
**July 16, 2015**

# Data Privacy + Security Insider

---

**HIPAA**

**St. Elizabeth's Medical Center Settles with OCR for $218,400 for HIPAA Violations**

The Office for Civil Rights announced on July 10, 2015 that it has entered into a Resolution Agreement with St. Elizabeth's Medical Center (SEMC), owned and operated by Steward Health Care System and located in Brighton, MA. The settlement includes the payment of a fine of $218,400 and the requirement to follow a Corrective Action Plan (CAP). The CAP includes completing a self-assessment on its workforce members' familiarity and compliance with procedures involving:

- the transmission of ePHI using unauthorized networks
- storing ePHI on unauthorized information systems, including unsecured networks and devices
- removal of ePHI from the medical center
- prohibition on sharing accounts and passwords for access or storage
- encryption of portable devices that access or store ePHI
- security incident reporting related to ePHI

The self-assessment report will be made available to the OCR. In addition, SEMC must review its policies and procedures, revise them as necessary, and provide them to the OCR for approval.

SEMC must also review and revise its workforce training, provide the training to OCR for approval, and then train all employees who have access to PHI within 60 days of the approval.

The settlement and CAP stem from two incidents—one that started with a complaint in 2012 and the second with a reportable data breach in 2014. The OCR received a complaint in November of 2012 alleging that SEMC was not complying with HIPAA because workforce members were using an internet-based document-sharing application to store documents containing ePHI of at least 498 patients. The OCR stated that based upon its investigation, it "determined that SEMC failed to timely identify and respond to the known security incident, mitigate the harmful effects of the security incident, and

document the security incident and its outcome."

On August 25, 2014, SEMC self-reported a data breach of 595 patients' information that was stored on a previous employee's personal laptop and USB flash drive.

The two incidents, involving 1,093 individuals were lumped together for the settlement. The settlement is consistent with the OCR's other settlements and is another lesson learned about the OCR's emphasis on the suggestion to utilize encryption technology for mobile devices and the importance of workforce training.

*– Linn Foster Freedman*

---

## Employer Health Plans: Taking Responsibility for Your Business Associates

The Anthem and Premera Blue Cross data breaches caused widespread panic throughout the employer health plan community earlier this year. For many, these data breach announcements served as a wakeup call for employer health plan sponsors to review and further refine their business associate contracts.

As a health plan sponsor, the employer is responsible for its health plan's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In carrying out its responsibilities under the plan, an employer may delegate some or all of those responsibilities to one or more business associates, but the employer remains ultimately responsible for the plan's HIPAA compliance. A "business associate" is any party providing services to the health plan that receives, or may receive, protected health information (PHI) from the health plan. A health plan typically has multiple business associates, which can include insurers, administrative service providers, consultants and claim administrators. It is, therefore, important that employer health plan sponsors be able to identify the health plan's business associates and to have on file copies of their service agreements and business associate contracts.

Although HIPAA mandates certain provisions be included in business associate contracts, it became clear in the aftermath of these data breaches that many service agreements and business associate contracts lacked transparency. Accordingly, employers may need to review their business associate contracts for necessary revisions to reflect the lessons learned from the Anthem and Premera Blue Cross data breaches, namely:

- clarifying the responsibilities of the employer health plan sponsor, the health plan and the business associate in the event of a data breach under both HIPAA and any applicable state breach notification laws;
- refining liability and indemnification provisions in the event of a breach; and
- describing the obligations of the business associate with respect to personally identifiable information (versus only addressing personal health information).

The recent large-scale data breaches serve as a reminder that HIPAA imposes significant responsibilities on group health plans and employers may wish to consider using this as an opportunity to review underlying business associate contracts so that they are prepared if their group health plans become subject to such a breach.

*– Virginia E. McGarrity*

**DATA BREACH**

## OPM Data Breach Update—21.5 Million Affected—Largest in Government History

It was confirmed on July 9th by President Obama that the OPM breach did in fact involve the theft of over 21 million individuals' personal information, including Social Security numbers. The confirmation was following an interagency forensic investigation that found two separate cybersecurity incidents—one involving OPM employees and former employees, and the other from the background investigation database. The information stolen affects individuals who underwent a background investigation since 2000 through forms SF-86, SF-85 or SF-85P, including fingerprints of 1.1 million individuals.

The breach started as early as 2014 but was not discovered until May 2015. As a result, OPM Director Katherine Archuleta has resigned her post.

The OPM will offer credit and identity theft monitoring for the 21.5 background investigation applicants, spouses and co-habitants whose sensitive information was stolen from the OPM databases, and the mitigation efforts are being led by the Department of Defense.

