NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

November 15, 2019

What's trending on NP Privacy Partner

The California Consumer Privacy Act's impact on out-of-state companies and the OCR imposes fine against health system for significant HIPAA violations. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

The California Consumer Privacy Act's impact on out-of-state companies

Have you ever wondered how much information and personal data companies have about you? The data could range from your email address to your social security number. Beginning on January 1, 2020 it may become easier for consumers to discover this information, after the California Consumer Privacy Act (the "CCPA") goes into effect. The CCPA, which includes various protections against the collection and disclosure of consumers' personal information, was signed into law in June 2018.

The CCPA will require many businesses to allow California consumers to direct the company to delete all information collected about them or prohibit the company from selling their personal information to third parties. The law also allows individuals to ask companies exactly what kind of information has been collected, why their data is being collected and sold, to learn about the types of third-party companies buying and using the data and to find out about the financial incentives the company receives for selling the data. If a company is subject to this law, the fines can add up quickly. Under the statute, penalties for noncompliance levied by the government can reach up to $7,500 for each intentional violation, or $2,500 per violation without the requisite intent. Consumers themselves can also collect between $100 and $750 for each violation, under the private right of action established in the CCPA.

While the law is on the books in California, its impact is not limited to companies based in California. The CCPA directly applies to many out-of-state companies that do business in California. A company must comply with the CCPA if it meets at least one of three requirements: (1) has $25 million or more in gross revenue; (2) buys, sells, or shares personal data of 50,000 or more Californians; or (3) makes 50% or more of its revenue from selling personal data.

The CCPA applies a broad definition of "personal data," covering any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This includes data such as IP addresses, browsing history, records of purchases, biometrics, geolocation, and employment- or education-related information. As a result, many out-

of-state companies may be subject to the CCPA because they buy, sell or share personal data of over 50,000 residents of California.

Even if a company is not currently subject to the CCPA, it is anticipated that other states may follow California in enacting similar legislation. The cost of compliance could be substantial depending on the size of the company and how much consumer data it possesses. Working toward compliance before a company's home state enacts similar legislation could streamline and potentially reduce the costs of compliance. – *Aya M. Hoffman*

Special thanks to Tevin Hopkins for his contributions to this post.

Health Care and HIPAA

OCR imposes $2.15 million fine against health system for multiple and significant HIPAA violations

On October 23, 2019, the Department of Health and Human Services Office for Civil Rights (OCR) announced that it had imposed a civil money penalty of $2,154,000 against Jackson Health System (JHS) for multiple HIPAA violations. JHS is a nonprofit academic medical system in Florida that provides health services to approximately 650,000 patients annually and employs about 12,000 individuals. What OCR evaluated to determine the civil money penalty of $2.15 million is discussed below and from OCR's notice of proposed determination to JHS.

Improper disclosure of PHI of an NFL player and unauthorized access to PHI by employee leading to selling of PHI

In July 2015, OCR started an investigation after a media report disclosed the PHI of an NFL player that was a JHS patient. OCR determined during its investigation that a nurse who treated the NFL player in the operating room continued to access his PHI thereafter even though she no longer had a reason to do so. Another employee also accessed the NFL player's PHI without authorization. While OCR recognized that JHS did sanction these employees, the employees' ability to have broad access demonstrated the lack of control of appropriate access to ePHI for employees.

Furthermore, on January 4, 2016, JHS's Office of Compliance and Ethics was notified by an anonymous caller that an employee was selling patients' ePHI. It was determined by JHS that the employee had access to ePHI without proper authorization or authority to access for over five years and had inappropriately accessed over 24,000 patient records.

OCR noted that based on the above, JHS failed to (i) implement procedures to regularly review audit logs and access reports to ensure there is proper access to ePHI and (ii) implement policies and procedures for granting access to ePHI so that JHS's workforce may only access the minimum necessary to fulfill their job duties.

Failure to timely report to OCR lost patient records

JHS had two incidents of lost patient records in December 2012 for 715 patients and January 2013 for 756 patients. While HIPAA requires a covered entity to report breaches of unsecured protected health information involving 500 or more individuals without unreasonable delay and in no case later than 60 calendar days after discovery of the breach, JHS did not submit a breach report to OCR until August 22, 2013 (meaning JHS was at least 160 days late to report the breach). Furthermore, the initial report to OCR only identified the January 2013 loss and JHS did not submit an addendum reflecting the December 2012 loss until June 7, 2016.

OCR also noted that JHS's breach notification policy implemented in October 2013 does not include specific procedures for ensuring notification will be submitted to OCR as required by the Breach Notification Rule.

Failure to conduct adequate risk assessments and implement security measures to identified risks and vulnerabilities as required by the Security Rule

In response to several data requests from OCR, JHS provided OCR "risks analyses" for JHS that were conducted by third-party vendors every year from 2014–2017. OCR noted the following about the risks analyses:

- Risks analyses conducted before 2017 erroneously stated that several provisions of the Security Rule were not applicable to JHS.
- All failed to include all ePHI created, received, maintained, or transmitted by JHS and did not identify the totality of threats and vulnerabilities that existed in JHS's systems.
- The 2017 risk analysis only included the main campus of JHS in the analysis.
- Two risk analyses had blank sections.

OCR noted that for the risk analyses provided, JHS did not remediate risks, threats, and vulnerabilities identified by the risk analyses to a reasonable and appropriate level as required by the Security Rule. Furthermore, "high risks" identified in 2014 and 2015 risk analyses still were identified as "high risks" in the 2016 risk analysis with no evidence from JHS to reduce these risks and vulnerabilities.

Takeaways

Covered entities can learn the following from OCR's notice of proposed determination:

- It is not enough to have the capability to create audit logs and access reports for systems that contain ePHI. Records of information system activity need to be reviewed on a regular basis.
- Have policies and procedures in place that address the Breach Notification Rule and include specific procedures for effectively providing notification under this Rule.
- Conduct yearly risk assessments that include all ePHI created, received, maintained, or transmitted by the covered entity.
- Review yearly completed risk assessments and identify and address threats and vulnerabilities that need to be remediated.

OCR's press release about the civil money penalty against JHS can be found here. – *Jena M. Grady*

For more information, please contact:

— Aya M. Hoffman at **ahoffman@nixonpeabody.com** or 585-263-1535

— Jena M. Grady at **jgrady@nixonpeabody.com** or 212-940-3114

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team