March 17, 2016

HIPAA

OCR Fines MN Hospital System $1.55M for Not Having BAA with Billing Vendor

Yesterday, March 16, 2016, the Office for Civil Rights (OCR) issued a press release announcing that it has settled its investigation of North Memorial Health Care System (NMHCS), located in Minnesota, for $1.55 million, saying that the settlement "underscores the importance of executing HIPAA business associate agreements."

The investigation started after NMHCS self-reported in September 2011 that an unencrypted laptop was stolen from the car of an employee of its vendor, Accretive Health, Inc., which performed billing services for NMHCS. The laptop included the protected health information (PHI) of 6,697 individuals.

The resolution agreement indicates that OCR alleged that NMHCS provided access to at least 289,904 of its patients' PHI without having a business associate agreement in place with Accretive.

Further, the resolution agreement alleges that NMHCS failed to conduct "an accurate and thorough risk analysis."

In addition to the fine of $1.55 million, NMHCS entered into a Corrective Action Plan indicating that it would develop policies and procedures related to business associate relationships, modify its existing risk analysis process, develop and implement a risk management plan, train its employees, report any additional events, and provide annual reports to the OCR on its progress.

There are several important lessons learned from this case. The importance of encrypting laptops cannot be underestimated, and this case is another example of a loss of data that could have been prevented if the laptop had been encrypted. Further, this fine resulted from a business associate's data breach that occurred from failing to encrypt a laptop containing the PHI of a covered entity, which underscores the importance of evaluating business associates' data security measures. Finally, this is the first OCR fine against a covered entity for failing to have a business associate agreement in place with the business associate. That message is loud and clear in the OCR's press release. Covered entities may wish to take this OCR guidance and review processes in place for business associate contract management.

— Linn Foster Freedman

DATA BREACH

21st Century Oncology Notifies 2.2 Million of Data Breach

In the continuing saga of health care entities being targeted by hackers, 21st Century Oncology (21st Century), located in Fort Meyers, Florida, late last week began notifying up to 2.2 million current and former patients about a hacking incident that compromised their names, Social Security numbers, insurance information and diagnostic information. In a regulatory filing, the company indicated that the information may have been copied and transferred.

21st Century operates 145 centers in 17 states in the United States and 36 centers in Latin America. The company has confirmed that patients resided in all 50 states.

It was notified by the FBI in November 2015 that it may have suffered a data breach and requested that notification be delayed during the investigation of the intrusion. The intrusion dates back to October 3, 2015.

21st Century is offering one year of credit protection services to the affected patients. Plaintiffs' attorneys are already "investigating."

— Linn Foster Freedman

Missing Laptop Returned after Premier Healthcare Reports Data Breach of 205,748 Patients

Premier Healthcare, a multi-specialty group located in Bloomington, Illinois, announced in early March that an unencrypted laptop has been missing from its billing department since early January and started notifying affected patients of the data breach pursuant to state and federal law. The unencrypted laptop contained the personal information of 205,748 patients, including the Social Security numbers and financial information of over 1,700 patients.

In a strange twist of events, right after Premier started notifying patients of the data breach, the laptop was returned to Premier—it just showed up in the mail. I am thinking there was no return address label on the envelope.

According to Premier, forensic tests were performed that showed the laptop had not been turned on or accessed since it went missing, and therefore, the incident was not really a data breach.

The lesson learned? The importance of encrypting all laptops—even if they are located in a locked administrative building.

— Linn Foster Freedman

Response to Data Breach at UCLA Creates Controversy

Universities are an attractive target for hackers because they contain many access points in their networks, and the networks contain financial and personal data as well as intellectual property. Last summer, hackers breached the computer network at the UCLA medical center. In response, the University's president, Janet Napolitano, covertly ordered a new security system to monitor and store Internet traffic on all of the University of California campuses. Napolitano stated that the purpose of the system is not to monitor individual emails or browsing history but to monitor cybersecurity.

Students and faculty who learned about the system do not see it that way. Faculty members have expressed concern that the security system impedes on their right to share in shaping policies at the university. Graduate students have also expressed concern that their research data is compromised because their human subjects were promised confidentiality and now their information is stored and can be subpoenaed. They also expressed concerns that this system calls into question their right to academic freedom, freedom of inquiry, and privacy.

