

**Compliance Client News – September 2019**

This newsletter summarizes compliance and HIPAA news from September 2019.

**OIG Enforcement**

1. **September Enforcement Summary**

**Stats.** Of 36 federal healthcare related settlements, civil monetary penalties, arrests, indictments and convictions this month\*:

* 28 involved false claims/health care fraud
* 25 involved criminal charges
* 13 involved kickbacks and/or Stark
* 11 involved enforcement against owners or executives
* 9 involved physicians
* 7 involved pharmacies
* 7 involved opioids or other controlled substances
* 4 were brought by whistleblowers
* 3 involved telemedicine
* 3 involved transport/ambulance
* 2 involved hospitals
* 2 involved home health
* 2 involved mental health counseling centers
* 2 involved exclusions
* There was one example of each of the following: self-disclosure, unlicensed providers, false statements, PHI theft, improperly accessing PHI, genetic testing, a pharmaceutical company, pharmacy reps, mobile diagnostic services, OT, an LPN, marketing, a hospital administrator, a SNF, a dentist, a medical device company, DME, and a CIA reportable event.

\* The 36 enforcements do not include the **10 Takedowns this month**, described below.

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

1. **Takedown September**

There were ten enforcement takedowns in the month of September, resulting in **380 individuals being criminally charged**, and involving more than **$2.6 billion in health care fraud**.

* **Midwest Takedown**: 53 individuals charged, $250 million in fraud (billing for medically unnecessary procedures, procedures that were never provided, and prescriptions that were not purchased or distributed to beneficiaries)
* **Southern Florida Takedown**: 30 individuals charged, $86 million in fraud (billing for medically unnecessary home health, prescription drug, DME and addiction treatment services)
* **Georgia Takedown**: 19 people charged, $400 million in fraud (trafficking orders and prescriptions and fraudulent billing for genetic testing, orthotic braces and pain creams)
* **Northeast Takedown**: 54 people charged, $800 million in fraud (fraudulent claims, opioid diversion, and illegal kickbacks)
* **Florida/Georgia Takedown**: 67 people charged, $160 million in fraud (billing for medically unnecessary home health, DME and prescription drug services)
* **Gulf Coast Takedown**: 33 people charged, $515 million in fraud (medically unnecessary psychotherapy, behavioral health services, DME and compounded medications; fraudulently obtaining opioids and other controlled substances)
* **West Coast Takedown**: 34 people charged, $258 million in fraud (billing for services, tests and prescriptions that were not medically necessary or were never provided)
* **Texas Takedown**: 58 people charged, $66 million in fraud (opioid trafficking, fraud and diversion)
* **Southern California Takedown**: 25 people charged, $150 million in fraud (billing for services, tests and prescriptions that were not medically necessary or were never provided)
* **Mid-Florida Takedown**: 7 people charged (fraud; conspiracy to illicitly obtain and distribute controlled substances)

1. **False Claims/Health Care Fraud**

* **Esformes sentenced in largest health care fraud scheme ever.**  Philip Esformes was convicted for his role in a $1.3 **billion** Medicare and Medicaid fraud and kickback scheme involving assisted living and skilled nursing facilities he owned. 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. He was sentenced to 20 years in prison.

Source: <https://www.justice.gov/opa/pr/south-florida-health-care-facility-owner-sentenced-20-years-prison-role-largest-health-care>

* **Fraudulent test bills add up to two million dollar settlement.** A Texan doctor entered a $2.1 million settlement to resolve allegations that he billed Medicare for medically unnecessary diagnostic tests. The U.S. Attorney’s office identified the claims because the doctor was “a significant statistical outlier for various metrics.” For example, he ordered an excessive amount of diagnostic tests, particularly highly complicated tests – often for patients on a recurring basis.

Source: <https://www.justice.gov/usao-sdtx/pr/mission-family-practitioner-pays-2-million-resolve-allegations>

* **Hospital administrator gets 10 years.** A hospital administrator in Texas was sentenced to 10 years in prison for Medicare fraud, and ordered to pay more than $6 million in restitution. The administrator worked with the hospital CFO and COO to submit false and fraudulent claims for to Medicare partial hospitalization program services. The parties paid kickbacks to group home owners and patient recruiters in exchange for Medicare patient referrals to the PHPs. The administrator also admitted many patients to the PHP program even though they did not quality for – and were not provided – legitimate partial hospital services.

