Preparing for a Data Breach - What to Know about Breach Notification

02.13.2015

Data breaches are at the forefront of the news, and many companies, including those dominant in the health care industry, have found themselves front and center in the headlines. Although recent news stories have focused their attention on attacks on major, nationwide companies resulting in massive data breaches, a data breach can be as simple and small as a lost or stolen laptop or improper disposal of data in either electronic or paper form. Data breaches are all too common, and all companies, especially health care providers, health plans, and others involved in the health care industry should be familiar with the data breach requirements in the states in which they operate.

Nationwide, companies that qualify as ?covered entities? under the federal Health Insurance Portability and Accountability Act of 1996 (?HIPAA?) must comply with the breach notification requirements set forth in 45 C.F.R. § 164.400 et seq. when ?protected health information? is compromised as a part of a breach.

Under HIPAA, a breach occurs when unauthorized access, use or disclosure compromises the privacy or security of protected health information maintained by a covered entity or a covered entity?s business associate (e.g., vendor or subcontractor). In fact, a breach is presumed where there is an unauthorized use or disclosure unless a formal risk assessment performed by the covered entity concludes there is a low risk that the information was compromised. *See* 45 C.F.R. § 164.402.

Upon identification of a breach, the covered entity must notify all individuals whose information is reasonably believed to have been compromised as soon as possible (but no later than 60 days) after discovering the breach. The covered entity must also notify the Secretary of the Department of Health and Human Services and, for certain large breaches, the media. A business associate is responsible for notifying the covered entity of a breach discovered by that business associate. *See* 45 C.F.R. § 164.404-410. Failure to comply with these breach notification requirements constitutes a violation of HIPAA, which can carry significant monetary penalties.

In addition, many states have their own individual data breach laws. In Virginia, only State entities (including State boards, bureaus, commissions, political subdivisions and governing bodies, and

companies primarily funded by State money) have responsibility to notify Virginia residents of the compromise of certain of their computerized medical data (*see* § 32.1-127.1:05).

However, Virginia has a more general data breach statute, Va. Code §18.2-186.6, that provides for breach notification procedures for breaches involving ?unencrypted or unredacted personal information? held in a computerized database that has resulted or could potentially result in identity theft or fraud. Under this statute, ?personal information? includes the first name or first initial and last name in combination with an SSN, state ID number (such as a driver?s license number), or financial account, credit card or debit card number (and any information that would allow access to the financial account, such as a username and password). Although this statute focuses primarily on financial information and identity theft, it could potentially apply to health care entities whose breached data meet the requirements of the statute.

The company facing the data breach must notify the affected individuals and the Attorney General of Virginia ?without unreasonable delay.? Extremely large breaches of over 1,000 individuals require notification of credit reporting agencies as well. A violation of this law can result in a penalty levied by the Attorney General of up to $150,000, and the statute does not preclude civil suits brought by affected Virginia residents. It is important to note that the State Corporation Commission has sole jurisdiction to enforce violations of the law for entities regulated by its Bureau of Insurance.

As data breaches become more common, the health care industry will be increasingly subject to scrutiny over their privacy and security practices and their data breach response. Health care providers, health plans, and other companies operating in the health care industry should be aware of the data breach laws and regulations in the states in which they operate to ensure that they can efficiently and effectively respond to a breach if it happens to them.

Related People

Related Services

- Health Care
- Data Protection & Cybersecurity