

**Compliance Client News – November 2019**

This newsletter summarizes compliance and HIPAA news from November 2019.

**OIG Enforcement**

1. **November Enforcement Summary**

**Stats.** Of 39 federal healthcare related settlements, civil monetary penalties, arrests, indictments and convictions this month\*:

* 31 involved false claims/health care fraud
* 23 involved criminal charges
* 17 involved kickbacks and/or Stark
* 10 involved enforcement against owners or executives
* 12 involved physicians
* 7 were brought by whistleblowers
* 7 involved opioids or other controlled substances
* 5 involved medical necessity
* 4 involved lab
* 4 involved hospitals
* 3 involved copay waivers
* 3 involved beneficiary inducements
* 2 involved hospice
* 3 involved exclusions
* 2 involved pharmacy
* There was one example of each of the following: consolidated billing, false statements, EMTALA, genetic testing, unlicensed providers, falsified records, a personal care aide, identify theft, a mental health clinic, a substance abuse treatment center, misbranded devices, a rural health clinic, a nursing home, a state department of health, home health, inpatient rehab, physical therapy, an insurance broker, telehealth, and a spinal implant company.

\* *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**

* **Company lied to patients about how much time they have left to live.**  A health care company’s owner, CEO, and medical director (who also happened to be the local mayor) were found guilty in a fraud scheme that involved lying to patients about their health: “Merida Group enrolled patients with long-term incurable diseases, such as Alzheimer’s and dementia, at group homes, nursing homes, and in housing projects by falsely telling them that they had less than six months to live….” These patients were not terminally ill – and in some cases were functioning quite well, to the degree of coaching athletic games. The medical director/mayor explained the reasoning behind this hospice fraud scheme: “the way you make money is by keeping them alive as long as possible.”

Source: https://www.justice.gov/opa/pr/three-individuals-including-former-texas-mayor-ceo-and-owner-found-guilty-154-million-money

* **Hospital settles false claims involving lack of supervision.**  A Manhattan hospital entered a $12.3 million settlement to resolve false claims allegations. The hospital was accused of billing Medicare for services that did not meet Medicare requirements, such as procedures performed by medical residents who were not appropriately supervised; medically unnecessary services; robotic surgeries performed when the physician left the surgery room; and designated health services involving an inappropriate compensation arrangement under the Stark Law.

Source: <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-123-million-settlement-lenox-hill-hospital-submitting>

* **Doctor indicted in upcoding scheme.**  A New York ophthalmologist was arrested and charged with healthcare fraud, and received a civil fraud complaint. The doctor is accused of billing Medicare, patients, and insurers for upcoded eye surgeries. The doctor is also accused of falsifying medical records and pressuring employees in order to support the scheme.

Source: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-and-arrest-ophthalmologist-healthcare-fraud

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.

* **Doctor agrees to 15 year exclusion.** A doctor agreed to pay $1.4 million and be excluded from Medicare and Medicaid for 15 years after he was accused of improperly prescribing opioids. The government alleged that the physician “wrote improper Schedule II prescriptions, including opioids, for his patients when those prescriptions had no legitimate medical purpose and were not issued in the usual course of professional practice.”

Source: https://www.justice.gov/usao-edpa/pr/montgomery-county-doctor-agrees-pay-14-million-resolve-allegations-improper-opioid

* **Rural health clinic executive agreed to sell drugs in parking lots.** A rural health clinic founder and former CEO agreed to sell 13 properties in order to resolve a Medi-Cal false claims lawsuit. The executive was accused of billing for services provided by unlicensed providers; services that were never provided; and for claims that involved patients picked up controlled substances in retail parking lots.

Source: <https://www.justice.gov/usao-edca/pr/former-ceo-central-valley-health-clinics-sell-13-properties-resolve-false-claims-act>

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).

