Cooley

September 28, 2015

Earlier this month, a California jury found the University of California, Los Angeles Health System (UCLA) not liable for damages that allegedly resulted when a medical office assistant, Alexis Price, improperly accessed and disclosed plaintiff Norma Lozano's medical records. Price, along with other staff in a UCLA affiliated medical office, had received credentials to access patient information from a physician, Dr. John Edwards. Price then used these credentials to view and take photos of Lozano's information, which she shared with others, including Lozano's ex-boyfriend (and Price's husband). Lozano claimed that her privacy was violated and such violation caused her to suffer emotional harm, and she thus sought $1.25 million from UCLA. She initially named Edwards as a defendant in her lawsuit as well, but Lozano and Edwards settled out of court.

Jury decision

After a short period of deliberations, the jury found that UCLA was not responsible for the improper access to and disclosure of Lozano's records. Jurors who spoke about the decision stated that they were persuaded by testimony from experts who concluded that UCLA's privacy protections were consistent with industry standards. The jurors were unwilling to hold UCLA responsible for an individual's poor judgment.

Practical considerations

From a general perspective of entities concerned about data breaches, this decision sets at least some precedent for limits on a plaintiff's ability to recover in situations where an employee has authorized access to information but exceeds that authorized access to engage in activities that could be privacy or security violations. It took the jury only an hour to decide that since UCLA did not release the plaintiff's records, it would not be liable for the alleged harm. This would seem to indicate that the mechanisms in place at UCLA (including a secondary procedure called "break the glass" for certain high priority patients) were considered by the jury to be adequate under the circumstances. The "break the glass" process involves the imposition of a second set of authentication requirements in certain cases, including entering a password a second time and specifying a reason for viewing the records. This is most frequently used for situations involving celebrities or others whose information might be of exceptional interest. Such a mechanism would be a deterrent to casual perusal of records but likely would not deter a determined entity who has a password that allows access. Perhaps the only thing that would have prevented this situation would have been a biometric authentication factor, which isn't viewed as a current industry standard for this type of access.

Other health systems and providers will likely view this case as a victory, since in determining responsibility, the jury focused on institutional controls over which UCLA had authority as opposed to rogue actions of individual employees. However, it is important to keep in mind the distinction between a private right of action for a privacy violation and claims under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires Covered Entities, such as UCLA, to train all members of the workforce, monitor their access of patient data, maintain access protections, and adopt other safeguards to limit the likelihood of an employee improperly using or disclosing patient information. In the event that the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) investigates Price's actions as a violation of HIPAA, UCLA may potentially face a different result. Price may also potentially face individual liability under HIPAA for willfully disclosing patient information with the intent to cause malicious harm.

Given the abundance of recent litigation and enforcement activity regarding the improper use or disclosure of patient data, entities such as providers and health plans that regularly interact with such data should ensure that they have taken legally required and best practice actions to safeguard the sensitive information in their possession or control. Regular employee training, keeping up to date with technical safeguards, and routinely conducing risk assessments to locate and address security vulnerabilities are just a few steps that such entities should be taking on a consistent basis. Such proactive steps can help to lessen the risk of significant fines, legal fees, and negative publicity in the event of a breach of patient data.

Our Health Care & Life Sciences Regulatory practice group works closely with our Privacy & Data Protection practice group to track these and other issues involving healthcare privacy and cybersecurity. We can provide

you with additional information or insights, tailored to your or your organization's needs.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090