pillsbury

Cybersecurity in the Health Care Sector

We live in an increasingly connected world—one that offers a wealth of convenience but also is susceptible to dangerous and reputation-threatening cyberattacks. These malicious acts disrupt critical business operations, impact the bottom line, and have the potential to affect the lives of millions of patients.

Hackers are becoming increasingly sophisticated in their mission, sparing no industry. The complexity and interconnectedness of the health care industry, including advances in medical devices, health information technology, and hospital operation systems, make the sector a highly coveted target. Meanwhile, as global security laws and regulations continue to expand and change, health care organizations must be up to date on trends and regulations, and work with qualified attorneys to remain safe and compliant in the face of cyber concerns.

Threats Landscape

Health care, life science organizations, and those which provide services or infrastructure to them are vulnerable to a variety of cyberattacks. Among the top trending are medical device hijacking and ransomware attacks, which have recently thrown organizations of all sizes into disarray for days to weeks.

- **Malware/Ransomware.** During a malware attack, hackers infiltrate systems and networks via harmful software that is intended to damage or disable the system's components. In the case of ransomware, the perpetrators often encrypt and hold accessed files, demanding a ransom to decrypt the data. Medical devices, which often lack robust built-in security features, are opportunistic back doors into an organization's network.
- **Data breaches.** Next to malware, data breaches are among the most common attacks perpetrated against health care organizations and those that serve them. A single attack can put in jeopardy millions of HIPAA-protected records.

Meanwhile, the growing incidence of attacks and the transition to electronic health records and operations systems have spurred lawmakers to issue new guidance specific to health care organizations. In July 2016, the Department of Health and Human Services released guidance for the health care sector regarding preparation for and response to ransomware attacks. This guidance states that, under HIPAA, a malware or ransomware attack is considered a "security incident," reportable by business associates to their covered entity customers, and will typically be considered a "breach" unless the affected entity is able to demonstrate that there is a low probability of that the privacy or security of protected health information has been compromised.

How Pillsbury Can Help

Pillsbury's Cybersecurity, Data Protection & Privacy and Health Care lawyers work together to help health care organizations prevent and respond to cyber threats.

- **Qualifications.** Recognized by *The Legal 500* as one of the world's foremost privacy and information law practices, Pillsbury's Cybersecurity, Data Protection & Privacy lawyers work with U.S.-based and multinational companies to address privacy requirements, needs and issues in a way that balances thorough compliance with the flexibility to conduct business. Together with our health care industry team, we tap into internal and external networks to pull together the appropriate personnel and resources to assist our clients at a moment's notice.
- **Regulatory.** We have experience with the unique regulatory and compliance obligations imposed on the health care sector. With our public policy experience, we work with U.S. lawmakers for advocacy and lobbying on any cybersecurity-related legislation. We also work with federal and state agencies such as the Centers for Medicare and Medicaid, the U.S. Department of Health & Human Services, and the Food and Drug Administration.
- **Clients.** We routinely help health care clients design and update their policies and procedures to remain compliant with industry regulations and standards. We have represented networks of hospitals and clinics, health plans, management companies, biopharmaceutical companies, medical claims processing companies, and a wide variety of financial services, technology, and telecommunications companies serving the health care industry. Our health care team also has a strong presence in California where we have longstanding relationships with key technology and health care service providers.

Comprehensive Cybersecurity Program

Pillsbury's Health Care Cybersecurity team is able to assist clients with the full spectrum of cybersecurity concerns before, during, and after an attack. We believe prevention is the most powerful tool and deterrent against attacks.

Security breach preparation/prevention

- **Policy Review.** Pillsbury helps clients audit, develop and implement effective data breach response policies and procedures and programs to deter and circumvent eventual attacks. Our team also can help determine whether an organization's cybersecurity products and/or policy are eligible for SAFETY Act protections.
- **Regulatory Compliance Assessment.** We routinely assess our clients' compliance with state and federal statutes that address the collection, use, sharing and protection of personal information.
- **Information Security.** Our attorneys assist clients in evaluating the robustness of their security systems and can make recommendations on third-party data security service providers. We can also help organizations modernize their legacy systems and integrate the world of electronic health records.
- **Training.** In addition to helping with solid policy design and infrastructure security assessments, our attorneys help craft training guides to ensure employees receive regular cybersecurity education to identify threats and ensure records are backed up.