The OPM resource website about the breach can be accessed here: www.opm.gov/cybersecurity/

Meanwhile, a second class action suit has been filed on behalf of the American Federation of Government Employees, and for the second time in the last month, the FBI has warned U.S. companies to be on the lookout for a malicious computer program that has been linked to the OPM hacking incident. The malware, called Sakula, is also believed to have been the cause of the Anthem breach.

*– Linn Foster Freedman*

---

## Army National Guard Announces Data Breach Affecting Both Current and Former Members

On July 10, 2015, the Army National Guard announced a breach of its current and former members' personal information, dating back to 2004. The breach occurred when files containing personal information were accidentally transferred to a non-Department of Defense data center by an employee. The data breached included members' names, Social Security numbers, date of birth, and addresses. After an investigation, the Army National Guard has determined that it will notify affected individuals so that they can protect themselves from potential fraud and identity theft. An Army National Guard representative stated, "The issue was identified and promptly reported, and we do not believe the data will be used unlawfully. This was not a hacking incident, in which the intent was to use data for financial gain." To learn more about the breach and the potential for identity theft, click here to go to a website that has been set up for members or call the toll-free hotline at 877-276-4729. The Army National Guard says that this breach is unrelated to the Office of Personnel Management (OPM) breach.

*– Kathryn M. Sylvia*

---

## A Website Coding Upgrade Error Causes a Breach Says Blue Shield of California

Blue Shield of California is sending out notification letters to 843 of its members advising them that as a result of a computer code update it made to its website, when three authorized administrators logged into

their own accounts, they were able to view another authorized user's information who logged into the user's own account at exactly the same time. The affected site was Blue Shield of California's secure health administrator website, which is used by group health benefit plan administrators and brokers to manage plan members' information. The website was taken down.

The information exposed included members' names, addresses, Social Security numbers, Blue Shield identification numbers, and dates of birth. The incident was caused by "human error" of Blue Shield personnel. Blue Shield is offering credit monitoring to the affected individuals.

This incident is a reminder that although we are hearing about cyber-hacking incidents, your own employees are still a large risk for any organization.

*– Linn Foster Freedman*

---

**SOCIAL MEDIA**

**Social Media Campaign Ends in Disbarment for Lawyer**

Lawyers using social media: beware!

The Louisiana Supreme Court has disbarred a lawyer for launching a "viral campaign to influence and intimidate" judges who presided over her friend's child custody dispute.

In a split decision, the Court found that the attorney used social media and blogs to disseminate false and misleading information about a judge's handling of the case, which amounted to an unethical attempt to influence additional rulings.

The Court further found that the use of online petitions, Twitter messages and blog posts to tell the public to call the judges and let them know they are watching them and were "horrified" by the rulings was in violation of the Louisiana Rules of Professional Conduct 3.5, attempting to influence judge improperly, and 8.4, violating rules through acts of another. The court stated that the messages the judges received from people who responded to the social media campaign constituted ex parte communications induced or encouraged by the lawyer. The lawyer alleged that her statements in social media were protected by the First Amendment.

Disciplinary counsel recommended that the lawyer be suspended for one year and one day. The Court rejected the recommendation and disbarred her. The dissenting justices indicated that they felt a three-year suspension was appropriate.

*– Linn Foster Freedman*

---

**Judge Stops Blogging but May Face Discipline**

A Nebraska federal judge called a United States Senator a "wacko" and unfit for a bid for the White House in his blog post…which was criticized by a GWU law professor blogger who said the blog post violated the federal judicial conduct rule prohibiting opposition or endorsement of political candidates…prompting an apology by the federal Judge who pledged to stop blogging permanently…this from the same federal Judge who reportedly has described himself as a dirty old man and appreciates a female lawyer's short skirts and ample chest…we haven't come as far as we think and we don't make

this up…

*– Linn Foster Freedman*

---

**Debtor's Founder Ordered to Turn Over Social Media Accounts to Reorganized Company**

A recent bankruptcy court decision highlights the importance of Facebook pages, Twitter accounts, and similar social media assets in today's business marketplace. It's not always clear how these might be best protected, but the decision provides some context for considering the very real problems business owners and their lenders face today.

To access the full article, click here.

*– Steven J. Boyajian, Michael R. Enright and Patrick M. Birney*

---

**CYBERSECURITY**

Our taxpayer dollars put to good use: big prosecutions and takedowns by the feds this week, including Darkode, Ventila and Ngo.

**Cybercrime Forum Darkode Nailed by the DOJ and FBI**

Yesterday, (July 15, 2015), the Department of Justice (DOJ) announced that the coordinated law enforcement efforts of 20 countries, including the U.S. effectively dismantled the computer hacking forum Darkode with criminal charges filed against 12 of the alleged hackers in the Western District of Pennsylvania, the Eastern District of Wisconsin, the Western District of Louisiana, and the District of Columbia.

