Q&A WITH
SUSAN WISE

Chief Privacy Officer

Biogen

1. What are your main responsibilities as Chief Privacy Officer?

I actually have a broader role as Chief Privacy Officer than you might expect. In addition to leading our Global Privacy Office, which now has team members in US, EU and APAC, I also have responsibility for Information Governance (data lifecycle management and records retention/management programs), and the Risk and Governance programs for Cyber, IT and Privacy. These latter two teams are responsible for defining and helping operationalize our SOX and security controls framework (NIST-based), and identifying and tracking gaps within those, along with other identified risks. With respect to data privacy, our Global Privacy Office is responsible for ensuring our teams have the training and tools necessary to handle personal data responsibly as part of their business activities. My background prior to moving into Privacy about five years ago was in strategy and operations, so I very much enjoy the opportunity to advance and operationalize all of these programs at Biogen.

2. Are privacy and information security aligned at your organization?

I actually report into the Security organization (CISO), so that drives inherent alignment, but there is definitely a balance between leveraging our operating model for synergies and maintaining an independent lens on privacy considerations. In this respect, it is helpful the GDPR mandates require the Data Protection Officer to be appropriately resourced and and helps ensure programs appropriately consider how to respect and protect data subject rights and freedoms. Also, I have responsibility for governing our technical controls framework, so I ensure our technical and organizational controls are aligned with expectations of privacy regulators. It doesn't necessarily solve all the execution and prioritization considerations in implementing those controls, but at least it gives me confidence the right foundation is there.

3. What kind of relationship do you have with the information security leaders?

There are really two different sides to the interactions I have. The first relates to partnering on new programs and capability building the CISO organization is undertaking to mature our cyber security posture, and the analysis that needs to be done on these programs to ensure they are designed in a way that fully considers the potential impact on individuals. This is particularly important in areas like monitoring, DLP, and DRM. We advise using the Privacy Impact Assessment process, and partner with legal if country-specific legal analysis is needed. Being part of the same team, we can start these conversations early.

The other area is helping provide the review of vendors from a privacy and security perspective. My risk team has responsibility for the vendor risk assessment which gives the Cyber Ops team confidence our vendors have reasonable cyber/privacy capabilities to handle our data.

4. How have GDPR and CCPA impacted your work?

GDPR was the genesis for Biogen to develop the Global Privacy Office in 2015. We've tried to approach this with an intent to design global elements that can be leveraged and tailored as required for other regions. As an example, we might not be able to rely on 'legitimate interest' as the basis for processing in APAC as we can in the EU, but we do have many areas where consent is required in the EU, and we can use these as springboards to create other consent templates. We also leverage our core 'Data Subject Rights' process we defined for the EU for requests from those regions, or by extension, under the pending CCPA. We post all of these on an intranet site to make them easily accessible to the business.

Both IT and security are key in operationalizing privacy, as we look for ways to build data protection considerations into other processes, rather than making them stand alone.

5. In general, how do you see future relationships between CPOs and CISOs evolving?

For me, I think it will be interesting to see how the relationship between privacy, security and risk-as-a-function evolve in organizations. Outside of financial services, I suspect not many companies have highly formalized risk functions, but I think we will see this changing as boards and regulators like the SEC expect more focus and discussion in a more actionable way on how privacy and security create risk for companies. This will require more explicit conversations in the organization about risk tolerance, risk thresholds, and risk acceptance. Creating a common taxonomy will be the first step to drive these discussions. Cyber and privacy are of course only two areas of risk in the enterprise, but if there is a coordination between cyber and privacy, there is a real opportunity to help organizations advance not only risk management in these areas, but across the enterprise as well.