

**Compliance Client News – December 2019**

This newsletter summarizes compliance and HIPAA news from December 2019.

**OIG Enforcement**

1. **December Enforcement Summary**

*There are fewer enforcements to report in December 2019, likely due to the holiday season.*

**Stats.** Of 19 federal healthcare related settlements, civil monetary penalties, arrests, indictments and convictions this month\*:

* 16 involved false claims/health care fraud
* 13 involved criminal charges
* 9 involved physicians
* 6 involved opioids or other controlled substances
* 5 involved enforcement against owners or executives
* 5 involved medical necessity
* 4 involved kickbacks and/or Stark
* 3 involved home health
* 3 involved falsifying records
* 2 were brought by whistleblowers
* 2 involved lab
* 2 involved pharmacy
* There was one example of each of the following: a pain clinic, a PT clinic, a hospice, an OT, an RN, upcoding, and antitrust.

\* *Most examples involve multiple categories.* *Rather than summarize all of the settlements, MPA summarizes some of the most salient and representative examples.*

1. **False Claims/Health Care Fraud**
* **Cardiologist in trouble for upcoding.**  A cardiologist and his company were sentenced for their roles in a healthcare fraud scheme. The doctor and his practice submitted false claims to Medicare and Missouri Medicaid when the doctor performed vascular embolization and occlusions on patients on the same day – but billed for the procedures as if they were provided on two different days. This resulted in the physician receiving $2,000 more per patient. The doctor and his practice also entered a $1.2 million civil settlement to resolve allegations that they submitted upcoded claims for office visits to Medicare. This case was brought by a whistleblower, a former employee of the cardiology practice, who will receive $240,000 as her reward.

Source: https://www.justice.gov/usao-edmo/pr/festus-doctor-and-his-company-sentenced-health-care-fraud

* **Physician billed for visits that were not medically necessary.**  A physician group that provides physician services for the elderly, and the group’s management services affiliate, entered a $829,611 false claims settlement. The government alleged that the entities “routinely caused…physicians to conduct patient visits that were not medically necessary and then billed Medicare…for those unnecessary visits.”

Source: https://www.justice.gov/usao-edwi/pr/physician-group-and-related-company-agree-repay-over-800000-medicare-unnecessary

* **Doctor billed for unnecessary tests.**  A Maryland internist entered a $176,686 settlement to resolve allegations that he billed Medicare for medically unnecessary tests. The doctor is accused of providing peripheral autonomic nervous function tests despite not having the proper equipment or training to perform these tests – and despite the fact that the patients had not been diagnosed with an autonomic nervous function disorder. He is also accused of performing vestibular function tests that were not medically necessary because they were not used for clinical decision making, and because the doctor failed to evaluate patient symptoms prior to the tests.

Source: https://www.justice.gov/usao-md/pr/cambridge-internist-pays-more-176000-united-states-resolve-false-claims-act-allegations

* **Doctor pleads guilty for using illegal imported drugs.**  A Pennsylvania doctor pleaded guilty to fraud and drug importation charges this December. The doctor illegally imported inexpensive drugs that were not FDA approved, and administered them to patients. In its press release, the DOJ said: “Dr. Whalen imported and used non-FDA approved drugs from Turkey and the United Kingdom, without any regard for the safety and health of his patients. In addition, he prescribed powerful pain killers to patients already struggling with addiction.”

Source: <https://www.justice.gov/opa/pr/pennsylvania-doctor-pleads-guilty-fraud-and-drug-importation-charges>

1. **Opioids & Other Drugs**

In 2017, the United States Department of Health and Human Services declared the U.S. opioid epidemic a public health emergency, and launched a 5-Point Strategy to Combat the Opioid Crisis: <https://www.hhs.gov/opioids/about-the-epidemic/index.html>.

In March 2018, President Donald Trump announced an Initiative to Stop Opioid Abuse and Reduce Drug Supply and Demand: <https://www.whitehouse.gov/briefings-statements/president-donald-j-trumps-initiative-stop-opioid-abuse-reduce-drug-supply-demand/>. Among other things, this Initiative gave the DOJ more resources to prosecute opioid fraud and abuse. It is not surprising that we have seen an increase in drug-related settlements, criminal charges and guilty pleas coming from the DOJ – often involving opioids.

In November 2018, the OIG identified “Reducing inappropriate prescribing and misuse of opioids” as its #1

Management & Performance Challenge.

* **Woman who sold controlled substances heads to prison.** The owner of a pain and physical therapy clinic pleaded guilty to conspiracy to distribute controlled substances and was sentenced to 11 years in prison. This individual distributed medically unnecessary controlled substance by selling appointments with pain doctors.