* **Hospital paid doctors more than fair market value.** Sutter Health and Sacramento Cardiovascular Surgeons Medical Group Inc. entered a $46,123,516 settlement to resolve false claims and kickback allegations. One of the hospitals was accused of violating the Stark Law when it billed Medicare for cardiovascular services provided by Sacramento Cardiovascular doctors – when Sutter paid those doctors more than fair market value for these services. The cardiovascular practice is also accused of knowingly sending duplicate bills to Medicare for services provided by leased physician assistants. This lawsuit was brought by a whistleblower, who will receive almost $6 million dollars as her reward.

Source: https://www.justice.gov/opa/pr/california-health-system-and-surgical-group-agree-settle-claims-arising-improper-compensation

* **Hospital gave improper inducements to Medicare patients.** A Kentucky hospital pharmacy agreed to a $10,101,132 false claims settlement this month. The hospital was accused of billing Medicare for prescriptions that failed to meet Medicare coverage requirements – for example, the prescriptions lacked the treating physician’s signature, and the hospital failed to document that medications were delivered. The hospital also allegedly violated the Anti-Kickback Statute by providing beneficiary inducements to Medicare patients: free blood glucose testing supplies, plus waived co-pays and deductibles for insulin.

Source: <https://www.justice.gov/opa/pr/kentucky-hospital-pay-over-10-million-resolve-false-claims-act-allegations>

* **APRN took kickbacks in exchange for prescribing off-label uses of Subsys.** An advanced practice nurse was sentenced for her role in a fentanyl spray kickback scheme. The APRIN worked at a pain treatment center, where she prescribed controlled substances such as Subsys: a fentanyl spray that is FDA approved only to treat breakthrough pain in cancer patients. The APRN prescribed Subsys to treat pain in patients who did not have cancer. Medicare will not pay for this non-FDA approved use of Subsys. In addition, Insys Therapeutics, which manufactures Subsys, paid kickbacks to prescribers – such as this APRN – via “Speaker Fees” that were, in effect, kickbacks to reward the practitioners for prescribing the drug.

Source: <https://www.justice.gov/usao-ct/pr/aprn-who-received-kickbacks-insys-therapeutics-prescribing-fentanyl-spray-sentenced>

1. **Excluded Providers**

Individuals and contractors can become excluded providers for a variety of reasons, including Medicare or Medicaid fraud; patient abuse or neglect; health care related felonies; controlled substance felonies; some misdemeanors; suspension or revocation of a health care license; provision of unnecessary services; submission of false claims; and kickbacks.

Medicare and Medicaid will not pay for services provided by excluded providers. Any Federal health care program payments made to a provider for services rendered by an excluded provider are to be multiplied by three and returned. In addition, providers can be assessed a Civil Monetary Penalty, and risk joining the list of excluded providers themselves.

* **Ambulance company and owner agree to 5-year exclusion.** An ambulance company and its owner agreed to be excluded from federal healthcare programs for five years. The company billed Medicare Part B for ambulance transport to and from nursing homes – when those transports were already covered by the SNF consolidated billing payment (Part A).

Source: <https://oig.hhs.gov/fraud/enforcement/cmp/index.asp>

**MPA Tip:** The OIG recommends that providers screen employees and contractors against Federal and state exclusion lists at hire and monthly. Monthly screening limits your penalty window! There are three lists to screen: the OIG’s LEIE, the SAM list of debarred contractors, and your state’s Medicaid exclusion list (if your state has made one publicly available).

1. **EMTALA**

A Georgia hospital entered a $40,000 settlement with the OIG to resolve allegations that it violated the Emergency Medical Treatment and Labor Act (EMTALA). According to the allegations, a 27-year old male presented to the hospital’s emergency room with pain resulting from priapism. The emergency physician evaluated the patient and contacted the on-call urologist. The urologist did not come to the emergency department to examine or treat the patient – instead, transferring the patient to a hospital 150 miles away. The hospital’s failure to treat this patient’s emergency condition led to the settlement.

