Proskauer

Responding to the Anthem Cyber Attack

February 6, 2015

Anthem Inc. (Anthem), the nation's second-largest health insurer, revealed late on Wednesday, February 4 that it was the victim of a significant cyber attack. According to Anthem, the attack exposed personal information of approximately 80 million individuals, including those insured by related Anthem companies. Anthem has reported that the exposed information includes member names, member health ID and Social Security numbers, dates of birth, addresses, telephone numbers, email addresses and employment information. The investigation of the massive data breach is ongoing, and media outlets have reported that class action suits have already been filed against Anthem in California and Alabama, claiming that lax Anthem security measures contributed to this incident.

Employers, multiemployer health plans, and others responsible for employee health benefit programs should take note that the Health Insurance Portability and Accountability Act (HIPAA) and state data breach notification laws may hold them responsible for ensuring that certain notifications are made related to the incident. The nature of these obligations will depend on whether the benefits offered through Anthem are provided under an insurance policy, and so are considered to be "fully insured," or whether the Anthem benefits are provided under a "self-insured" arrangement, where Anthem does not insure the benefits, but instead administers the benefits. The most significant legal obligations on the part of employers, multiemployer health plans, and others responsible for employee health benefit programs will apply to Anthem benefits that are self-insured.

Where notifications must be made, the notifications may be due to former and present employees and their dependents, government agencies, and the media. Where HIPAA applies, the notifications will need to be made "without unreasonable delay" and in any event no later than 60 days after the employer or other responsible party becomes aware that the breach has affected its own health plan participants. Where state data breach laws apply, notifications generally must be made in the most expedient time possible and without unreasonable delay, subject to certain permitted delays. Some state laws impose outside timeframes as short as 30 days. Under the state laws, reporting obligations on the part of employers, multiemployer health plans, and others responsible for employee health benefit programs will generally turn on whether they, or Anthem, "own" the breached data. Since the state laws apply to breaches of data of their residents, regardless of the states in which the compromised entities and data owners are located, and since former employees and dependents could reside anywhere, a comprehensive state law analysis is required to determine the legal requirements arising from this data breach. Fortunately, depending on the circumstances, some (but not all) state data breach notification laws defer to HIPAA breach notification procedures, and do not require additional action where HIPAA applies and is followed.

As potentially affected parties wait for confirmation from Anthem as to whether any of their employees, former employees or their covered dependents has had their data compromised, we recommend that affected parties work with their legal counsel to determine what their responsibilities, if any, might be to respond to this incident. Among other things, for self-insured arrangements, HIPAA business associate agreements and other contracts with Anthem should be reviewed to assess how data breaches are addressed, whether data ownership has been addressed by contract, and whether indemnification provisions may apply. Consideration should also be given to promptly reaching out to Anthem to clarify the extent to which Anthem will be addressing notification responsibilities. Once parties are in a position to make required notifications, we also recommend that companies consult with legal counsel to review the notifications and the distribution plans for those notifications to assure that applicable legal requirements have been satisfied.

Proskauer's employee benefits, health care, and privacy and security lawyers are available to assist with your response to this matter.

Related Professionals

- **Ellen H. Moskowitz**
  Senior Counsel