PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SARA BERKSON

Chief Privacy Officer and Head Global Privacy Counsel, Vertex Pharmaceuticals

HEADQUARTERS: Boston, MA

EMPLOYEES: 2,500+

ANNUAL REVENUE: $3.04 Billion

When Sara Berkson, the Chief Privacy Officer at Vertex Pharmaceuticals Incorporated, graduated from Yale Law School, she imagined a career of lobbying for changes in health care laws. But the federal privacy law, the Health Insurance Portability and Accountability Act (HIPAA), had just gone into effect and her law firm, Ropes & Gray, needed associates to help with compliance projects for their health care clients. "It was an all hands on deck type of moment," Berkson remembers, "and I was hooked." What intrigued Berkson the most about the new health care law, and the myriad of state privacy and security laws that soon followed, was the risk-based nature of the determinations – the laws themselves were not so black and white and the interesting questions involved the areas of interpretation in between.

After leaving Ropes & Gray, Berkson worked in-house at Genzyme, a rare disease biotech company, then moved on to another law firm, Verrill Dana, to help grow their life sciences practice in Boston. In both of these positions, she worked heavily in privacy on areas such as clinical trials, patient support programs, and international data transfers. One of these projects was for Vertex, relating to a new division they were setting up that would involve the handling of data about enrolled patients and, after the project was complete, Vertex hired Berkson in January of 2015 to help set up the data protection standards surrounding the new program. "I wasn't focused on going back in-house at the time," Berkson recalls, "but the opportunity to join an organization that felt so passionately about bringing new treatments to patients was not something I could pass up."

In May of 2016, the European Union passed its privacy regulation, the General Data Protection Regulation (GDPR), which had a wide territorial scope, applying directly to many companies outside of the EU. Berkson, along with the Chief Compliance Officer, approached the Executive Committee to address how they would handle GDPR and the impact it would have on Vertex. So began a two year implementation project, led not just by Berkson and a colleague in the Compliance department, but by an individual in the IT group as well. "While you can have security without privacy, you cannot have privacy without security," Berkson says. "It is simply impossible to design and implement a data privacy program without a strong partnership with information security."

Vertex rolled out a new global privacy program, built on the principles of GDPR, across all of its affiliates and in March of 2019, the company created a designated privacy office with Berkson as its Chief Privacy Officer. One of the aspects of the new privacy office that was imperative for Berkson, and heavily supported by her leadership, was the need to have technical IT expertise alongside the legal. With this in mind, the company decided to hire an additional full-time employee on the information security team who would have a dotted line up to Berkson – an individual who could bridge the

THE CPO/CISO RELATIONSHIP

"Ultimately, information security and privacy really need to be aligned in order to best protect a company. Information security is best positioned to make sure that the development of systems account for data protection requirements through a principle called privacy by design. It's a true symbiotic relationship because, in order for IT to fully understand and appreciate what those requirements are, they need to work closely with the privacy office."

Given this, Berkson feels it is "extremely important that CPOs and CISOs have close relationships and are working together." Berkson herself has bi-weekly meetings with Vertex's CISO, discussing many topics including protecting intellectual property, privacy laws, upcoming information security initiatives, vendor contracts, and a multitude of other areas. She comments, "There's a lot of intellectual property and highly confidential clinical trial data that we worry about in the biotech space. And the information security team is tasked with making sure it is protected. The CISO and I will talk a lot about what projects he's working on, what new initiatives they're rolling out, and then I advise on how we can do so in a way that's compliant with privacy laws."

privacy office and IT, and help translate the legal and company requirements into technical ones.

WORKING CLOSELY WITH INFORMATION SECURITY

"I think that privacy and security are often different sides of the same coin, working towards the same goals." Berkson continues, "I really look to information security to help me make sure that we're being compliant as an organization. Usually when there are security requirements baked into a legislative framework, whether it's in the U.S. or otherwise, they are not directive in that they don't say 'you have to do these exact things.' They say, 'you must take reasonable security measures based on the risk of what you're trying to protect.' There's a lot of discretion in those frameworks and I rely on my colleagues in information security to tell me what those reasonable measures are for a given project."

In order to translate legal or privacy language into security requirements, Berkson also relies on the information security team to interact with vendors and work closely with the business as they are developing initiatives. She explains, "For example, if we have a project that's being set up where we need to transfer information and it's a transfer that makes sense legally, I'm always asking the business if they have worked with people in our information security team. The information security team can walk them through the options to help make sure that the transfer is protected."

Berkson also has advice for companies that are just starting to think about how to weave together a privacy office and information security. She says, "Some companies still put privacy within the IT group, but with GDPR, there has been a movement away from this. The European regulators have recommended organizing a privacy office outside of any part of the business that makes actual decisions on how data is used so that privacy can be truly an independent function. Because of that, we are starting to see companies with a global presence set up privacy outside of IT but with a close connection between the two."

GDPR AND CCPA

Being compliant with GDPR requires Berkson to work very closely with the information security team to tackle the many complex questions it has raised. She explains, "While GDPR was meant to harmonize privacy laws across Europe, that's not exactly what we're seeing, and a lot of the member states in the EU are allowed to pass their own derogations, or exceptions, under their member state law about how they want to handle something. And often, especially in the information security space, you need to look at specific country-level laws in addition to GDPR to see whether you're allowed to do something."

To tackle these challenges, Berkson says she takes a cross-functional approach, with her team presenting the legal/privacy aspects and her information security colleagues translating those into technical considerations. For example, under the GDPR, individuals have certain rights with respect to their data. Berkson works closely with her IT colleagues more broadly on handling such requests, as they often necessitate not only locating but accessing data across multiple systems.

Having set up their global program in-line with GDPR will help Berkson ensure they will meet the California Consumer Privacy Act (CCPA) requirements as well. She says, "When we're looking at complying with CCPA, we're going to be able to leverage a lot of the processes we set up for GDPR. For example, one of the big areas under CCPA is that data subjects in California are going to have similar rights to what people in the EU have. So, you can leverage a lot of your procedures and ways of working between IT and privacy when those sorts of requests come in."