Having trouble viewing this message? Please click here.

July 30, 2015

Data Privacy + Security Insider

DATA BREACH

Member Information Accessed Through Healthfirst's Online Portal During Fraud Scheme

On July 25, 2015, Healthfirst Inc. notified approximately 5,300 of its members that their information may have been compromised during a criminal fraud scheme perpetrated against it.

The fraudulent scheme was discovered by Healthfirst in 2013, and it notified the Department of Justice (DOJ), which began an investigation and ultimately charged the perpetrator with fraud. The DOJ discovered during its investigation that the criminal accessed and stole member information through Healthfirst's online portal between April 2012 and March 2014, and the DOJ informed Healthfirst of this fact on May 27, 2015. The information compromised included members' name, address, date of birth, health insurance plan information, description of missing services, physician number, Healthfirst member ID number, patient ID number, claim number, diagnosis codes, Medicare and Medicaid ID number.

Healthfirst is providing affected individuals with credit monitoring and restoration services and has cautioned its members to review their Explanation of Benefits statements closely.

— Linn Foster Freedman

OPM Data Breach Update

The Senate Appropriations Committee has approved funding to provide the 22 million individuals affected by the OPM data breaches with 10 years of credit monitoring services and $5 million in liability protection for damages, extending the OPM's offer of three years of services for those affected by the background check breach and 18 months for those affected by the breach of personnel records.

OPM also requested an appropriation of $37 million to beef up its security, but the request was rejected

by the Committee.

The voice vote approval must move through both the House and the Senate before the protections can become available to affected individuals.

— Linn Foster Freedman

DATA SECURITY

Dodge, Ram, and Jeep Vehicles Recalled due to Hacking Vulnerabilities

As technology moves forward, more and more of our everyday gadgets will be connected to the Internet. With that convenience may come some vulnerabilities. On July 24, 2015, Chrysler and its parent company FCA US LLC (FCA US) announced a recall of 1.4 million Dodge, Ram, and Jeep vehicles due to the vehicles' software hacking vulnerabilities that were discovered at a media demonstration. Chrysler determined that hackers could potentially access a vehicle's radio, windshield wipers, and transmission remotely. Chrysler's vehicles have not been hacked at this point, but they want to recall the vehicles to prevent any such attack in the future. Chrysler is installing new security features and adding additional anti-hacking measures to protect its vehicles and its customers. Chrysler made a statement assuring the public that "[n]o defect has been found. FCA US is conducting this campaign out of an abundance of caution. The software manipulation addressed by this recall required unique and extensive technical knowledge, prolonged physical access to a subject vehicle, and extended periods of time to write code."

However, Chrysler's software update is not the end of this issue. After the recall announcement, the National Highway Traffic Safety Administration (NHTSA) opened an investigation into the effectiveness of the software updates. Additionally, Sen. Edward J. Markey and Sen. Richard Blumenthal introduced the Security and Privacy in Your Car Act (or SPY Car Act) which would direct the NHTSA to develop cybersecurity standards for vehicles.

This recall and investigation is one of the first in the new Internet of Things era. This will certainly not be the last.

— Kathryn M. Rattigan

OIG Confirms Clinton Sent Classified Emails Through Private Account

The Office of the Inspector General for the State Department recently confirmed in a Memo that former Secretary of State Hillary Clinton sent emails with classified information in them through her private email account without marking them as classified.

Freedom of Information Act officials have confirmed that their initial review of 55,000 pages requested through FOIA requests have discovered "hundreds of potentially classified emails within the collection."

The OIG stated that the State Department "should ensure that no classified documents are publicly released."

— Linn Foster Freedman

HEALTH INFORMATION PRIVACY

House Passes Medical Innovation Bill That Would Revise HIPAA

On July 10, the U.S. House of Representatives approved the 21st Century Cures Act (the Act), a bill intended to support advancements in medical innovation. The Act includes measures aimed at spurring medical research, reducing the regulatory burden on medical device development, improving health information interoperability, and expanding telehealth coverage.

In order to facilitate collaborative research, the Act proposes revisions to HIPAA regarding the ways in which protected health information (PHI) may be used or disclosed for research purposes. The Act directs HHS to "revise or clarify" HIPAA's Privacy Rule to:

1. allow the use or disclosure of PHI by a covered entity for research purposes, including the pursuit of generalizable knowledge, to constitute a use or disclosure of PHI for health care operations purposes;

2. remove a current limitation on payment for disclosures of PHI for research purposes;

3. add the sharing of PHI with entities subject to FDA oversight for research activities as a permitted disclosure of PHI for which a patient authorization is not required;

4. permit researchers to remotely access PHI; and

5. enable researchers to obtain one-time authorizations for uses and disclosures of PHI for future research purposes.

The Act's HIPAA provisions have generated controversy among health privacy experts. Although some commenters have praised the relaxed requirements for sharing PHI for research purposes, others have expressed concerns that the Act goes too far to reduce individuals' abilities to consent to the use or disclosure of their PHI, and that the Act seeks to eliminate a perceived barrier to medical research posed by HIPAA that does not actually exist. It remains to be seen how the U.S. Senate will address these concerns as it reviews and drafts its own version of the Act, which is not expected to pass until early 2016.

— Conor O. Duffy

NIST Releases Draft Guide for Use of Mobile Devices for Medical Providers

The National Institute of Standards and Technology (NIST) cybersecurity center released a draft guide last week for health IT professionals to use to bolster security for the use of mobile devices in the health care industry. The use of smartphones and other mobile devices have exploded in use in the health care industry and according to NIST "Mobile devices are being used by many providers for health care delivery before they have implemented safeguards for privacy and security."

