NAVIGANT
A Guidehouse Company
On Healthcare

HEALTHCARE

DATA PRIVACY AND THE CHANGING LANDSCAPE IN GLOBAL PRIVACY REGULATIONS

Announcer: Welcome to Navigant On Healthcare, offering insights for healthcare leaders striving for success in an evolving industry.

Host: Welcome to Navigant On Healthcare. I'm your host Alven Weil, and today we're discussing data privacy as it relates to global med tech and pharmaceutical organizations to include the great risk from the substantial obligations and fines stemming from global privacy regulations.

With us today to discuss this are Navigant's Stephanie Lewko, a life sciences governance, risk, management, and compliance director with 15 years of consulting experience spanning a variety of healthcare and life sciences clients, including medical device and pharmaceutical manufacturers.

Also with us, Brian Segobiano, Navigant director and head of data privacy solutions, who leads Navigant's service offering to help clients assess their data privacy risks, build data governance frameworks, and operationalize those programs. Welcome to you both.

Brian Segobiano: Thanks, Alven, happy to be here.

Stephanie Lewko: Thanks, Alven.

Host: So, as a brief introduction to our listeners, can you provide an update on the global privacy trends as it relates to life sciences?

Brian: Absolutely, happy to. So, looking back at where we've been and where we are today…so, obviously 2017 and the early parts of 2018, there was a lot of focus on the European Union's general data protection regulation, or the GDPR, as many folks know it. And the lead up to that involved a lot of risk assessments and developing the policies and procedures. As we turned, at least focusing on outside of the U.S., we're starting to get into the enforcement phase with that, now that it's been in place for nearly a year, at this point.

So, we're seeing some fines, as we would expect. For example, in France, where there's the $50M fine of Google. We've seen other ones in Austria. There were fines for cameras capturing information in public places. And within the healthcare/life science space, we've

SPEAKERS

STEPHANIE LEWKO

Director
Life Sciences Governance,
Risk Management and Compliance
+1.202.973.2458
slewko@navigant.com

BRIAN SEGOBIANO

Director
Life Sciences Governance,
Risk Management and Compliance
+1.312.583.2749
brian.segobiano@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

seen in Portugal, as an example, the supervisory authority there issuing a 400,000 euro fine for access to patient information by those who did not have the credentials to be accessing it.

So, I think outside of the U.S. we're starting to see a lot of enforcement around these laws, and, certainly, other ones that are coming into play, such as Brazil's data protection law is coming in place, and I think folks even waking up to existing laws like what's in China and other locations around the globe.

Concerning the focus to the U.S. side, at this point, now all states have a data breach notification law, so organizations need to be aware of, if there is a breach, what are there reporting requirements, whether it's to agencies or to individuals.

And, then the big news on the U.S. side is the California Consumer Privacy Act. So, this goes into effect January 1, of 2020, and certainly a lot that we think will change, but that's the first phase of what we see as importing those requirements from the GDPR and other international laws in terms of having individuals the right to be notified of how their information is used, particular attention being paid to that information being transferred to or sold to other entities.

And, then within the U.S. we're seeing many other states. This seems to be good bipartisan politics, if you will. Washington, as an example, has a law that's come out of their state senate that's much more GDPR-like in terms of the rights it extends to individuals and differentiating between what we call processors and controllers of information. So, we're seeing a lot of this import into the U.S., and if you were not impacted by the GDPR, you likely are now, or are going to be.

At the federal level, we talked about the U.S. states. There's a call for privacy in cyber security regulations. There's a lot of questions about it. Those would preempt some of these laws, or they would have exceptions, which I think is a whole analysis in itself. But calls for the National Institute of Standards in Technology, or NIST, to issue a comprehensive cyber security self-assessment framework, also see a number of bills going in front of the senate and the representative chamber that propose something — again — like a GDPR-ish national regulation.

