July 28, 2016

DATA BREACH

Behavioral Health Provider StarCare Specialty Notifies 2,900 Patients of Breach of PHI

StarCare Specialty Health System, located in Lubbock, Texas, is notifying 2,900 patients "who received Intellectual Developmental Disabilities program services, Behavioral Health program services, and Therapeutic Treatment Community services" that their protected health information (PHI) and behavioral health information was compromised in the theft of five laptop computers from its office.

The theft occurred on May 30, 2016, when thieves broke into its offices and stole the five laptops. One of the laptops contained patients' names, medical record numbers, telephone numbers, diagnosis, admission and discharge dates, dates of birth, Social Security numbers, and Medicaid and Medicare numbers.

StarCare is offering the affected patients with one year of identity monitoring and has set up a call center to answer questions of patients.

— Linn Foster Freedman

Athens Orthopedic Clinic's EMR Compromised by Hackers Using Vendor's Log-In Credentials

Athens Orthopedic Clinic in Georgia reported on July 25, 2016, that a hacker gained access to its electronic medical record system at the end of June using the log-in credentials of a third-party vendor.

It has determined that patient records in the electronic medical record system were compromised during the hack and it is in the process of notifying affected patients. It appears that Athens is notifying all current and former patients of the data breach.

The data that may have been accessed includes names, addresses, Social Security numbers, telephone numbers, and some medical data.

— Linn Foster Freedman

HIPAA

University of Mississippi Medical Center Settles HIPAA Violations for $2.75 Million

The Office for Civil Rights (OCR) has obtained another big settlement from a covered entity resulting from a data breach. This most recent settlement of fines and penalties and a resolution agreement is with the University of Mississippi Medical Center (UMMC) for $2.75 million.

The OCR commenced an investigation against UMMC after UMMC self-reported a data breach on March 21, 2013. The breach was caused when an unencrypted, but password protected laptop went missing from the intensive care unit. The laptop contained the unsecured protected health information (PHI) of approximately 10,000 patients, which triggered the investigation.

As it frequently does, the OCR asked UMMC for all of its HIPAA policies and procedures and, according the OCR, UMMC "failed to implement policies and procedures to prevent, detect, contain, and correct security violations, including conducting an accurate and thorough assessment of the potential risks and vulnerabilities" to PHI from the HIPAA Security Rule implementation compliance date of April 20, 2005 to the present date.

According to the OCR, UMMC also failed to implement physical safeguards for workstations, failed to assign a unique user name and/or number for identifying and tracking user identity in the IT systems, and allowed a shared department network drive to be accessed through a generic account so an accounting of which user was accessing information was impossible.

Finally, and significantly, the OCR found that UMMC failed to provide individual notification of the data breach, as it failed to notify the individuals whose unsecured PHI was contained on the laptop and only provided notification on its website and through local media outlets.

The lessons from this enforcement action provide guidance to covered entities that they may wish to consider: (1) update policies and procedures to comply with the Security Rule; (2) confirm that physical safeguards are in place for workstations; (3) confirm and update security risk assessment and management policies and procedures; (4) implement access control measures, including specific user names and passwords for access to PHI; and (5) implement a breach notification policy that includes processes to notify individuals in the event of a data breach and follows the HIPAA breach notification requirements.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

France's National Data Protection Commission Orders Microsoft to Protect is Users' Data

An investigation by France's National Data Protection Commission (CNIL) has found that Windows 10 has been "collecting excessive user data" and has been tracking users' web browsing without their consent. The CNIL has ordered Microsoft to take steps to uphold the "security and confidentiality" of its users' personal information.

The investigation found Windows 10 tracks apps downloaded by the users and the time spent using the apps. Microsoft reported it uses the information to fix bugs and improve Windows 10. However, CNIL found the tracking was not essential to operating Windows 10 and therefore an infringement on a user's privacy.