Source: https://www.justice.gov/opa/pr/owner-detroit-area-health-care-clinics-sentenced-prison-diversion-scheme-involving-500000-0

1. **Kickbacks**

The Federal Anti-Kickback Statute makes it a criminal offense to offer, solicit, pay or receive any remuneration to induce or reward referrals of items or services reimbursable by a Federal health care program such as Medicare or Medicaid. “Remuneration” can mean anything of value, such as money, free goods or services, discounts, or cross-referrals. This means it is illegal to give or receive (or attempt to give or receive) anything of value for Federal health care program referrals (i.e. Medicare and Medicaid patients).

* **Boston Heart enters multi-million kickback settlement.** Boston Heart Diagnostics Corporation, a lab, entered a $26.67 million false claims, kickback and Stark Law settlement to resolve allegations brought by two whistleblowers, who will receive $4.36 million as their reward. Boston Heart was accused of providing physician practices in-office dieticians – if the physicians referred patients to Boston Heart for lab services. Boston Heart was also accused of paying doctors kickbacks disguised as investment returns.

Source: https://www.justice.gov/opa/pr/laboratory-pay-2667-million-settle-false-claims-act-allegations-illegal-inducements-referring

1. **Falsifying Records**
* **RN falsifies Medicare audit records.** A New Orleans nurse pleaded guilty to conspiracy to alter or falsify records in connection with a federal investigation. The registered nurse worked as the administrator of a hospice facility. Medicare audited the hospice and noted that its billing was not supported by patient documentation. Medicare reversed the claims at issue, totaling $383,107. Two years later, Medicare again audited the hospice and requested patient documentation for 99 patients. The registered nurse, knowing the records were not in place, “altered and falsified patient records to hide the fact that Company 1 lacked required medical records to justify bills submitted to Medicare for purported hospice services for the beneficiaries at issue in the audit.” Notably, even after the records were falsified, the audit still found the hospice’s documentation to be deficient.

Source: <https://www.justice.gov/usao-edla/pr/mandeville-nurse-pleads-guilty-conspiracy-alter-or-falsify-records-federal>

## OIG Work Plan Updates

## In December 2019, the OIG added five items to its Work Plan:

##

<https://oig.hhs.gov/reports-and-publications/workplan/updates.asp>

MPA recommends reviewing the recently added work plan items every month, determining if any items are relevant to your organization, and documenting your review and any audits or other compliance action items that are necessary.

**Licensure News**

1. **Providers pay up after employing fake nurse**

A Tennessee woman pleaded guilty to fraud charges after securing work as a nurse despite never graduating from nursing school or becoming licensed. Misty Dawn Bacon worked as a nurse in long-term care facilities and for other providers for six years, securing employment by using the nursing credentials of third parties. Bacon used the credentials of registered nurses with similar names (e.g. Misty Dawn Vennett). Because of Bacon’s fraud, two health care providers that employed her repaid more than $500,000 to health care programs.

Source: <https://www.sfgate.com/news/crime/article/Fake-nurse-pleads-guilty-to-fraud-charges-in-14904974.php>; <https://www.wvlt.tv/content/news/Fake-nurse-put-lives-at-risk-signs-federal-plea-deal-prosecutors-say-565788462.html>

1. **Nurse suspended for accessing patient information to determine work schedule**

A nurse faced disciplinary action from the Iowa Board of Nursing after she accessed patient census information from home on eleven occasions. This access violated hospital policy, because the nurse did not have authorization for remote access, and also because the nurse did not have a legitimate work reason to access these records. The nurse claimed she looked at the information in order to view ICU staffing so she could determine if she would be needed to work upcoming shifts.

The nurse was suspended for two 12-hour shifts and required to complete HIPAA training.

Source: <https://www.nurse.com/blog/2019/12/04/rn-breaches-patient-confidentiality-policy-check-work-schedule/>; <https://casetext.com/case/leach-v-iowa-bd-of-nursing>

**HIPAA & Social Media News**

##  [OCR announces](http://www.healthcareperformance.com/blog/breaking-news-ocr-announces-a-1.6-million-hipaa-settlement) another Right of Access settlement

The Office for Civil Rights entered an $85,000 settlement with Korunda Medical, LLC, which provides primary care and pain management in Florida. The OCR received a complaint asserting that Korunda failed to respond to a patient’s repeated requests to send medical records electronically to a third party. The OCR found that Korunda 1) failed to respond to the requests in a timely manner; did not provide the records in the electronic format requested by the patient; and charged more than the reasonable cost-based fees permitted by HIPAA. In addition, OCR provide Korunda with technical assistance to enable Korunda to properly provide the records, and Korunda still failed to comply.