According to the DOJ, Darkode "represented one of the gravest threats to the integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world."

Darkode allowed computer hackers, in a password-protected forum, to buy, sell, trade and share illegal methods of hacking and intrusions. It is a member referral forum that was infiltrated by the FBI as part of Operation Shrouded Horizon, but the DOJ touted the coordinated efforts of the coalition of law enforcement agencies in 20 nations "to charge, arrest or search 70 Darkode members and associates around the world."

*– Linn Foster Freedman*

---

**ATM Skimming Crook Sentenced**

The U.S. Attorney's Office in Newark, NJ has announced that Marius Ventila, a Romanian native, was sentenced to 10 years in prison and to pay $7.5 million in restitution for his part in a credit card skimming scam that used card-reading devices to steal bank information from ATMs. The card-reading devices were attached to ATMs to steal account information from the magnetic strips of ATM cards. Ventila also

used pinhole cameras to record customers typing their personal information numbers at ATMs. The scheme allowed Ventila and his cohorts to steal over $5 million from individuals' bank accounts.

*– Linn Foster Freedman*

---

**25-Year-Old Sentenced to 13 Years for Hacking Data Broker Databases**

The Department of Justice has announced that 25-year-old Hieu Minh Ngo has been sentenced to 13 years in prison. His sentence was lighter than expected because he has cooperated with authorities to catch more identity thieves. His crime? He admitted hacking and illegally gaining access to databases belonging to the world's largest data brokers and amassed the personal information, including Social Security numbers, of more than 200 million Americans.

According to the U.S. Attorney's Office, Ngo "used Internet marketplaces to offer for sale millions of stolen identities of U.S. citizens to more than a thousand cyber criminals scattered throughout the world" from his home in Vietnam. His sale of this information has reportedly resulted in the filing of false tax returns with the IRS. The IRS has confirmed that 13, 673 American citizens' personal information was used to file fraudulent tax returns totaling $65 million.

*– Linn Foster Freedman*

---

**E-DISCOVERY**

**PII in Your ESI: The Intersection of Data Privacy and E-discovery**

There is a significant nexus between data privacy and security and e-discovery that grows more pronounced as the volume of data generated multiplies exponentially and the ability of e-discovery tools to collect and process that data grows increasingly sophisticated. Specifically, the e-discovery process presents a very real risk of inadvertently compromising Personal Identifying Information (PII).

Although the definition of PII or protected information varies by jurisdiction, there are certain categories of information that are generally recognized as sensitive and should be safeguarded from unnecessary dissemination in the discovery process. These categories include:

- Social Security Numbers
- Driver's license, passport or state identification numbers
- Taxpayer identification numbers
- Any financial account numbers, credit card numbers or other personal financial information
- Any log in/password information
- Personal Health Information (PHI)

- Birthdays in conjunction with any other identifying information

The following strategies can help minimize the potential for producing arguably protected data in discovery:

- **Conduct targeted collections.** Over-collection of ESI causes many problems, the inclusion of personal identifying information among them. The more targeted the collection is, the lower the likelihood of sweeping up personal identifying data.

- **Have sensitive information highlighted.** If you are using an electronic review platform, it likely has the ability to highlight terms or numbers that may be sensitive.

- **Emphasize the importance.** When preparing training manuals for document reviews, attorneys generally focus on identifying responsive materials and protecting privileged information. Consider devoting a section to identifying PII.

- **Give reviewers the right tools.** Make sure the review team knows what to do when it comes across PII, such as whether it should be withheld or redacted.

- **Perform QC searches.** Perform additional quality control searches prior to production to ensure that you are not letting any PII out the door unknowingly.

*– Andrea Donovan Napp*

---

**ENFORCEMENT + LITIGATION**

**FCC Becomes Another Active Regulator over Data Security Through $3.5M Settlement with Two Telecom Companies**

The FCC has announced that it will receive a settlement payment of $3.5 million from two telecommunications companies—TerraCom Inc. and YourTel America—for allegations around the companies' failure to safeguard customers' personal information. The companies must notify all individuals who were affected and provide credit monitoring for the affected consumers. The companies have also agreed to conduct a privacy risks assessment and implement a security program and data breach response plan.

The settlement arose out of a data breach affecting up to 300,000 individuals' names, addresses, driver's license numbers and other customer information on unprotected Internet servers related to applications for Lifeline, a telephone service program. According to the FCC, the information could be accessed by "anyone with a search engine."

This settlement is a promise made good by the FCC in March when it publicly announced that it would increase enforcement action against broadband service providers for privacy and data security practices.

**–** *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

---