

What's Your Compliance IQ?

Volume 4

Issue 7

July, 2021



HIPAA News

President Biden has signed an executive order asking the FTC to establish new rules about how tech firms can collect & use customer data to offer more privacy protection for American customers. It also instructs the DOJ & other federal agencies to step up antitrust enforcement especially when it is large tech companies buying smaller companies that can stifle competition.

It focuses on companies such as Facebook, Google, & Amazon collection & use of customer data. It further asks the FTC to take action such as increasing access to broadband internet services, restoring net neutrality rules, reducing anti-competitive clauses in employee contracts & allowing banking customers to more easily transfer their data.

Kroger has a \$5M settlement to re-

solve lawsuits filed by victims of data breach exposing their personal information & PHI. Kroger was one of many victims of Accellion File Transfer Appliance in 12-20. About 1% of Kroger's money & health customers has their sensitive data stolen. While both sides have agreed to the settlement, the courts have not yet approved it.

A recent study of security incidents & data breaches 61% of data breach incidents in healthcare are from external threat actors & 39% by insiders. Information Access Management & Access Control are two HIPAA Security standards governing access to ePHI.

Access management requires covered entities & business associates to implement policies & procedures for granting access to ePHI. Access control allows access only to

those in accordance to need for the job.

U.S. Custom & Border Protection (CBP) has not always protected its Mobile Passport Control (MPC) applications making travelers' personal identifiable information (PII) vulnerable to exploitation according to the Dept. of Homeland Security. CBP is responsible for securing travelers' data from cybersecurity threats with oversight over 6 MPC apps designed to expedite travelers through CBP's inspection process.

For the 3rd. consecutive month, the number of breaches of 500 or more records increased. June saw an 11% increase in breaches from May with 70, the highest monthly total since 9-20 & above the average of 56/month over the past year. The largest June breach was a phishing attack of 214,956 people.

Compliance News

Avaddon Ransomware-as-a-service was shut down 6-18-21 & the threat group released the decryption keys for all victims (2934 victims & private keys). The shut down suggests they got nervous with the increased focus of governments & law enforcement agencies on ransomware gangs.

In one of the first enforcement actions, the TX parent of an Iowa nursing home has agreed to repay \$214,000 in federal monies for not following Coronavirus safety protocols April-July, '20. The case shows that failure to follow COVID-19 protocols can result not only in public health fines & penalties, but also liability under the False Claims Act.

Labs submitting bills during the pandemic knowing they were out of compliance with COVID-19 protocols

run the risk of liability for submitting a false claim. The money paid in this case was "restitution" or pay back of money received by mistake.

HHS issued an important bulletin affecting how the ban on sex discrimination will now be enforced. Specifically, it will go beyond just a person's sex/gender, but also include their sexual orientation and/or gender identity. The LGBTQ+ community can now file discrimination suits against a lab & the OCR will investigate any such claim. Legal proceedings can be initiated if there is any evidence of discrimination. In addition to money damages & potential corrective actions, this can lead to very unfavorable publicity against the laboratory.

One open question is how the new

protections will interact with the legal obligation of OCR under the ACA to enforce the civil rights rules under the Religious Freedom Restoration Act which bans the government from unduly interfering with a person's exercise of religion.

The average ransom paid by a victim dropped 38% in the 2nd. Quarter of 2021 compared to Quarter 1; it dropped to an average of \$136,576. The threat of leaking exfiltrated stolen data to pressure victims to pay appears to be losing some of its efficacy according to the same report. Attackers, however, doubled down on actual or claimed exfiltration increasing demand from 76% to 81% in Quarter 2. Phishing, brute forcing remote desktop credentials still rule; exploiting vulnerabilities a distant 3rd.

Safety

Reminder that it is unacceptable to store chemicals including specimens in formalin above eye level because of the risk of leak or spill into an individual's face.

Best practice in areas of the lab using microscopes is for any associate who wears glasses to remove those glasses with an ungloved hand prior to reading slides under the scope. There is no specific regulation about this but one purpose for the Blood-borne Pathogens standard is to eliminate hand-to-face actions in the lab; there is an obvious infection risk when handling glasses with gloved hands.

NFPA 45 states any flammable material requiring refrigeration or freezing must be designated or approved for flammable storage or be explosion-proof.

HHS has announced the Public Health Emergency (PHE) has been extended another 90 days to now end 10-18-21. CMS & accrediting agencies have indicated leniency may be shown to hospitals in the middle of a COVID-19 patient surge & still actively working under their emergency incident command structure during the PHE

3 unwritten safety rules every lab should follow:

- You cannot chew gum in the

lab: although it is not an OSHA rule, it is now a CAP standard. You cannot prove it was not put in your mouth outside the lab.

- **How long to wear PPE?** Gloves lose effectiveness after 2 hours, but change sooner if visibly soiled. Any type of lab coat can be worn 1 week in the general lab unless it is soiled. Face shields can be cleaned with alcohol products for disinfection.
- **Mesh shoes are not allowed in the laboratory.** These are only not allowed by CLSI guidelines. OSHA does, however require protection of the feet.

These can be hard to enforce, so staff must be educated of their need.

Miscellaneous

Ochsner Health & Rush Health Systems have announced a merger that should be completed by mid-2022. Seven Rush hospitals & more than 30 clinics in eastern MS & western AL will be rebranded Ochsner Rush Health.

In March, '21 OSHA issued an update extending existing OSHA protections for workplace safety Whistleblowers, explicitly noting these protections apply to those reporting COVID-19 workplace vi-

olations. Higher risk sites such as healthcare entities should expect more OSHA scrutiny & possibly more OSHA surveys.

The U.S. government has launched a new website to help public & private organizations defend against the rise in ransomware cases. StopRansomware.gov provides a central location for ransomware alerts & resources.

As post-pandemic work shifts to hy-

brid or fully remote, the stage is set for interactions to take on a new light. A 2021 Pew report on online harassment showed 4 of 10 Americans have experienced online harassment, including sexual harassment or stalking. Working remotely can make reporting complex. Non-reporting can embolden harassers. Companies should remind associates of sexual harassment laws & company policies, track & address remote harassment, launch or re-launch sexual harassment education.

Fun Spot



June Puzzle Answer: A fire

July Puzzle:

What kind of room has no doors or windows?

Trivia:

- There are more collect phone calls on Father's Day than on any other day of the year.
- It would take a sloth one month to travel one mile.
- Ketchup was used as a medicine in the 1930's.
- A waterfall in Hawaii goes up sometimes instead of down.

- During your lifetime, you will produce enough saliva to fill two swimming pools.
- The cigarette lighter was invented before the match.
- The tongue of a blue whale weighs more than most elephants.
- Months that begin on a Sunday will always have a "Friday the 13th."
- Beetles taste like apples, wasps like pine nuts, & worms like fried bacon.
- A ball of glass will bounce higher than a ball of rubber.