NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

MARCH 31, 2017

What's trending on NP Privacy Partner

NY AG settles with medical app developers, NM will be next state with data notification law, concerns arise about Privacy Shield, and a health care data breach derives from mistaken forms. Here's what's trending in data privacy and cybersecurity.

Health Care and HIPAA

NY Attorney General issues Warning to Medical App Developers

Citing misleading claims and irresponsible privacy practices, the NY Attorney General's Health Care Bureau entered into settlements with three mobile health application developers this past week. Two of the app developers claimed that their apps accurately measured heart rates during strenuous exercise, and a third claimed that its app could be used with a smartphone as a fetal heart monitor, even though the app was not an FDA-approved fetal heart monitor. The Attorney General stated, "We won't tolerate non-evidence based apps that threaten the well-being of New Yorkers."

In addition to paying a penalty, the app developers will now post clear and prominent disclaimers informing consumers that their apps are not medical devices and are not approved by the FDA. The developers also agreed to make changes to their privacy practices to require affirmative consent from consumers to accept their privacy policies for the apps. The developers will also disclose to consumers the types of personally identifying information that are collected by the apps and how such information will be used and shared with third parties.

More information about the app developers and the settlements can be found at here.

Last year, the Federal Trade Commission issued Best Practices for mobile health app developers which can be found here, as well as an interactive tool to assist mobile health app developers to determine whether the FTC Act, the FTC's Health Breach Notification Rule, HHS's Health Insurance Portability and Accountability Act (HIPAA), or the FDA's Federal Food, Drug & Cosmetic Act applies to their product. The tool can be found here.—*Laurie T. Cohen*

State Measures

New Mexico is about to become the 48th state with a data notification law

On March 15, the New Mexico Legislature passed the "Data Breach Notification Act," which has been transmitted to Governor Susana Martinez. If enacted, New Mexico will become the forty-eighth state with a data notification law, leaving only South Dakota and Alabama without such laws.

The Act requires individuals to be notified should their personal information be involved in a security breach, and also states that consumer reporting agencies, the attorney general's office and card processors in certain circumstances must be notified as well. The timeframe for individual notice is "in the most expedient time possible," but no later than 30 calendar days after the discovery of the security breach unless delayed reporting is appropriate due to a law enforcement investigation or out of necessity to determine the scope of the breach. The Act defines a "security breach" as the unauthorized acquisition of computerized data that compromises the security or integrity of personally identifying information.

A person who owns or licenses personally identifying information must "implement and maintain reasonable security procedures and practices appropriate for the nature of the information." The Act requires the "proper disposal" of records containing personal identifying information of a New Mexico resident when such records are no longer reasonably needed for business purposes. Proper disposal means shredding, erasing or otherwise modifying the personal identifying information contained in the records to make the personal identifying information unreadable or undecipherable.

The Act does not account for medical information or health insurance data. The legislation also specified that it "shall not apply to a person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996."

"Personal identifying information" includes an individual's first name or first initial and last name in combination with one or more of the following:

- Social Security number
- Driver's license number
- Government-issued identification number
- Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account
- Unique biometric data, including the person's fingerprint, voiceprint or retina or iris image

The definitional inclusion of biometric data is especially significant, as states are recognizing the growing prevalence of biometric identifiers in transactions.

While affording no individual private cause of action, the Act authorizes the attorney general to bring an action on behalf of affected individuals. Businesses or organizations violating the Act may face a civil penalty up to $25,000 or, in the case of failed notification, $10 per instance of failed notification, up to a maximum of $150,000.—*Steven M. Richard*

International

E.U. Civil Liberties Committee says Privacy Shield deficient

On March 23, 2017, with the first joint annual review of the Privacy Shield on the horizon, the European Parliament Civil Liberties, Justice and Home Affairs Committee narrowly adopted a resolution identifying "key deficiencies" in the E.U.-U.S. Privacy Shield. The resolution, which was passed by a vote of 29 in favor, 25 against and one abstention, details a number of deficiencies with the personal data transfer framework. In particular, while acknowledging improvement over the E.U.-U.S. Safe Harbor that was invalidated by the European Court of Justice in 2015, the resolution raises concerns regarding the lack of specific rules on automated decision-making and the general right to object to data transfers.

Additionally, in a show of skepticism of U.S. authorities, the resolution specifically notes the insufficient protections surrounding mass and indiscriminate collection of personal data despite assurances attached to the Privacy Shield by the U.S. Director of National Intelligence. The resolution also urged an immediate assessment of whether rules approved by the U.S. in early 2017 allowing the National Security Agency to share private data with other agencies are consistent with the U.S.'s responsibilities under the Privacy Shield. Finally, the lack of a judicial remedy for individuals in the European Union whose data is transferred under the Privacy Shield and processed by both private organizations and U.S. law enforcement agencies is yet another concern of the committee.

The resolution is expected to be voted on by the European Parliament as a whole in April.—*Steven M. Maffucci*

Data Breach

UNC Health Care sends 1,300 prenatal patients a possible data breach notification

In a March 20, 2017, press release, the University of North Carolina Health Care System (UNC Health Care) announced that it had notified 1,300 patients about a potential breach of information that involved the mistaken disclosure of forms used to collect patient information. Patients seen at two UNC Health Care clinics between April 2014 and February 2017 may have been affected.

The forms at issue are completed by Medicaid-eligible prenatal patients during their clinic visits and are shared with local health departments to determine patients' eligibility for further support services. The forms contained certain identifying information, such as name, address and Social Security numbers, as well as sensitive physical and mental health information, such as HIV status, drug and alcohol use and information related to prior and current pregnancy. The Privacy Office of UNC Health Care discovered that a potential breach may have occurred when forms completed by patients who were not eligible for Medicaid may have inadvertently been forwarded to the patients' local county health departments.

UNC Health Care has requested all local county health departments involved to return any paper forms for patients not covered by Medicaid to the clinic and purge any electronic records about non-Medicaid patients from their electronic information systems. Additionally, the UNC Health

Care states in the press release that its obstetric clinics revised their procedure to ensure that only forms completed by Medicaid patients are sent to local county health departments.

UNC Health Care has also provided a number of support options available to patients whose information may have been breached, including credit report monitoring and fraud resolution services.

Over the past several years, there has been a heightened focus by regulators on breaches of electronic health information resulting from aggressive hacking and other security deficiencies. This incident is a reminder that a breach of patient information can occur in any form, including paper. The breach notification requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires certain notifications to be made following a breach of "unsecured protected health information." Protected health information is secure only where it is rendered unusable, unreadable or indecipherable through certain government-specified technology. Paper records generally cannot be rendered secure through technology. A breach carries considerable exposure for health care entities subject to HIPAA, as such entities are required to notify the affected patients, report the breach to the U.S. Department of Health and Human Services and in cases involving more than 500 individuals, report the breach to the media. Once the breach is reported to HHS, the health care entity could potentially be audited for compliance with the HIPAA privacy and security requirements, and deficiencies can result in significant penalties. For this reason, health care entities should routinely audit their policies and procedures related to the privacy and security of protected health information, both paper and electronic.—*JoAnna R. Nicholson and Jena M. Grady*

For more information, please contact:

— Laurie T. Cohen at **lauriecohen@nixonpeabody.com** or 518-427-2708
— Jena M. Grady at **jgrady@nixonpeabody.com** or 312-977-4106
— Steven M. Maffucci at **smaffucci@nixonpeabody.com** or 585-263-1079
— JoAnna R. Nicholson at **jrnicholson@nixonpeabody.com** or 516-832-7611
— Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020

NP PRIVACY PARTNER BLOG

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