NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

May 24 2019

NP What's trending on NP Privacy Partner

Canada may require express consent for cross-border transfers of personal information, $3 million settlement emphasizes the importance of a robust HIPAA compliance program and more. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

Canada may require express consent for cross-border transfers of personal information

Canada's comprehensive privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), has permitted companies in receipt of individuals' personal information to transfer such data outside Canada for processing or storage without the express consent of the individuals. That may change, however.

This potential change arises from the 2017 Equifax data breach. In its wake, Canada's Office of the Privacy Commissioner (OPC) determined that the personal information of over 19,000 Canadians had been compromised. They had provided their personal information to Equifax Canada, which had transferred their information for processing and storage to its U.S.-based affiliate, Equifax, Inc., the subject of the subsequent breach. Because the cross-border transfer for processing was consistent with the purpose for which the individuals originally provided their data, their express consent to that transfer was not required, pursuant to OPC guidance in place since 2009.

As a direct result of the compromise of the Canadians' personal information, last month the OPC issued a proposal that would require Canadians' consent to similar cross-border transfers in the future. It would accomplish this by reclassifying such transfers from "uses" to "disclosures." A "use" of personal information by a recipient is something consistent with the original purpose for which it was given – e.g., processing or storage – whereas "disclosure" is for a different purpose altogether – e.g., sending it to marketing research or advertising agencies. The former does not require express consent of individuals, whereas the latter does. Thus under the OPC's proposal, even transfer of data to a U.S.-based affiliate or vendor for storage would require the individual's express consent. Obtaining express consent would include providing individuals with alternatives to the transfer of their information outside Canada.

U.S. companies that receive personal data of Canadians should be aware that the proposed changes could increase the cost and complexity of cross-border transfers. Their Canadian affiliates may demand more burdensome arrangements and compliance procedures for handling such information.

It remains to be seen whether this proposal will take effect. A comment period on the OPC's proposal remains open until June 28, 2019. *–Benjamin R. Dwyer*

Consumer private right of action blocked; penalties still strong under the California Consumer Privacy Act

As we've reported, the California Consumer Privacy Act of 2018 (the "CCPA") is facing many amendments. One of these amendments, introduced on February 22, 2019, by California State Senator Hannah Beth-Jackson, sought to expand the CCPA's private right of action and remove the thirty-day cure period required for enforcement actions brought by the state's attorney general. However, the amendment did not receive a vote in the Senate Appropriations Committee, effectively blocking the bill.

Specifically, the bill sought to allow consumers whose rights were violated under the CCPA to bring a private right of action. As the CCPA currently stands, the private right of action is limited to circumstances where a consumer's non-encrypted or non-redacted personal information is part of a data breach that occurs as a result of a business's failure to maintain reasonable security measures. Enforcement actions for other violations can only be brought by the Attorney General's Office.

While SB 561 is blocked and no longer threatens to expand the consumers' private right of action, penalties under the CCPA will still be powerful. Penalties for violations of the Act range from $100–$750 per consumer per violation or actual damages, whichever is greater. Penalties also can include injunctive or declaratory relief. For actions for statutory damages, a consumer must provide a business with thirty days' written notice and an opportunity to cure the violation. If the business cures, then the consumer cannot bring an action for statutory damages. For actual damages, a consumer is not required to provide thirty days' notice and opportunity to cure. *–Jenny L. Holmes*

Health Care & HIPAA

Three million dollar settlement emphasizes the importance of a robust HIPAA compliance program

On May 6, 2019, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced a settlement with Touchstone Medical Imaging (Touchstone), a diagnostic medical imaging services provider, requiring a three million dollar financial settlement and a two-year Corrective Action Plan.

There are a number of lessons that HIPAA covered entities and business associates can glean from the Touchstone enforcement action, a notable one being that an entity should promptly and thoroughly investigate any security incident or potential data breach. Both OCR and the Federal Bureau of Investigation (FBI) notified Touchstone that one of its FTP servers was allowing uncontrolled access to patients' protected health information (PHI). After initially denying the exposure, Touchstone eventually reported a breach of more than 300,000 social security numbers and other PHI. OCR found that both Touchstone's investigation of the incident, as well as its notification, were not handled in a timely manner.

