SpencerFane®

Data Privacy and Cybersecurity

Keeping clients out of crisis mode.

Our Data Privacy and Cybersecurity team is equipped to handle the urgent and unexpected. When facing a cybersecurity incident or data breach that threatens critical functions, systems, and data, we are in quick command. But we are equally adept – and eager – to help clients prevent emergency data and cybersecurity situations from arising.

Overview

A calming force, minimizing financial exposure and reputational damage

When data breaches and cyber incidents occur, our Data Privacy and Cybersecurity lawyers respond with steady guidance, attention to detail, and knowledge of a client's business that enables us to focus immediately on what's best for the client and their operations.

Building effective data privacy and cybersecurity programs

We work hard to prevent crisis situations by collaborating closely with clients to develop and implement programs to preserve the privacy of data and thoroughly secure it. After identifying and assessing the specific risks related to a client's data collection, we work with them to develop strategic plans that mitigate those risks.

We don't view cybersecurity as tack-on measures. Instead, we integrate best practices into a business's existing workflow and create essential response plans aligned with current business operations.

Our attorneys build detailed knowledge of both a client's risk profile and risk tolerance, and we tailor our input and guidance accordingly. This includes both protecting clients' data and protecting clients from their data and the damage that can be done when data handling protocols are not followed.

We provide clients with identifiable action plans that move them toward normalcy, and we work with them on managing notification obligations and resolving any resulting regulatory investigations or litigation.

We provide consistent and timely review of all policies, procedures, contractual terms, training programs, and data security strategies to make sure all aspects of a program remain up to date.

Our attorneys have experience with HIPAA, 42 CFR Part 2, HITECH, Gramm-Leach-Bliley, FDIC guidance, PCI DSS, EU GDPR, and state cybersecurity and data protection laws such as California's CCPA, allowing them to identify the legal requirements applicable to an organization's use, disclosure, and safeguarding of personal information.

Experience

Data Management Strategies

- Counseled a private equity firm regarding the assessment of the types of data gathered and maintained by its multiple entities, including applicable regulatory requirements for each entity and relevant risks and considerations for the private equity firm.
- Worked with numerous financial institutions in the implementation of the FDIC's Financial Guidance on Response Programs.
- Drafted policies and procedures for numerous covered entities and business associates to implement revisions to the HIPAA regulations under HITECH.
- Drafted privacy and security policies and procedures for regulated financial institutions to comply with the Gramm-Leach-Bliley Act.
- Coordinated security risk assessments for organizations handling personally identifiable information or protected health information, including engagement of security consultants for HIPAA assessments, PCI DSS audits, and red team assessments.
- Developed a vendor management program for a large health care organization, including implementation of a vendor risk assessment process, standard business associate and non-business associate vendor agreements, and training for contracting staff regarding effective implementation.
- Created a data extraction process for a company serving as third-party administrator to standardize and coordinate the processing of data requests from its self-insured health plan clients and their other contracted vendors.

Privacy Policies and Notices

- Prepared consumer notices for numerous banking institutions under Gramm-Leach-Bliley.
- Revised Notice of Privacy Practices for health care providers and health plans to incorporate revisions under HITECH and the Omnibus HIPAA regulations.
- Created an organized health care arrangement among a group of covered entities, including a Joint Notice of Privacy Practices, to structure a new primary care service model.
- Drafted privacy notices and terms of use for multiple organizations engaged in online retail and e-commerce.

Breach Investigation and Notification

- Analyzed a wide variety of privacy and security incidents occurring within organizations that are covered entities or business associates to determine the probability of compromise to the protected health information and whether notification is required under HIPAA or state law.
- Managed the investigation of a breach at a large physician group that included financial information collected through an online payment portal and online employment applications and provided notifications to affected individuals across 42 states.
- Coordinated the investigation and notification process on behalf of a critical access hospital following the unauthorized access and disclosure of patient records by one of its former employees.
- Participated in the development of notifications on behalf of one of six covered entities affected by a business associate breach that involved collective notification to over three million individuals.
- Managed the incident response of a consumer products firm regarding a breach of customers' personal data from its e-commerce platform, including investigation, response, and notification requirements.

Regulatory Investigations and Litigation

- Resolved an investigation with Office for Civil Rights through voluntary compliance following a breach reported by the hospital after its vendor inadvertently published the financial information of over 8,000 individuals on the internet.

- Responded to inquiries from several state attorney generals related to voluntary breach notifications or consumer complaints regarding privacy or security practices.
- On behalf of a nonprofit organization, resolved an Office for Civil Rights and attorney general investigation following a ransomware attack affecting the organization's computer systems and storage of personal information.
- Defended claims brought by patients alleging privacy violations against hospitals and other health care providers in state court.