This settlement is part of a recent OCR initiative to enforce patients’ right of access to their medical records.

Source: <https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html>

## [Ambulance](http://www.healthcareperformance.com/blog/breaking-news-3-million-unencrypted-mobile-device-hipaa-settlement) company enters $65,000 HIPAA settlement

West Georgia Ambulance, Inc. filed a breach report involving a lost unencrypted laptop containing the PHI of 500 people. OCR investigated, and found:

* Failure to conduct a HIPAA Security Risk Analysis
* No security awareness and training program
* HIPAA security policies and procedures were not implemented

**MPA Tip:** Much of the OCR’s recent enforcement cites lack of a HIPAA Security risk analysis as grounds for a settlement. If you have not conducted this analysis or recently updated yours, this is high risk.

Source: <https://www.hhs.gov/about/news/2019/12/30/ambulance-company-pays-65000-settle-allegations-longstanding-hipaa-noncompliance.html>

## Hospital employee puts patient meal tickets in the garbage

## For more than four months, a hospital employee put patient meal tray tickets in the trash – rather than shredding them. As a result, more than 1,000 patients’ personal information was potentially breached. The meal tickets listed patient names, day and month of birth, hospital unit and bed number, and diet and menu information.

## MPA Tip: Patient Health Information exists beyond the medical record. HIPAA training should extend beyond clinical staff so that all employees are able to identify PHI and handle it appropriately.

## Source: <https://www.beckershospitalreview.com/cybersecurity/zuckerberg-san-francisco-general-hospital-alerts-1-000-patients-of-data-security-incident.html>

## Snooping scenarios

## A hospital employee inappropriately accessed medical records at a Michigan hospital for more than three years. Another employee alerted the hospital to the snooping. An investigation confirmed that the employee in question accessed thousands of electronic health records, seemingly out of curiosity.

## Source: <https://www.mlive.com/news/muskegon/2019/12/curious-hospital-employee-improperly-accessed-thousands-of-medical-records.html>

## Nebraska Medicine discovered employee snooping during a routine audit. The audit discovered that an employee improperly accessed patient records for almost three months.

## Source: <https://fox42kptm.com/news/local/nebraska-medicine-discloses-patient-data-breach>

## At a Chicago children’s hospital, an employee inappropriately accessed medical records for a year. This employee viewed patient names, addresses, dates of birth, diagnoses, medications, appointments, and procedures.

## Source: <https://abc7chicago.com/health/lurie-patient-data-wrongfully-accessed-hospital/5791304/>

## MPA Tip: Routine audits can help you discover inappropriate medical record access sooner rather than later, limiting the scope of any potential breach.

## Cyber-attack creates state of emergency in New Orleans

## The City of New Orleans was the target of a successful cyber-attack in December. When ransomware was discovered on the City’s network, the City responded by ordering all city employees to power down computers, disconnect from wireless internet, unplug all devices, and power down servers. While these actions caused much of the city to cease functioning, emergency communications, police and fire departments continued to operate.

## MPA Tip: A strong malware defense can increase your organization’s odds of preventing ransomware and the emergencies it brings.

## Source: <https://www.forbes.com/sites/daveywinder/2019/12/14/new-orleans-declares-state-of-emergency-following-cyber-attack/>

## Stolen unencrypted devices

## Truman Medical Centers in Kansas City reported a breach this December. An unencrypted laptop containing PHI for more than 100,000 patients was stolen from an employee’s vehicle.

## Source: <https://www.kcur.org/post/stolen-laptop-contained-data-more-114000-patients-truman-medical-centers#stream/0>

## In California, La Clinica de la Raza reported a breach after a Blackberry containing PHI for 2,477 patients was stolen. The thief took a briefcase containing the blackberry from the employee’s vehicle. The Blackberry contained two emails, downloaded onto the Blackberry, containing PHI.

## Source: <https://www.laclinica.org/wp-content/uploads/2019/12/Notice-of-Stolen-Blackberry.pdf>

## MPA TIP: UNENCRYPTED PHI SHOULD NEVER BE STORED ON MOBILE DEVICES.

## Another ransomware attack on an IT provider

## A ransomware attack targeting an IT company left 100 dental practices unable to access their records and schedules. This was a highly sophisticated attack, in that the cyber criminals used unique encryption for every single device. One dentist affected by the attack commented: “You are absolutely paralyzed in the same way as if you lost your location physically.”

## Source: https://www.ada.org/en/publications/ada-news/2019-archive/december/colorado-ransomware-attack-leaves-100-dental-practices-without-access-to-patient-data

## Mailing error leads to breach

## The Colorado Department of Human Services notified 12,230 people about a HIPAA breach caused by a mailing mix-up. The Department mailed Notice to Reapply forms for food and cash assistance – but the forms contained information for incorrect individuals.