Source: <https://oig.hhs.gov/fraud/enforcement/cmp/index.asp>

**CMS Updates**

## [Phase 3 Nursing Home Compliance Update!](http://www.healthcareperformance.com/blog/phase-3-nursing-home-compliance-update)

On November 22, 2019, CMS issued a [**memorandum**](https://www.cms.gov/files/document/qso-20-03-nh) with an update on the Phase 3 Requirements of Participation. In this memo, CMS advised:

* CMS will not release updated Interpretive Guidance and training addressing Phase 3 until the second quarter of 2020.
* But... nursing homes are **still expected to require with Phase 3 by November 28, 2019.**

Here is what CMS said:

"While the Phase 3 requirements will be effective November 28, 2019 and facilities are required to comply with these and all requirements, our ability to survey for compliance with these requirements will be limited until the Interpretive Guidance is released."

### What does this mean??



It means that, right now, nursing homes are required by law to comply with the Phase 3, including the Compliance and Ethics Program requirements - and CMS expects nursing homes to be in compliance.

 Time will tell if or to what degree state surveyors evaluate nursing home compliance programs - but this CMS memo makes clear that survey review is fair game.

MPA recommends that nursing homes implement Phase 3 compliance relying on available guidance (the regulation, [**42 CFR 483.85**](https://www.govinfo.gov/content/pkg/CFR-2017-title42-vol5/pdf/CFR-2017-title42-vol5-sec483-85.pdf)), and keep an eye out for forthcoming updates and guidance. CMS will have guidance in second quarter 2020. In addition, in July 2019, CMS issued a [**Proposed Rule**](http://www.healthcareperformance.com/blog/cms-changes-snf-compliance-program-requirements-again) that would, if made final, modify 42 CFR 483.85, and potentially postpone enforcement. The Proposed Rule has not progressed to a Final Rule yet, which means the proposed changes to Phase 3 Compliance, and the proposed enforcement delay, *are not effective at this time*. Until that rule is made final, MPA suggests relying on the CMS memo issued last week and complying with Phase 3. If and when the CMS Proposed Rule becomes final and an enforcement delay goes into effect, MPA will post an update to the blog.

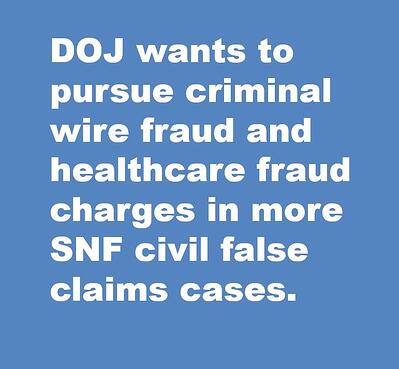
Finally, remember: regardless of what Phase 3 requires, the OIG is still the gold standard for compliance programs - and [**OIG expectations should be followed as well**](http://www.healthcareperformance.com/blog/cms-changes-snf-compliance-program-requirements-again).

Please let MPA know if you have any questions.

## DOJ News

## [DOJ cracking down on nursing homes](http://www.healthcareperformance.com/blog/doj-cracking-down-on-nursing-homes)

The Department of Justice (DOJ) aims to use its [**Elder Justice Initiative**](https://www.justice.gov/elderjustice) to pursue [**more criminal charges in nursing home investigations**](https://news.bloomberglaw.com/health-law-and-business/doj-crackdown-on-nursing-homes-to-include-criminal-counts). Typically, the DOJ uses civil lawsuits to pursue False Claims Act violations against nursing homes. Toni Bacon, a DOJ associate deputy general, [**explains the shift**](https://news.bloomberglaw.com/health-law-and-business/doj-crackdown-on-nursing-homes-to-include-criminal-counts): "We need to go after cases civilly because they [are] providing grossly substandard care and, in the appropriate case, refer it for a parallel criminal prosecution."



Potential criminal charges that could be pursued alongside a false claims case include wire fraud and healthcare fraud. [**For example**](https://news.bloomberglaw.com/health-law-and-business/doj-crackdown-on-nursing-homes-to-include-criminal-counts), submitting claims to Medicare or Medicaid for services that were not actually provided constitutes criminal wire fraud.

