THE
NATIONAL LAW REVIEW

How Employers Can Handle Their Biggest Threat to Data Privacy, Their Employees

Wednesday, June 27, 2018

Article By Dickinson Wright PLLC
Sara H. Jodka Healthcare Legal News

Communications, Media & Internet
Health Law & Managed Care
Labor & Employment
All Federal

Given the ever-expanding landscape of privacy laws and regulations, employers are becoming increasingly aware that they are responsible for data breaches caused by their employees. When looking to formally put obligations upon employees to modify employee conduct, employers tend to start with policy, such as in an employee handbook to allow a means of internal discipline, and move to contractual obligations, such as confidentiality/non-disclosure agreements to allow a means for criminal/civil legal penalty. What does this mean in the employment law context in terms of disciplining employees, and what can employers do to keep employees from exposing protected/confidential data? The two case examples discussed below shed some light.

With respect to employers that have privacy requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the policy requirements have long been in place and can help guide other employers who may not have such regulated privacy requirements.

Take for example a matter that finalized in June 2018 with the New York State Education Department suspending a nurse practitioner's (NP) license for violating the privacy of patients by providing their contact information to her new employer. Come to find out, back in April 2015, the NP had taken a spreadsheet containing the personally identifiable information of approximately 3,000 patients of her former employer and gave the information to her new employer. Not surprisingly, the NP was not supposed to have the spreadsheet and her having it, not to mention disclosing it to her new employer, constituted a data breach under HIPAA. The privacy violation was uncovered after several patients complained to the former employer's hospital about being contacted by the new employer about changing healthcare providers.

The Department of Health and Human Services' Office for Civil Rights (HSS OCR) investigated the matter and fined the former employer. While criminal penalties were not pursued against the NP, the matter was investigated by the New York State Education Department which suspended the NP for 12 months. The NP also faces 2 years of probation when she returns to practice.

In an even more recent case, Terrell v. Main Line Health, Inc., Case No. 18-0702 (E.D. Pa. June 1, 2018), Terrell worked for Lankenau Hospital since 1974 and had been the operating room secretary for 35 years. Lankenau Hospital was a "covered entity" meaning it was subject to the Security and Privacy Rule promulgated under HIPAA and required to protect the privacy, security and confidentiality of employee information and patient health information. In line with HIPAA's requirements, Lankenua implemented a "fair warning" privacy monitoring system that used algorithms to monitor and analyze instances of record access to identify any access that lacked the appropriate legitimate business purpose.

Terrell was eventually terminated after the fair warning system identified her as accessing confidential information of a co-worker on two separate occasions without a legitimate purpose. Terrell was replaced by someone significantly younger than her and, as such, filed a lawsuit claiming that she was terminated because of her age in violation of the Age Discrimination in Employment Act (ADEA) and comparable Pennsylvania state law.

To prevail on an age discrimination claim where there is no direct evidence of age discrimination, i.e., there were no comments to or about the terminated employee regarding her age. Terrell had to prove that the employer had no legitimate, nondiscriminatory reason for terminating her and, if it did come up with a reason, that its reason was a made up reason for illegal age discrimination.

As the employer's legitimate, nondiscriminatory reason for terminating Terrell, it noted that she had accessed protected information about a co-worker on two separate occasions. The court agreed that was a legitimate, nondiscriminatory reason for terminating Terrell and dismissed her claims. In other words, the court found that Terrell was terminated because she violated the hospital's HIPAA and patient confidentiality policies by twice accessing a co-workers' protected records without a legitimate reason for doing so. Thus, Terrell's termination was warranted under the hospitals' code of conduct and the HIPAA sanctions guidelines. It was not a violation of federal or state age discrimination laws.

Takeaways: Data privacy is a major concern for all business, not just those in the healthcare space. In fact, with the May 25, 2018 effective date of the General Data Protection Act (GDPR), which impacts some US businesses, and the endless string of data breaches, data privacy is an issue all businesses should be taking seriously.

The two cases discussed above demonstrate that privacy issues are going to continue to be an issue for employers. The remedies against breaching entities and persons will be pursued through administrative, criminal, and civil means. While the cases discussed above should give businesses some reassurance that they can discipline employees who violate privacy policies/laws, they also highlight the need for privacy policies and protocols in the first place. These policies and protocols should be focused on three separate, but equally important, objectives: (1) data protection; (2) loss prevention; and (3) employee discipline.

All employers should have proper and adequate controls limiting employee access to protected information and protocols in place to detect any security incident. A large issue for companies is they do not know the protected information they have, who has access to it or means to detect it. Unless and until companies take steps to audit their protected information and build privacy policies and protocols to protect it, they stand at risk for severe data losses and resulting sanctions and penalties from a number of enforcement agencies.

Source URL: https://www.natlawreview.com/article/how-employers-can-handle-their-biggest-threat-to-data-privacy-their-employees