Source: <https://www.justice.gov/opa/pr/texas-hospital-administrator-sentenced-10-years-prison-role-16-million-health-care-fraud>

* **Ambulance company self-discloses false claims.** An ambulance company entered a $138,285 settlement to resolve allegations that it billed Medicare for nonemergency ambulance transportation. In the press release, the DOJ noted the **impact of the company’s self-disclosure and cooperation**: “Capital voluntarily disclosed these results to the U.S. Attorney’s Office…. Capital also cooperated throughout the investigation, and implemented enhanced internal compliance and remedial measures. Federal authorities encourage health care providers to cooperate with investigations involving the possible submission of false claims to federal programs. Entities or individuals that make proactive, timely and voluntary self-disclosures to the U.S. Attorney’s Office may receive credit during the resolution of a later FCA case.”

Source: <https://www.justice.gov/usao-me/pr/bangor-ambulance-company-settles-false-claims-act-allegations>

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.

* **Clinic owner pleads guilty to drug distribution.** The owner of pain and physical therapy clinics in Detroit pleaded guilty to a drug diversion scheme. The owner employed physicians to write medically unnecessary controlled substance prescriptions, and accepted payments from patients and recruiters in exchange for doctor visits. At these visits, patients signed physical therapy documentation in order to receive controlled substances.

Source: <https://www.justice.gov/opa/pr/owner-detroit-area-health-care-clinics-pleads-guilty-drug-diversion-scheme>

* **LPN takes morphine from patient.** A Massachusetts licensed practical nurse pleaded guilty to drug tampering. The LPN was working at a nursing home when she tampered with three bottles of morphine sulphate prescribed for a hospice patient – and replaced the morphine with another liquid, lowering its potency to 4-29%. Source: <https://www.justice.gov/usao-ma/pr/haverhill-nurse-pleads-guilty-drug-tampering>

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).

* **MobilexUSA settles for $8.5 million.** MobilexUSA (also known as Trident USA Health Services, LLC), a mobile diagnostic services company, entered an $8.5 million false claims and kickback settlement for **swapping** arrangements with nursing homes. MobilexUSA was accused of providing mobile x-rays to SNFs at below-cost or below fair market value. In exchange, the nursing homes referred Medicare patients to MobilexUSA. This type of trade is called “swapping” and is an illegal kickback arrangement. The case was brought by two whistleblowers: the chief information officer who will receive $2 million, and a regional sales manager who will receive $106,250. MobilexUSA tried to use its bankruptcy proceeding to avoid this government settlement. The U.S. Attorney asserted that **bankruptcy cannot avoid federal enforcement settlements and penalties.**

Source: https://www.justice.gov/usao-edpa/pr/trident-usa-health-services-llc-pay-85-million-resolve-false-claims-act-liability

* **$2.1 billion genetic testing fraud scheme.** 35 individuals (including nine doctors) were charged in a health care fraud and kickback scheme involving medically unnecessary cancer genetic tests. Telemedicine companies and cancer genetic testing labs were accused of paying kickbacks in exchange for the referral of Medicare patients who received unnecessary and expensive cancer genetic tests. The tests were often never provided – or were “worthless to their actual doctors.” A telemarketing network was used to lure elderly patients, with scare tactics, into receiving the tests.

Source: <https://www.justice.gov/opa/pr/federal-law-enforcement-action-involving-fraudulent-genetic-testing-results-charges-against>

1. **Improper Access & Theft of PHI**

This month, two Department of Justice enforcements involved protected health information:

* **Occupational therapist snooped PHI in order to burglarize patient homes and steal their opioids**. In Iowa, an occupational therapist improperly accessed the private health and residence information for 1,900 patients while working at a hospital – and then used this information to enter or burglarize 13 homes in order to steal prescription opioids. She was sentenced to 14 months in federal prison.

Source: <https://www.justice.gov/usao-ndia/pr/occupational-therapist-sentenced-federal-prison-illegally-accessing-private-health-data>

* **EHR records stolen and sold for false claims**. Three Texas residents were charged with health care fraud after they “breached a health care provider’s electronic health record (EHR) system in order to steal protected health information and personally identifiable information belonging to patients of the provider. The information that was stolen from the provider was ‘repackaged’ in the form of false and fraudulent physician orders and sold to [DME] providers and contractors.”