The long-term care industry has already seen some criminal enforcement. Philip Esformes, owner of multiple assisted living and skilled nursing facilities, was [**recently convicted**](https://www.justice.gov/opa/pr/south-florida-health-care-facility-owner-convicted-role-largest-health-care-fraud-scheme-ever) for his role in a $1.3 billion Medicare and Medicaid fraud and kickback scheme. Esformes bribed doctors to admit patients to his facilities; billed Medicare and Medicaid for services that were not provided or that were medically unnecessary; and provided inadequate care. Esformes also bribed a state regulator to receive notice of state inspections. Esformes was [**sentenced**](https://www.justice.gov/opa/pr/south-florida-health-care-facility-owner-sentenced-20-years-prison-role-largest-health-care) to 20 years in prison.

### Another reason to invest in compliance

The DOJ's increased interest in pursuing criminal charges against nursing homes provides another compelling reason to invest in an effective compliance program. While [**CMS' delay of enforcement of Phase 3**](http://www.healthcareperformance.com/blog/cms-changes-snf-compliance-program-requirements-again) compliance requirements has some providers waiting to invest in compliance, the DOJ's announcement is a warning. Even though Phase 3's Compliance and Ethics program requirements might not be enforced via state survey until 2020, federal enforcement of compliance laws remains high. Use your compliance policies and training programs to prevent false claims; and your auditing and reporting systems to detect and correct (and self-report) false claims - before they amount to a civil or criminal matter.

## OIG Work Plan Updates

## In November 2019, the OIG added 16 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.

**HIPAA & Social Media News**

## [OCR announces $1.6 million HIPAA penalty](http://www.healthcareperformance.com/blog/breaking-news-ocr-announces-a-1.6-million-hipaa-settlement)

The Office for Civil Rights [**announced its second HIPAA enforcement**- this time, with a governmental agency.](https://www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html)

The Texas Health and Human Services Commission (TX HHSC) received a $1.6 million civil monetary penalty from the OCR for HIPAA Privacy and Security violations committed by the Texas Department of Aging and Disability Services (DADS), which is now part of TX HHSC.

In 2015, DADS notified OCR of a breach after it discovered that the ePHI for 6,617 individuals was accessible via the internet. [**OCR explains**](https://www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html): "The breach occurred when an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials."

When it investigated the breach, OCR found:

* DADS did not conduct an enterprise-wide HIPAA Security risk analysis
* DADS' information systems and applications lacked access and audit controls (making it impossible for DADS to identify how many people inappropriately viewed the ePHI).

### When was your last HIPAA Security Risk Analysis?

Out of the [**seven HIPAA resolution agreements issued by the OCR in 2019**](https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html), five involved covered entities or business associates who failed to conduct a sufficient HIPAA Security risk analysis.

If your organization has not conducted a HIPAA Security risk analysis - or if you have not revisited that analysis within the past year or since your IT environment or PHI uses have changed - it's time to conduct one (and mitigate the risks and vulnerabilities you find).

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

The Office for Civil Rights (OCR) announced a [**$3,000,000 HIPAA settlement**](https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html) with the University of Rochester Medical Center (URMC). This settlement resolves Privacy and Security Rule allegations.

[](https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html)

In 2013, URMC submitted a breach report to OCR after an unencrypted flash drive containing PHI was lost.

In 2017, URMC again submitted a breach report, after an unencrypted laptop containing PHI was stolen.

OCR investigated and found:

* URMC did not conduct an enterprise-wide HIPAA Security risk analysis
* URMC lacked security measures to mitigate risks and vulnerabilities
* URMC did not use device and media controls
* URMC did not encrypt ePHI "when it was reasonable and appropriate to do so"

The OCR also pointed out that URMC continued to store ePHI on unencrypted mobile devices even though it was aware of the high risk of unencryption.

### HIPAA reminders:

* If your organization has not conducted a HIPAA Security risk analysis - or if you have not revisited that analysis within the past year or since your IT environment or PHI uses have changed - it's time to conduct one (and mitigate the risks and vulnerabilities you find).
* The OCR seems [**increasingly hesitant**](http://www.healthcareperformance.com/blog/hipaa-update-the-cost-of-not-encrypting) to find reasons for not encrypting "reasonable and appropriate." If you have unencrypted ePHI on mobile devices or stored or transmitted elsewhere, make encryption a high priority. The OCR makes clear that organizations who identify security risks and fail to mitigate them in a timely manner will face consequences.

