Connecticut AG Sues Health Plan for Security Breach under New HITECH Act and State Consumer Protection Laws, Signaling New Enforcement Landscape for Health Care Providers

New HIPAA Enforcement Authority

Beginning February 17, 2009, HITECH authorized state Attorneys General to file suit, on behalf of their residents, to enforce the privacy and security protections of HIPAA. State Attorneys General may seek injunctive relief, monetary damages of $100 per violation with a limit of $25,000 for violations of an identical requirement per year, and reasonable attorney fees. In addition, HITECH also instituted a tiered increase in the amount of penalties which may be imposed by HHS for HIPAA violations, depending upon the nature and extent of the violation and harm. The highest tier imposes a penalty of $50,000 per violation, not to exceed $1.5 million for violations of an identical requirement per year. These penalties are in addition to those which may be sought by state Attorneys General under state consumer protection and data breach notification laws.

Background of Breach

On or about May 14, 2009, Health Net of the Northeast Inc. (Health Net) learned that a portable computer disk drive containing information relating to approximately 1.5 million individuals, 446,000 of whom were residents of Connecticut, had disappeared. The drive contained 120 different types of documents and included both personal information and protected health information, thereby triggering notification obligations under HIPAA as well as state data breach statutes. A computer forensic consulting firm hired by Health Net issued a report that indicated that the information on the portable drive was not encrypted or otherwise protected from access by unauthorized persons. Six months later, on November 18, 2009, Health Net posted a notice on its website regarding the breach, and on November 30, 2009, began sending letters directly to its enrollees.

Details of Complaint

Attorney General Blumenthal filed a complaint in federal court, on behalf of the residents of Connecticut, alleging violations of HIPAA and state consumer protection and data breach notification statutes. The complaint alleges the following failures by Health Net:

- The failure to notify properly and promptly the Connecticut Attorney General, and other state agencies, of the missing protected health information and personal information;
- The failure to encrypt the protected health information and personal information on the computer drive, in "deliberate disregard of its policies and procedures and requirements under federal law";
- The failure to create a log file of the portable drive before transporting it between California and Connecticut, which increased the risk of disclosure of the protected health information and personal information to unauthorized individuals and delayed efforts to safeguard the data or otherwise mitigate the data breach;

- The failure to promptly notify affected individuals of the security breach; and
- The failure to design and implement policies and procedures that appropriately and reasonably safeguard protected health information and to supervise and train its workforce on safeguarding protected health information and personal information.

The complaint alleges 12 violations of HIPAA for failure to comply with certain standards, requirements, and implementation specifications, including: failure to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to a covered entity; failure to protect against any reasonably anticipated threats or hazards to the security of electronic protected health information; and failure to implement policies and procedures to prevent, detect, contain, and correct security violations.

The complaint also alleges that Health Net willfully violated the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110b, by unreasonably delaying the disclosure of the breach of security.

The State seeks a preliminary and permanent injunction prohibiting Health Net from committing any further violations of HIPAA (as amended by HITECH and the HHS regulations promulgated thereunder), or Connecticut state law. The Complaint also seeks statutory damages under HIPAA (as amended by HITECH), and additional civil penalties up to $5,000 per each willful violation of the Connecticut Unfair Trade Practices Act.

Conclusion

Connecticut's lawsuit against Health Net signals a new enforcement landscape for health care providers facing the continuing challenge of safeguarding patient health and personal information and effecting appropriate incident responses in the event a security breach occurs. Prior to the enactment of HITECH, and despite the authority to do so, HHS and the Centers for Medicare & Medicaid Services often did not seek civil monetary penalties for violations of the HIPAA privacy or security rule, instead focusing their efforts on working with health care providers short of enforcement action to enhance compliance with those rules.

The state Attorneys General, however, approach data security from an enforcement perspective, customarily taking aggressive action against companies who have suffered data breaches. The state Attorneys General will focus both on *pre-breach conduct*—what protections were in place prior to the breach to safeguard data and detect security breaches—and *post-breach conduct*—how the entity responded upon discovering the breach, including how promptly it notified regulators and affected individuals.

The HITECH amendments to HIPAA, particularly the enforcement authority afforded state Attorneys General, have raised the stakes for data security incidents. Pursuant to the new civil monetary penalty provisions under HITECH, there is increased potential monetary exposure for health care providers resulting from a breach of data. Given the statutory damages provisions, and the high priority state Attorneys General afford data security matters, investigations and lawsuits by state Attorneys General in the wake of breaches of protected health and personal information are likely to increase.

In the face of this regulatory environment, health care providers should review their information security programs to reduce the risk of breach and develop incident response programs so that any breach that does occur is promptly detected and mitigated, and any notification obligations promptly satisfied. If a breach does occur, health care providers should involve counsel early, given the increased chance of enforcement action by state Attorneys General and federal health care regulators.

If you would like to learn more about the issues raised by this update, please contact your usual Ropes & Gray attorney.