Last week, the Graduate Assembly passed a resolution opposing this "Coordinated Monitoring." The resolution cites the University of California's Electronic Communications Policy, which states that, except under some limited circumstances, "[t]he University does not examine or disclose electronic communications records without the holder's consent" and that "any such examination or disclosure of data is subject to the 'least perusal' standard." Furthermore, "the University is required to notify any affected individual of the examination or disclosure of their data, along with the reason(s) for such actions." The resolution calls for a cessation of the "Coordinated Monitoring," among other things.

Universities are faced with unique challenges to prevent cyberattacks. Unlike a company that can control how employees access its network, universities don't have that option. In the face of other breaches, some universities have chosen less extreme measures by consolidating business systems with sensitive data and placing controls on how that data is used. Ultimately, universities are looking to balance protecting the security of their data without compromising the privacy of their students and faculty or them from doing their work.

— Kathleen E. Dion

ENFORCEMENT + LITIGATION

FCC Unveils Broadband Privacy Rules for Internet Service Providers

We have been waiting for—and the Federal Communications Commission (FCC) delivered—its long anticipated broadband data privacy and security rules on March 10, 2015. Through the proposed rules, the FCC has declared its enforcement authority over the data privacy and security practices of Internet service providers (ISPs), much to the chagrin of the industry, which argues that the FTC framework is sufficient to protect consumers and that there is no need for another regulatory body to get into the enforcement fray of data privacy and security.

Under the proposed rules, which are being considered by the full commission, broadband providers must obtain express opt-in consent from customers before using and sharing the customers' data outside of providing services to customers. Like provisions in the Gramm-Leach-Bliley Act applicable to financial institutions, the providers would be able to use customer data to market other products or services offered by affiliates unless the customer opts out of the sharing of the information with those affiliates.

Consistent with other laws applicable to other industries, the proposed rules require ISPs to implement reasonable data security measures to protect consumer data. Significantly, the rules include requirements to notify customers within 10 days of a data breach and the FCC within 7 days of discovery of the breach, which is shorter than most laws applicable to other industries.

The commission will review the proposed rules during its next meeting on March 31.

— Linn Foster Freedman

FINRA Fines Raymond James Financial Services $500,000

Financial services firm Raymond James Financial Services Inc. (Raymond James) has agreed to settle an investigation by the Financial Industry Regulatory Authority (FINRA) for $500,000. The investigation stems from allegations that Raymond James requested that new financial advisers disclose and bring confidential customer information to Raymond James when joining the firm from other brokerage firms, without getting the customers' permission or providing an opt-out from the disclosure to the new firm. FINRA further alleged, that in some cases, financial advisers who were being recruited by Raymond James gave customer information to Raymond James even when the customer opted out from the disclosure. Finally, FINRA alleged that Raymond James recruits didn't get affirmative consent when the customer lived in a state that required opt-in consent. FINRA noted that Raymond James did not have proper processes in place to determine whether consent had been obtained appropriately.

FINRA alleged that bringing private customer information to Raymond James without customers' permission to do so violates Rule 10 of the Securities and Exchange Commission's Regulation S-P.

Raymond James agreed to pay the $500,000 fine and a censure from FINRA, as well as a review of its internal controls to ensure compliance going forward.

Enforcement actions by FINRA for data privacy and security issues are few and far between, and valuable lessons can be learned from this one. Financial services firms would do well to take a look at their processes for disclosure of customer information and the opt-in and opt-out requirements of state and federal laws and regulations, as applicable.

— Linn Foster Freedman

FTC Files Complaint against Solar Panel Company for Do-Not-Call Violations

The Federal Trade Commission (FTC) filed a complaint against Francisco J. Salvat and his companies KFJ Marketing, LLC; Sunlight Solar Leads, LLC; and Go Green Education (collectively, Defendants) for violations of the Telemarketing Sales Rule (TSR), failure to honor do-not-call requests, failure to transmit caller identification, and initiation of unlawful prerecorded telemarketing messages. In the FTC's press release, Jessica Rich, director of the FTC's Bureau of Consumer Protection, said, "Mr. Salvat's companies ignored the Do Not Call Registry and made illegal robocalls. Breaking the law isn't a great way for a company to introduce itself to potential customers."