Source: <https://www.justice.gov/usao-edtx/pr/north-texans-charged-health-care-fraud-violations>

**MPA Tip:** Protect your medical records from insider and outsider threats.

## OIG Work Plan Updates

## The OIG did not update its Work Plan in September.

**CMS Update**

## [CMS Changes SNF Compliance Program Requirements – Again](http://www.healthcareperformance.com/blog/cms-changes-snf-compliance-program-requirements-again)

Ladies and gentlemen, long-anticipated compliance program requirements are changing, one more time. Let’s take a look at what has changed – and what hasn’t.

### ****The proposed rule****

On July 16, 2019, [**CMS published a proposed rule**](https://www.federalregister.gov/documents/2019/07/18/2019-14946/medicare-and-medicaid-programs-requirements-for-long-term-care-facilities-regulatory-provisions-to) that would modify multiple aspects of Phase III of the Long-Term Care Facilities Requirements for Participation (the “Proposed Rule”). The goal of the Proposed Rule is to reduce regulatory burdens and costs, allowing nursing homes to focus resources on providing quality resident care. Some of the most discussed proposed amendments are those to the Compliance and Ethics Program requirements (42 CFR 483.85), which, if finalized, will become effective one year later. With comments from the public due September 16, 2019, our best guess is that enforcement will begin October or November 2020.



### ****Good news: fewer compliance-related F-tags ahead****

Nursing homes: LeadingAge (and other associations) successfully lobbied on your behalf.

The prior rule required nursing homes to designate specific personnel as 1) compliance officers, 2) individuals to receive compliance reports, and 3) for chains of five or more nursing homes, compliance liaisons. The message conveyed to CMS was that these requirements were too burdensome, and took staff time away from resident care. The Proposed Rule seems to incorporate this message loud and clear.

The Proposed Rule removed more than the designated personnel requirements. Annual review, annual training, discipline for volunteers and contractors, and more requirements are gone. For a complete summary of the proposed changes, see [**the tables in the attached memo**](https://cdn2.hubspot.net/hubfs/378557/MPA%20Compliance%20Update%20-%20Phase%20III%20Proposed%20Rule%209-3-19-3.docx). What is left is a more general compliance program framework from CMS.

Because the Proposed Rule reduces the number of compliance survey requirements, there are fewer potential F-tags on your survey. These largely new and untested requirements would also have been subjected to variation in surveyor interpretations come November 28, 2019.  The bottom line is that the Proposed Rule potentially brings good news for nursing homes: reduced compliance requirements and reduced potential F –Tags.

### ****But don’t forget about the OIG****

But, be careful. Everything CMS removed from the Proposed Rule is still recommended by the OIG in its[**Compliance Program Guidance documents**](https://oig.hhs.gov/compliance/compliance-guidance/index.asp) for nursing facilities. For three decades, providers, including nursing homes, have followed this [**OIG guidance**](https://oig.hhs.gov/compliance/compliance-guidance/docs/complianceguidance/nhg_fr.pdf) when developing compliance programs – and it’s still the gold standard. CMS’ comments in the Proposed Rule acknowledge this when they recommend that nursing homes refer to the OIG guidance. Nursing homes still need to develop and maintain compliance programs that adhere to the OIG guidance.

### ****What is the difference between survey enforcement and OIG enforcement?****

When the Proposed Rule becomes final, the Phase III Compliance and Ethics Program requirements will be enforced through the survey process. The OIG, on the other hand, enforces compliance related laws, such as the False Claims Act, the Anti-Kickback Law, the Stark Law, and the Civil Monetary Penalties Law. OIG enforcement is far more serious: civil monetary penalties, costly settlements, potential jail time, legal expenses, and loss of government reimbursement.

The OIG recognizes that compliance programs prevent and detect the types of misconduct that violate these laws. More than one Assistant US Attorney has told MPA that all providers should have an effective compliance program in place. If the OIG knocks on your door to conduct an investigation, they will look for a working compliance program. If one is not in place, the provider will likely face larger exposure to federal fines and penalties.  And, if a provider has a compliance program, that provider is more likely to prevent the type of violations that can lead to an OIG investigation in the first place.

### ****Proceed with caution****

While it is OK to celebrate the reduction in regulatory requirements, please be careful.



