CASE STUDY

FTI Technology Leads HIPAA Assessments, Privacy Program Implementation for Global Medical Device Company

The Information Governance, Privacy & Security practice within FTI Consulting's Technology segment was engaged to lead HIPAA Security Rule risk assessments for several U.S. entities owned by a German-based medical device company. Recent changes in the business operations of these companies triggered potential HIPAA implications and the need for an initial risk assessment. The team's initial work focused on the technical, administrative and physical safeguards required under HIPAA's Security Rule. The strengthening of those safeguards and analysis of the security data privacy practices of each company led to a broader engagement to design and implement a complete privacy program across each of the U.S. companies. FTI's work eventually grew to include privacy solutions for entities in India and the client's German headquarters .

SITUATION

As a German-based multinational conglomerate, the client was operating under an enterprise privacy program designed specifically for compliance with GDPR. U.S. entities, which had not previously been subject to many U.S.-based privacy obligations, did not have policies or resources to enable their own compliance programs.

At the guidance of outside counsel, one of the client's U.S. entities engaged FTI to examine its use of protected health information (PHI) and existing data privacy and security controls HIPAA obligations, particularly the Security Rule. The findings revealed opportunities to strengthen controls and processes for protecting PHI. This outcome prompted the two related U.S. entities to engage FTI for similar HIPAA-related risk assessments. While these projects were underway, the California Consumer Privacy Act (CCPA) went into effect, adding another set of data privacy obligations these companies—each with significant operations and customers in California—would need to address in addition to HIPAA requirements.

FTI proposed a comprehensive, holistic privacy program across the company's U.S.-based operations. Despite an initial lack of executive support from the German parent (which remained

focused on GDPR compliance), and a persistent shortage of dedicated privacy-focused resources, FTI worked with key stakeholders at each of the U.S.-based companies to secure approval for a privacy program that would satisfy both CCPA and HIPAA requirements.

OUR ROLE

FTI conducted detailed on-site reviews of the client's administrative, technical and physical privacy and security controls. Policies were reviewed, to inform an in-depth report of potential risks and the changes needed to align with regulatory standards. These assessments provided the client and FTI's team with important insights into the key areas the new privacy program would need to address.

Early on in the project, FTI's team also worked closely with outside counsel to establish consistent definitions of what data would and would not be considered PHI and what business operations were potentially in scope for CCPA. As part of the foundational work, FTI developed a framework around NIST standards to help the client understand the key elements that would need to be a part of the privacy program. For example, a data map was developed to serve as the source of truth for all instances and uses of data generated across the organization's 178 unique systems and 12 entities in the U.S., Canada and Mexico.

In working with the CISO, FTI led a privacy assessment of one company's software development lifecycle, which quantified its maturity level and provided specific recommendations to further incorporate Privacy by Design into processes.

The privacy program roll-out also included designing and implementing a privacy framework based on NIST to serve as the foundation for their privacy program going forward. This spanned setting up and supplementing a records of processing system with information gathered as part of the data mapping efforts, developing a privacy impact assessment (PIA) process for vendors, marketing, software development, etc., to assess risk against a consistent set of criteria on an ongoing basis, updating privacy policies and notices, creating an incident handling playbook and defining roles and workflows for handling data subject access requests. Additionally, FTI built upon the client's existing data protection training program to provide training modules specific to CCPA and other data privacy requirements. The team also led refreshes of the HIPAA assessments, and provided HIPAA advisory services to help design net-new business processes. The team continues to provide ongoing services to manage the new privacy program.

OUR IMPACT

FTI's work with the client's U.S. stakeholders gained the attention of German headquarters and leaders in the company's India division, which are now engaging FTI to support additional data privacy projects and help the company maintain a robust privacy position as the regulatory landscape evolves. FTI is also now engaged in the client's product lifecycle to help assess privacy implications early on in the process of developing and launching new products and lines of business.

The HIPAA assessment reports served as critical documentation to the U.S. Office of Civil Rights of the steps the company was taking to remedy a potential HIPAA violation that occurred prior to FTI's engagement. After regulators reviewed FTI's reports and understood the privacy gaps the company was working to fill, the investigation was closed with no fault found.

FTI's program helped the client significantly reduce privacy risk under HIPAA and CCPA. The team is providing ongoing guidance for global privacy issues, in addition to headcount to maintain the program.

LOUISE RAINS-GOMEZ
Managing Director
+1 (404) 270-1415
louise.rains@fticonsulting.com

ADAM INGBER
Senior Director
+1 (213) 452-6029
adam.ingber@fticonsulting.com

THOMAS HINEY
Director
+1 (617) 747-1714
thomas.hiney@fticonsulting.com

MELISSA COHEN
Director
+1 (312) 252-9359
melissa.cohen@fticonsulting.com

FTI CONSULTING