CalOHII Communications

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

- **New Chief Counsel** - CalOHII welcomes back Jennifer Schwartz as our Chief Counsel. Jennifer returns to CalOHII after a few years at the Department of State Hospitals where she was their Chief Privacy Officer.
- **SHIPM 2019 Update** – CalOHII is finalizing 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 – a communication will be sent to impacted departments when it is available.
- **Compliance Program** – CalOHII is monitoring three active Corrective Action Plans (CAPs) with previously reviewed state entities. CalOHII completed one request for technical assistance and one targeted compliance review.
- **State Legislation Review** – CalOHII continues to review and track legislation related to the HIPAA and/or healthcare data privacy. We are tracking 25+ bills that could impact SHIPM 2020 or our Compliance Review program.

HHS News

- **HHS Announces Changes to Civil Monetary Penalties** – HHS has reduced the cumulative annual limit for three of the four categories.
- **Office for Civil Rights (OCR) weighs in on application programming interface (API) development** with five new frequently asked questions (FAQs) regarding whether data used by medical apps is HIPAA covered.

- **Federal Notice of Proposed Rulemaking (NPRM) Update -**
  - [Centers for Medicare and Medicaid Systems (CMS) and Office of the National Coordinator for Health Information Technology (ONC) have extended the comment period (to June 3rd)](#) for the interoperability and other 21st Century Cures Act items. Comments on this NPRM are being coordinated by the California Health and Human Services Agency Information Officer (AIO) office. For more information, email Colin.Stevens@chhsaio.ca.gov.

Other News

- **[Amazon Web Services (AWS) Chief Technology Officer Allays Fears about Cloud Security…](#)** – the biggest takeaway from this article is that all users of AWS cloud services should "encrypt everything" that is stored on AWS. For departments that are HIPAA covered entities and/or business associations using cloud services (including those offered by the Department of Technology), the article points out that "by encrypting data, companies meet the requirements of…HIPAA, and other federal and state regulations."
- **[Data security incident response analysis report](#)** provides interesting insight into data breaches – some highlights are:
  - Office 365 is the most common method for phishing
    - [In a related article](#) it points out that in 2018 Microsoft limited the available logs that help identify what attackers accessed/viewed, making it more difficult to pin down the extent of the data breach. However, the article provides some insights on how this risk can be mitigated.
  - Phishing is the most common cause of data breach (at 37%)
  - Average time to detect a breach is 66 days – for healthcare it took an average of 36 days to discover, 10 days to contain, 32 days to complete an investigation, and 49 days to issue notifications
- **[Developing an Incident Response Plan for a Cyber Attack](#)** – this article is a good reminder about the areas to cover in an Incident Response Plan.
- **[5 Questions Corporate Counsel Should Ask about Cyber Risk Assessments](#)** – this article includes several thought-provoking questions pertinent to all departments.

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](#) page.