NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

December 6, 2019

What's trending on NP Privacy Partner

Amazon's "smart doorbell" raises privacy concerns and multi-state health system's refusal to properly report breach to OCR leads to $2.175 million settlement. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

Today, smart devices are increasingly making their way into our everyday lives. While the smart phone may be the first example that comes to mind for many, so called "smart" technology has made its way into our cars, watches, and even our homes. Amazon, one of the world's largest technology companies, has a "smart home" store on its website where it offers many devices, including light bulbs, microwaves, printers, televisions, and speakers.

Another smart device finding a place in today's homes is the Wi-Fi powered "smart doorbell." Ring, a company recently bought by Amazon, provides its own version of the smart doorbell on Amazon's online marketplace. The Ring Video Doorbell is a device that monitors homes with HD video and uses sensors to send alerts to homeowners when motion is detected. The device even provides on-demand video, allowing homeowners to check-in on their homes even when the sensors have not been activated.

Although the features of the Ring Video Doorbell have provided its users with a greater sense of security, they have also recently raised concerns relating to privacy. Ring has agreed with police forces throughout the United States to provide access to homeowners' video footage, allowing law enforcement to request footage from specific times and places. Ring users have the option to deny police requests to access footage captured by their devices. However, this partnership between law enforcement and technology exposes visitors and even innocent passersby to increased government surveillance, and poses a potential threat to civil liberties.

In September, Senator Edward J. Markey (D-MA) wrote to Amazon, in a letter addressed to the company's CEO and president Jeff Bezos, with questions addressing the privacy concerns surrounding smart doorbell technology. In response to a question regarding facial recognition, Amazon indicated that adding this feature to Ring products has been contemplated and said that privacy would be considered should it be implemented in the future. In making a decision on incorporating facial recognition into smart doorbell devices going forward, Amazon and Ring will have to find a balance between security and privacy. – *Jenny L. Holmes*

Special thanks to Christian Albano for his contributions to this post.

Health Care and HIPAA

Multi-state health system's refusal to properly report breach to OCR leads to $2.175 million settlement

On November 27, 2019, the Department of Health and Human Services Office for Civil Rights (OCR) announced Sentara Hospitals (Sentara) has agreed to pay $2.175 million to OCR and adopt a corrective action plan that includes two years of monitoring to settle possible violations of HIPAA. Sentara has 12 acute care hospitals and more than 300 sites of care in Virginia and North Carolina.

In April 2017, OCR received a complaint that an individual received a bill from Sentara that contained PHI for another patient. Once OCR initiated an investigation to review the complaint, OCR determined that Sentara improperly disclosed PHI of 577 patients to wrong addresses. This occurred when Sentara accidentally merged these patients billing statements into mailing labels of more than 16,342 other individuals. Information included patient names, account numbers, or dates of services. Sentara, however, incorrectly concluded from its risk assessment that the improper disclosure leading to a breach actually only affected eight individuals. Specifically, Sentara wrongly believed that notification to OCR and affected individuals only had to be made if patient diagnosis, treatment information, or other medical information had been improperly disclosed.

Even after OCR advised Sentara of its duty to properly report the breach for the remaining 569 individuals, OCR noted that "Sentara persisted in its refusal to properly report the breach…" OCR's investigation also led to OCR finding that Sentara failed to have a business associate agreement in place with Sentara Healthcare, an entity that performs business associate services for Sentara, until October 17, 2018.

The penalty and corrective action plan is an important reminder to covered entities to accurately and timely report breaches to OCR. Under HIPAA, covered entities must perform comprehensive risk assessments when determining whether a breach occurred and thoroughly evaluate the probability that PHI had been compromised. Once a reportable breach has been determined, covered entities are required to notify OCR of a breach affecting 500 or more individuals without unreasonable delay and in no case later than 60 days following the breach. If a breach affects fewer than 500 individuals, a covered entity may notify OCR of such breach on an annual basis.

To drive the reporting requirement point further, OCR Director Roger Severino stated, "When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."

OCR's press release about this settlement can be found here. – *Jena M. Grady*

For more information, please contact:

— Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
— Jena M. Grady at **jgrady@nixonpeabody.com** or 212-940-3114