. We complied with law."

And then the plaintiff is saying, "Yes, but you disclosed location in Google because you also could use all the information from your phone. You could then track who exactly we're talking about for each individual piece." So then the plaintiff started claiming that they're going to have some sort of ownership in that data and therefore they should make off of whatever Google's making money off, so I think that will be very telling in the next year or two when that's decided. I have a feeling that will probably go to the Supreme Court because it's such a big deal.

Ian ONeill

And that's an ongoing discussion. I'm sure you see it in your practice, I know I saw it all the time when I was in private practice, I definitely see it now in how some of these health-tech platform. We have literally, as I said, hundreds of millions of active users and data files, and hundreds of millions of dollars in revenue each year coming through, that type of velocity, the discussion is constant onto who owns data.

Emily Weber

And it really depends on who you're talking with because I put it every which way, even from internally the same client because some people will say the patient owns the data, and some people will say "no, the patient has access to the data, and that the provider owns the data." Some will say that the health system owns the data. Someone says no one owns the data, and all of this is just copies of a set of numbers. I will tell you that I don't think that there's any one right position on it.

Ian ONeill

And ownership is also a variable based upon usage. I would say if you're going to do any analysis with respect to ownership of data, you have to have an X- and Y-axis with respect to usage too. An example I'll give you out of a practice point about a deal that I've been recently negotiating my way through. You have two entities, each of which is a covered entity, each of which provides some distinct portion of health-tech, where the one is the provider, one is a health-tech application provider, but because the patient at one point is receiving access to the health-tech provider via the first covered entity, they belong as a data subject there, effectively bound to that covered entity number one.

Then once they access the health-tech application, and they've signed up and they've agreed to their terms of use, they start to provide different data on monitoring biometrics, they're effectively become a data subject that is bound to covered entity number two. Covered entity number one still needs and has rights to use that data, and there's an exception in the HIPAA for coordinated care, so it can be shared, but you really now have the same data being provided. There's nothing different about the data, but both entities are covered entities, but theoretically, they appear to own the data.

By virtue of the fact that I am giving information to covered entity one out of one side of my mouth, and giving the same information to covered entity two, and they don't have to talk, but they are talking, I now have this dual data ownership, and that's where usage has completely become the dictator on who actually owns the data.

Emily Weber

I know that we'll get into this more when we talk about data monetization, but I think we also have to think of the issue of the numbers itself. The core data, whether you own that or if individuals are really saying they own the outcome of the data, it's sort of an academic discussion.

Before we get to that, I think that there's some really interesting developments that you are very much on top of. Maybe we can spend just 15 or 30 seconds, if at all possible, and I'm going to sort of name them out to you and you can briefly go into them.

One would be FCC developments.

Ian ONeill

FTC and FCC, in all of these areas, there's always a question, there's always developments going on with respect to how the health care exemptions apply. So FCC, for example, they have governance over things like the TCPA, and so therefore using text message tied to data to send out messages to try incentivize people is sometimes covered under the TCPA exemption put in place by the FCC, and sometimes not, if it's not truly a health care message. It's constantly changing, and they're constantly issuing new guidance.

There's a lot of action going on in that space right now with deciding on what the scope, the scale, and the boundaries of the health care exemption for all the TCPA is. So that's a great example.

The FTC, similarly has a lot of action going on right now with respect to determining health care exemptions and if certain types of data, and certain types of messaging, are exempt form the various rules—things like telemarketing sales rules, and things like that—in terms of the type of messaging they are. That's a constant moving target you need to keep in your sights if you are in any way using data in a way that involves outbound communication.

Emily Weber

The two other I'll ask you briefly to touch on, one is GDPR. As an Englishman you should know about.

Ian ONeill

GDPR is one of those things that we all thought was going to be in the rear view mirror as of 2019 after it was implemented in May 2015, and proves to constantly still be a moving target with respect to how it's interpreted. GDPR is obviously the European General Data Privacy Regulation with respect to how you can and can't collect data, what you can do with it, how you need to protect it, what rights you need to pass along to the data subject if they're Europeans with regards to those rights being to know what's on file, rights to change what's on file. Obviously, that becomes a larger issue when you have competing data requirements, especially record retention requirements. If you are keeping records for mental reasons, if you're keeping records for contractual reasons where you've agreed with a provider who is a client or a partner that has Medicare or Medicaid retention agreements, various states now have flow down requirements on any of their Medicare or Medicaid patients you collect data on. Florida is a big example, they have security requirements, so GDPR is one of those laws that was written completely and totally without any regard to obviously American state laws. You obviously have to do that if there's any chance that a European data subject is involved.

