**CalOHII Communications**

**June 2019**

***In this month’s communication,*** the California Office of Health Information Integrity (CalOHII) provides updates on CalOHII activities, news from the federal Health and Human Services (HHS) as well as links to various news articles related to the Health Insurance Portability and Accountability Act (HIPAA) and healthcare industry.

**CalOHII Updates**

* **SHIPM 2019** – CalOHII has published the annual update of Statewide Health Information Policy Manual (SHIPM) – 39 policies and one attachment were updated (refer to the Change Log for specific information). SHIPM 2019 and associated documentation can be found on the [2019 SHIPM page](https://www.chhs.ca.gov/ohii/shipm/statewide-health-information-policy-manual-shipm-documents-version-6-2019/) of the CalOHII website.
* **Compliance Program** – CalOHII started a new targeted review. In addition, the team continues to monitor three active Corrective Action Plans (CAPs) with previously reviewed state entities.
* **State Legislation Review** – CalOHII continues to review and track legislation related to the HIPAA and/or healthcare data privacy. We are tracking 20+ bills that could impact SHIPM 2020 or our Compliance Review program.

**HHS News**

* **Office for Civil Rights (OCR) reached a $3M settlement with Touchstone Medical Imaging** due to a breach of protected health information caused by uncontrolled access into a server via search engines. For more information about the breach and settlement, refer to the [OCR press release](https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/tmi/index.html).
* **OCR reached a $100K settlement with Medical Informatics Engineering** due to a breach that allowed hackers access to 3.5M peoples medical records by using a compromised user ID and password.  The investigation revealed the company did not conduct a risk analysis prior to the breach. For more information about the breach and settlement, refer to the [OCR press release](https://www.hhs.gov/about/news/2019/05/23/indiana-medical-records-service-pays-100000-to-settle-hipaa-breach.html).
* **OCR issued a new fact sheet (entitled “Direct Liability of BA under HIPAA”)** that provides a clear compilation of all provisions through which a business associate can be held directly liable for compliance with certain requirements of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (“HIPAA Rules”), in accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The new fact sheet can be found on the [OCR website](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html).
* **The National Committee on Vital and Health Statistics (NCVHS) provided their 13th Report to Congress** on the status of the implementation of Administrative Simplification provisions of HIPAA. The report can be accessed from the [NCVHS site](https://ncvhs.hhs.gov/wp-content/uploads/2019/03/13th-Report-to-Congress.pdf).

**Other News**

* **HIPAA Journal reported that ransomware attacks are up by 195%** in the 1st quarter of this year, however Trojans continue to be biggest threat. The [full article](https://www.hipaajournal.com/ransomware-attacks-increased-by-195-in-q1-2019-but-trojans-remain-the-biggest-threat/) can be found on their website.
* **The latest Verizon Data Breach Investigations report was released** – the [full report](https://www.verizon.com/about/news/verizon-2019-data-breach-investigations) can be accessed on the Verizon website. [HIPAA Journal](https://www.hipaajournal.com/2019-verizon-data-breach-investigations-report-findings/) provides a summary of the report – including several findings such as 90% of malware arrives via email, executives are 12 times more likely to be targeted in social engineering attacks.
* **Post-Breach: Preparing for a HIPAA Investigation** – [this article](https://www.jdsupra.com/legalnews/post-breach-preparing-for-a-hipaa-53565/) provides some good tips on actions to take after the breach to prepare for an OCR investigation.
* **Causes of HIPAA Breaches: Why Does it Matter** – [this article](https://hallbenefitslaw.com/causes-of-hipaa-breaches-why-does-it-matter/) provides some good reminders of how to prevent data breaches.
* **Deeper Dive: The Landscape of Healthcare Data Breaches** – [this article](https://www.dataprivacymonitor.com/medical-privacy/deeper-dive-the-landscape-of-healthcare-data-breaches/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original) provides a high-level view of data breach statistics for healthcare.
* Department of Homeland Security (DHS) issued security best practices to mitigate risks associated with Office 365 migrations. The best practice information can be found on the [DHS website](https://www.us-cert.gov/ncas/analysis-reports/AR19-133A). HIPAA Journal published [an associated article](https://www.hipaajournal.com/dhs-issues-security-best-practices-to-mitigate-risks-associated-with-office-365-migrations/) with further insights.
* **New Study Uncovers Serious Holes in Healthcare Cybersecurity** – [HIPAA Journal reports](https://www.hipaajournal.com/new-report-uncovers-serious-holes-in-healthcare-cybersecurity/) that the healthcare industry is over reliant on legacy software, vulnerable protocols and unsecured medical devices which are compromising security of health data.
* **OCR data indicates April was the worst ever month for healthcare data breaches** – [this article](https://www.hipaajournal.com/april-2019-healthcare-data-breach-report/) provides some insights on the 46 breaches reported to OCR.

**Contact Us…**

**If you have any questions or comments about the content of this newsletter, contact us at** **OHIComments@ohi.ca.gov****.**

*Past month’s CalOHII Communications can be found on the* [*CalOHII Communications - Archive*](https://www.chhs.ca.gov/ohii/about-calohii/calohii-communications-archive/) *page.*