December 2019

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

SDNY Rejects Standing under "Increased Risk" Theory Where Data Not Targeted or Stolen

The Southern District of New York rejected a settlement that would have resolved a class action based on the unauthorized (and accidental) emailing of personal information of one group of employees to another group of employees. Because plaintiffs admitted the breach did not lead to the theft of any class members' identity, the company filed a motion to dismiss the suit for multiple reasons including lack of Article III standing. The parties ultimately opted to settle before the court ruled on the motion. When the plaintiffs filed a motion to enforce the settlement, the court determined that the plaintiffs' "increased risk" theory was too speculative. It distinguished other cases that found standing based on that theory because the employees' data was neither intentionally targeted nor stolen.

TAKEAWAY

Defendants in breach cases in federal court should always test standing as a potential way to terminate the case early.

OCR Follows Through With 2019 HIPAA Right of Access Initiative

The Office of Civil Rights (OCR) has released details of a resolution agreement with a company that failed to forward a patient's medical records in electronic format to a third party after the patient asked multiple times. This is the second enforcement action and settlement involving the right of access provision of HIPAA following the OCR's 2019 Right of Access initiative to enforce the rights of patients to have prompt access to their

SUBSCRIBE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

medical records in a readily producible format without being overcharged.

TAKEAWAY

HIPAA's right of access provision has rarely been a basis for an enforcement action, and this agreement demonstrates that the OCR is following through with its 2019 Right of Access Initiative. Companies should take patients' data access requests seriously and provide timely responses.

Comcast Subscribers Ordered to Individually Arbitrate Privacy Claims

In a class action against Comcast Cable Communications LLC involving claims under the Cable Privacy Act and the Massachusetts consumer protection statute, the District of Massachusetts has ordered that subscribers must individually arbitrate those claims. The lawsuit alleges that Comcast unlawfully gathered, maintained and used consumers' private video-viewing data for targeted advertising without consent. The court ordered individual arbitration on the basis of the Comcast subscriber agreement, which contains a class action waiver. The court also rejected the plaintiff's argument that the arbitration provision was unenforceable because Comcast could modify the subscriber agreement.

TAKEAWAY

Arbitration provisions and class-action waivers should be considered for any consumer-facing agreement as more courts uphold their use.

Texas Health and Human Services Commission Incurs $1.6 Million HIPAA Fine

The Texas Health and Human Services Commission's Department of Aging and Disabilities Services (DADS), which administers long-term care services for aging individuals, faces a $1.6 million fine for alleged HIPAA violations relating to a breach exposing patients' electronic protected health information (ePHI). In 2015, DADS reported to Office of Civil Rights (OCR) that because "an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials," ePHI of 6,617 individuals could be viewed over the internet. DADS is unsure of how many unauthorized viewers accessed the ePHI due to insufficient audit controls. Additionally, an OCR investigation revealed that DADS

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Ben Patton
Associate
206.344.7625
bpatton@shb.com

Lischen Reeves
Associate
816.559.2056
lreeves@shb.com

violated the HIPAA Security Rule when it "failed to conduct an enterprise-wide risk analysis, and implement access and audit controls on its information systems and applications."

TAKEAWAY

A HIPAA risk analysis is a key first step in ensuring PHI is secure. The risk analysis reveals critical needs in a healthcare system's overall data privacy and security strategy. Once completed, the analysis should be revisited regularly to ensure HIPAA compliance.

Washington Updates Regulations Affecting Data-Breach-Notification Requirements under the Washington Consumer Loan Act

The Washington Department of Financial Institutions (DFI) adopted final rules amending regulations of the Washington Consumer Loan Act (WCLA) and the Washington Mortgage Broker Practices Act (WMBPA). The final WCLA and WMBPA rules include data-breach-notification provisions that reduce from 45 days to 30 days the deadline for regulated businesses to report breaches to the DFI.

TAKEAWAY

Sector-specific data-breach-notification laws may become the norm. Sectors are now adding their own requirements, making it extremely important to know all the data-breach-notification laws that may apply to a company.

Medical Center Pays Hefty Price for Failing to Encrypt Devices

The HHS Office of Civil Rights (OCR) reached a $3 million settlement with the University of Rochester Medical Center (URMC), one of the largest health systems in New York, as a result of two data breaches in which electronic protected health information (ePHI) was disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop. OCR's investigation revealed that URMC failed to: (i) conduct an enterprise-wide risk analysis; (ii) implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; (iii) utilize device and media controls; and (iv) employ a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate to do so. Additionally, OCR provided technical assistance to URMC after a similar breach occurred in 2010 and URMC noted that its lack of encryption standards were

a high risk to ePHI. Nevertheless, URMC continued to allow unencrypted mobile devices to be used, which likely resulted in the larger monetary settlement.

TAKEAWAY

As employees become more mobile, all company-owned devices should be encrypted, especially mobile devices that are more at risk to be lost or stolen.

Brazil Legislature Seeks Delay of New Data-Protection Law

Brazilian Member of Congress Carlos Bezerra has introduced Bill 5762/2019, which would delay the effective date of Brazil's comprehensive Data Protection Law (LGPD) for two years to August 15, 2022. In support of the request, Bezerra cites the small number of Brazilian companies that have undertaken compliance efforts as well as the sluggish pace of the government's efforts to establish the country's first Data Protection Authority (ANPD). Currently, the GDPR-esque LGPD—which establishes a maximum per-infraction fine of up to 2% of the company's Brazilian revenue, up to 50 million Brazilian reals (approximately $11.9 million)—is set to take effect on August 15, 2020. We will monitor the bill's progression closely.