Again, the question on the U.S. side, because we have so many sectoral laws, like HIPAA, obviously, is an example within the life science industry, where will one take precedence versus the others is an ongoing debate, but it certainly seems to be a question much more now of when as opposed to if these things will be passed.

Host: So, it's clear that keeping informed of these global trends is a must in today's repertoire environment. Now, what are some of the best practices you'd recommend to global life sciences organizations that are looking to build programs to manage evolving risks?

Stephanie: Yeah, that's a really, great question, Alven. And obviously, given what Brian has just walked us through, there's so much to take into account when building these programs to really ensure that they can adapt and stay compliant with all the privacy requirements and the evolving risks that are out there.

Obviously, privacy, for lack of a better word, is still such a hot topic right now with more and more data breaches, the new laws and regulations, and, really, just a continued increase on individual personal data privacy rights that having that solid privacy program in place is just so critical. But it's also important to remember you not only want to have a program with policies and procedures and documentation to demonstrate compliance on a global level, you want to make sure that your employers are able to implement it, but also so that you're not disrupting your day to day operations.

So, when thinking about a framework for a privacy program the first thing you want to do is know your data. It's really going be critical to know what type of information your organization collects, how it's used, its location, what retention schedules are around it…things like that.

So, really starting with a documented data inventory or matrix gives you that baseline to really start to assess where your risk areas might be. And, actually one of the great things about these inventories is they're not only going be useful for data privacy, but they're useful for compliance needs, for legal, for business intelligence projects, any other data management type initiative that might be out there.

So, the next thing is really to take that inventory and utilize it as a baseline for identifying your risks or doing gap assessments. If you think about GDPR, as an example, these might be your DPIAs, or data protection impact assessments. You want to identify where those high risk areas or sensitive processes might be. So identifying any immediate compliance gaps that exist to starting to develop a plan or a phased approach on how to remediate those gaps, which might be things like, "Do we have a retention schedule in place? Do we have the necessary policies and procedures in place? Do we need to update any of our notifications?" things like that. One thing to keep in mind here — also — as your building up this framework, is how your organization might want to leverage tools that are out there to automate some of this.

And, then, finally, one thing is thinking about who's going to handle the privacy. It really shouldn't be limited to just compliance or IT alone. It's going to be really important to establish a privacy or governance office, or team or liaisons that include representatives of key functions from across the organization. So, not just from compliance, legal, IT, etc., you also want to build in different business functions and geographies to help not only socialize data privacy in the organization, but also just make sure all these efforts are rolled out in an efficient, in a complete, and in a compliant manner.

You want this team to be involved in the policy and procedure development, too, obviously. And this is really to get them involved from the ground up. Where possible, it's really important to avoid developing silo policies and procedures that are narrow and only focus on one function in the organization. That's going to be really, really difficult to implement, especially as all these global requirements continue to evolve. So, it's really important to create these policies and procedures that can be easily amended to cover these new regulations as they emerge and adapt and just continue to grow.

And, finally, it really helps to have defined ownership of the area. You're allowing people to get in from the beginning, to provide feedback, express concerns, get trained and also train others, and a lot of times, having the people involved from the very beginning will help identify issues or gaps that may not be evident to all other areas of the business.

Host: Brian and Stephanie, what are some of the common data protection challenges that organizations need to overcome to manage and protect their businesses?

Brian: Yes, great question. I'll provide a few, and I know Stephanie will have some, as well. Really, it starts with culture and Stephanie previously alluded to the concept of operationalizing these. And once you go from paper policies and procedures to making sure that those are actually being followed and can audit those throughout the organization can be a great challenge, actually, in their self. That tone from the top and making sure that the organization feels its guidance coming out from executive leadership. Also, that the frontline employees feel like they've had input in the process through that governance model that we talked about previously, can really help to start to overcome some of those cultural barriers.

Ultimately, we always say privacy should be something that you advertise as a commercial advantage. So it's another way we help get over that cultural hump, is our customers, healthcare providers, the patients —privacy is important to them, and if you can advertise that and make that an advantage that your product has, it helps, again, get over those cultural barriers within an organization.