Emily Weber

And then the last one, which I think is one of the most interesting new laws, is the China Cyber Security Law.

Ian ONeill

Again, we're still getting our heads around that, but following on from the GDPR development, where some of the Asian and Pacific region, China in particular also have its own developments with respect to who owns data, what data can and cannot be used for. It's coming into effect as we speak, throughout 2020 it will be a large issue for anybody that collects data from any person in China. Basically, what it boils down to is it's going to be almost impossible to get data out of China.

If it's collected there, then that's a different analysis because you probably are there for a valid business reason, you have localization, local servers, that type of thing that's there. The issue is what if you are using some kind of cross border play and you have a reason to go there in and out, once it's in, it's in. As you say, it has to be saved on a server located within the PRC. It has to remain in the PRC, unless there's various ways to get it out, and there are very narrow exceptions. The problem is collection, or even transmitting data, into the PRC is going to result in lots and lots of restructuring with respect to

commercial transactions, with respect to how you use and other B2B type approach to actually get that data back out.

Basically, there's a locked box. It goes in, it stays in, unless you can get it out through any of the narrow key holes.

Emily Weber

Let's go next into the second issue. We're going to dive into data monetization, and we touched on this issue when we were talking about who owns the data? Who is the who and who has access to data and can give authorization to pass it? We, certainly in our field, refer a lot to the term “data lake.” Can you talk a little bit about “data lake,” what that means to you, and after that I'll speak about what that means on the providers side.

Ian ONeill

“Data lake,” is one of those terms that you are hearing more and more, especially in the health tech space as we realize the power of layer to data. As we try to figure out things along the lines of how most effectively to move people to go towards beneficial action, whether it's health actions, like we said earlier on.

Even outside the health tech space, as you start to realize the power of data to really try and help to create change or create action, “data lake” is one of the expressions you will hear more and more of, where you realize, instead of having a database for PHI and a database for publicly available but privately collected information that you purchased from someone like a Lexus Nexus or Equifax, or to have a marketing database that you are keeping segregated, all of your marketing information. You realize the value of this should all be stored in one large “data lake.”

You can have more enhanced security, more enhanced control, but that also comes with more enhanced complexity in terms of managing things like permissions, managing things like access and how it's actually used.

Emily Weber

And also, I think that a lot of entities want, once they withdraw their consent, to be able to go back and say you do not have authority to use my data anymore, to say get my data out of the lake. It’s technical issue.

Ian ONeill

It's a very technical issue, and in some ways that's probably one of the primary drivers of this trend we're seeing. We have laws, like GDPR, we have laws like the California Consumer Privacy Act, CCPA, all of which, that is a trend we're are seeing move across, all of which have this concept that really goes back to what you said, the individual owns that data. If I own my data, I should have a right to tell you to change it. I should have a right to tell you to delete it. It's really not a new concept, which seem the right

to be forgotten enshrined in European law for almost a decade now when it came around through the various Google search engine lawsuits. We've seen it here in the US for almost two decades, where it really existed in a very limited way for the respective minors under the age of thirteen, from COPA, so the concept itself was not a new concept that maybe individuals should have the right to say what you can and can't know about them. From a legal point of view, we're seeing this rapid momentum of laws that are actually enshrining it.

The statutes are written so that not only do I have the right to know what you know about me, and how you store it, I have a right to tell you to delete it and not use it, to change it, and that includes all of your downstream all the derivatives and all the service providers. That's where I think the “data lake” concept is from.

In the system that we're all developing in the last decade, you may have, in your case, Emily Weber, and say your social security number, or your age, or your driver's license number, or your address, or your family size, and how many children you have, and all these disparate pieces of information. In the past it would have been, I would have had my database, and then I would have had 30 vendors. I would have had the hosting provider, I would have had the direct mail provider, I would have had a list management provider, I would have shared it with every service provider that provides a service for which I need them to have that information with they email something out to you because I am fulfilling something where we're going to email you. Whether they are going to run analytics for me to know what offers you would be susceptible to, whether they are going to process your benefits so that I know if you are covered by insurance, any of that type of stuff.

