CalOHII Communications

April 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 Update** – CalOHII is preparing for the review cycles of the recent updates to the Statewide Health Information Policy Manual (SHIPM) – over 40 policies and attachments have been updated. SHIPM 2019 will be available on our website in early June.
- **Compliance Review Activities** – the Compliance Review team delivered the results of a desk review and began coordination with a department to provide technical assistance for a federal review.
- **State Legislation Review** – CalOHII continues to review and track legislation related to the HIPAA and/or healthcare data privacy. We are "tracking" a number of bills that could impact SHIPM 2020 or our Compliance Review program.

HHS News

- **HHS Centers for Medicare and Medicaid Services (CMS) announce the start of their Compliance Review Program** – HHS will randomly select nine (9) HIPAA-covered entities to participate in the reviews. If your department is contacted by CMS, please notify CalOHII at **OHIComments@ohi.ca.gov.**
- **HHS Office for Civil Rights (OCR) Cybersecurity Newsletter –** OCR has moved to a quarterly newsletter, this quarter's newsletter focuses on advanced persistent threats and zero day vulnerabilities.

Other News

- **Compliance Checkup: Mastering HIPAA: Part 1 – The Best Offense is a Good Defense** – this article provides some good insight on what is needed from OCR in the event of a HIPAA breach.
- **Key Privacy and Security Program Elements to Survive a HIPAA Audit** - recent research into OCR audits provides insights on what triggers an audit, what is OCR looking for during an audit, and how penalties are assessed.
- **Beazley Report Reveals Major Increase in Healthcare Hacking and Malware Incidents** – this article states that healthcare accounts for 41% of all breaches, with hacking/malware and accidental disclosure both accounting for 31% (each) of the reported breaches.
- **Healthcare's Strong Network Security May Reflect Outdated Model** – the good news is that healthcare ranks 5th for network security (as reported by SecurityScorecard in the recent 2019 Healthcare Cybersecurity Report). This is the strongest showing for healthcare – which could be due in part to efforts to comply with HIPAA regulations. On the downside, the report states that healthcare employs an outdated "eggshell security model" (hardened perimeter defends soft, vulnerable internal network).
- **Study Confirms Healthcare Employees are Susceptible to Phishing Attacks** – researchers found some interesting insights into what types phishing emails are "clicked" more than others. In addition, the researchers suggest ways to counter the threat from phishing.
- **Serious Security Risks found in Healthcare Laptops** – analysis by Clearwater CyberIntellence Institute found laptops rank 6th among sources of risk in healthcare organizations. Not only are laptops portable and easily lost or stolen, but they were also found to have endpoint data loss, excessive user permissions, and dormant accounts.
- **CHIME: Health IT Cybersecurity Gaps Lie in Data Inventory, Patching Issues** – in response to a request for comment from Senator Mark Warner, CHIME outlined the biggest IT security gaps in the healthcare industry.

Contact Us…

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