Certainly, within our space with the clients we have in life sciences, med tech, and the Internet of things introduces a whole new set of challenges, so I think that goes back to understanding we're developing new products and very connected devices that starts to introduce a lot of new points of data collection and third parties and third party software development kits. So, having a good structure in place to identify what those risks might be proactively and develop what we call privacy by design is very important.

Another one that we see very frequently in the life science space relates to just the general lifecycle of the industry. Early on, many organizations are incredibly small, maybe less than a few hundred people, but they have these trials going on throughout the world, and add on to that, we've just mentioned a lot of very disparate global laws, the obligations are very high and the resources might be incredibly thin and stretched. So that can certainly be a challenge, and that goes in with the organization matures and all of a sudden once you become commercial the activities you engage in and the marketing you do is very different, so what you develop in terms of your program and your policy needs to be flexible as the organization matures.

And, the same goes for M&A activities. Many organizations become acquired or spin-offs or in parts of their business, making sure that the policies that existed under the old regime still make sense and can be operationalized under the new structure is incredibly important.

And, Steph, I know you have a few others you can probably add on there, as well.

Stephanie: Yeah, absolutely, Brian, and, I think you touched on probably a lot of the main ones that are out there. Obviously, one of the biggest challenges is just the constantly changing landscape, like you mentioned, with the regulations that currently exist and that are coming in the future. So, it's really thinking about how can companies make those privacy and data governance practices and programs compliant, but still flexible enough to adapt as changes occur.

And, I think utilizing that cross functional team, the privacy team, is one of the easiest areas to start. It really allows you to make sure that you have not just compliance and legal involved in things, but you really have those business stakeholders involved. If you think about privacy and how it's going to be impacting your business, you want to think about it from, not just one data point, but think about the data lifecycle as a whole.

So, an example, for instance, if we're using a third party for something, you want to make sure that you're vetting that third party, making sure that they're doing all the proper disclosures, etc., before you utilize them. So, it's not just one point in time, it's the whole continued life cycle of the data that you want to consider. So, it's not just privacy, it's data management. You want to make sure that you're integrating with other key initiatives that are data governance in nature throughout the organization.

And, then, finally, I think, Brian, you touched on this too, but the digital health space. It's such an important and exciting area. Companies are always growing in this area, and with digital health and connected health — while it's becoming more available in so many aspects and creates so many benefits and opportunities for increased patient care and for health — it brings with it so many areas for increased risks from a privacy perspective.

So, it's really important to account for those risks early and that idea of a cross functional privacy team can, again, be an important first step in dealing with this and ensuring that your data inventories are updated, that they're shared with other areas of the business, it's really going to help with efficiencies, remediating gaps, and just ensuring compliance.

Host: Brian, Stephanie, any final thoughts before we sign off today?

Brian: I think if there's anything the last several years have shown us is that the privacy and enhanced regulations and the importance to patients and other consumers is certainly here to stay and the requirements are only going to be enhanced. It's critically important for organizations to make sure that they're developing a structure around data lifecycle management, managing third parties, understanding that information they have, that's truly sustainable for them and doesn't just sit in a shelf on paper. It's something that they can be audited against and, again, going back to demonstrating that it's a commercial advantage.

Host: Outstanding information. Stephanie, Brian, thank you so much for joining us today.

Brian: Thank you, Alven. It was our pleasure.

Stephanie: Thanks so much, Alven.

Announcer: That concludes today's episode. Be sure to check in with us for future installments of the Navigant On Healthcare Podcast Series on navigant.com/healthcarepodcast. Navigant On Healthcare is a podcast series produced by Navigant's healthcare practice. If you enjoyed this episode, please share with friends and colleagues on social media. Learn more at navigant.com.

linkedin.com/company/navigant-healthcare twitter.com/naviganthealth