Everything CMS took out is still recommended by the OIG.

What does this mean?

* CMS will not require you to designate a compliance officer, but the OIG does.
* CMS will not require you to review your compliance program every year, but the OIG does.
* CMS will not require chains of five or more nursing homes to provide compliance training, but the OIG expects all nursing homes to provide annual compliance training.
* CMS will not require chains of five or more nursing homes to designate compliance liaisons, but the OIG expects all nursing home chains to do this.

### ****The bottom line****

Under the proposed rule, CMS compliance requirements do not meet OIG expectations for compliance programs.

Enjoy the survey break!

But don’t jeopardize your compliance effort over the Proposed Rule. The OIG should be, and still is, the last word on compliance. Your compliance program should be created to meet OIG expectations. If the OIG shows up at your nursing home, will you be ready?

### ****Coming soon****

Stay tuned for more MPA updates on the CMS Proposed Rule:

* Phase III: Do you need a Compliance Officer?
* Phase III: Do SNFs need to conduct a compliance program annual review?

## [CMS' New Affiliate Screening Requirements Are Coming](https://www.healthcareperformance.com/blog/cms-new-affiliate-screening-requirements-go-into-effect-nov.-4)

On November 4, CMS' [**Program Integrity Enhancements to the Provider Enrollment Process**](https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-19208.pdf) final rule goes into effect.

The "Affiliates" provision of this rule requires Medicare, Medicaid and CHIP providers to disclose to CMS any affiliations with organizations that have had a "disclosable event." Providers who fail to make these disclosures can be denied enrollment - or have their enrollment revoked. The [**purpose of this new process**](https://www.cms.gov/newsroom/press-releases/cms-announces-new-enforcement-authorities-reduce-criminal-behavior-medicare-medicaid-and-chip) is to stop fraud and help CMS find parties that have committed fraud.



### What's an "affiliation"?

There are five ways a provider can have an "affiliation' with an organization:

* a 5% or more direct or indirect ownership interest in another organization
* a general or limited partnership interest (of any percentage) in another organization
* an interest in which an individual or entity exercises "operational or managerial control over, or directly or indirectly conducts, the day-to-day operations of another organization," by contract of another arrangement. This includes sole proprietorships.
* when an individual is acting as officer or director of a corporation
* a reassignment or payment assignment relationship

### What's a "disclosable event"?

Providers must disclose "affiliations" within the past five years to CMS if the affiliated organization has a "disclosable event:"

* current uncollected debt owed to Medicare, Medicaid or CHIP
* current or prior payment suspension
* current or prior OIG exclusions
* Medicare, Medicaid or CHIP enrollment denial, revocation or termination

### When does this go into effect?

CMS has adopted a "phased-in" approach to implementing the affiliation disclosure requirements:

**Phase One:**

* After the final rule's November 4, 2019 effective date, and after CMS updates Form CMS-855, CMS will begin requesting certain providers and suppliers to disclose all affiliations. CMS will make these requests only when it determines that a provider or supplier has at least one affiliation with a disclosable event.

**Phase Two:**

* After public comment on "potential approaches for obtaining affiliation information... in terms of timing, mechanism, and priority," CMS will publish a new proposed rule outlining additional procedures for handling affiliation disclosures. After the final rule, the disclosure requirements will go into effect.

### What do we do?

Start evaluating your screening processes and be prepared to identify affiliates and determine if they have disclosable events.

This is easier said than done - as [**Michael Rosen from ProviderTrust adds**](https://www.providertrust.com/blog/cms-announces-higher-compliance-standards-provider-enrollment/): "Currently, there are no public databases of Medicare payment suspensions or revocations for healthcare providers to evaluate...."

Look for further guidance from CMS, which is asking for further comment on the best way to collect and report this information. Hopefully this guidance will help clarify some of the challenges providers and suppliers face with complying with this new rule.

Work on developing or streamlining your processes to [**gather information about and screen your a**](https://www.providertrust.com/vendorproof/)**ffiliates**.

Finally, polish your [**excluded provider screening process**](http://www.healthcareperformance.com/blog/excuded-providers-falling-through-the-cracks) and make sure that it includes affiliates.