In investigating Touchstone, OCR also found that the entity did not conduct an accurate and thorough risk analysis—a key enforcement priority of OCR in recent years. As part of its Corrective Action Plan, Touchstone is required to conduct an enterprise-wide risk analysis, including creating an inventory of all of its equipment, systems, applications and off-site storage facilities that contain PHI. This is a key

element for any organization in order to decide what systems and processes best secure PHI and other sensitive data.

In addition, OCR detailed that Touchstone failed to execute business associate agreements with its vendors, including its information technology vendors, prior to the disclosure of PHI. Similar to prior settlements, the Touchstone settlement emphasizes the importance of understanding which vendors will receive or have access to an organization's PHI and having the parties involved execute a business associate agreement at the outset of the arrangement. –*Valerie Breslin Montague*

OCR revises HIPAA annual penalty limits to address culpability

In April 2019, the Department of Health and Human Services Office for Civil Rights (OCR) issued a Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties (the Notification). OCR published the Notification to alert the public that OCR is exercising its discretion in assessing Civil Money Penalties under HIPAA as amended by the HITECH Act.
In February 2009, the HITECH Act established four categories for HIPAA violations with increasing penalty tiers based on the level of culpability. It also amended HIPAA by eliminating the prohibition on the penalties for a covered entity if it did not know and with reasonable diligence would not have known of a HIPAA violation. The four categories for HIPAA violations became the following:

- No Knowledge: The person did not know (and, by exercising reasonable diligence, would not have known) that the person violated the provision
- Reasonable Cause: The violation was due to reasonable cause, and not willful neglect
- Willful Neglect—Corrected: The violation was due to willful neglect that is timely corrected
- Willful Neglect—Not Corrected: The violation was due to willful neglect that is not timely corrected

While the HITECH Act applied four different annual penalty limits (ranging from $25,000 to $1,500,000) based on the level of culpability, in the Interim Final Rule to implement the enhanced penalty provisions of the HITECH Act, OCR applied the highest annual cap of $1.5 million to all violations regardless of the level of culpability (see first table below). OCR provided that applying the highest annual limit for all levels of culpability was "the most logical reading" of the HITECH Act since this was "consistent with Congress' intent to strengthen enforcement."

Culpability	**Minimum Penalty/Violation**	**Maximum Penalty/Violation**	**Annual Limit**
No Knowledge	$100	$50,000	$1,500,000
Reasonable Cause	$1,000	$50,000	$1,500,000
Willful Neglect - Corrected	$10,000	$50,000	$1,500,000
Willful Neglect – No Corrected	$50,000	$50,000	$1,500,000

However, the Notification provides that upon further review OCR has concluded that a "better reading of the HITECH Act" is to apply annual limits based on the level of culpability (see second table below).

Culpability	Minimum Penalty/Violation	Maximum Penalty/Violation	Annual Limit
No Knowledge	$100	$50,000	$25,000
Reasonable Cause	$1,000	$50,000	$100,000
Willful Neglect - Corrected	$10,000	$50,000	$250,000
Willful Neglect – No Corrected	$50,000	$50,000	$1,500,000

OCR will use the above penalty tier structure, as adjusted for inflation, until further notice and plans to have future rulemaking to modify the penalty tiers in the current regulation "to better reflect the text of the HITECH Act."
Given the significant decrease of the annual limits for all but one category for HIPAA violations, covered entities and business associates may welcome OCR's revised reading of the HITECH Act. This change in the annual limits may be especially welcomed since OCR under the previous penalty tiers collected $28.7 million from settlements and cases in 2018 (see February 27, 2019 NP Privacy Partner Blog Post). *–Jena M. Grady*

For more information, please contact:

- Benjamin R. Dwyer at **bdwyer@nixonpeabody.com** or 716-853-8122
- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
- 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