## Source: <https://www.coloradopolitics.com/news/state-sends-personal-information-of-applicants-to-unintended-recipients/article_1bf7a01a-1545-11ea-9f29-9b9da8352d8f.html>

## Resident video leads to nursing home fine

## A Connecticut nursing home was fined $1,320 by the Department of Public Health after a nurse aide posted a video of a resident to Snapchat. The video depicted a resident wearing a helmet and seated in a wheelchair requesting a grilled cheese sandwich – and was posted one day after staff were reminded of the nursing home’s cell phone policy. The nursing home learned of the video when one of the resident’s family members called to complain.

## MPA Tip: REMEMBER: DEMEANING OR HUMILIATING PHOTOS OR RECORDINGS OF RESIDENTS ARE MENTAL ABUSE. And, when shared on social media, they represent potential HIPAA violations as well.

## Source: <https://patch.com/connecticut/northhaven/north-haven-nursing-home-fined-over-snapchat-video-report>; http://c-hit.org/2019/12/05/snapchat-post-a-fall-and-a-death-lead-to-nursing-homes-fines/

##  HIPAA Lawsuit update

## Four patients sued DCH Health System in Alabama, alleging that a ransomware attack that shut down operations for 10 days caused them harm. The patients allege they had “their medical treatment as well as their daily lives disrupted.” For example, patients alleged that, due to their inability to obtain care during this 10-day period, their medical records were compromised or lost; follow-up treatment for prior care was disrupted; prescription medications could not be obtained; or patients were unable to receive care for severe conditions.

## Source: <https://www.tuscaloosanews.com/news/20191227/patients-file-lawsuit-over-dch-cyber-attack>; <https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html>

## A proposed settlement has been agreed to that would end the Banner Health breach lawsuit that affected 3.7 million patients in 2016. The breach involved hackers accessing Banner’s payment processing system for its food and beverage outlets. The hackers used this access to get into Banner’s health network, including its services where patient health information is housed. Patients impacted by the breach filed a class action lawsuit, alleging that Banner’s security defense was insufficient to prevent the attack.

## Source: <https://healthitsecurity.com/news/proposed-6m-settlement-reached-in-banner-health-data-breach-lawsuit>

**Features**

## [Compliance Officer Burnout](http://www.healthcareperformance.com/blog/compliance-officer-burnout)



How many hats does your compliance officer wear? Here are some of the additional roles compliance officers have mentioned to me:

* HR Director
* Administrator/CEO
* Nursing Home Admissions Director
* Training Manager
* Clinical Director or QAPI Director
* Assistant Administrator or VP
* CFO
* Privacy Officer and/or Security Officer
* Director of Nursing
* Marketing/PR Director

Sometimes people just laugh when I ask if they have roles in addition to Compliance Officer – because they have so many.

**Give them a break**

Use your Compliance Committee for support. An engaged Compliance Committee that meets regularly and chips in can offer enormous support to your Compliance Officer.  Your Compliance Committee can be a sounding board that brings diverse perspectives and knowledge areas to the compliance effort. There are also opportunities for Compliance Committees to share some of the workload – if your Compliance Officer is overworked and the Committee members can contribute a little time. Can the Committee review audits in a Committee meeting? Brainstorm training content together (what if each Committee member writes two hypotheticals for your upcoming annual training session?) Could each Committee member conduct one audit each year? That’s not a lot of work to add to each member’s plate – but it frees up your Compliance Officer to achieve significantly more.

**Share the love**

If your Compliance Committee members aren’t the right source of extra manpower, are there tasks other employees [**can fit onto their plates**](http://www.healthcareperformance.com/blog/whats-on-your-compliance-officer-wish-list) (without these employees becoming overburdened)? Perhaps an audit, or management of one risk area? Sometimes the right solution is shifting a few tasks around – rather than abandoning those tasks or completely re-structuring your job titles.

**Inspire them**

Attending a conference with fellow colleagues can be both reassuring and motivating. The opportunity to hear from other professionals, many of whom also wear multiple hats, can refresh one’s perspective and recharge those batteries. I recommend the Health Care Compliance Association’s [**Compliance Institute**](https://www.hcca-info.org/conferences/national/2020-compliance-institute) (coming to Nashville in 2020).

**Outsource (if it fits your budget)**

If your Compliance Officer (or department) is struggling with multiple roles or the weight of the compliance workload, consider enlisting help with one or more select tasks. A consultant might be able to provide your compliance program effectiveness review, training, or policies and procedures far more cost-effectively than an in-house effort.

****