CalOHII Communications

State of California
Office of Health
Information Integrity

March 2019

***"CalOHII Communications"* gets a new look** – starting this month, the format of the California Office of Health Information Integrity (CalOHII) monthly *"CalOHII Communications"* has changed and we are now posting it to our website for easy reference.

CalOHII Updates

- **SHIPM 2019 Update** – CalOHII continues work on the updates to Statewide Health Information Policy Manual (SHIPM) for our 2019 revision. SHIPM 2019 will be available in early June.
- **State Legislation Review** – CalOHII has reviewed over 90 bills related to the Health Insurance Portability and Accountability Act (HIPAA) or data privacy. We are "tracking" many that could impact SHIPM or our Compliance Review process.
- **HIPAA Conferences** – CalOHII attended the Health Information and Management Systems Society (HIMSS) conference and the 28th National HIPAA Summit in March. Following are a few takeaways from these conferences:
    - U. S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR) Director Roger Severino talked about the latest civil money penalties (CMPs) totaling $28.6M with a single fine of $16 million to Anthem in October 2018.
    - OCR Director Roger Severino talked about enforcement activities and that OCR will also make business associate compliance and patient access a priority.
    - OCR reviews have identified a trend in issues with risk assessments that they review:
        - Risk assessments have been found to not be accurate or thorough enough. Assessments should include electronic protected health information (ePHI) risks and vulnerabilities; not just technical scans or just physical risks.
        - Scope of risk assessments should be enterprise-wide and include all systems where ePHI is stored, transmitted, or maintained. Include a map of where the ePHI flows and through what systems.
    - HHS Chief Technology Officer Ed Simcox referenced the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, which aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity

objectives and outcomes. See the Public Health Emergency site for additional information.

HHS News

- **Federal Notice of Proposed Rulemaking (NPRM) Update** -
    - **OCR Request for Information (RFI): Modifying HIPAA Rules to Improve Coordinated Care (Regulation Identification Number [RIN]-0945-AA00)** – due to changes in the review process with the new Administration, we have contacted OCR and will be submitting the State's response late. OCR has released all comments for public review.
    - **National Council for Prescription Drug Programs (NCPDP) NPRM Modification of the Requirements for use of the HIPAA NCPDP D.0 Standard (RIN-0938-AT52)** – CalOHII did not receive any comments on this NPRM and therefore will not be submitting a response.
    - **Centers for Medicare and Medicaid Systems (CMS) and Office of the National Coordinator for Health Information Technology (ONC) have released NPRMs** – Although there is reference to HIPAA in the CMS NPRM, it does not propose to make changes to any of the HIPAA regulations. The NPRMs related to interoperability and other 21st Century Cures Act items are linked below. Comments are due May 3, 2019 for both NPRMs.
        - **CMS (RIN-0938-AT79)** - Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-facilitated Exchanges and Health Care Providers
        - **ONC (RIN-0955-AA01)** - 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program
- OCR concludes all-time record year for HIPAA enforcement with $3 million Cottage Health settlement**.** Highlights from the OCR communication include:
    - Cottage Health left a server accessible to the internet due to a flaw in security configuration settings – revealing over 62,000 patients' data. Two years later they had another served misconfigured.
    - In 2018, OCR settled 10 cases and was granted summary judgment in a case before an Administrative Law Judge, together totaling $28.7 million from enforcement actions. This total surpassed the previous record of $23.5 million from 2016 by 22 percent.
    - In addition, OCR achieved the single largest individual HIPAA settlement in history of $16 million with Anthem, Inc., representing a nearly three-fold increase over the previous record settlement of $5.5 million in 2016.

- A related article on the enforcement actions illustrates the themes of the actions are consistent with other years (i.e. lack of business associate agreements, risk analysis).

Other News

- **Why complete an enterprise risk assessment?** – this article, while written for private sector, addresses the concept of "enterprise-wide" risk assessments. OCR has recently noted risk assessments are too narrowly focused and should be enterprise-wide (see HIMSS conference notes above for related information).
- **OCR is getting more patient complaints** – the largest number due to reporting breaches.
- **Two-Factor Authentication: A Top Priority for HIPAA Compliance** – this article provides information about how two-factor authentication is "the best way to comply with the HIPAA password requirements."
- **A summary of 2018 healthcare data breaches** – while the number of data breaches slightly increased, the number of health records impacted nearly tripled. "Insiders" continues to account for the largest percent (28.09%) – this can be due to human error or wrongdoing.
- **In a HIMSS survey**, they found 74% of healthcare organizations experienced a significant security breach in the past 12 months – common themes are online scam artists such as phishing (28%) and insiders (20%). Additionally the survey found that continued use of legacy (unsupported) systems (such as Windows Server and Windows XP) raise "grave concerns" about overall security.
- **5 Common HIPAA Privacy Gaps** – an interesting list that is consistent with OCR and other compliance findings.

Contact Us…

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