According to the complaint, prerecorded calls from the Defendants about consumers' energy bills were made, saying "stop the 14% increase coming soon," and then if a consumer "pressed one," they were transferred to a telemarketer who tried to sell them solar panels. When consumers asked the Defendants to stop calling, the FTC alleges that those requests were most often ignored. The FTC asks the court to award monetary civil penalties for the TSR violations and to enter a permanent injunction to prevent future violations. We will watch for a settlement in the near future.

— Kathryn M. Rattigan

CYBERSECURITY

Data Security Firm Staminus Victim of Hacking

Hackers apparently amused themselves by hacking into the database of security firm Staminus' and

dumped the information, including customer information and credit card numbers, online. Staminus is quick to note that it does not collect tax ID numbers or Social Security numbers of its customers.

The hackers intruded into the company's server, seized control of its routers, and reset the routers to factory settings, which brought the whole system down. This is a very scary proposition for any company.

Staminus is working with law enforcement on the intrusion. Staminus is recommending that its customers closely watch their credit card statements and report any unauthorized charges, as well as reset their Staminus account passwords, that is, when the company account is operational again.

— Linn Foster Freedman

TruShield Report Says More Cyber Threats in 2016 Than Ever Before

TruShield released its *2015 Annual Cyber Threat Intelligence Report.* The outlook: 2016 will see even more ransomware and phishing attacks than last year. And guess who is facing the biggest threat? Law firms. Paul Caiazzo, principal, chief security architect for TruShield says, "The attackers know law firms process highly sensitive information for their clients, and a lot of the time...attackers also know that law firms and the legal industry in general lacks standardization on security program structures, controls, and oversight. This divergence can result in security weaknesses." The report also predicts that email will be the most vulnerable access point for hackers and that mid-sized law firms (between 50-150 attorneys) will be the most targeted. How will the hackers target these firms? Through the firms' employees. Anyone with a public profile could fall victim to a phishing attack. For law firms this year, TruShield advises frequent (and thus early) detection of any threats to their information technology systems.

What else does TruShield's report tell us? Well, last year, most of the cyber-attacks were initiated in China and Russia, but in the U.S., the source of cyber-attacks came most frequently from California, Michigan, Kansas, and Washington state. And the report predicts that cyber-crime will grow by 15-40 percent in 2016, along with a jump in cybercrime-as-a-service attacks (i.e., a hacker enters a backdoor on a victim's computer or device and downloads malware, ransomware, or other malicious software to the device or network enabling the hacker to resell the victim to another data harvester). Check out the full report and start updating your security systems right away.

— Kathryn M. Rattigan

DATA PRIVACY

Body Hackers: Implanting RFID Chips in the Human Body

An RFID chip can hold encrypted information, unique enough to say; identify you as the owner of your smartphone (to unlock it); or open a door (to your home). A bizarre new company, Grindhouse Wetware, started by Amal Graafstra (Graafstra), introduced its RFID chip implants to the world through an Internet video where "Northstar" (an RFID chip) was shown being implanted into a person's hand. This group of people who are willing to implant these chips in their bodies believe technology has reached the point where it can improve the human body—they are known as body hackers.

Graafstra says, "A patient may someday come very soon and say, 'My eye is totally fine, but I want an eye that can see infrared. And I want an eye that can zoom." Graafstra says that this RFID chip is a way of merging digital identity and physical identity. At what point have we gone too far? Graafstra says we haven't gone far enough. He says, "I think once people realize, 'Oh it's OK that my grandma has a

pacemaker'…people are going to start to accept this. You know, the era of transhumanism, I would say, is here. So let's accept that and then see where that logically takes us." Not only does this movement propose new questions about human and potentially cyborg identities but it also brings forth questions about whether we will live in a world where our identities are written on our sleeves (almost literally).