**HIPAA & Social Media News**

## Ransomware attack interferes with patient care

## Campbell County Health in Gillette, Wyoming experienced a ransomware attack on September 20, 2019. The attack limited CCH’s access to medical records, patient contact information, appointments and medication histories. As a result, some services have ceased functioning for outpatient orders (Lab, Radiology, Respiratory Therapy, Sleep Center and Wellness blood draws). Some surgeries were cancelled, CCH stopped taking inpatient admissions, and many patients were transferred to regional facilities. The organization was without email and had limited faxing abilities for over a week. As of October 2, CCH still had not restored their information, and patients were being asked to confirm their appointments and bring medications with them.

## Source: <https://www.cchwyo.org/News/Press_Center/Health_News/2019/Service_Disruptions_at_CCH_no_ETA.aspx?furl=sd>

## Sensitive medical information faxed to wrong number

## A clinic in Australia has been faxing sensitive patient information – including mental health information – to the wrong number for two years. The information includes medical histories, and mental health plans for women with postnatal depression. The recipient has received misdirected faxes for 10 patients.

## MPA Tip: Remember to double check all fax numbers – and avoid sending sensitive PHI by fax.

## Source: <https://www.smh.com.au/national/victoria/detailed-and-graphic-clinic-faxes-patients-highly-sensitive-medical-histories-to-wrong-number-20190916-p52rsy.html>

**Features**

## [HIPAA question of the day: Do your employees snoop?](http://www.healthcareperformance.com/blog/hipaa-question-of-the-day-do-your-employees-snoop)

### **By Margaret Scavotto**

### ****Nurse snooped records of 1,309 patients****

A medical center employee [**snooped medical records of 1,309 patients**](http://www.sandiegouniontribune.com/news/health/sd-no-patient-breach-20180112-story.html) over 15 months. The nurse looked up records for patients assigned to herself, or to another nurse - but did not have a treatment reason to view the records. The patients were notified.

### ****Car accident leads to firing of 12 employees for snooping****

A health system [**suspended approximately 12 employees**](https://observer-reporter.com/business/washington-health-system-suspends-about-a-dozen-employees/article_9da949b2-72fb-11e8-8153-bb9481b9c73b.html) while it investigated a potential HIPAA breach involving employees looking at patient records without authorization. The investigation likely involves a fatal motor vehicle accident involving a health system employee. The driver and another passenger from the car accident were treated at local hospitals for injuries.

### ****Receptionist fired for looking up co-worker contact info in EHR****

A [**hospital operating room secretary was fired for twice accessing the EHR to find a co-worker’s phone number**](https://www.natlawreview.com/article/how-employers-can-handle-their-biggest-threat-to-data-privacy-their-employees). First, the secretary was asked to find out if a co-worker would be coming in to work that day. The secretary could not find the hospital’s employee contact information sheet, so she logged in to the hospital’s EHR system to find the co-worker’s phone number (the co-worker had been a patient of the hospital). The secretary also used the EHR to find the co-worker’s phone number on another occasion.

The secretary was terminated because she did not have a work-related reason to access the co-worker’s EHR record. The secretary was replaced by a younger employee, which prompted the secretary to file an Age Discrimination claim against the hospital. The hospital [**won this case.**](https://www.casemine.com/judgement/us/5b14e7c4340c810f433a22df) The court found that the hospital had a legitimate, non-discriminatory reason for terminating the secretary (violations of hospital HIPAA and confidentiality policies).

### ****What you can do****

Car accidents, news stories, and other incidents can quickly make your patients “celebrities,” tempting employees to snoop. Sometimes, employees go to the EHR to look up information simply out of curiosity or convenience.

* **Train, train, train.**To counter these temptations, your HIPAA training must be top-of-mind, rather than an annual or semi-annual reminder that is soon forgotten. Train staff vigilantly about the types of medical record access that are outside the scope of your policies and HIPAA.
* **Use your security program.**Address snooping in your HIPAA security risk analysis and policies, and in your security management plan. Consider limiting access, and using access termination procedures, information system activity review, access log review, access controls, and setting up alerts within your electronic records system.
* **Take extra precautions when you have celebrities.** You don’t have to be a Los Angeles provider to have celebrities. The Ebola virus made a Dallas hospital – and a few of its patients – front page news. Car accidents, criminals on the run, shootings, and other events can turn seemingly low-profile towns into front-page news. When you have a “celebrity,” take extra precautions. This might include admitting a patient under an alias, explaining the benefits of opting out of inclusion in the directory, conducting extra audits of medical records activity, and putting additional limits on medical record access.