The idea behind “data lake” really is, all of these complex layers, and all these points of ownership, are much more manageable if you have this one big pool that gives you all this ability to layer into search and to manage and to give you the step. It also means if you come to me, and say, "Hey, I am Jane Doe. Please delete everything you know about me," or even, "Hey, I'm Jane Doe, please tell me everything you know about me."

A data map is that much flatter. If you can say, "Here's everything I know about you from my data lake." As opposed to, "Give me a couple of days, I need to ask 36 different vendors to tell me what they have in their database that I've shared with them. And if you tell me that I need to delete, I need to now send out data deletion requests to 36 different vendors and hope that they do so, but I need to do so in a way that I'm going to have whatever assurances that are going to be required as the laws continue to evolve.”

GDPR is probably the strictest. We have to get back within a specific time-frame to let the data subject know if we have deleted their information or, if not, why not and what actions we're going to be taking so they can go to their local data protection authority. CCPA has something not quite as intrusive, but still along the same conceptual lines, and that's the floodgates opening for that rolling across all the different state privacy laws across the U.S., for the same type of thing. Ultimately, within the next five years, or so, or decade at the latest, we'll probably be at a stage where every state allows every individual to control who knows what about them, and to delete it subject to applicable restrictions on the law. I can't ask you to delete things that you have a right to know, and that's where it becomes very complicated.

Emily Weber

I would also say that it's actually incredibly difficult because while the new world order seems to be that people have the right to control their data and have access, as you mentioned, to know where it's going, but we're also now in a world of data. Whether it's my cellphone or me walking down the street and there's a picture of me, everything that we do is data, so it's hard to reconcile those two issues. I think that's what we talk about with the issue of data and derivatives and what's coming from that. There's the technical issue of saying, can you actually even delete downstream derivatives of that data? Or if there is an innovation or an improvement to something based off of my data. Do we say that I have some right of that?

Ian ONeill

That's a good question because we deal with that all the time, and in private practice, I had lots of clients that dealt with that. In my current position, we deal with that. The question is: where do you draw the difference between data and data constructs?

Emily Weber

And part of it is consent.

Ian ONeill

That's right, and then once you get into a stage where you have business to business to consumer, or business to business to business to consumer, or you have provider to patients, you get into a more nuanced set, where it's like, "where do you consent?" If I take 20 million people's data files—even though it contains something along the lines of PHI—if I take that PHI and I throw it on my database, it's very easy. Because I am governed by HIPAA, I'm probably governed by the state law with respect to if I have a data breach.

I'm in Colorado, we have our own, but all 50 states now have some variation of that. I'm probably governed by my contractual relationships with who gave me that data in the first place that we agreed to some standards, maybe an ISO standard, I might use some kind of audit standards that I've agreed to do in order to show that I'm keeping it safe in a manner that can be trusted, but that's still relatively simple.

Emily Weber

I will submit that you're also governed by if an individual signs a consent, what's in the consent? I think it's very often that the consents do not match reality.

Ian ONeill

The problem is that consents don't keep up with reality because then the next point becomes, “that's all very simple,” but then I start to do stuff about the data. The next layer of complexity to me is I share it,

or I just use it to do a function. I share it with a direct mail list vendor because I want to send lots of pieces of mail out.

Emily Weber

Or I figure it out myself. I manipulate that data myself.

Ian ONeill

Then you get into larger complexity about what if I do things that aren't just using that data? And this is where it becomes ironic, because the very laws that held all the rules—that help protect the individual and help us use the data—there are rules on things like de-identification aggregation. They start to work the other way in that they give more right to the people that have done the de-identification aggregation, because if I aggregate 20 million people's PHI together in order to see what type of person is likely to respond to a text message to go visit their doctor.

The model I built from that doesn't contain any PHI. I don't know that Jane Doe was that person. I don't know that John Doe was that person. I just know if I was to send the text message to this type of person, 70% of them would listen to it and go to their doctor. If I send a text message to that same group, 30% wouldn't go unless we called them via the phone. So, now I have a product of that data. I have a model, or an algorithm, or a scorecard, and who owns that, at that point?

