

Aaron T. Maguregui

Partner

amaguregui@foley.com

Tampa

813.225.4129



Aaron Maguregui is a health care lawyer who advises innovative health care and technology companies on complex compliance, cybersecurity, data governance, data privacy, and risk management matters. Working with leading health care insurers, government-sponsored managed care organizations, health care providers, and technology companies, he delivers pragmatic legal advice and action-oriented solutions guidance to help clients reach their goals and objectives.

Aaron provides advice and counsel in all phases of cybersecurity attacks and data breach events. He works closely with chief information security officers, compliance officers, general counsels, and incident response teams to prepare them for cyberattacks and data loss events. By using preventative and anticipatory strategies, he advises and prepares health care companies to appropriately, efficiently, and successfully communicate, respond, and recover from all types of security incidents. Aaron has developed and implemented best-in-class cyber practices, including:

- Data privacy and information security frameworks, governance architecture, and response programs
- Written privacy and cybersecurity policies and procedures
- Board and executive training and education modules on cybersecurity preparedness and ongoing enterprise risk management activities
- Cybersecurity and privacy insurance coverage review and negotiation
- Negotiation and drafting of data agreements with vendors, including cybersecurity, risk-sharing, and indemnification
- Leading and managing privacy and security breach investigations and corrective actions, including reports to federal and state regulators
- Customized table-top exercises and penetration testing to simulate actual cybersecurity incidents

Aaron advises health insurers, providers, digital health entrepreneurs, and technology companies on regulatory issues and contract negotiations related to compliance, cybersecurity, data privacy, and data

governance. He routinely advises companies on the Health Insurance Portability and Accountability Act; text messaging and the Telephone Consumer Protection Act; the EU's General Data Protection Regulation; the California Consumer Protection Act; and other federal, international, and state privacy and security laws, regulations, and directives. He also helps health companies refine their big data business strategy, realistically assess risk, and achieve their goals.

Prior to joining Foley, Aaron was in-house counsel at one of the country's largest publicly traded managed health care insurance organizations, helping lead the company's Privacy & Information Security Department and build its security incident response team. Aaron has managed dozens of privacy and security incidents; successfully resolved multiple publicly reported data breaches; and led responses to inquiries, complaints, and investigations from various federal and state government agencies, including the Office of Civil Rights, the Department of Justice, the Centers for Medicare & Medicaid Services, the Department of Health & Human Services Office of the Inspector General, state Medicaid agencies, and state attorney generals offices. Aaron also counseled the company in obtaining HITRUST certification, a highly coveted certification that provides assurances to all stakeholders of the company's security practices.

Aaron is a Certified Information Systems Security Professional, a global standard and essential industry credential accredited by the International Information Systems Security Certification Consortium. He is a member of the Privacy, Security, & Information Management Practice Group and Telemedicine and Digital Health Industry Teams.

The Biggest Challenge To the Telemedicine Industry

Representative Experience

- Counseled a publicly traded health insurer subject to a cyberattack in its incident response and communications with multiple government regulatory agencies. The advice included interfacing with various state officials across multiple states and law enforcement to explain the dynamics of the attack, the company's response plan, and the impact to affected individual members. The work allowed the company to demonstrate its response capabilities to the satisfaction of regulators and showcase its ongoing compliance with its contractual obligations and commitment to data security.
- Advised Medicaid and Medicare managed care organization in development and implementation of an online beneficiary portal. The company sought a secure manner to interface with its beneficiaries and provide an easily accessible alternative to traditional customer service methods. Successfully assisted the company with privacy and security concerns and navigated the regulatory approval process with multiple state Medicaid agencies, allowing the company to provide real-time information to beneficiaries in a secure and cost-effective manner.
- Represented a health insurer in a multi-state data privacy breach caused due to a business associate's mail processing error. Counseled the insurer in its responses to multiple government agencies and the media notification process. The advice enabled the insurer to responsibly respond to its members privacy concerns and alleviate any future abrasion with regulators.

- Provided regulatory counseling and legal advice for Medicaid-managed care organization seeking to improve its telephone and text message outreach communications to its beneficiaries. Helped company navigate the Telephone Consumer Protection Act, comply with its contractual restrictions under Medicaid rules, and close care gaps. The work allowed the company to substantially increase its outreach capabilities, positively impact coordination of care efforts, and assist in the effort to close member care gaps.
- Counseled publicly traded company in its reporting of cybersecurity posture and ongoing information security efforts to board of directors. The company was seeking to share evidence of its cybersecurity preparedness with its board of directors. Assisted the company in the development and rollout of a cybersecurity dashboard and enterprise-wide cybersecurity framework that showcased the company's performance. The company was able to communicate to its leadership through key performance metrics that evidenced a strong focus on cybersecurity readiness.
- Advised a government-sponsored health plan in the company's development and implementation of its privacy and cybersecurity framework. The company was seeking to create scalable processes and procedures in order account for future growth. The work enabled the company to rollout policies and procedures that allowed for the efficient integration of acquisitions and the ability for the new entities to seamlessly incorporate themselves into the established framework.

“Foley is the premier firm for telehealth counsel.”

“A market leader in telemedicine issues.” “This is the Dream Team.”

– Chambers USA: America's Leading Business Lawyers (2020 – 2021)

Presentations and Publications

- Co-author, “HHS Updates Pixels and Trackers Guidance for HIPAA Regulated Entities,” *Health Care Law Today* (March 19, 2024)

Affiliations

- Member of the International Association of Privacy Professionals
- Member of the American Health Lawyers Association
- Member of the Health Law Section of the Florida Bar

Community Involvement

- Member of the board of directors for the Jason Ackerman Foundation/Because of Jason

Sectors

- [Artificial Intelligence](#)
- [Health Care & Life Sciences](#)



FOLEY & LARDNER LLP

- Innovative Technology
- Telemedicine & Digital Health

Practice Areas

- Behavioral Health
- Cybersecurity
- Health Care
- Health Care Regulatory
- Intellectual Property
- Privacy, Security & Information Management
- Technology Transactions, Cybersecurity, and Privacy

Education

- Indiana University Maurer School of Law (J.D., 2010)
- University of South Florida (B.A., 2007)

Admissions

- Florida
- Washington, D.C.