## OCR announces $2.175 million HIPAA settlement

## The OCR announced a third HIPAA settlement this November, with Sentara Hospitals, for violating the Privacy and Breach Notification Rules. The OCR received a complaint claiming that Sentara sent a patient a bill for another patient. Upon investigating, the OCR identified 577 Sentara bills sent to the wrong address. Sentara, however, only reported this breach for eight individuals “because Sentara concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred.” Sentara refused to update the breach report even after OCR advised it to. OCR also found that Sentara failed to have a business associate agreement in place.

## MPA Tip: PHI is any information that identifies a patient, and relates to that patient’s treatment, payment or condition. Assess every potential breach using the steps outlined in the Breach Notification Rule (or MPA’s Breach Assessment Form).

## Source: <https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html>

## OCR releases Fall 2019 Cybersecurity Newsletter

## The OCR’s Fall Cybersecurity Newsletter is titled: “What Happened to My Data? Update on Preventing, Mitigating and Responding to Ransomware.” This newsletter includes helpful basic information about malware and ransomware to be shared with your HIPAA team. You can access the newsletter here: <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html>

## HIPAA penalties increase for inflation

## As of November 5, 2019, the new penalties are:

|  |  |  |  |
| --- | --- | --- | --- |
| Penalty Tier | Culpability | Minimum/Maximum penalty per violation | Maximum penalty per year |
| 1 | No knowledge | Old: $114.29 - $57,051New: $117 - $58,490 | Old: $1,711,533New: $1,754,698(the annual cap is the same for all culpability levels) |
| 2 | Reasonable cause | Old: $1,141 - $57,051New: $1,170 - $58,490 |
| 3 | Willful neglect – corrective action taken | Old: $11,410 - $57,051New: $11,698 - $58,490 |
| 4 | Willful neglect – no corrective action taken | Old: $57,051 - $1,711,533New: $58,490 - $1,754,698 |

## 110 Nursing homes affected by IT company breach

## VCPI, a Wisconsin IT company that provides cloud data hosting, internet access, IT consulting and security services to nursing homes, was struck by a ransomware virus called Ryuk. The ransomware encrypted all of the data VCPI hosts for its clients, and the hackers demanded a $14 million ransom to unlock the data. This means that nursing homes that use VCPI for data hosting cannot access their data. Karen Christianson, VCPI’s CEO and owner, said: “We’ve got some facilities where the nurses can’t get the drugs updated and the order put in so the drugs can arrive on time… In another case, we have this one small assisted living place that is just a single unit that connects to billing. And if they don’t get their billing into Medicaid by December 5, they close their doors.”

## Source: <https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/>

## Misconfigured calendar leads to potential breach

## Children’s Minnesota learned that its internal digital calendars were misconfigured for years. As a result, calendar information – such as name, DOB, appointment information, procedure types and insurance details – could have been accessible by outside parties. Children’s Minnesota has notified almost 38,000 patients of the potential breach.

## Source: https://healthitsecurity.com/news/ransomware-attack-forces-great-plains-health-to-ehr-downtime

## Phishing attacks on the rise

## According to APWG’s 3rd Quarter 2019 Phishing Activity Trends Report, phishing attacks are surging. APWG detected 266,387 phishing attacks in Q3 2019, almost double the amount identified in Q2 2019. Software-as-a-Service and webmail sites were the number-one target of phishing attacks. In business e-mail compromise attacks, gift cards are the number one form of payment requested – most often for Google Play. Payroll diversion and direct transfer are also requested. The report also advised that Tuesday is the most popular day for phishing attacks. Finally, businesses and individuals should be aware that phishers increasingly use encryption (https links) in their scams: 68% of phishing sites now use SSL. This means that employees who are trained to look for https links as a sign of security should be re-trained: encrypted websites are not necessarily safe.

## Source: <https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf>

## Paper PHI breaches

## Smith’s Food and Drug, a Kroger Co. pharmacy, announced that a former employee discarded 12 boxes of records for a Las Vegas pharmacy in the pharmacy trash compactor. The records included 57,600 paper prescription records.