There's lots of analyzes from all the companies and all the industries, like a credit report, or a credit bureau. It's pretty well settled that credit bureaus have always argued that they own the product of the output. It gets trickier when we're in the health space because before you even get that data, it's gone through a round of different laws and different consents to get to you.

The health care provider has collected it from the doctor, who has provided it to their medical records in the first place when they were seeing the patient. In the health system, the payer has then decided if they're going to pay out on that, and maybe the payer is the one that requires that private data because they want to model it. Our data, even before we get to the de-identifier aggregate portion, you've got to worry about the commissioning stream, and then you can own, or not own, depending on what it is, things like the product and the output.

The reality is, in today's world, the data about you is not just information about you anymore. You were right with the cellphone. Data about you really is a fundamental characteristic of all of us. I liken it to—there's a tenet in Buddhism—all people are just a physical case for a spiritual being that is passing through, all you're doing with your body is moving energy around. I liken data to the same type of thing right now, all we are is carriers of information about us and all we're doing is moving information about us and people can use that information to also make us move in certain ways.

Emily Weber

I think that comes with an argument at least to say that we do need to recognize that because data is everywhere, is it reasonable, maybe that's not a legal question, but is it reasonable to say that one has

the ability to control all of their data? Looking at all these different state laws, especially that are being promulgated, or is it just like, "this is how we live now," and is it all data?

I think this is kind of a good segue into our last question or issue we're going to look at, which is, the different perspectives of entities out there looking at data. We could say, look at health systems and providers, which I think often say, "we get consent from the patient to be able to, depending on the health system, use their data on a wide variety of cases. There's many clients who differ between the clients themselves about who owns the data, but they say, "we're going to use this data to make improvements on health care." Ultimately, they want to make health care more efficient and less costly. There's different ways to do that, as long as you can get consent from the patient to be able to do that, and say, "we're going to be able to use your data," this is outside of the normal HIPAA consent. There's an argument to say as long as the patient has meaningful consent to whatever is being done with their data, then ultimately that's it. Bottom line.

Ian ONeill

I would say HIPAA even supports the idea of that as a philosophical thrust behind it in that HIPAA is one of those data laws that, while at the same time it requires very specific consent, and very specific publication of privacy notices, it has a fundamental, philosophical bent built into it that there lots of exceptions like for coordinated care, where you can share data without patient consent. It's one of those very complex, nuanced laws that depending, again, on the usage in the scenario, you have to be very careful. I think this boils down, in some ways from a legal perspective, to that your permissioning path over how you get permission when you collect the data, is probably one of the single most important legal documents that you have in this area. Even if you don't need to have that permission, if your permissioning path protects you, you're in great shape. If you do need to have that permission, and your permissioning path does not give you the right consents, then you're in terrible shape. It's one of those scenarios where the best legal advice I think I ever received, or would ever give, is what's so hard in getting the consent?

Marketing folks always have a view that it suppresses the response rate, but we're talking about health information here, we're not talking about marketing information. The reality is, I can't use PHI information for marketing purposes, anyway. Permissioning path is absolutely vital to make sure for that process.

Emily Weber

And part of it is, sort of a lesson learned, is spending a lot of time being creative or thoughtful in those consents, in not thinking about how the data is being used now, but thinking about how it could possibly be used in the future. What I see clients getting frustrated with, understandably so, is when data is being used for a use unanticipated in the original consent, then they have to go back and re-consent patients. Then the question is, if someone doesn't re-consent the patient, for whatever reason—they can't get in touch with them, or whatever reason—does that mean that the consent is being withdrawn?

With medical devices, I certainly know that Welltok is not a medical device, but I'm curious to see what your position is in your industry on the consent issue. What do you see?

Ian ONeill

We do interact with companies that provide and use medical devices. Our tech partners that are medical device companies are some of the most diligent and buttoned up with respect to consent, because there are also sorts of rules, whether it's the CMS rules, whether it's on the various state rules, we go to biometrics. Medical devices by their nature tend to collect biometric information, because they're somehow tracking something on your body whether it's a diabetes monitor, or it's a heart rate monitor, whether it's a small molecule monitor. They are, by their nature, much more likely to be collecting much more restricted information, so permissioning consent is even more important when some kind of durable device is involved.