## [Email HIPAA Breaches on the Rise](http://www.healthcareperformance.com/blog/email-hipaa-breaches-on-the-rise)

By Margaret Scavotto

According to the U.S. Department of Health and Human Services Office for Civil Rights (OCR), email breaches are on the rise.

The OCR maintains a [**database of breaches**](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) of unsecured protected health information affecting at least 500 individuals. MPA crunched some numbers, looking at OCR breach reports still under investigation for each six month period for the past 24 months. The number of email breaches reported to the OCR between the second half of 2017 and the first half of 2019 more than quintupled.

Let’s look at some real world examples to see how email use can breach HIPAA.



### Hospital accidentally gives PHI for Suboxone patients to newspaper

A communications employee at a Maine hospital accidentally[**emailed information about 300 patients with opioid use disorder to the local newspaper**](https://bangordailynews.com/2019/04/18/mainefocus/acadia-hospital-mistakenly-released-confidential-information-of-300-suboxone-patients/).

The information included the patient names, their providers, and the fact that they take Suboxone, which is known as a treatment for opioid addiction.

The email forwarded an email with a patient spreadsheet to the newspaper’s investigations editor by mistake. Fortunately, the newspaper employee destroyed the file. But this accident reminds us of risks associated with emailing PHI.

### Email Attachment Breaches Data of 993 Veterans

A VA medical center announced a [**HIPAA breach involving 993 veterans**](https://www.disabledveterans.org/2019/01/16/veterans-affairs-admits-to-hipaa-violation-of-993-elderly-veterans/).

The breach occurred after a veteran’s family member asked the VA for a list of nursing home facilities that work with the VA medical center. In response, the VA accidentally emailed the family member a list that included veterans’ names, abbreviated SSNs, diagnoses, nursing homes where they were admitted, and service-connection disability rating percentages.

### ****What you can do****

To mitigate the risks of a HIPAA email breach, take a look at the excellent precautions the VA put in place after its breach:

* The VA is no longer keeping historic, rolling files.
* The VA has also encrypted and restricted this data, so a limited number of individuals can access them.
* The VA is no longer sending email attachments.

The corrective actions taken by the VA are excellent examples of practices that recognize the inherent risk of human error involved with email.

If you do decide to email PHI, consider getting patient consent first. In addition, MPA does not recommend using email to communicate patient information unless it is encrypted. And, when it comes to sending sensitive PHI, email should be avoided at all costs. Finally, if you have not done so already (or recently), MPA recommends using your HIPAA Security Risk Analysis to evaluate any email practices in your organization.

## [\* Breaking News; OCR enters first HIPAA settlement in Right of Access Initiative](http://www.healthcareperformance.com/blog/ocr-enters-first-hipaa-settlement-in-right-of-access-initiative)

By Margaret Scavotto

\* Breaking News \*

The Office for Civil Rights (OCR) [**just announced**](https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html) its first settlement in the HIPAA Right of Access Initiative.

Bayfront Health St. Petersburg paid an $85,000 settlement and entered a corrective action plan with the OCR to resolve allegations that it violated the HIPAA Privacy Rule by denying a patient the right to timely access to the medical records of her unborn child.

The patient requested prenatal records of her unborn child from Bayfront, a 480-bed hospital in Florida. HIPAA requires covered entities to comply with such requests within 30 days. When the patient did not receive her records, she filed a complaint. The patient eventually received her records - more than nine months after her original request.

### Don't forget patient rights



HIPAA gives patients rights, and providers who don't protect those rights can face hefty settlements.

Patients have the right to:

* receive your notice of privacy practices
* see or copy their PHI
* ask to make changes to their medical records
* restrict how their PHI is used and communicated
* ask who has received their PHI
* give permission to discuss PHI with family and friends
* have their PHI protected after they die

### What you can do

* Implement **policies** protecting patient privacy rights.
* **Train** staff to be aware of these rights, so they know what to do if a patient asks about how to exercise their rights.
* **Audit** your organization's adherence to these policies. For example, do you honor medical records requests within 30 days? If a patient requests a communication restriction, is it documented and followed? Use what you find in your audits to improve your policies and training and continually improve your efforts to honor patient privacy. Your patients and your employees will thank you.

****