## Source: <https://www.smithsfoodanddrug.com/topic/pharmacy-privacy-notice>

Aegis Medical Group reported a breach involving unauthorized access of paper records. A former employee tried to sell patient information to third parties in a fraud scheme. 75% of the records involved where paper records.

## Source: <https://aegismedicalgroup.com/potential-breach-of-protected-health-information/>

## MPA Tip: There is no such thing as paper PHI, unless and until it is encrypted or destroyed (shredded).

## Wash. U. notifies patients of stolen laptop

## The Washington University School of Medicine notified patients of a breach involving its Department of Ophthalmology and Visual Services. An unauthorized person took an employee’s laptop and used it to access the employee’s School of Medicine email account for four months. The school learned of the breach when several patients received a letter about the employee. Upon investigating, the school learned that the unauthorized person – who knew the employee – accessed patient information via the employee’s email account.

## Source <https://medicine.wustl.edu/news/washington-university-school-of-medicine-notifies-patients-of-privacy-breach/>

## Breach results in missing records

The Guidance Center, a mental health services provider in California, notified patients of a data breach after it discovered that two employee email accounts had been compromised. The Guidance Center learned of the breach when employees reported that files and backups were missing. Upon investigation, the Center discovered that email accounts and a computer had been subject to unauthorized access – and files had been deleted.

Source: <https://www.tgclb.org/security-notification/>; <https://www.hipaajournal.com/former-employee-the-guidance-center-ca-unauthorized-access-file-deletion/>

## Healthcare hackers try to lure patients with fake PayPal email

## Utah Valley Eye Center’s business portal was hacked. The hackers stole patient information and used this information to send phishing emails to 5,764 patients falsely notifying patients they had received a PayPal payment.

## Source: <https://www.heraldextra.com/news/local/central/provo/utah-valley-eye-center-reports-hipaa-breach-after-system-hacked/article_3c1e986a-0532-520f-9d25-5569b843dd01.html>

## Building evacuation leads to PHI theft

Employees of Main Street Clinical Associates had to evacuate the building after an explosion next door. When staff evacuated, files and equipment were left on desks. Staff could not access the building until more than a month later. When they re-entered the building, staff learned that their offices had been looted: two laptops, a cell phone, and a printer were stolen. The devices were password protected – but not encrypted. As such, Main Street notified patients of the breach.

**Source:** <https://www.hipaajournal.com/phi-theft-incidents-reported-by-loyola-medicine-and-main-street-clinical-associates/>

## Camera with autopsy pictures stolen

A camera containing autopsy photos for 18 patients was stolen from Loyola University Medical Center. For nine of the patients, the autopsy photos had not yet been uploaded to the electronic medical record and are thus permanently lost. Because the hospital did not have a functioning cable to upload photos from the camera, patient autopsy photos accrued on the camera for a year.

Source: <https://chicago.cbslocal.com/2019/11/08/more-patients-autopsy-photos-were-lost-after-camera-was-stolen-from-loyola-medicine/>; <https://chicago.cbslocal.com/2019/09/13/loyola-university-medical-center-autopsy-photos-stolen/>

## Nurse tweets about comedian’s hospital visit

Magda Szubanski, star of the Australian sit-com Kath & Kim, tweeted her dissatisfaction after she learned a nurse discussed her hospital stay on twitter. Szubanski received an operation in the hospital. Following her stay, Szubanski discovered that a nurse who cared for her had tweeted about her time in the hospital – and suggested that she was a difficult patient. The nurse’s tweet has since been removed – but Szubanski’s complaints remain on twitter.

Source: <https://www.news.com.au/entertainment/celebrity-life/magda-szubanski-slams-unethical-nurse-for-tweeting-about-her-recent-hospital-stay/news-story/2fe388c2b72660d09b397304e6a6a331>

**Features**

## [Smartphones: The biggest HIPAA and abuse offenders](http://www.healthcareperformance.com/blog/smartphones-the-biggest-hipaa-and-abuse-offenders)

By Margaret Scavotto

It can be a HIPAA problem and an abuse problem: when nursing home staff take pictures of residents with their smartphones. Here’s an example.