Incident Response

The Pillsbury Team is available to assist with:

- **Reporting and Mandated Disclosures**. When a security incident or data breach occurs, our attorneys can assist clients to assess and comply with their reporting obligations, and coordinate with clients' public response to the events.
- **Litigation.** When a loss or potential loss occurs, our team is available to advise and litigate to enforce clients' coverage rights. If an action is filed, our team brings a wealth of experience to the client's aid, having defended companies of various sizes and industries in class action lawsuits arising from unauthorized disclosure or theft of confidential information.
- **Investigations.** Pillsbury has handled some of the largest data breaches and high-profile cyberattacks and can guide clients in navigating investigations and working with third-party forensic companies.
- **Recovery.** In addition to helping with the required disclosures, our attorneys can help organizations recover from an attack by conducting "post-mortem" assessments to confirm the root cause(s) of a breach. We also help insure that vital encryption and application security features are implemented promptly to mitigate the risk of recurrence.

Cyber Insurance

With the proliferation of regulations governing data security and privacy, it has become common for companies that handle sensitive information to insure themselves against data security and privacy claims and investigations. A large and quickly-growing market has evolved for insurance that is specifically designed to cover these risks—marketed under names like "privacy breach insurance," "network security insurance," and "cyber insurance."

Health care companies, which handle legally protected information, increasingly view this new kind of insurance as a cornerstone of their risk management programs. We have deep experience in helping clients structure and negotiate insurance programs to protect themselves from data and security breaches, and recover from their insurers on cyber claims—even when they lack insurance policies specifically designed to cover these risks.

Representative Matters

Recent privacy and cybersecurity experience for health care and life sciences companies includes:

Investigations

- Advised a company in FTC investigation involving a data breach involving customer financial and medical information.
- Counseled a health insurance company in its investigation into a security breach that may have compromised personal information of 1.9 million current and former customers.
- Represented a health facility in handling a data security breach after storage tapes and a laptop containing more than 300,000 people's personally-identifiable information were stolen from an employee's car.
- Represented a number of other health care providers in connection with their reporting and remediation activities following a variety of breaches involving electronic and non-electronic protected health information.

Policy Review

- Represented a major health care system in reviewing its cybersecurity policies and procedures, as well as submitting those policies to a federal agency in order to obtain liability protections in the event of a cyber-attack.
- Created vendor policies and services agreement for a medical supplies company to protect sensitive client information.

Litigation/Class Action

- Represented a bank, a retailer, a restaurant and other companies in connection with the massive Anthem health information data breach.
- Represented a hospital in litigation related to disclosure of medical information.
- Defended an academic medical center against a variety of privacy claims, including alleged violation of the California Confidentiality of Medical Information Act, because of information disclosed to the patient's insurer.
- Defended a major hospital in class action lawsuits arising from unauthorized disclosure of patient health information by a hospital vendor.
- Represented a health care company in a class action lawsuit seeking damages for the theft of client medical and financial information, including claims for violation of California's Confidentiality of Medical Information Act and Unfair Competition Law.

Cyber Insurance

- Represented numerous health care, professional services, and medical services companies in successful prosecution claims for insurance coverage arising out of data security and privacy breaches, including some of the largest reported claims.
- Successfully represented a national managed care organization in recovering under its cyber and professional liability insurance policies for data security breach lawsuits seeking billions of dollars in damages.
- Represented a major university research hospital in recovering under cyber and D&O policies for an eight-figure data security breach claim.
- Represented a stem cell bank in recovering under cyber insurance for ten-figure privacy breach claim.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 877.323.4171

pillsburylaw.com

Austin • Beijing • Hong Kong • Houston • London • Los Angeles • Miami • Nashville
New York • Northern Virginia • Palm Beach • Sacramento • San Diego • San Diego North County
San Francisco • Shanghai • Silicon Valley • Taipei • Tokyo • Washington, DC