EPSTEIN BECKER GREEN
health care & life sciences
CLIENT ALERT

Beyond HIPAA: New Jersey Law Requires Encryption of Personal Data by Health Insurance Carriers

by Mollie K. O'Brien

January 2015

In response to data breaches that have occurred across the United States, several of which involved the theft of laptop computers, beginning August 1, 2015, health insurance carriers in New Jersey will be obligated to do more to protect patient information than simply comply with the federal Health Insurance Portability and Accountability Act ("HIPAA"). A new law, signed by Governor Chris Christie on January 9, 2015, specifically requires health insurance carriers to encrypt electronically gathered and stored personal information.

The key terms in the law are defined as follows:

- "Health insurance carriers" means "an insurance company, health service corporation, hospital service corporation, medical service corporation, or health maintenance organization authorized to issue health benefits plans in this State."

- "Personal information" means "an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number of State identification card number; (3) address; or (4) identifiable health information."

Although New Jersey already has a law requiring notification to individuals in the event of a data breach of their personal information, the new law is aimed at preventing breaches in the first place and further reducing the risks of misappropriation and identity theft.

In addition, while HIPAA mandates the protection of personal information, HIPAA suggests encryption only when sufficient risk is identified and encryption is reasonable. New Jersey's new law goes a step further by mandating that *all* computerized data be rendered "unreadable, undecipherable, or otherwise unusable by an unauthorized person." The law applies to "end user computer systems" (e.g., desktop and laptop

computers, tablets, and mobile devices), and to "computerized records transmitted across public networks."

With the new law, password-protected user access will no longer be legally sufficient security for protecting personal information. Failure to comply will be deemed a violation of New Jersey's Consumer Fraud Act, which can result in treble damages.

What Should New Jersey Health Insurance Carriers Do to Prepare?

Health insurance carriers inside New Jersey should do the following:

- Revise existing risk assessment criteria and modify any protocol that permits discretion with regard to data protection.
- Confirm that no end-user computer system, including laptops or mobile devices, contains unencrypted personal information.
- Establish protocols and procedures to ensure that all personal identification on end-use computer systems is secured by encryption, regardless of the potential difficulty, cost, or maintenance of such a program.
- Establish routine audits/testing to confirm and ensure the integrity of the encryption programs once installed. Scans should be performed to determine whether hidden or unknown repositories of personal information (e.g., email servers) are contained within the environment.
- Review any "Bring Your Own Device" policy and procedures to ensure that employees' personal devices used for business have the necessary encryption of protected personal information.

What Should Health Insurance Carriers Outside New Jersey Do?

Health insurance carriers outside New Jersey should stay tuned. While a similar law already exists in Massachusetts, it would be reasonable to forecast that other states will follow suit in the near term.

The federal government also has taken heed. As recently as last week, it was reported by the Centers for Medicare & Medicaid Services that the agency is adding layers of encryption to the HealthCare.gov website to protect enrollees.

* * *

This Client Alert was authored by **Mollie K. O'Brien***. For additional information about the issues discussed in this Client Alert, please contact the author or the Epstein Becker Green attorney who regularly handles your legal matters.*

About Epstein Becker Green

Epstein Becker & Green, P.C., established in 1973, is a national law firm with approximately 250 lawyers practicing in 10 offices, in Baltimore, Boston, Chicago, Houston, Los Angeles, New York, Newark, San Francisco, Stamford, and Washington, D.C. The firm's areas of practice include health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. For more information, visit www.ebglaw.com.

If you would like to be added to our mailing list or need to update your contact information, please contact Lisa C. Blackburn at lblackburn@ebglaw.com or 202-861-1887.