In addition, the CNIL expressed its concern for the PIN security feature in Windows 10. The feature allows users to enter a PIN to log into the system. There is no restriction on the number of times a PIN may be entered, which makes it susceptible to brute force hacking.

Microsoft responded to CNIL's notice by stating it will be working closely with CNIL and will be releasing an updated privacy policy next month.

There are approximately 10 million Windows users in France and 270 million users in the U.S.

— Kathryn M. Rattigan and Leonel Gonzalez

CYBERSECURITY

Turkish Hackers Claim Hacking into Library of Congress Website

A hacking group that has dubbed itself the "Turk Hack Team" is taking credit on an online message board that it hacked into the Library of Congress website and hosted systems of Congress.gov, the Copyright Office, the Congressional Research Service, and other governmental sites.

As a result of the hacking, the Library of Congress website was shut down for an unspecified period of time.

— Linn Foster Freedman

Auto-ISAC Announces Automotive Cybersecurity Best Practices

Members of the Automotive Information Sharing and Analysis Center (Auto-ISAC) recently released an overview of comprehensive Automotive Cybersecurity Best Practices, developed as a proactive measure to further enhance vehicle cybersecurity throughout the industry. Cybersecurity has been a significant concern in the automotive industry, especially since the *Wired* article in July 2015 that described hackers remotely taking control over a Jeep while it was driving 70 miles per hour on a highway. Fortunately, the subject was participating in an unofficial test with the hackers who used previously unknown exploits to control the vehicle. The new Automotive Cybersecurity Best Practices represent the work of over 50 automotive cybersecurity experts who worked more than five months to advance automotive cybersecurity capabilities. As an example of where the Internet of Things (IoT) meets real-world risk, this is a major step forward in public safety. As stated by the Alliance of Automobile Manufacturers, the Best Practices provides guidance to assist an organization's development in seven key topic areas, including the following:

- Governance: Aligns a vehicle cybersecurity program to an organization's broader mission and objectives.
- Risk assessment and management: Mitigates the potential impact of cybersecurity vulnerabilities by developing processes for identification, categorization, prioritization, and treatment of cybersecurity risks.
- Security by Design: Follows secure design principles in developing a secure vehicle, as well as the integration of cybersecurity features during the product development process.
- Threat detection and protection: Detects threats, vulnerabilities, and incidents to proactively monitor environments and mitigate risk.

- Incident response: Enables automakers to respond to a vehicle cyber incident in a reliable and expeditious manner.
- Awareness and training: Cultivates a culture of cybersecurity and ensures that individuals understand their role and responsibility in promoting vehicle cybersecurity.
- Collaboration and engagement with appropriate third parties: Enhances cyber-threat awareness and attack response.

— Richard M. Borden

Illinois Voter Registration Database Hacked

The Illinois State Board of Elections has notified voters that its online voter registration site has been hacked.

According to the letter sent to Illinois voters by the Board of Elections, “We have found no evidence that they added, changed, or deleted any information in the database. Their efforts to obtain voter signature images and voter history were unsuccessful.”

It is unclear what specific information was obtained during the hacking. The Board of Elections reported that “[T]he attackers took advantage of a programming flaw in the website’s database.” The attack, known as an "SQL injection," occurs in databases using the SQL programming language.

— Linn Foster Freedman

DRONES

Drones Used for Accident Analysis – Quickly, Safely, and Accurately

Last week, the results of an experiment conducted by the Las Vegas Metropolitan Police Department (LVMPD) and Unmanned Experts Inc. (Unmanned Experts), a Denver-based unmanned aircraft systems (UAS) technology applications company, using UAS to analyze accidents were released. The experiment involved LVMPD and Unmanned Experts comparing the process of recording and measuring evidence at an accident scene using all the traditional methods against the process used by UAS.

The two teamed up to simulate a car hitting a pedestrian and then running off the road. First, the LVMPD diagrammed the accident scene using a traditional, ground-based GPS total station. Then Unmanned Experts used an Aeron SkyRanger UAS to do the same. The UAS was positioned about 20 meters over the accident scene. It was programmed to fly a grid pattern with the camera pointed straight down. Additional photos were taken from 15 meters and 10 meters as well.