What happens, not only if you don't collect the correct consent in the first place, and then you have to re-consent and you don't get that, not only is it not getting the second consent, but is an implied withdrawal of the original consent. You then also get into your other issues that go along the lines of consent has to be informed on the HIPAA, just as it does in the most sensitive data laws.

If you are hitting people up with multiple consents, each dealing with a slightly different but highly technical medical issue, at what point are you stepping over the degree that folks like the HHS experts will step in and say, "How the heck is that informed? You're just confused the blazers out of that person with ten different consents, each of them are very highly technical explanation of what you're going to use it for, and why. And they're supposed to know what you're using that for?"

One simple singular consent is always going to be better, than twelve focused small technical things on different medical purposes.

Emily Weber

I think that the last point I'd like to talk about is just the general issue of monetization. It seems that for us—traditional health care attorneys—we look at data as just the data in the medical record. but then there's a billion other companies out there that are making billions of dollars out of not medical record data, just general data. It astounds me how much money is being made off of data and why entities want that data.

Ian ONeill

The reality is data is a power to know about the individual, but in knowing the individual is also the power to make the individual do something whether it's making them buy something or making them subscribe to something. That's what we see outside of this area, but that's also true within this area.

What I would propose, what I would put out there and pause it is, monetization is not, and shouldn't be, an ugly word. Monetization for monetization's sake sounds extremely crass and mercenary in the context of health care, and that I would agree with, but what monetization really is, what we're talking about there, is companies doing something to incentivize specific behaviors.

Emily Weber

So it's almost utilization?

Ian ONeill

It's utilization. If a company is using that data to utilize healthy actions—for example, it's helping make sure that children get their immunizations, making sure that people get their regular doctor's checkups, making sure that they take their medicines—they do certain physical or psychological acts that will help alleviate depression.

Emily Weber

Even things like standing up. For us attorneys that certainly sit on our butt all day, it's nice to say get up. Walk around.

Ian ONeill

Exactly, even using social determinants to help engineer healthy and well-being behavior is utilization and the monetization of companies doing that in a way that they are viable is not necessarily the ugly word that it's associated with.

Emily Weber

I don't think it's mutually exclusive to say, "You can incentivize and encourage healthy behaviors by this sort of data, whether we're calling it monetization or utilization, and at the same time have companies that make money out of it." You live in a capitalist society.

Ian ONeill

Frankly, even individuals are subject to that. Incentivization of individual actions using some kind of reward, some kind of gamification, "You do these ten things and you will get a gift card," is an incredibly powerful incentive to help people that may not otherwise have done those things for their own well-being or health. [They] may not have even known those ten things would be helpful to them, so there’s even an education component to it.

The monetization of data, it brings up these big scary images of Google being some kind of shadow government with a star chain that is tracking everything you're doing. That's not really what the industry is talking about. What the industry is talking about is using what we know about people to create some type of model to really get people to work in a much healthier, better way, whether it's health insurance companies that want to effectively monetize the data by making sure the people they insure and cover don't have expensive procedures or medical conditions because they were avoided earlier on. They manage and mitigate them.

It's people like employers wanting to incentivize their employee base to be much more active and healthy and mindful of their wellness by using the data of what we know about them to create social determinants and social models to make them take those actions.

Its health care providers trying to stop things like unnecessary conditions, or repeat conditions, or frequent flyers by incentivizing and using that data to get them to help themselves.

Emily Weber

It's even as simple as saying, data could be when I go on my Peleton, and it says you've worked out two days in a row. Keep it up! Work out the third day. It could be as simple as that, and as complicated in the health care world of saying, don't take this medicine because it might kill you, but we only know that by looking at these 15,000 different—

Ian ONeill

There's 15 million people have been analyzed that we know 45 different data points, and by the way, we know from the model that you have six of those data points, so this is not the right one for you.

Emily Weber

That's exactly right. Ian, thank you so much for joining us today. As always, I could talk with you forever. Hopefully all the listeners found this to be helpful, and if you have any questions at all, please feel free to contact me, Emily Weber at Foley and Lardner, or Ian ONeill at Welltok.