21 November 2014

Practice Group:

Commercial Disputes

Class Action Litigation Defense

Cyber Law and Cybersecurity

Health Care

Connecticut Supreme Court Issues Decision That Could Expand State Law Liability in Data Breach Class Actions for Businesses Subject to HIPAA

U.S. Commercial Disputes Alert

By Nicholas Ranjan and Anna Shabalov

Health care providers have not escaped the recent proliferation of data breach class actions, but plaintiffs generally have been unsuccessful in bringing claims based on the Health Insurance Portability and Accountability Act ("HIPAA") when their protected health information ("PHI") has been compromised.[1] Recently, however, the Connecticut Supreme Court, in *Byrne v. Avery Center For Obstetrics and Gynecology PC*, No. 18904 (Conn. Nov. 11, 2014), held that although there is no direct cause of action under HIPAA, a plaintiff can still pursue state law claims based on the standards for PHI security announced in HIPAA regulations. Although it remains to be seen how broadly this decision's reasoning will be applied or if it will be applied by courts outside of Connecticut, such a decision poses the potential of significantly increasing class action exposure for entities subject to HIPAA. Potential targets include not only health plans and health care providers but also a range of companies providing services to those plans and providers and employers with self-insured plans or on-site clinics.

Byrne v. Avery Center For Obstetrics and Gynecology PC

In *Byrne*, the Connecticut Supreme Court held that HIPAA did not preempt, and could provide the applicable standard of care for, state common-law negligence-based torts. However, the court reserved the question of whether such tort claims were otherwise viable. The plaintiff, Emily Byrne, received gynecological and obstetric care from the Avery Center. Ms. Byrne specifically instructed the Avery Center not to disclose her PHI to a particular individual, Andro Mendoza, who had filed paternity actions against Ms. Byrne. Mr. Mendoza subsequently subpoenaed the Avery Center for Ms. Byrne's medical records. The Avery Center complied and provided Mr. Mendoza with the records, without informing Ms. Byrne about the subpoena, moving to quash it, or appearing in court. Ms. Byrne alleged that Mr. Mendoza then used the information in her records to harass and threaten her, filing numerous civil actions against her, her attorney, her father, and her father's employer. Ms. Byrne filed suit against the Avery Center for the unauthorized disclosure of her PHI, alleging breach of contract, negligence, negligent misrepresentation, and negligent infliction of emotional distress.

On appeal from a trial court decision dismissing the complaint's negligence-based claims, the Connecticut Supreme Court addressed two issues: (1) whether HIPAA's preemption of "contrary" state law precluded claims for negligence and negligent infliction of emotional

[1] *See, e.g.*, *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 469 (D.N.J. 2013) (finding plaintiff lacked standing where alleged injury was loss of information in violation of HIPAA).

Connecticut Supreme Court Issues Decision That Could Expand State Law Liability in Data Breach Class Actions for Businesses Subject to HIPAA

distress where a health care provider breached patient privacy in the course of complying with a subpoena, and (2) whether HIPAA could inform the standard of care applied to common-law negligence. Looking to statutory and regulatory text, history, and intent and citing a handful of cases, the court reinstated Ms. Byrne's negligence-based claims, concluding that HIPAA was not meant to preempt state law tort actions for the unauthorized release of PHI. The court reasoned that such actions, rather than precluding, conflicting with, or complicating HIPAA compliance, in fact supported HIPAA's goal of preventing wrongful disclosure of PHI. The court further stated that HIPAA-mandated procedures could serve as the standard of care in negligence-based actions if those procedures were common practice among health care providers in the state.

Byrne's Implications for PHI Data Breach Class Actions

Courts have broadly recognized that HIPAA lacks an express or implied private right of action and preempts "contrary" state laws. As a result, to date, class action plaintiffs in data breach cases have been largely unable to bring causes of action based on a defendant's failure to comply with HIPAA regulations. Although *Byrne* did not involve a class action, the decision is likely to be used by class action plaintiffs as an alternative method of enforcing HIPAA standards against defendants. Although *Byrne*'s holding was limited to negligence and negligent infliction of emotional distress, its broad reasoning could be applied to find no HIPAA preemption of other claims favored by class action plaintiffs in data breach cases, including torts such as invasion of privacy and state statutory violations. Additionally, *Byrne* could provide a basis for class action plaintiffs to argue that other federal privacy statutes that lack a private right of action should be applied as standards of care for state-law claims.

Byrne may have significant impact not only on the exposure of health care plans and providers, but also on the exposure of other companies that have only relatively recently come within HIPAA's orbit. In 2009, the Health Information Technology for Economic and Clinical Health ("HITECH") Act extended the bulk of HIPAA's security provisions to "business associates" of covered health plans and providers. Business associates are entities (and their sub-contractors) who provide services that require them to handle PHI and might include, for instance, third-party administrators, vendors of electronic health records systems, law firms, accounting firms, and consultants. Under the HIPAA Security Rule, this broad array of companies must maintain "reasonable and appropriate" administrative, technical, and physical safeguards for electronic PHI. Failure to do so may result in government enforcement and, now, potential class action liability.

Companies that are or may be subject to HIPAA should closely watch if, and how, *Byrne*'s reasoning is applied outside of Connecticut, particularly in the context of data breach class actions.

Authors:

Nicholas Ranjan
nicholas.ranjan@klgates.com
+1.412.355.8618

Anna Shabalov
anna.shabalov@klgates.com
+1.412.355.8966

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates comprises more than 2,000 lawyers globally who practice in fully integrated offices located on five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.