The result? The UAS was able to detail the accident scene in a three-dimensional point cloud (allowing for precise calculations of distance between points of interest at the scene), keep officers off the road (one of the greatest causes of death for police officers has been traffic-related accidents), and complete the process significantly faster than the LVMPD on the ground. Unmanned Experts said, “We’re getting inquiries from many local and state police agencies asking about how to incorporate this technology into their accident and crime teams. We see drones becoming an essential tool for quick, safe, and legally sound investigation support.”

— Kathryn M. Rattigan

STUDENT PRIVACY

Judge Seals Transcript of Title IX Hearing

A federal judge in North Carolina sealed a transcript of a University of North Carolina (UNC) hearing to determine whether the plaintiff was responsible for committing sexual acts without consent. In the case in question, the defendant brought suit against UNC, Jane Doe, and various school administrators after the Administrative Judicial Board found him responsible for committing sexual acts without Jane Doe's consent. Jane Doe, the student who brought the complaint, moved that the court seal the transcript of the hearing and permit her to proceed under a pseudonym.

Jane Doe claimed that Family Educational Rights and Privacy Act (FERPA) provided evidence of a compelling governmental interest in keeping the transcript private that outweighed any presumption that court records should be public. The plaintiff argued that the transcript was only part of his educational records, not Jane Doe's records, and that FERPA did not provide a mechanism for sealing court documents. The court disagreed.

The court held that the hearing transcript constituted an "education record" as defined by FERPA and that the transcript was part of both the accused student and the alleged victim's records. Accordingly, it held that Jane Doe had a compelling interest in sealing the hearing transcript.

— Kathleen E. Dion

PRIVACY TIP #45

Evaluate the Data Security of Your Dream Car before You Buy It: Tesla Is on Top for Data Security Right Now

We have previously reported on hackings of automobiles [view related posts here, here, and here]. Not only can hackings obtain information about your driving habits, your GPS usage and location, the use of your cell phone, access to your contacts, and other information, it can also be dangerous to your physical health.

A car hacking can take control of your car, turn off the lights, open the door to your vehicle, and alter the steering, all of which can cause you harm.

According to security experts, most automobiles are manufactured without data security in mind, and manufacturers are just starting to incorporate data security measures into the manufacturing process. If you are in the market for a new car, check out the data security of the vehicle before you buy it for the protection of your personal information and your physical safety.

Recently, a white hack hacker observed that "Tesla is on the path to be the most secure car." According to the security researcher, Tesla cars are some of the toughest to hack. Why? Because it uses new technology, and it boasts of being a technology company first and a car company second.

Tesla was one of the first car manufacturers to invite hackers to try to hack into its vehicles' security and to establish a bug bounty program that allows security hackers who find serious vulnerabilities to get paid for their efforts. It actually hires hackers as employees to test the security of its manufacturing process—

full time. It is reported that Tesla has 40 hackers on who are strictly devoted to finding security vulnerabilities in Tesla models during the manufacturing process.

It is the only car manufacturer to my knowledge that uses strategies employed by nation-states (hiring full-time hackers to hack into U.S. government and companies' systems) to focus on hacking into the data security vulnerabilities of its own products. Brilliant. Of course, that is what has been said about Elon Musk.

A Tesla just might be my new dream car—because of its security. Well, that and the fact that the Model S is **really** cool. Did I say dream car?

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team members regularly serve as presenters at topic-related seminars and participate on panels that discuss developments in the area. The following, are several upcoming speaking engagements:

- August 10 – NSPA Regional Meeting in Washington, D.C. (Linn F. Freedman)
- September 12 - 15 – (ISC)² Security Congress in Orlando, FL (Linn F. Freedman)
- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)
- November 15 – ABA Webinar: "Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears" (Linn F. Freedman)

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.