**CalOHII Communications**

**November 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**

* CalOHII submitted a coordinated response to the Substance Abuse and Mental Health Services Administration (SAMHSA) Notice of Proposed Rulemaking (NPRM) regarding updates to 42 CFR Part 2. The [NPRM](https://www.federalregister.gov/documents/2019/08/26/2019-17817/confidentiality-of-substance-use-disorder-patient-records) can be found on the Federal Register site.
* CalOHII closed a Corrective Action Plan with a state entity.
* CalOHII has two (2) active Targeted Reviews underway.
* CalOHII is launching a Focused Review on state organizations Risk Analysis/Risk Assessment efforts.
* CalOHII is preparing formal comments to the Department of Justice (DOJ) proposed regulation regarding the Controlled Substance Utilization Review and Evaluation System (CURES). The [regulation package](https://oag.ca.gov/bciis/regs) can be found on the DOJ site.
* CalOHII and California Department of Technology (CDT) have determined CDT is a business associate – separate communication on this item is forthcoming.
* CalOHII is providing technical assistance to several state entities.
* State Legislation Review– CalOHII is reviewing several signed bill to determine possible updates to the Statewide Health Information Policy Manual (SHIPM) in the next cycle. CalOHII will communicate any items effective 1/1/2020 in the December newsletter.
* CalOHII has been awarded a grant from the California Food Policy Advocates to provide an update to the State Health Information Guidance (SHIG).

**HHS News**

* **HHS Issues Final Rule to Rescind the Adoption of the Standard Unique Health Plan Identifier and Other Entity Identifier** – Effective December 7, 2019, the Health Plan Identifier (HPID), Other Entity Identifier (OEID) are rescinded along with two definitions for Controlling Health Plan and Subhealth Plan. SHIPM will be updated in June (specifically policy 4.3.1 – Transactions and Code Sets) to reflect these changes. The [official text of the final rule](https://www.govinfo.gov/content/pkg/FR-2019-10-28/pdf/2019-23507.pdf) can be found on the Government Publication website.
* **Office for Civil Rights (OCR) Imposes a $2.15 million Civil Money Penalty for Repeated HIPAA Violations –** Jackson Health System had several violations of the HIPAA Security and Breach Notification rules between 2013 and 2016. OCR found that the organization “had been in disarray for a number of years.” More information about [this case](https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jackson/index.html) can be found on the OCR website.
* **New Version of the HHS Security Risk Assessment Tool is Available -** OCR and Office of the National Coordinator for Health Information Technology (ONC) released version 3.1 of the tool. More information about [the tool](https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool) can be found on the ONC website.
* **OCR Updates from 11th Annual HIPAA Conference –** [highlights of Director Severino’s presentation](https://www.hipaajournal.com/ocr-hipaa-enforcement-priorities/) at the October conference can be found on the HIPAA Journal website.

**Other News**

* **Tips for Reducing Cyberattack Related Costs –** a recent survey found that the enterprise-level costs associated with a data breach has risen from $1.23 million to $1.41 million in the last year. This article provides some tips on how to reduce costs – including setting up an internal security operations center. The [full article](https://www.hipaajournal.com/an-internal-security-operations-center-cuts-data-breach-costs-by-more-than-half/) can be found on the HIPAA Journal website.
* **Security Advisories on Multiple Virtual Private Networks (VPNs)** – several popular VPN products are being exploited to gain access. For more information on the VPNs and advisories issued, refer to the [full article](https://www.hipaajournal.com/pulse-connect-globalprotect-fortigate-vpn-vulnerabilities-being-actively-exploited-by-apt-actors/) on the HIPAA Journal website.
* **Increase in Ransonware Attacks** – the Federal Bureau of Investigations (FBI) is warning state and local governments along with health care organizations about increasing threats from ransomware. The attacks are initiated through phishing and Remote Desktop Protocol vulnerabilities. The [full article](https://www.dataprivacyandsecurityinsider.com/2019/10/fbi-warns-of-sharp-increase-in-ransomware-attacks-in-certain-sectors/#page=1) can be found on the Data Privacy and Security Insider website.
	+ In a related article, Proofpoint provides some details on the types of cyberattacks hitting the health care industry – such as what is being emailed, who is being targeted to get people to click. [More information](https://www.hipaajournal.com/report-reveals-the-most-common-cyber-threats-faced-by-healthcare-organizations/) can be found on the HIPAA Journal website.

**Contact Us…**

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

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