September 14, 2018

What's trending on NP Privacy Partner

New York Attorney General settles with nonprofit social services agency over HIPAA violation and CTIA announces new programs to certify safety of Internet of Things devices. Here's what's trending in data privacy and cybersecurity.

Data Breach

New York Attorney General settles with nonprofit social services agency over HIPAA violation

Following a report of a breach of protected health information, on August 29, 2018, the New York Attorney General announced a settlement with Arc of Erie County, a social services agency that serves persons with developmental disabilities and their families. Arc of Erie County received a $200,000 financial penalty plus a Corrective Action Plan, which requires Arc of Erie County to conduct a HIPAA-required security risk assessment and submit a report of that assessment to the attorney general's office.

Under HIPAA, Arc of Erie County and other covered entity health care providers are required to implement appropriate physical, technical and administrative safeguards to protect clients' protected health information. In March 2018, Arc of Erie County notified impacted clients and the attorney general of a breach of client health information involving a website designed for internal staff access that was visible online, with information from that site found through search engines as well. The data that was available to the public included full names, social security numbers, addresses and dates of birth. A forensic investigation demonstrated that individuals outside the United States accessed the links to the sensitive data many times. The data breach impacted 3,751 New York residents.

In addition to the Department of Health and Human Services, Office for Civil Rights, the HIPAA regulations provide state attorneys' general with HIPAA enforcement authority. The New York Attorney General's office concluded that Arc of Erie County failed to implement appropriate physical, technical and administrative safeguards to protect its clients' health information, as required by HIPAA. The attorney general's office determined that this resulted in an impermissible disclosure of electronic protected health information.

This enforcement action emphasizes the need for all organizations, even not-for-profit, community-based providers, to conduct enterprise-wide security risk assessments. Data gleaned from such assessments should be the basis for the organization's risk management plan, which is also a HIPAA

requirement. These items are fundamental parts of a covered entity or business associate's HIPAA compliance program and elements that will be requested in any governmental audit or investigation of HIPAA compliance. –*Valerie Breslin Montague*

Cybersecurity

CTIA announces new programs to certify safety of Internet of Things devices

The Cellular Telecommunications Industry Association ("CTIA") announced this week the creation of the CTIA Cybersecurity Certification Program for cellular-connected Internet of Things ("IoT") devices. Through the program, CTIA will certify that IoT connected devices meet certain cybersecurity-related requirements that were established in collaboration with security experts, industry participants, technology companies and test labs. According to CTIA, the program's requirements incorporate security recommendations from the National Telecommunications and Information Administration and the National Institute of Standards and Technology.

"America's wireless industry has long been a leader in cybersecurity best practices and establishing an industry-led cybersecurity certification program of IoT devices is a major step in building a trusted, secure wireless ecosystem for the Internet of Things," CTIA SCP and Chief Technology Officer Tom Sawanobori said in a press release announcing the new program.

According to CTIA, the program is meant to help protect the IoT space by certifying that devices were "built from the ground up with cybersecurity in mind." The certification program will offer three levels of certification. The first level will signify that an IoT device meets the most basic recommended cybersecurity and privacy measures, including things like password requirements and user authentication processes. To meet the second level of certification the device must not only meet all of the first level requirements, but also must pass tests related to its ability to safely update software and that it supports encryption of data communications. Finally, the third and most comprehensive level incorporates levels 1 and 2, and tests for more advanced forms of data encryption and other, more advanced security features.

CTIA anticipates that its authorized test labs will begin accepting devices for certification through the program in October of this year. – *Eric M. Ferrante*

For more information, please contact:

— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
— Eric M. Ferrante at **eferrante@nixonpeabody.com** or 585-263-1362