

**CalOHII Communications**

**August 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**

* **Statewide Data Sharing** 
  + CalOHII is leading an effort to create data sharing between California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Health and Human Services (CHHS)
  + CalOHII is involved in efforts with the Governor’s Office to draft data sharing agreement with all California agencies/departments
  + CalOHII is co-leading a workshop with Department of State Hospitals (DSH) to assist CHHS departments with fully implementing the Data De-Identification Guidelines
* **CHHS 5th Annual Data Expo** – CalOHII coordinated all logistics for Agency’s Data Expo in August and also participated as a presenter. The [Data Expo has been posted on YouTube](https://www.youtube.com/watch?v=jdoziIaAMrs) – fast forward to 42:40 for the beginning of the presentations.
* **Compliance Review Tools –** CalOHII has reviewed and revised tools to reflect the 2019 Statewide Health Information Policy Manual (SHIPM). The updated tools can be found on the [Compliance Review](https://www.chhs.ca.gov/ohii/compliance-review/)page.
* **State Legislation Review** – CalOHII continues to review and track legislation related to the HIPAA and/or healthcare data privacy. We are tracking 23 bills that could impact SHIPM 2020 or our Compliance Review program.

**HHS News**

* **The Spring Agenda for Notice of Proposed Rulemaking (NPRM) was published –** CalOHII is watching ten items for possible actions in the coming months. Potential rule making items include revisions to 42 CFR Part 2; new standards for attachments, acknowledgements, e-signatures; final actions on the Interoperability and Patient Access NPRMs issued by Centers for Medicare and Medicaid Services (CMS) and Office of National Coordinator (ONC); and others.

**Other News**

* **Study Reveals Increase in Ransomware Attacks** – During the 2nd quarter of this year ransomware payments have increased 184%. The most common method of attack was via remote desktop protocol (RDP) ports. The [full article](https://www.hipaajournal.com/study-reveals-increase-in-ransomware-attacks-and-3x-hike-in-ransom-demands/) can be found on the HIPAA Journal website.
* **US Cert released a Joint Ransomware Statement** with recommendations for state and local governments to build resilience against ransomware. The [recommendations](https://www.us-cert.gov/ncas/current-activity/2019/07/30/steps-safeguard-against-ransomware-attacks) can be found on the US Cert website.
* **2018 Cyber Incident and Breach Trend is All Bad** – according to a [2018 Cyber Incident and Breach Trend Report](https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf) - while the number of data breaches and exposed records decreased, the costs associated with breaches went up.  Ransomware cost businesses $8B last year and is expected to grow to $20B by 2021.  The report ends by saying that 95% of all incidents could have been prevented – data security still comes down to people.  The trend report includes a checklist for incident readiness. The [full article](https://www.dataprivacyandsecurityinsider.com/2019/07/2018-cyber-incident-breach-trends-report-all-bad/#page=1) can be found on the Data Privacy and Security Insider website.
* **Compliance Checkup: Mastering HIPAA – Mailing Protected Health Information (PHI)** – Incorrect mailing/sending of PHI is a common theme for data breaches – this article provides some good reminders about how to protect PHI in mailings. The [full article](https://www.brouse.com/compliance-checkup-mastering-hipaa-part-4-mailing-protected-health-information) can be found on the Brouse McDowell website.
* **US Cert released an infographic on 5G wireless network risk factors** – the [infographic](https://www.us-cert.gov/ncas/current-activity/2019/07/22/5g-wireless-network-risk-factors) can be found on the US Cert website. Some of the risks outlined in the materials include - use of 5G components manufactured by untrusted companies, the proliferation of 5G infrastructure may lead to more malicious attacks, unknown security vulnerabilities, and others.

**Contact Us…**

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