NewsOK Q&A: Healthcare data hacking likely to require new state laws

Published: March 9, 2015
Click to see full story – Across the U.S., more state laws are likely for mandated encryption of health data

Phillips Murrah's Joshua Edwards discusses healthcare data hacking – Hacking may bring more state laws, encryption of health data

Josh Edwards

Q: How serious of a problem are healthcare data hacks for insurance companies, employer health plans and others in the healthcare industry?

A: Last month Anthem Inc., the second-largest health insurer in the U.S., announced hackers had stolen personal information, including names, dates of birth, member ID/Social Security numbers, addresses, phone numbers, email addresses and employment information of up to 80 million individuals

covered under its health plans. The Anthem breach alone affects one out of every four Americans. This data can be sold on the black market and then used by identity thieves to commit financial crimes, as well as fraudulently obtain medical services and prescriptions. The FBI previously warned insurers and other companies in the healthcare industry that their data security systems lagged behind those of the financial and retail sectors and that they were particularly susceptible to cyberattacks given the value of such data to cybercriminals.

Q: What federal and state laws govern the security of healthcare data and a company's obligations after discovery of a breach?

A: The primary federal law is the Health Insurance Portability and Accountability Act (HIPAA), which was amended in 2009 by the Health Information Technology for Economic and Clinical Health Act specifically to address electronic transmission and storage of protected health information (PHI). HIPAA governs the privacy and security of an individual's PHI and requires certain kinds of technological safeguards to protect against unauthorized use and disclosure. In addition to HIPAA, earlier this year New Jersey passed a law requiring health insurers to encrypt all electronically-stored personally identifiable information of New Jersey residents, and it seems likely we will see similar laws passed by other states as well. HIPAA also requires a company to notify affected individuals after discovering a breach of PHI. Forty-seven states also have their own breach notification laws, each of which have their own unique content and timing requirements.

Q: How does an insurer's data breach impact employers who use the insurer for their health plans?

A: Events such as the Anthem breach affect not only the insurer, but also companies that partner with the insurer to provide health coverage to their employees. For companies with

a fully-insured health plan, the insurer will be a “covered entity” under HIPAA and have primary responsibility for protection of PHI and compliance with the breach notification requirements. However, for self-insured health plans, an insurer serving as a third-party administrator will be considered a “business associate” under HIPAA, meaning primary responsibility for protecting PHI and notifying affected individuals and government agencies would fall to the employer. Regardless, employers should have a plan to address such concerns and keep employees informed.

Q: What should insurers and employers do upon discovery of a breach of healthcare data?

A: After a breach, both insurers and employers should review their contracts, including any business associate agreements, to determine their relative responsibilities as well as any indemnification rights and obligations. It’s also essential for both parties to know their duties under HIPAA and state breach notification laws so that compliant and timely notifications can be crafted and delivered to affected individuals and applicable federal and state agencies. Finally, a plan should be implemented for keeping affected individuals informed of the ongoing investigation, as well as strategies for protecting against identity theft and credit monitoring options that may be available.

Joshua L. Edwards, a Director and the Transactional Practice Group leader, is a corporate attorney whose business practice includes representing clients in a variety of commercial transactions across a number of industries, with an emphasis in the restaurant, insurance and real estate industries.