Areas of Focus

Breach Investigation and Notification

Swift and detail-oriented responses, allowing clients to minimize interruptions to operations and financial loss. The Spencer Fane Data Privacy and Cybersecurity team provides support to companies in cyber crisis mode to not only meet legal requirements for data breach notifications and disclosures, but also to determine how and why a breach occurred.

Working to enable clients to maintain the trust of their customers, vendors, and other partners, our attorneys:

- **Give each case the individual attention and tailored service needed** to ensure the approach is appropriate based on the needs of the company and the industry involved.
- **Identify the specific details of the incident and apply the necessary resources** to effectively manage the situation from start to finish. We don't make assumptions or pull template policies or procedures.
- **Incorporate national best practice standards**.
- **Provide guidance on incident response plans**, including development and implementation.
- **Analyze breach notification requirements**.
- **Advise on management of notification obligations**.
- **Work with affected business partners**.
- **Help clients resolve resulting regulatory investigations or litigation**.

Cybersecurity Regulatory Investigations and Litigation

Putting safeguards in place so clients are in a position of strength if faced with a regulatory investigation or litigation. When companies face cyber and privacy-related regulatory investigations or litigation, Spencer Fane Data Privacy and Cybersecurity attorneys serve as fierce protectors, working to minimize risk and preserve businesses' reputations by showing they appropriately use and protect customer information.

Whether working proactively or in response to an incident, members of our team:

- **Help identify and manage risk**, by understanding a client's business and overall objectives.
- **Develop strategies to manage a breach** and then effectively resolve related issues – up to and including the litigation process.
- **Defend clients in a wide range of scenarios**. We have a strong track record representing clients in investigations with the Office for Civil Rights (OCR), Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and state regulators such as the attorneys general and Department of Insurance.

Cyber Risk Management

Protecting against breaches and other threats to systems, data, and customer information. The Spencer Fane Cyber Risk Management team guides business leaders through each important phase of the cyber and data risk analysis and management process, giving them confidence that their systems and data will remain secure.

Members of our team:

- **Build out phased plans** that allow companies to quickly address the most critical and immediate risks while also safeguarding against future threats.
- **Build relationships with third-party vendors** for deep assessments of systems.
- **Test incident response plans** through tabletop exercises, and reassess and reformulate plans at regular intervals.
- **Establish a review cycle** – thorough and recurring – to keep policies and procedures up to date.
- **Advise on the purchase of comprehensive cyber insurance**.

We focus on the long-term health of a business, learning the types of work it performs, its customers or consumers, and the data it collects. Our attorneys then identify potential risks and develop a strategic, customized plan to minimize them.

Privacy Management Strategies

Developing sound strategies to safeguard the privacy of patients and customers

The risks companies face in handling personally identifiable information (PII) and protected health information (PHI) continue to increase. The Spencer Fane Privacy Management Strategies team helps organizations in health care, banking, and other industries reach a stronger privacy state by guiding them to best practices for using and disclosing consumer information.

We provide legal counsel aimed at creating a business culture of care and compliance in handling data. Our lawyers:

- **Assess our client's role as they gather information** so that the applicable laws can be identified and incorporated into the privacy strategy.
- **Identify steps to improve** privacy best practices.
- **Develop training regimens and policies** for staff.
- **Create extra value for clients by handling privacy and security matters**, helping business leaders to better understand both how to both protect PII and PHI and handle it appropriately.

Our team employs a proactive approach to privacy management, enabling our clients to prevent unintentional violations of federal and other privacy rules, while also handling the rare but critical intentional violations by an employee.

Privacy Policies and Notices

Translating dense laws and rules into effective and practical policies – tailored to your business. Spencer Fane attorneys help clients across industries create sound privacy policies and notices, allowing business leaders to protect the privacy of those they serve and avoid litigation.

Whether the organization is a health care provider, insurance company, financial institution, e-commerce company, or other business, our team develops customized policies and notices to comply with applicable requirements.

There are no one-size-fits-all solutions for privacy needs. While some firms try to commoditize privacy work, Spencer Fane emphasizes doing what's best for a specific business, investigating and solving data privacy problems and not just relying on templated policies and notices.

Our Data Privacy and Cybersecurity team works closely with our Health Care and Financial Services teams to address the unique needs of organizations in those industries. Our firm's knowledge of both key privacy issues and our clients' businesses allows us to deliver uniquely tailored policies and notices.