The how-to guide assists with directions on implementing security procedures across the network, including a mobile device management platform. The guide examines security risks that threaten patient data including the loss of mobile devices, and the importance of encryption was emphasized.

The guide is a useful tool for health IT professionals and it is worth a closer look. Public comment is open

on the guide until September 25.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

The Facebook Warrant Decision

Last week a New York state appeals court recognized that "Facebook users share more intimate personal information through their Facebook accounts than may be revealed through rummaging about one's home." Nonetheless, the court held that online providers and their users are powerless to stop the government from obtaining details about the users' online activities once a search warrant has been issued, even where the search warrant may be improper.

The court held, consistent with well-established law, that once a law enforcement official possesses a search warrant directing a third party (e.g., Facebook, Google, cable company providing internet access) to provide details about an individual's online activity (e.g., Facebook account, Google email account, search history), that third party and the individual whose account is under investigation have no ability to prevent law enforcement from obtaining those account details. According to last week's decision, courts should not intervene until after the production is made. The individual's remedies come later, such as by filing a motion to suppress the evidence in a subsequent criminal case brought against the individual. But that remedy simply keeps those often sensitive details away from the jury. By then, the government has spent months or years in possession of them.

The decision highlights the difference between a subpoena and a search warrant as tools to compel production of information and documents from a third party. A subpoena is typically served on the recipient, who then has a set period of time to make the production or file a motion in court challenging the subpoena prior to production. The recipient may promptly share the existence of the subpoena with the target, such as the Facebook user, whose information is the subject of the subpoena. The target may file his own motion to quash in court, seeking to block the production. Effective lawyers can often negotiate the subpoena, reaching agreements to narrow the scope of what must be turned over and to provide copies of documents rather than originals.

A search warrant's execution can be far more dramatic and disruptive. Law enforcement officials often appear at the recipient's office or home, warrant in hand, and immediately start rummaging through cabinets and drawers hunting for the documents in question, which are then seized and carted away. In the case of electronic data, that may mean the government seizes the recipient's computers.

Facebook argued that its situation was more akin to a subpoena compliance than a warrant because the government relied on Facebook employees to gather the targeted details, and therefore it should have the ability to context the warrant prior to execution. The appeals court disagreed, finding that distinction as irrelevant since a warrant need not be executed through a forcible entry, search and seizure.

In the court's view, Facebook and its users have sufficient pre-execution protections because a warrant can only be issued after a "neutral and detached judicial officer or magistrate" has determined that all constitutional safeguards are satisfied. The problem there, many privacy advocates would argue, is that the judicial officer's determination is made behind closed doors and with only the government's side of the story.

— Edward J. Heath

LifeLock Inc. Sued by FTC for Allegedly Violating Order and Misleading Customers

In 2010, LifeLock Inc. entered into a settlement with the Federal Trade Commission (FTC) and 35 state attorneys general for $12 million for allegations involving false promises and lack of security. The settlement was memorialized with an order and agreement.

On July 21, 2015, the FTC filed suit against LifeLock in the U.S. District Court of Arizona alleging that the company has violated the order and agreement as it continues to make deceptive claims about its security practices and fails to notify individuals when breaches occur. In the settlement, LifeLock agreed to provide the same level of security to its customers as financial institutions, but the FTC says LifeLock hasn't implemented those security measures, including protecting sensitive personal information such as credit card information, Social Security numbers, and bank account numbers.

LifeLock responded to the suit by stating "We disagree with the substance of the FTC's contentions and are prepared to take our case to court."

Coincidentally, that same day, a federal judge dismissed a proposed class action case against LifeLock claiming it misled its investors about compliance with the FTC Order in its annual 10-K filing. The suit alleged that the FTC investigation was buried in small print in the middle of the disclosure which constituted a deceptive practice. The Judge disagreed and dismissed the suit.

— Linn Foster Freedman

DATA PRIVACY

tyntec Releases BYOD Survey 2015

tyntec, a telecom-web convergence company, recently released its *BYOD Survey 2015: Employees' Choice for Mobility* white paper. The paper is the culmination of an online survey of 1,320 respondents from May 16 - May 22, 2015. The responses were from the U.S., U.K., and Spain.

The survey is interesting, and reveals what we are seeing in the industry—that there is "sluggish adoption of BYOD policies while employees voice strong privacy concerns and preference on device usage."

While more and more employees are using their personal devices for business purposes for convenience, employers are getting into issues when the boundaries for using those personal devices are not clear for employees. That's where an enterprise-wide BYOD policy is useful and might want to be considered.

"BYOD is the new norm, and the sooner enterprises embrace sound BYOD policies and user friendly features, the sooner they can increase productivity and eliminate concerns from its employees and IT," said Thorsten Trapp, Co-founder and CTO of tyntec. We agree.

— Linn Foster Freedman

Consumer Financial Protection Bureau Releases Consumer Protection Principles

In response to advanced payment technology and consumers' preference to non-traditional payment systems of writing checks, paying cash, or swiping a credit or debit card, the Consumer Financial Protection Bureau (CFPB) recently released a list of nine "Consumer Protection Principles" that CFPB says is its "vision of consumer protection in new faster payments systems….faster payments could enable faster, safer, and more accessible commerce."

The nine principles are:

1. consumer control over payments;

2. data and privacy;

3. faster and error resolution protections;

4. transparency about transaction status and timely disclosures to consumers about costs, risks, funds availability, and security of payments;

5. affordable cost and disclosure of costs to consumers for comparison;

6. broad accessibility to consumers through qualified intermediaries and non-depositories, such as mobile wallet providers and payment processors provided they are functional and secure;

7. faster funds availability;

8. security and payment credential value; and

9. strong accountability mechanisms to curtail system misuse.

— 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

---