### CNA took photo of deceased resident and shared it to Snapchat

Five CNAs at a New York nursing home took photos and videos of residents—including one deceased resident—on their cell phones [**and shared them on Snapchat**](https://www.mpnnow.com/news/20190525/details-emerge-in-thompson-health-snapchat-case).

The nursing home was notified of the incident when a member of the public called the administrator and reported that a CNA sent her a photograph of a deceased resident. This CNA admitted taking and sharing photos and videos of eight residents. Her reason for photographing the man who died was “because she was upset that the resident had passed away.” She also took five videos of another resident “mostly yelling and swearing” and sent them to another CNA.

Another CNA admitted that “everyone on the unit on the evening shift was using their cell phones.”

The registered nurse manager reported that “all staff had been educated on the policy not to take and disseminate photographs previous to these incidents.”

### CMS 16-33

CMS has stated that humiliating or demeaning photos or videos of nursing home residents [**are mental abuse**](https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-16-33.pdf). Surveys will determine if nursing homes are protecting residents from this type of this abuse.



CMS outlines the steps nursing homes must take in order to do well on this survey – and meet expectations for preventing this type [**of mental abuse**](http://www.healthcareperformance.com/blog/tweet-tweet-resident-abuse-takes-a-new-and-dangerous-form):

* Implement policies and procedures prohibiting abuse. These policies need to address mental abuse arising from demeaning or humiliating pictures or recordings.
* Train staff on mental abuse arising from these pictures or recordings.
* Take training one step further and “provide ongoing oversight and supervision of staff in order to assure that these policies are implemented as written.”
* Treat these incidents of mental abuse as any other abuse allegation: with investigation and reporting.

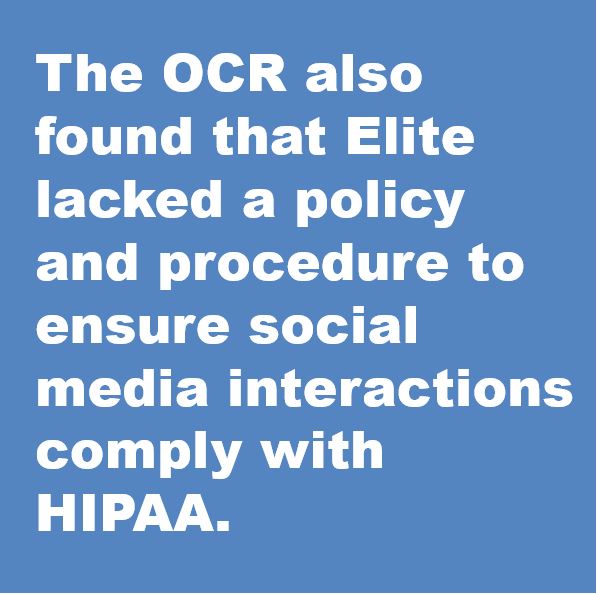
### What else you can do

Social media use in nursing homes – and other providers – is a [**rampant HIPAA headline**](http://complianceandethics.org/the-5-social-media-posts-your-privacy-officer-fears-most/). Remind staff that photos or videos of residents violate HIPAA; and, time on phones can lead to lapses in care. Also conduct HIPAA walk throughs to monitor adherence to your cell phone policy.

## [First social media HIPAA settlement!](http://www.healthcareperformance.com/blog/breaking-news-first-social-media-hipaa-settlement)

By Scott Gima

Whenever a settlement agreement is announced, the OCR is sending a message to all providers. On October 2nd, The OCR announced a [**$10,000 settlement agreement**](https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html) with Elite Dental Associates in Dallas Texas. At first glance, it is easy to overlook this settlement; $10,000 does not seem to be a big deal when there are other cases with fines in the millions of dollars. For example, [**Anthem paid a record $16 million**](http://www.healthcareperformance.com/blog/anthem-makes-hipaa-history) following the PHI breach of close to 79 million people; the largest health data breach in history. So what is the big deal? Or more importantly, what are the lessons to be learned from this breach? There are several.