— Kathryn M. Rattigan

Lesson in the History of the Gramm-Leach-Bliley Privacy Protections: Victoria's Secret Started It All

Did you know that a Victoria's Secret catalog is one of the top reasons that Congress included privacy protections in the Gramm-Leach-Bliley Act (GLB Act)? The GLB Act protects consumers' financial information and requires financial institutions to explain their information-sharing practices to consumers. These privacy protections were introduced by Representative Ed Markey of Massachusetts. The GLB Act's privacy protections are known as Title V. Markey did not receive much support at the get-go; however, Representative Joe Barton of Texas expressed his support (and concern) for protecting financial information. Barton explained that his credit union had sold his address to Victoria's Secret and that he started receiving catalogs at his home. Of course, we all receive catalogs all the time, but Barton's concern was that he did not want his wife thinking that he had bought lingerie for women in Washington, D.C. (where his wife presumably did not spend most of her time). With Barton's support, the Markey Title V amendment to the GBL Act was passed, and Barton could rest easy that his credit union would no longer sell his information to lingerie stores. Note, however, that Barton's address was most likely not sold to Victoria's Secret directly. Many financial institutions furnish customer data to credit reporting agencies, which was most likely then sold to a third-party advertiser. Thankfully, Barton received that Victoria's Secret catalog or perhaps there wouldn't have been enough support to include these important privacy protections that we still support and follow today. You never know where the inspiration for privacy protections may have come from.

— Kathryn M. Rattigan

PRIVACY TIP #26

Get in Compliance with State Data Security Laws—This Week: CT

We previously reported that several states, including Connecticut (view related post) and Rhode Island (view related post), have adopted data security requirements, similar to the Commonwealth of Massachusetts' data security regulations that have been in effect since 2010. The compliance dates for different sections of the Connecticut data security standards were July 1, 2015; October 1, 2015; July 1, 2016; and October 1, 2017. We are working with clients on compliance with these new laws and thought it would be beneficial to remind everyone about the provisions and upcoming compliance deadlines.

This week we will point out some important dates and compliance issues that are set forth in the Connecticut data security law, and next week, we will focus on the new provisions in the Rhode Island data security law. Of course, this assumes that companies with Massachusetts residents' personal information are already complying with the Massachusetts data security regulations and have a written information security program in place (i.e., if you have any Massachusetts employees).

Here is a cheat sheet for Connecticut (this list is not exhaustive, but informative only):

As of July 1, 2015:

All state agencies must require by contract that all state agency contractors:

- "Implement and maintain a comprehensive data-security program for the protection of confidential information…which shall include: (A) security policy for contractor employees related to the storage, access and transportation of data containing confidential information; (B) reasonable restrictions on access to records containing confidential information, including the area where such records are kept and secure passwords for electronically stored records; (C) a process for reviewing policies and security measures at least annually; and (D) an active and ongoing employee security awareness program that is mandatory for all employees who may have access to confidential information provided by the state contracting agency that, at a minimum, advises such employees of the confidentiality of the information, the safeguards required to protect the information and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law"
- Limit access to state confidential data
- Maintain state confidential information in secure servers with firewall protection and intrusion detection
- Implement a data breach investigation and response procedure
- Appropriately store state confidential information

What does this mean if you are a company that contracts with the State of Connecticut? These requirements apply to you, and if you do not have these measures in place, you might consider implementing policies and procedures so you are not at risk of losing a state contract.

As of October 1, 2015 (effective October 1, 2017):

All health insurers, health care centers, or other entities licensed to do health insurance business in the state; pharmacy benefits managers; third party administrators; and utilization review companies:

- shall implement and maintain a comprehensive information security program to safeguard the personal information of insureds and enrollees that is compiled or maintained by such company. We call it a CISP.
- The CISP must be in writing.
- The CISP must contain administrative, technical and physical safeguards appropriate to the size and scope of the company.
- The CISP shall be updated as necessary and practicable, but at least annually.
- The CISP must contain very specific security requirements outlined in the law (Sections A-L).

As of October 1, 2017, those companies must:

- Certify annually to the Insurance Department…that it maintains" a CISP that complies with the law
- Provide a copy of the CISP to the attorney general or insurance commissioner as requested

So the Privacy Tip for this week is "Get in Compliance." It's never too early.

— Linn Foster 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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP