

# What's Your Compliance IQ?

Volume 3

Issue 1

January, 2020



## HIPAA News

A lawsuit against DCH Health System in the wake of the ransomware attack that disrupted medical services for several days alleged the organization failed to maintain and safeguard its computer system and data.

The lawsuit is seeking class action status alleging the lack of a data security system adequately reducing the risk of data breaches and cyberattacks. This incident has not been posted on the DHHS site but the attack may be a reportable HIPAA data breach.

Organizations must have technologies in place to detect inappropriate system activity and look for telltale signs of intrusion. This incident might advance but no word yet.

\*\*\*\*\*

After a data breach, if stolen PHI is

offered for sale on the Dark Web, that potentially bolsters class action suits filed by the plaintiffs against the breached organizations. Offering it for sale actually shows some-one is trying to monetize victim PHI.

The likelihood of it being purchased or used is heightened because there is proof it is for sale or available making connecting the dots much more clear.

\*\*\*\*\*

Cybercriminals are now moving away from the dark web to sell data and directly extorting potential individual victims. This opens a new front in the cyber warfare battlefield and further challenges organizations to put a high priority on patient data.

A Florida plastic surgery practice had a ransomware attack in 11-19

And 15-20 patients have contacted the practice to report individual ransom demands threatening public release of their personal photos, etc. This is in addition to the ransom demands to the practice.

\*\*\*\*\*

On 1-23-20, a federal court vacated the "third party directive" within the individual right to access "insofar as it expands the HITECH Act's third party directive beyond requests for a copy of an EHR with respect to PHI of an individual .... within an electronic format."

Also, the fee limitation will apply only to an individual's request for access to their own record, and not to an individual's request to send records to a third party. The Omnibus rule to expand the third party directive beyond an EHR in electronic format was vacated.

## Compliance News

The Department of Justice has filed a lawsuit alleging Indiana-based Community Health Network violated the Stark Law banning physician referrals.

The lawsuit alleges the network conditioned paying bonuses to physicians based on their achieving a minimum target of referrals to the hospital. It also says the network submitted claims to Medicare with knowledge the claims submitted for referred services were not eligible for payment.

\*\*\*\*\*

The Department of Justice (DOJ) received \$2.6B in recoveries involving fraud and false claims in fiscal 2019. The recoveries involved all sectors of the healthcare industry including laboratories. While this is federal losses, many cases also

assisted in recovering millions more for state Medicaid programs.

Whistleblowers filed 633 *qui tam* suits in fiscal 2019 and the DOJ recovered \$2.1B in these and earlier filed suits. The government paid out \$265M to whistleblowers in successful cases.

\*\*\*\*\*

Equifax's mega breach lawsuit has been settled for \$1.38B. Attackers took advantage of unpatched software; a patch was issued but Equifax failed to apply it. This is the largest and most comprehensive recovery in a U.S. data breach case by several orders of magnitude.

\*\*\*\*\*

Three weeks into the new year several hacking incidents involving email have already been added to the federal tally of major health breaches.

The largest incident so far has involved more than 49,000 people in MN associated with a county facility there.

So far there have been 7 data breaches involving nearly 131,000 persons. Other incidents have occurred, but are not yet posted.

As of this week the 2019 tally has been 505 incidents impacting more than 41.2M people.

It is predicted ransomware will continue to be an issue in 2020 but the focus of the hackers is predicted to shift from PHI to personally identifiable information. Many organizations do not have written policies including personally identifiable information which is needed, too.

# Safety

On 1-5-20 OSHA raised its civil penalties by about 1.8%. For each posting requirement violation the maximum penalty goes from \$13,260 to \$13,494.  
\*\*\*\*\*

OSHA is beginning to focus its enforcement efforts on what it defines as Leading Indicators. These indicators can help a lab determine how effective its overall safety program is. Some indicators can include safety audits and follow up actions, safety meeting attendance, and culture assessments.

They measure events leading up to injuries, illnesses, and other incidents and reveal potential

problems in your program.  
\*\*\*\*\*

Labs should check with manufacturers to see if the microscopes in place are a potential source of UV light. If there is no actual light emission that poses a threat, there is no need for the signage required for CAP accredited labs wherever there is any UV light used.

Of course, this signage is needed in any area where UV light is used.  
\*\*\*\*\*

Managers, please be aware that gum chewing is not allowed in the laboratory. With the chemicals and blood borne pathogens in the laboratory, it is not safe to chew gum.  
\*\*\*\*\*

ANSI nor OSHA require checking an eyewash for bacteria but it is recommended by CLSI as a best lab practice.  
\*\*\*\*\*

There is no regulation prohibiting the use of fans in the laboratory but it is not a good practice. Fans blow contaminants. They also will interfere with safety airflow of a chemical fume hood or BSC.  
\*\*\*\*\*

There is no longer a OSHA requirement for a "hands on" fire extinguisher training. There is, however, an OSHA requirement for training if fire-fighting equipment is available for staff use. The type of training is not specified. "Hands on" would be best practice for this.

# Miscellaneous

An audit has revealed CMS's controls were generally effective in ensuring Medicare beneficiaries were assigned Medicare Beneficiary Identifiers (MBI). However, in a small percentage of cases, CMS's control did not stop multiple MBI's from being assigned to beneficiaries or prevent mailing of new Medicare cards to deceased beneficiaries. Also, CMS made improper payments of \$2.3M on claims for deceased beneficiaries.  
\*\*\*\*\*

Ransomware gangs are now exfiltrating data from victims before leaving systems crypto-locked. Threatening to leak stolen data provides greater leverage to force them to pay the ransom. First, they leak chunks of information before leaking much more or all of it. This tactic is being used both on organizations and individuals.  
\*\*\*\*\*

Louisiana has rescinded Medicaid managed care contracts of United

Healthcare, Humana and two others due to problems with the bidding process. This will result in another round of bidding unless the decision is appealed and overturned.  
\*\*\*\*\*

The final rule has updated the salary level test for white-collar overtime exemptions under the Fair Labor Standards Act. Under the new rule, the minimum salary level for exemption is raised from \$455 to \$684 per week (\$35,568 annually).

# Fun Spot



**December Puzzle Answer:**  
Mushroom

**January Puzzle:**  
**What word is missing from this sequence?**  
Begin inch chapel elastic (??) cellar arisen end  
\*\*\*\*\*

**Trivia:**

- During a solar eclipse, the shadow of leaves makes the same crescent shape of the eclipsing sun.
- The ice covering 98% of Antarctica holds 90% of the world's fresh water.

- The ice cream cone was originally a way to hold flowers, not ice cream.
- There are 293 ways to make change for a dollar.
- A duck's quack has no echo.
- The hummingbird is the only bird that can fly backwards.
- A lightning bolt is 4 times hotter than the sun.
- One inch of rain is equal to 10 inches of snow.
- Night butterflies have ears on their wings so they can avoid bats.
- A cockroach can live up to 3 weeks without its head.