European Commission Issues Third Annual Review of the EU-US Privacy Shield

The European Commission has published its third annual review of the EU-US Privacy Shield, a framework designed to protect personal data transferred from the EU to participating U.S. companies. The third review recognizes areas in which the Privacy Shield has improved and areas of growth for upcoming years.

Improvements:

1. The U.S. Department of Commerce has streamlined its monthly checks with a sample of companies to ensure compliance under the Privacy Shield.
2. U.S. Federal Trade Commission (FTC) involvement in Privacy Shield enforcement actions has increased.
3. Redress mechanisms for individuals exercising their rights under the Privacy Shield are functioning well.

Areas of growth:

1. Shorten the time it takes for companies to receive (re)certification to participate.

2. Expand compliance checks by increasing investigation into false claims associated with participating in the Privacy Shield framework.
3. Increase and streamline information exchange between the FTC and EU data protection authorities as investigations progress.

TAKEAWAY

Despite threats from litigation and continued European skepticism toward U.S. data practices, Privacy Shield continues to be a viable framework for companies to use for international data transfers.

Hospital System Settles $2.175 Million HIPAA Violations

Sentara Hospitals settled potential HIPAA violations for $2.175 million as a result of a breach exposing patients' protected health information (PHI). OCR was notified of the breach via a complaint "alleging that Sentara had sent a bill to an individual containing another patient's [PHI]." OCR's investigation revealed that Sentara "mailed 577 patients' PHI to wrong addresses that included patient names, account numbers, and dates of services." The investigation also revealed Sentara Hospitals lacked the required business associate agreement with Sentara Healthcare, which performed business associate services for the hospital system. Notably, Sentara improperly reported the breach as only affecting eight patients because of an incorrect conclusion that breaches only become reportable if the wrongful disclosure included patient diagnoses, treatment information or other medical information. Even with the OCR's insistence that Sentara comply with its duty to properly report the breach, Sentara refused to do so. The settlement also subjects Sentara to two years of monitoring.

TAKEAWAY

HIPAA compliance requires a focus on many moving parts, but timely, appropriate and accurate notification is the cornerstone of any HIPAA breach strategy. A blatant refusal to properly report a HIPAA violation will be costly.

Ireland's Data Protection Commission Releases Recommendations on Properly Storing Personal Data

Ireland's Data Protection Commission (DPC) has published recommendations on general portable storage devices for

controllers under the GDPR. The recommendations are focused on appropriate security of stored personal data. Key recommendations include:

1. Only whole-drive encrypted, passphrase-protected, portable-storage devices, issued by the organization to authorized personnel, should be utilized. No unauthorized device should be used on any of the organizations' systems.
2. To prevent data leakage, organizations should operate restricted permissions to restrict staff from copying data to portable-memory devices.
3. Where possible, data transferred to a portable-storage device should have an expiry.
4. Enforce USB key scanning for all computers whenever a USB key is plugged in. This can help ensure that no malware or malicious programs are present on the USB key.
5. An asset register should be maintained of all organization portable-storage devices and the authorized personnel in which they have been issued to.

TAKEAWAY

DPC's recommendations show an increased focus on protecting personal data. Companies should have a firm grasp on security protocol relating to personal data and should conduct employee training often to ensure compliance.

OCR Issues Guidance on Preventing, Mitigating and Responding to Ransomware

In its Fall 2019 cybersecurity newsletter, the Office of Civil Rights (OCR) issued guidance on how the HIPAA Security Rule can help covered entities prevent, mitigate and recover from ransomware attacks by providing insight into new developments and trends that have been observed regarding ransomware attacks and how organizations can improve their security posture in response to this threat. The article discusses the history of ransomware attacks and details new threats such as targeted ransomware attacks designed and tailored to efficiently infiltrate a specific organization or industry. The Security Rule lays the groundwork for covered entities to comply and prevent these threats through risk analysis and management, information-system-activity review, security awareness and training, developing security-incident procedures, and having a contingency plan for recovering from an attack. The newsletter concludes by echoing the FBI's recommendation not to pay any ransom demands.

TAKEAWAY

These cybersecurity measures are steps that every business should take regardless of whether HIPAA applies. While combating

threats should be a part of every security program, disaster may inevitably strike. Having a contingency plan is fundamental for recovering in a worst-case scenario.

SHOOK PRIVACY SPOTLIGHT

Kate Paine

Kate Paine joined Shook after completing a two-year clerkship with The Honorable John E. Steele (Middle District of Florida - Fort Myers Division), prior to which she worked as a commercial litigation associate at a large law firm in Pittsburgh, Pennsylvania. Kate leveraged this work experience, along with her propensity for languages (she speaks English, French and Spanish and is learning Brazilian Portuguese), to become an integral member of Shook's Privacy and Data Security team, with a focus on international privacy compliance and domestic litigation. Drafting privacy notices and data transfer agreements, implementing international compliance

programs, dissecting GDPR fines for operational advice and assisting the defense of BIPA and data breach class actions, Kate has been instrumental in assisting clients with navigating the various data privacy challenges that can arise in the course of doing business.

When she's not helping clients get lawsuits dismissed and avoid the pitfalls of non-compliance with data protection laws, Kate enjoys spending time at the beach, sweating it out at Orange Theory Fitness, cooking with her culinarily superior French fiancée, and planning her next Camino de Santiago pilgrimage. (See above for Kate posing with her "compostela" certificate after completing the 500-mile journey by foot through northern Spain.)