[](https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html)

### ****Background****

The OCR received a complaint from a patient on June 4, 2016 that Elite [**“responded to a social media review by disclosing the patient’s last name and details of the patient’s health condition.”**](https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html) The OCR investigated and found that “Elite had impermissibly disclosed the [PHI] of multiple patients in response to patient reviews on the Elite Yelp review page.” Elite’s responses included the patient’s last name, treatment details, charges and insurance information. The OCR also found that Elite lacked a policy and procedure to ensure social media interactions comply with HIPAA.

### ****Lessons to be Learned****

The first lesson is obvious: don’t post PHI on social media without a valid HIPAA authorization. This is not the first time providers have responded to Yelp posts that included PHI or information that could identify the patient. Providers can respond to reviews with generic information about their practice – or ask patients to call. Provider responses should never reveal any information about the patient or their visit.

Another lesson is that the OCR is an equal-opportunity enforcement agency. All providers big and small can be investigated. In this instance, the patient notified the OCR of the breach. And within five months of the notification, the investigation started. That should be a “wow” moment for everyone.

Lastly, if you are unsure of what needs to be in place to comply with HIPAA to protect PHI, read the Elite Dental [**resolution agreement**](https://www.hhs.gov/sites/default/files/elite-dental-ra-cap.pdf). The OCR provided Elite with “Corrective Action Obligations." These obligations can be used as a checklist to be used to evaluate your current privacy rule practices. Here are some (but not all) key requirements:

* Policies and procedures that comply with the Privacy Rule.
* The policies should cover the following:
  + Permissible and impermissible uses and disclosures of PHI
  + Administrative, technical and physical safeguards to protect the privacy of PHI
* Privacy authorization form
* A Notice of Privacy Practices – **that lists the way PHI is used on social media**
* Provider contact to address Privacy issues – usually the designation of a Privacy Officer
* Internal reporting mechanisms of possible violations
* Policies that address corrective action of privacy policy violations
* Privacy practice employee training

## [Have you tested your compliance hotline lately?](http://www.healthcareperformance.com/blog/have-you-tested-your-compliance-hotline-lately)

By Margaret Scavotto

*Published on HCCA’s Compliance and Ethics Blog:* <https://complianceandethics.org/have-you-tested-your-compliance-hotline-lately/>

The Kansas Medicaid fraud and abuse complaint email inbox went unchecked for 17 months.

According to [**a report issued by the Kansas Office of the Medicaid Inspector General**](https://ag.ks.gov/docs/default-source/reports/omig-audit-reports/19-01.pdf?sfvrsn=ce71d21a_4), 209 emails were unread. 95 of these emails "alleged fraud, waste, abuse, or illegal acts related to Medicaid, MediKan, or SCHIP, or were seeking information on how to report suspected fraud." 42 of these emails contained "partially or wholly substantiated allegations of Medicaid or SCHIP fraud, waste, abuse or illegal acts....

### How did it happen?

The complaint inbox went unchecked from August 2, 2017 to January 9, 2019.



On June 1, 2017, the Kansas OIG, which oversees the Kansas Medicaid program - and had been completely unstaffed since 2014 - was moved from the Kansas Department of Health and Environment (KDHE) to the Kansas Attorney General's Office. Because the OIG was unstaffed, there were no staff to notify the AG's office to check the complaint inbox. Further, a KDHE administrative employee [**monitored the account**](https://www.kansascity.com/news/business/health-care/article233465682.html) until her departure in August 2017 - but nobody checked the inbox after she left.

### Could this happen to you?

When I conduct a compliance program annual review, I test the compliance reporting methods. This means calling hotlines, sending test emails, and chatting with live hotline operators. I have had a lot of lovely chats, and received many encouraging email replies and return calls.

But I have also gotten a fair amount of busy signals, email bounces, annoying fax machine noises and disconnected phone messages. And the most disappointing of all: days, weeks, or months of silence when nobody gets back to me.

When is the last time you tested your compliance reporting methods? And if yours fails, who will your employees call instead?

****